Data Protector

Version : 11.01

PDF Generated on : 27/04/2022 17:33:17

MICRO FOCUS

Table of Contents

主页

Data Protector 是一款为快速增长的业务数据提供可靠的数据保护和高度可访问性的备份解决方案。Data Protector 具有专门为整个企业和分布式环境特别定制的综合备份和还原功能。Data Protector 可用于从多个站点上的一个系统到数千个系统的各种环境。

Data Protector 还支持以“通用标准”模式进行部署。有关 Micro Focus Data Protector 的通用标准配置的详细信息，请参阅通用标准指南和通用标准配置部分。

发行说明

了解此版本中的最新功能和所有新增内容。

快速入门

开始理解 Data Protector 的关键概念和体系结构。

安装

按照这些过程来安装、设置、部署和维护 Data Protector。

升级

按照这些过程从先前版本升级到当前版本。

集成

查看有关将其他独立产品与 Data Protector 集成的信息。

管理

按本节中的过程来配置和管理 Data Protector。

使用

按照本节中的过程优化 Data Protector 的潜在使用。

故障诊断

解决安装和使用 Data Protector 时可能遇到的问题。

开发

使用这些资源开发解决方案并最大化 Data Protector API 的实用性。

视频库

观看本节中列出的视频，了解 Data Protector 的简短介绍。

发行说明

除了修复问题之外，此发布的 Data Protector 还引入了新增功能和增强功能。

Data Protector 11.01 中的新增功能

Data Protector 11.01 引入了以下新增功能或增强功能:

适用于云工作负载的 Data Protector

Data Protector 11.01 引入了适用于云工作负载的 Data Protector 以提供对以下范围的备份和还原支持:

- 云数据存储库，例如 Microsoft 365 (Exchange、SharePoint、Teams、OneDrive)
- 虚拟化环境，例如 Citrix XenServer、KVM、Nutanix
- 其他数据平台，例如 OpenShift、OpenStack

有关详细信息，请参阅适用于云工作负载的 Data Protector 简介。

增强型自动灾难恢复

Data Protector 增强了 EADR 以支持新的系统和功能，如下所示:

对 RHEL 8.x 和 SUSE 15.x 的 EADR 支持	使您能够执行 RHEL 8.x 和 SUSE 15.x 系统的 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR UEFI+Secureboot 支持	使您能够对配置为使用 UEFI 安全启动的主机执行 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR NIC 聚合支持	使您能够对配置了 NIC 聚合的系统执行 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR 分区调整大小支持	默认情况下，使您能够将源系统中磁盘的原始分区调整为新替换的磁盘大小
对 Windows 2022 的 EADR 支持	此功能使您能够执行 Windows Server 2022 系统的 EADR

基于角色的访问控制

Data Protector 11.01 提供基于角色的访问控制 (RBAC) 的技术预览，允许您根据用户角色和权限来管理查看、备份和还原访问。

> 重要说明： RBAC 功能目前不受支持，仅在测试环境中可供预览。不要在生产环境中使用此功能。

有关在测试环境中使用基于角色的访问控制的信息，请参阅基于角色的访问控制文档。

从 Data Protector 界面管理和控制 SAP HANA 备份

除了从 SAP HANA 界面进行的现有备份和还原之外，Data Protector 11.01 还支持从 Data Protector GUI 和 CLI 配置和备份 SAP HANA 数据库。它现在支持单节点配置中的完整备份和增量备份类型。您可以使用高级和旧版调度程序来计划备份。

有关详细信息，请参阅 SAP HANA 集成。

Postgres 11、12、13、14 系列备份和还原

Data Protector 11.01 增加了对 PostgreSQL 版本 11、12、13、14 的备份、还原和恢复的支持。参阅支持矩阵以获取有关平台的信息

有关受支持平台的信息，请参阅支持矩阵。

集成虚拟磁盘开发套件 (VDDK) 7.0.3

Data Protector 11.01 包 VDDK 7.0.3 以支持新的备份代理主机。

有关受支持平台的信息，请参阅支持矩阵。

Data Protector 重复数据删除存储

Data Protector 11.01 增强了重复数据删除存储以支持以下功能:

- 跨多个存储的单一端口
- 来自公共云提供商的存储配置，例如 AWS S3、Microsoft Azure、Google GCP 和 S3 兼容云目标
- 增强的稳定性和性能
- VMware 备份的缓存粒度恢复
- 三向 NDMP 备份
- 静态数据加密

有关详细信息，请参阅 Data Protector 重复数据删除存储。

数据域提升

Data Protector 11.01 支持三向 NDMP 备份。

安全增强功能

以下 Data Protector 组件已升级，从而使 Data Protector 比以前的版本更安全:

组件	升级到版本
WildFly	23.0.2
Keycloak	15.1.1
OpenSSL	1.0.2zd
报告服务器数据库 (PostgreSQL)	11.5

已修复问题

类别	问题 ID	描述
备份和还原	OCTCR19Q1499321	浏览大型卷以进行基于块的还原会超时。
集成	OCTCR19Q1493736	找不到邮箱的备份数据库。
升级	OCTCR19Q1491226	在 SLES for SAP 12.4 上将 Data Protector 10.10 升级到 10.91 客户机后，VBDA 意外关闭。
CLI	OCTCR19Q1478161	omni_rinst.sh 脚本包含错误的命令。
文档	OCTCR19Q1499871	无法查看 SAP R/3 集成文档的页面。
集成	OCTCR19Q1477768	Data Protector 10.91: MySQL 备份失败并显示错误: 消息 "MSG_CON" 的格式无效。
GUI	OCTCR19Q1475286	无法使用 GUI 安装 SSP/HF。
CLI	OCTCR19Q1473516	omnidb 命令允许没有 DP 用户权限的基本用户使用选项 -remove_msgs 和 -strip。
升级	OCTCR19Q1471287	从 Data Protector 10.20 升级到 10.91 后，Data Protector 群集经常崩溃。
升级	OCTCR19Q1471283	有关升级顺序的文档问题。
CLI	OCTCR19Q1469159	运行 omnib2dinfo -list_objects 命令时在 StoreOnce 上发现垃圾 Data Protector 对象。
安装/升级	OCTCR19Q1466632	如果在 /tmp 文件系统上设置了 noexec ，则客户机安装/升级失败。
文档	OCTCR19Q1465165	备份失败后恢复功能需要文档更新。
文档	OCTCR19Q1463134	重新启动备份后更改会话 ID 需要文档更新。
升级	OCTCR19Q1452045	将 Data Protector 10.20 升级到 10.91 后，IDB 备份会引发密钥管理错误。
备份	OCTCR19Q1447052	Data Protector 11.01: 在 IDB 备份过程中启动的 Amazon S3 备份失败。
CLI	OCTCR19Q1444137	omnib2dinfo 仅列出有限数量的对象。
集成	OCTCR19Q1442109	VMware GRE 对象未找到或访问被拒绝。
备份	OCTCR19Q1441449	将 Data Protector 从 10.91 升级到 11.00 后，在 PostgreSQL 备份期间发生错误。
Cell Manager	OCTCR19Q1437256	CRS 内存泄漏问题。
许可证	OCTCR19Q1437221	Data Protector 10.91: LINUX Cell Manager 许可证报告问题。
还原	OCTCR19Q1437218	较差的还原性能会影响 MoM 单元。
Cell Manager	OCTCR19Q1437189	Data Protector 10.50: EndofSession 通知在选择“正常”级别时不会发送完整会话报告。
备份	OCTCR19Q1437074	备份 IDB 时出错。
集成	OCTCR19Q1436517	Data Protector 10.91: 请求查看有关对象/介质复制支持的 NDMP 文档，并删除有冲突的声明。
升级	OCTCR19Q1432072	Data Protector 10.40: IS 升级后无法升级 Windows 客户机。
升级	OCTCR19Q1423072	从 Data Protector 9.09 升级到 10.91 后，IDB 备份失败。
介质代理	OCTCR19Q1421133	Data Protector 10.40: MS Azure 云设备创建失败并出现未知错误。
升级	OCTCR19Q1417779	如果不存在 Web 用户名，则 CPU 使用率会很高。
安装	OCTCR19Q1417456	本地和远程客户机部署在 RHEL 8.x 上失败。
灾难恢复	OCTCR19Q1416072	未能收集自动 DR 信息。
Cell Manager	OCTCR19Q1415311	RecoveryIndexDir=FullPathToTheBackupDir 全局选项应该是强制性的，而不是可选的。
集成	OCTCR19Q1412132	如果 LVM 分区是从不受支持的分区类型创建的，Data Protector VMware GRE 清理将不起作用。

集成	OCTCR19Q1360416	VMware GRE 恢复出现问题。
集成	OCTCR19Q1359888	Data Protector 10.50: 搜索 VMware GRE 逻辑卷时出现问题。
安装	OCTCR19Q1328562	input.in 运行 omnicc -secure_comm -regenerate_cert 命令不会更新文件。
Cell Manager	OCTCR19Q1320430	当 cell_info 文件包含控制字符时升级失败。
CLI	OCTCR19Q1312099	omnidb -veagent 命令不显示 Hyper-V 对象。
Cell Manager	OCTCR19Q1247124	Data Protector 10.90: 如果前几个插槽包含空白和损坏的数据域插槽，则介质扫描中止。
Cell Manager	OCTCR19Q1245196	Data Protector 10.90: 如果前几个插槽包含空白和损坏的数据域插槽，则介质扫描中止。
安装	OCTCR19Q1206644	通过 INET 部署 SSPHF 失败。
CLI	OCTCR19Q1153321	通过 omnimm 命令导入 MCF 失败。
CLI	OCTCR19Q1053786	Data Protector 10.60: omnidbzdb --diskarray 3PAR --exclude 命令不按预期工作。
安装	OCTCR19Q727713	Data Protector 10.50: 必须时常重新启用安装服务器中的 SMB 签名。
升级	OCTCR19Q331889	在 Windows 2012 上将 Data Protector 10.04 升级到 10.10 失败。
IDB	OCTCR19Q331287	无法使用区域设置初始化 IDB ja_JP.SJIS.

已知问题

“已知问题”主题列出了产品发布时尚未解决的发布前缺陷。本主题特定于产品版本，因此发布后不会因任何发布后缺陷而进行更新。

类别	问题 ID	描述	在版本中找到
基于角色的访问控制	OCTCR19Q1508158	在您的环境中启用 **RBAC** 后添加用户时，当此类用户执行集成备份时会显示以下警告: Error parsing the user list:"[2] No such file or directory " 但是，当已迁移的用户帐户执行备份时，不会显示此类错误。 变通方法：忽略警告消息。	11.01
报告服务器	OCTCR19Q1521292	在 SLES15 和 RHEL 7 上运行的报告服务器上，无法执行以下操作: • 导入或导出报告服务器配置设置 • 使用用户界面配置报告服务器日志级别	11.01
重复数据删除存储	OCTCR19Q1520024	对加密存储和非加密存储使用相同的容器可能会导致稍后备份失败。 变通方法：在任何云存储备份期间，对加密存储和非加密存储使用单独的容器。	11.01
	OCTCR19Q1412374	在备份期间，重复数据删除设备会在 DP GUI 会话消息中显示非压缩大小。 变通方法：无。	11.01
	OCTCR19Q1516102	如果重复数据删除磁盘已满，则不会显示特定的错误消息。 变通方法：如果备份失败并显示通用会话消息“无法写入设备”，您必须检查创建存储的主机上的磁盘空间。	11.01
	OCTCR19Q1519421	DPDUtils -restart 选项不是从云目标恢复损坏的存储数据的稳定方法。 发生这种情况是因为: • fd 文件无法恢复，或 • 当 you use DPDUtils restart -s 或 -w 选项在还原期间恢复已删除的数据或存储时，数据会损坏。 变通方法：无。	11.01
	OCTCR19Q1456126	不支持使用本地化名称创建存储 变通方法：无。	11.01

弃用和过时功能

已弃用的项目

已弃用的项目包括没有进一步增强计划的组件、功能或参数。对这些项目的支持将继续，直到发出过时通知。此外，这些已弃用项目的错误修复和支持案例将继续得到处理，直到已弃用的项目变为过时为止。

此版本中不启用任何项目。

过时的项目

过时的项目包括不再受支持的组件、功能或参数。

过时的项目	描述	从以下版本起过时
Microsoft 365 Exchange Online	Data Protector 不再支持 Microsoft 365 (M 365) Exchange Online 进行备份和还原。随着适用于云工作负载的 Data Protector (DP4CW) 的引入，Data Protector 中包含的 M365 Exchange Online 功能将被废弃。 但是，DP 11.01 仍然支持还原使用以前的 DP 10.91 (DP 2021.02) 或 DP 11.00 发布进行的任何现有 M365 Exchange Online 备份，直到在将来发布中逐步废弃。 有关适用于云工作负载的 Data Protector (DP4CW) 的详细信息，请参阅适用于云工作负载的 Data Protector 简介。	11.01
Windows 7 Windows 8 Windows 8.1	Data Protector 不再支持这些桌面 Windows 平台。	11.00
Windows Server 2008	Data Protector 不再支持 Windows Server 2008。	11.00
Windows Server 2008 R2	除了作为磁盘代理或介质代理之外，Data Protector 不再支持 Windows Server 2008 R2。	11.00
HP-UX 11.23 Itanium HP-UX 11.31 PA-RISC	Data Protector 不再支持 HP-UX 11.23 Itanium 和 HP-UX 11.31 PA-RISC 系统。	11.00
CentOS 6 Oracle Linux 6 RHEL 6	Data Protector 不再支持 CentOS 6、Oracle Linux 6 或 RHEL 6	11.00
Oracle 数据库 10g Oracle 数据库 11g	Data Protector 不再支持 Oracle 数据库 10g 和 Oracle 数据库 11g。	11.00
SLES 11	Data Protector 不再支持 SLES 11	11.00
x86 (32 位) 平台	Data Protector 不再支持 Windows x86 和 Linux x86 平台。	11.00
AIX 6.1	Data Protector 不再支持 AIX 6.1。	11.00
SCO OpenServer	Data Protector 不再支持 SCO OpenServer。	11.00
Mac OS X	Data Protector 不再支持 Mac OS X 系统。	11.00
Exchange Server 2013	Data Protector 不再支持 Exchange Server 2013。	11.00
SQL Server 2012	Data Protector 不再支持 SQL Server 2012。	11.00
vStorage + openStack 方法	Data Protector 不再支持 vStorage 和 OpenStack 方法	11.00
VMware vCloud Director	Data Protector 不再支持 VMware vCloud Director。	11.00
EMC VNX 和 VMAX 存储提供程序	Data Protector 不再支持与 EMC VNX 和 EMC VMAX 存储提供程序集成。	2020.11
EVA 和 EMC Symmetrix 阵列	Data Protector 不再支持与 EVA 和 EMC Symmetrix 阵列集成。	2020.08
基于 Flex 的 VMware Granular Recovery Extension (GRE)	Data Protector 不再支持基于 Flex 的 VMware Granular Recovery Extension (GRE)。Data Protector 2020.05 支持新的 HTML5 版本的 VMware GRE。如果要使用 VMware GRE，必须在升级到 DP 2020.05 后安装 HTML5 插件。	2020.05
omnidbutil -enable_common_criteria_mode	Data Protector 不再支持此命令行选项。	2019.12
HP-UX	Data Protector 不再支持在 HP-UX 系统上安装 Cell Manager 和安装服务器。	2019.08
Windows Server 2008 R2	Data Protector 不再支持在 Windows Server 2008 R2 上安装 Cell Manager 和安装服务器。	2019.08

相关主题

有关 Data Protector 发布 10.00 中所有已弃用项目和过时项目的列表，请参阅 https://docs.microfocus.com/DP/Obsolescence/DeprecationList.htm。

发布日志

Data Protector 发行日志是每个发行版中引入的功能的累积列表。当您从很早的发行版执行单步升级时，将跳过各种中间版本。该日志可帮助您快速查看为每个发行版添加的所有新功能。

Data Protector 11.01 中的新增功能

Data Protector 11.01 引入了以下新增功能或增强功能:

适用于云工作负载的 Data Protector

Data Protector 11.01 引入了适用于云工作负载的 Data Protector 以提供对以下范围的备份和还原支持:

- 云数据存储库，例如 Microsoft 365 (Exchange、SharePoint、Teams、OneDrive)
- 虚拟化环境，例如 Citrix XenServer、KVM、Nutanix
- 其他数据平台，例如 OpenShift、OpenStack

有关详细信息，请参阅适用于云工作负载的 Data Protector 简介。

增强型自动灾难恢复

Data Protector 增强了 EADR 以支持新的系统和功能，如下所示:

对 RHEL 8.x 和 SUSE 15.x 的 EADR 支持	使您能够执行 RHEL 8.x 和 SUSE 15.x 系统的 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR UEFI+Secureboot 支持	使您能够对配置为使用 UEFI 安全启动的主机执行 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR NIC 聚合支持	使您能够对配置了 NIC 聚合的系统执行 EADR
对 RHEL 8.x 和 SUSE 15.x 的 EADR 分区调整大小支持	默认情况下，使您能够将源系统中磁盘的原始分区调整为新替换的磁盘大小
对 Windows 2022 的 EADR 支持	此功能使您能够执行 Windows Server 2022 系统的 EADR

基于角色的访问控制

Data Protector 11.01 提供基于角色的访问控制 (RBAC) 的技术预览，允许您根据用户角色和权限来管理查看、备份和还原访问。

> 重要说明： RBAC 功能目前不受支持，仅在测试环境中可供预览。不要在生产环境中使用此功能。

有关在测试环境中使用基于角色的访问控制的信息，请参阅基于角色的访问控制文档。

从 Data Protector 界面管理和控制 SAP HANA 备份

除了从 SAP HANA 界面进行的现有备份和还原之外，Data Protector 11.01 还支持从 Data Protector GUI 和 CLI 配置和备份 SAP HANA 数据库。它现在支持单节点配置中的完整备份和增量备份类型。您可以使用高级和旧版调度程序来计划备份。

有关详细信息，请参阅 SAP HANA 集成。

Postgres 11、12、13、14 系列备份和还原

Data Protector 11.01 增加了对 PostgreSQL 版本 11、12、13、14 的备份、还原和恢复的支持。参阅支持矩阵以获取有关平台的信息

有关受支持平台的信息，请参阅支持矩阵。

集成虚拟磁盘开发套件 (VDDK) 7.0.3

Data Protector 11.01 包 VDDK 7.0.3 以支持新的备份代理主机。

有关受支持平台的信息，请参阅支持矩阵。

Data Protector 重复数据删除存储

Data Protector 11.01 增强了重复数据删除存储以支持以下功能:

- 跨多个存储的单一端口
- 来自公共云提供商的存储配置，例如 AWS S3、Microsoft Azure、Google GCP 和 S3 兼容云目标
- 增强的稳定性和性能
- VMware 备份的缓存粒度恢复
- 三向 NDMP 备份
- 静态数据加密

有关详细信息，请参阅 Data Protector 重复数据删除存储。

数据域提升

Data Protector 11.01 支持三向 NDMP 备份。

安全增强功能

以下 Data Protector 组件已升级，从而使 Data Protector 比以前的版本更安全:

组件	升级到版本
WildFly	23.0.2
Keycloak	15.1.1
OpenSSL	1.0.2zd
报告服务器数据库 (PostgreSQL)	11.5

Data Protector 11.00 中的新增功能

Data Protector 11.00 引入了以下新增功能或增强功能:

Data Protector 重复数据删除存储

Data Protector 11.00 提供了一种新的基于软件的重复数据删除设备，可确保高效利用存储空间和网络带宽。该存储类似于现有集成，例如 StoreOnce 软件与设备和数据域。

Data Protector 重复数据删除存储:

- 对备份数据进行重复数据删除，仅存储唯一数据和引用以复制数据块。
- 支持源端、目标端和服务器端重复数据删除。
- 根据设计提供以 PB 为单位的容量。截至目前，已通过高达 250 TB 的测试。
- 在物理机和虚拟机上的 Windows Server 2016、Windows Server 2019 和 Linux 系统 (RHEL、SLES) 中均受支持

有关详细信息，请参阅 Data Protector 重复数据删除存储。

VMware 增强功能

Data Protector 11.00 增强了与 VMware 的虚拟环境集成，包括以下内容:

- **数据存储和存储视图：** 您可以使用“备份”上下文中的“数据存储和存储” 视图来浏览和备份按数据存储和数据存储群集分组的虚拟机。
- 并行磁盘还原**:** 您可以并行还原多个 VMware 磁盘。有关详细信息，请参阅 VMware 的虚拟环境集成。
- **VMware VDDK** 升级**: VMware** 虚拟磁盘开发套件 **(VDDK)** 已升级到适用于 Windows 和 Linux 备份主机的 7.0.2 版。这增强了与当前和即将发布的 VMware vSphere 及 ESXi 版本的兼容性。有关受支持的 Windows 和 Linux 备份主机的列表，请参阅支持矩阵。

Hyper-V 并行磁盘备份

使用 Data Protector 11.00，可在 VM 级别备份多个 Hyper-V 磁盘。您可以并行 (默认) 或按顺序备份它们 (通过使用 omnirc 变量 OB2_VEAGENT_THREADED_DISK_BACKUP)。有关详细信息，请参阅 Microsoft Hyper-V 的虚拟环境集成。

H3C CAS 单个盘备份和还原

当您使用缓存方法时，Data Protector 11.00 使您能够备份和还原连接到 VM 的单个磁盘。您可以仅包括或排除备份和还原所需的磁盘。有关详细信息，请参阅 H3C CAS 的虚拟环境集成。

Microsoft 365 Exchange Online 增强

Data Protector 11.00 增强了 Microsoft 365 Exchange Online 集成以包括以下内容:

- 增量备份和还原
- 还原特定的邮箱文件夹
- 电子邮件别名支持
  如果用户的电子邮件 ID 发生更改，Data Protector 会考虑电子邮件 ID 更改之前的用户邮箱。
- 重新启动失败的备份
  您可以使用 omnidb 命令 (omnidb -restart <*session_id*>) 中的 -restart 选项重新启动失败的备份。
- Azure 应用程序凭据的自动续订
- 管理 Azure 应用程序
- 在备份期间排除邮箱文件夹

Data Protector 11.00 还增强了“备份”和“还原”页面的可用性，以提供更好的用户体验。要还原 Data Protector 2021.02 进行的 Microsoft 365 备份，请使用 omnir 命令。不能使用“还原”页面还原此类备份。

有关详细信息，请参阅 Microsoft 365 Exchange Online 集成。

安全 SMTP 支持

通过 Data Protector 11.00，您可以使用安全 SMTP 协议来发送使用电子邮件 (SMTP) 发送方法配置的报告和通知。有关详细信息，请参阅配置安全 SMTP。

应用程序服务器重新配置实用程序

Data Protector 11.00 提供了一个应用程序服务器重新配置实用程序来修复不一致的应用程序服务器配置。有关详细信息，请参阅升级期间和之后的其他应用程序服务器问题和 omniasfix 。

GNU Compiler Collection 版本升级

Data Protector 11.00 将用于构建组件的 **GNU Compiler Collection**（**GCC)** 版本升级到 **GCC 10.2**。这会提高稳定性和性能，同时增强与新的第三方应用程序的兼容性。

Data Protector 2020.11 中的新增功能

Data Protector 2020.11 引入了以下新增功能:

Hyper-V RCT 备份和还原

Data Protector 支持 Windows Server 2016 和更高版本上的 Hyper-V VM 的弹性更改跟踪 (RCT) 备份和还原。与基于 VSS 快照的备份提供的更改跟踪相比，RCT 提供了更好的弹性。它在数据块级别跟踪备份之间虚拟机上发生的更改。RCT 可以在特定的时间点检测更改，从而无需扫描整个磁盘以检测更改。这样可以加快备份和还原操作并减少系统负载。

此版本的 Data Protector 仅支持“完整” 备份和还原类型，为 Hyper-V 增量备份和 GRE 提供了基础，它们将在即将发布的版本中推出。有关更多信息，请参阅 Microsoft Hyper-V 的虚拟环境集成。

基于块的增量备份、还原和恢复

Data Protector 增强了基于块的备份功能，以支持 Windows Server 2012 和 Windows Server 2012 R2 平台的增量备份。它还为 Windows Server 2016 和 Windows Server 2019 平台引入了增量备份 (差异备份) 支持。您现在可以执行以下操作:

- 基于块的增量备份 (在 Windows Server 2012 和 Windows Server 2012 R2 上) 和差异备份 (在 Windows Server 2016 和 Windows Server 2019 上)
- 从增量或差异备份还原和恢复。

有关更多信息，请参阅基于块的备份、还原和恢复。

Microsoft SharePoint GRE 增强功能

Data Protector 现在支持与 Microsoft SharePoint Server 版本 2016 和 2019 集成。

VMware GRE 增强功能

最新版本的 VMware GRE 具有以下增强功能:

- 搜索 - 搜索功能用于在搜索框中键入名称或关键字来轻松找到要恢复的文件或文件夹。
- 在装载代理上恢复 - 此选项用于将文件还原到选定的装载代理，从而在 VM 环境遇到任何问题时提供备用的还原位置。

有关这些增强功能的详细信息，请参阅使用 HTML5 GRE Web 插件恢复。

IDB 还原增强功能

Data Protector 增强了 IDB 还原和恢复方法，以优化和自动化许多需要手动执行的步骤。请参阅还原 IDB。

安全增强功能

以下 Data Protector 组件已升级，从而使 Data Protector 比以前的版本更安全:

组件	升级到版本
WildFly	20.0.1
Keycloak	11.0.3

Data Protector 2020.08 中的新增功能

Data Protector 2020.08 引入了以下新增功能:

VMware 增强功能

与 VMware 的虚拟环境集成已得到增强，具体如下:

- **“标记和类别”视图**: 通过 Data Protector，您可以使用“备份”上下文中的“标记和类别”视图，来备份和还原按标记和类别分组的 VMware vCenter 虚拟机。标记是可以创建并分配给 vSphere 库存中的 VM 的标签。类别将相关标记分组在一起。
- **改进了 Windows 计算机上的 VMware GRE 浏览性能和可用性**: 此版本的 Data Protector 在 VMware GRE 浏览性能和可用性方面进行了重大改进，从而缩短了搜索时间并加快了还原操作。

安全增强功能

以下 Data Protector 组件已升级，从而使 Data Protector 比以前的版本更安全:

组件	升级到版本
OpenJDK	1.8.262
WildFly	19.1.0
Keycloak	10.0.2

Data Protector 2020.05 中的新增功能

Data Protector 2020.05 引入了以下新增功能:

内部数据库 (IDB) 升级

Data Protector 2020.05 带有高级 IDB。IDB 已升级到 PostgreSQL 11.5，从而显著提高了安全性。如果要从较旧的 Data Protector 版本进行升级，则 IDB 会在升级过程中自动更新。有关成功进行 IDB 升级的建议，请参阅升级 Data Protector 服务器。

限制通过 INET 升级的能力

引入了新的 omnirc 变量 OB2RESTRICTUPGRADEOVERINET 来限制通过 INET 升级，这样只有知道客户机密码的管理员才能升级。如果 OB2RESTRICTUPGRADEOVERINET 设置为 1，则升级使用 SSH/SMB 而不是 INET，并且如果配置了基于密码的 SSH 访问，则每次启动升级时都会提示您输入密码。有关使用此变量的详细信息，请参阅升级 Data Protector 客户机。

HTML5 VMware Granular Recovery Extension (GRE) 插件

新的 VMware GRE 插件是旧 GRE 插件的独立于 Flash 的 HTML 5 版本。HTML5 插件具有新的外观，以改善用户体验。它适用于 VMware vCenter 版本 6.5 u2 或更高版本。
从 Data Protector (DP) 2020.05 开始，仅支持 GRE 插件的 HTML5 版本。不再支持旧的基于 Flex 的 GRE 插件。如果您使用的是基于 Flex 的插件，则必须在升级到 DP 2020.05 后安装新的 HTML5 插件。

有关详细信息，请参阅使用 GRE HTML5 Web 插件进行恢复。

对 H3C CAS 新体系结构的支持

Data Protector 支持以下功能:

- 缓存的备份方法: 您可以将磁盘直接备份到目标设备，而无需暂存路径或备份主机。您可以执行完整、增量和差异缓存的备份。
- CBT 跟踪器: 更改块跟踪器 (CBTer) 跟踪虚拟磁盘数据块中的更改。您只能将此跟踪器与缓存的备份一起使用。

有关详细信息，请参阅 H3C CAS 的虚拟环境集成。

支持 Amazon S3 Glacier 和 Amazon Deep Archive

Data Protector 支持将 Amazon S3 Glacier 和 Amazon S3 Glacier Deep Archive 作为磁盘 (B2D) 云设备的新备份。这些是归档云设备，可用于备份和还原大量数据。有关详细信息，请参阅云设备 - Amazon S3 Glacier 和 S3 Glacier Deep Archive。

基于块的备份、还原和恢复 - 增强功能

作为对基于块的备份和还原功能的进一步增强，Data Protector 现在支持基于块的恢复功能。恢复功能使您可以浏览基于块的备份，并选择单个文件或目录进行恢复。它使您能够将感兴趣的单个文件或目录恢复到所需的目标位置。有关详细信息，请参阅基于块的备份、还原和恢复。

备份和还原操作的性能得到增强，以具有较小的备份和还原窗口。

增强的基于 Web 的调度程序

基于 Web 的调度程序提供了以下增强功能:

- 在基于 Web 的调度程序中支持 24 小时格式 - 基于 Web 的调度程序现在支持 12 小时和 24 小时时间格式。它根据用户的区域设置以 12 小时制或 24 小时制显示时间。例如，如果用户区域设置为“德语(德国)”，则时间以 24 小时制显示；如果用户区域设置为“英语(美国)”，则时间以 12 小时制显示。
- 在计划创建向导中搜索规范的选项 - 创建计划时，可以通过浏览规范类型来选择规范，也可以通过在“搜索”框中键入规范名称来搜索规范。

有关 24 小时支持和“搜索”选项的更多选项，请参阅基于 Web 的调度程序。

对 systemd 的支持

Data Protector 现在支持在 Cell Manager 和客户机上使用 systemd 。在旧版本的 Data Protector 中，需要在目标系统上安装 xinetd 程序包。由于支持 systemd ，因此不再需要 xinetd 程序包。

注意: systemd 在 RHEL 8.0 和更高版本以及 SLES 15 和更高版本中受支持。

Postgres Professional 数据库的备份和还原

Data Protector 提供了基于脚本的解决方案来执行 Postgres Professional 数据库的备份和还原。您可以在 ITOM Marketplace 下载 Postgres Professional 的备份和还原脚本。

安全改进

以下 Data Protector 组件已升级，从而使 Data Protector 比以前的版本更安全:

组件	升级到版本
OpenSSL	1.0.2u
OpenJDK	1.8.0_242
WildFly	18.0.1
Keycloak	8.0.1
StoreOnce 客户机	4.2.0

Data Protector 2019.12 中的新增功能

Data Protector 2019.12 引入了以下新增功能:

基于块的备份和还原

Data Protector 引入了一种新的备份类型 (称为基于块的备份)，使您可以在块级别执行文件系统备份。它按块在磁盘上保存的顺序读取块，而不是按文件中显示的顺序读取。系统仅备份已使用的块，从而减少了备份时间。

同样，通过基于块的还原，您可以还原在块级别备份的数据。您可以在备份时还原整个块。有关更多信息，请参阅基于块的备份和还原。

改进的仪表板、报告和基于 Web 的调度程序

为了更好的外观和可用性，对以下用户界面页面进行了改进:

- 仪表板 - 新的仪表板提供了备份环境的更详细和可自定义的概述。
- 基于 Web 的调度程序 - Web 调度程序提供了专门为大型环境设计的新排序和过滤功能。您可以根据需要隐藏高级配置项。
- 报告和遥测 -“报告”和“遥测”页面具有新的外观。此外，“遥测”页面已从主页上下文的登录页面移出。现在可以在右上方的“设置”菜单下找到它。

有关更多信息，请参阅仪表板、基于 Web 的调度程序和遥测。

许可增强

- 报告服务器许可证 (适用于基于功能的许可的用户) - 报告服务器许可证以前仅是基于套接字的 (精简) 许可证和基于容量的 (高级) 许可证的一部分，现在可以作为基于功能的许可证用户的附加独立许可证使用。借助报告服务器许可证，您可以通过 DP GUI 使用 Data Protector 的基于 Web 的增强报告。您可以浏览任何 Cell Manager 的所有可用 Web 报告。有关详细信息，请参阅许可证。
- 添加到 omnicc -check_licenses -detail 命令的新选项:
  - -online 您可以使用此选项查看使用联机许可证的主机列表。
  - -exact 您可以使用此选项来计算最近 90 天前完整备份的受保护数据总数。

有关 omnicc 命令的更多信息，请参阅 omnicc。

VMware 增强功能

与 VMware 的虚拟环境集成已得到增强，具体如下:

- 支持 vSAN 6.6.1 和 6.7 平台上的 VM 的开机和实时迁移。
- 支持 vCenter 和 VCSA 6.7 U3。
- 支持 VDDK API VixDiskLib_QueryAllocatedBlocks()，它在完整磁盘备份期间仅备份使用的块。
- VDDK 6.7 U3 随该版本打包。
- 从 vSAN 数据存储备份的 VM 支持 GRE。

对 Dell-EMC Unity 和 NetApp 存储系统的即时恢复支持

存储系统集成代理已得到改进，以支持即时恢复和远程复制功能。主要重点是恢复时间目标 (RTO)，使您可以在尽可能短的时间内还原大型数据集。有关更多信息，请参阅配置 Dell EMC Unity 存储和配置 NetApp 存储。

MySQL 和 PostgreSQL 代理增强

现在，增强的 MySQL 和 PostgreSQL 代理在备份配置、备份和还原活动期间显示数据库的状态。您也可以自动停止或启动数据库以准备还原。

在 Nutanix AHV 基础结构上进行备份和还原

Data Protector 为管理员提供了基于脚本的解决方案，以执行 Nutanix AHV 基础结构上 VM 的备份和还原。有关更多信息，请参阅 Nutanix AHV 集成。

Data Protector 2019.08 中的新增功能

Data Protector 2019.08 引入了以下新增功能。

安全改进

Data Protector 包括以下安全增强功能：

- 通过一致地保护凭据来提高处理存储凭据时的安全性。
- 数据通道安全性和审核与安装工作流集成。
- OpenJDK 更新，可受益于最新 Java 修复。
- 通过包括其他加密模式进行 OpenSSL 安全性修复。
- 缓冲区溢出修复。
- 仅限 Data Protector 管理员执行的IDB 恢复。
- 加密密钥导入/导出加固，以确保导出数据的安全。

有关 Data Protector 安全性的详细信息，请参阅保护 Data Protector 环境。

对 Dell EMC Unity 存储系统的零宕机备份支持

Dell EMC Unity 系统的零宕机备份 (ZDB) 使 Data Protector 可以利用基于阵列的快照来备份文件系统、SQL、VMware 和 Oracle，从而为 Dell-EMC Unity 存储系统上托管的数据提供快速高效的备份。

有关配置 Dell EMC Unity 的详细信息，请参阅配置 Dell EMC Unity 存储。

MySQL 代理增强功能

增强的 MySQL 代理增加了列出单个数据库和表并将其还原到 MySQL 实例的功能，从而为用户提供了灵活的还原方法。MySQL 群集备份允许用户在 MySQL 环境中备份和还原高可用性群集。

有关配置 MySQL 的详细信息，请参阅 MySQL 集成。

CLI 更改

Data Protector 2019.08 包括以下 CLI 更改:

- omnidbutil 命令包含一个新选项 -enable_common_criteria_mode 。有关详细信息，请参阅 omnidbutil 命令页。
- omnikeytool 命令包含一个新选项 -password *password* 。有关详细信息，请参阅 omnikeytool 命令页。
- omnicc 命令包括以下新选项：
  - -enable_secure_data_comm *Value*
  - -enable_auditlog *Value* [-retention_months *retentionValue*]

  有关详细信息，请参阅 omnicc 命令页。

弃用

- Data Protector 不再支持 HP-UX 系统作为安装 Cell Manager 和安装服务器的平台。Data Protector 继续支持客户机使用 HP-UX 系统。要将现有 Cell Manager 从 HP-UX 迁移到 Linux，请参阅迁移 HP-UX Cell Manager。
- Data Protector 不再支持 Windows Server 2008R2 作为安装 Cell Manager 和安装服务器的平台。有关受支持平台的详细信息，请参阅最新支持矩阵。

Data Protector 2019.05 中的新增功能

Data Protector 2019.05 引入了以下新增功能:

Chromium Web 渲染引擎

在 Data Protector 中，Chromium 将替代 Internet Explorer 作为 Web 渲染引擎。通过在 Data Protector UI 中集成 Angular、UX 特性及其他组件，Chromium 改善了用户体验 (UX) 且具有新的用户界面 (UI)。

安全增强功能

- 由于进行了白帽渗透测试和国家信息安全保证联盟 (NIAP) 预检查测试以抵御安全漏洞，改进了安全增强功能。请参阅保护 Data Protector 环境，以了解有关安全性的详细信息。
- Data Protector 建议在备份文件系统或磁盘映像期间使用 AES 256 位加密以确保数据安全性。选择安全性更低的“编码”选项后，Data Protector 将显示错误消息。请参阅数据安全性，以了解有关数据安全性选项的详细信息。

支持 Microsoft Visual Studio 2017

Data Protector 的安装包中包含适用于 Windows 操作系统的 Microsoft Visual C++ Redistributable for Visual Studio 2017。Data Protector 安装程序会检查现有 Microsoft Visual C++ Redistributable for Visual Studio 2017 安装是否在 Windows 服务器或客户机中可用。如果此包不可用，则 Data Protector 会自动将其安装在合格的系统上。

请参阅 Microsoft Visual Studio 2017 要求，以了解详细信息。

.NET Framework 要求

Microsoft Exchange Server 要求安装以下版本的 .NET Framework:

- Data Protector 需要 .NET Framework 2.0 及更高版本，才能安装 Microsoft SharePoint Server 客户机。
- 在安装了适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension (GRE) 的系统中，Data Protector 需要 .NET Framework 3.5.1。

请参阅 .NET Framework 要求，以了解有关 .NET Framework 要求的详细信息。

适用于 H3C CAS 环境的虚拟环境集成

适用于 H3C CAS 的虚拟环境集成已得到增强，具体如下:

- 增量备份和差异备份现在受支持。
- **还原到另一个 CAS 服务器**: 现在可以选择将虚拟机还原到除原始 CAS 管理服务器之外的 CAS 服务器。
- 更改后的块跟踪: 您现在可以启用更改后的块跟踪 (CBT) 以提高备份的效率和速度。
- 还原为新虚拟机: 现在可以使用“还原”上下文中的“还原为/还原到”选项将已备份的虚拟机还原为新虚拟机。

自定义全局选项

可以在位于 \ProgramData\OmniBack\Config\Server\Options (Windows) 和 /etc/opt/omni/server/options (Linux) 中的“全局”文件中自定义全局选项。Data Protector 不支持使用 GUI 自定义全局选项。请参阅自定义选项以自定义全局选项。

NetApp SnapMirror 的零宕机时间备份

NetApp SnapMirror 可复制相同或不同存储系统中的数据。Data Protector 支持 NetApp SnapMirror 卷的零宕机时间备份 (ZDB)。通过采用 ONTAP 9.3 C-mode 的 NetApp SnapMirror 的 ZDB，Data Protector 可以利用基于阵列的复制功能以备份文件系统、SQL、VMware 和 Oracle，从而快速高效地备份主 NetApp 存储系统和次要 NetApp 存储系统。在 NetApp SnapMirror 配置的卷中，将从镜像卷而非源卷执行备份。请参阅配置 NetApp 存储，以了解有关为 NetApp SnapMirror 配置 ZDB 的信息。

报告增强功能

- Data Protector 支持在运行 Ubuntu 操作系统的服务器上安装报告服务器。有关详细信息，请参阅安装报告服务器。
- Data Protector 报告中会提供详细的问题描述和建议采取的操作，以便更快地找到备份失败的根本原因，从而加快问题解决。有关详细信息，请参阅会话错误报告。

支持 PostgreSQL 群集

支持 PostgreSQL 群集后，用户可以在 PostgreSQL 环境中备份和还原多主机高可用性群集。请参阅 PostgrSQL 集成，以了解有关备份和还原 PostgreSQL 群集的信息。

Data Protector 2019.02 中的新增功能

Data Protector 2019.02 引入了以下新增功能:

适用于 H3C CAS 的虚拟环境集成

适用于 H3C CAS 的虚拟环境集成已得到增强，包括以下功能:

- 并行还原: 现在可以从主机中并行还原多个虚拟机。
- 预览备份：预览备份选项已启用。

Data Protector Express 中的文件系统备份和灾难恢复

Data Protector Express 现在支持 Cell Manager 的端到端备份和灾难恢复。

有关详细信息，请参阅灾难恢复。

报告

Data Protector 报告现在支持以下内容：

- Data Protector 环境中的管理器之管理器 (MOM) 配置。
- 以下新报告提供了对 Data Protector 环境的深化了解：
  - 未配置的客户机报告
  - 许可报告
  - 备份规范错误时间线报告
  - 重复数据删除率报告
  - 会话特定信息报告
  - 对象最新备份报告
  - 没有备份的对象报告
  - 平均备份对象大小报告
  - 会话特定计划报告
  - 未使用的已配置设备报告
  - 重复数据删除率预测报告
  - 会话错误报告
  - 运行状况评估报告

有关详细信息，请参阅 Data Protector 报告。

NetApp C-mode 的零宕机时间备份

带有 ONTAP 9.x 的 NetApp C 模式的零宕机备份 (ZDB) 使 Data Protector 可以利用基于阵列的快照来备份文件系统、SQL、VMware 和 Oracle，从而提供快速有效的备份。

有关详细信息，请参阅 Data Protector NetApp ONTAP C 模式。

支持 MySQL 8

Data Protector 支持 MySQL 8 的备份和恢复。

有关详细信息，请参阅支持矩阵。

在 ZDB 代理中支持 NetApp 存储

Data Protector 使用 NetApp 存储管理计划规范 (SMI-S) 提供程序与 NetApp 存储系统集成。NetApp SMI-S 提供程序插件在 Data Protector 零宕机备份 (ZDB) 代理中启用 NetApp 存储支持。

文档变更

- 联机帮助:
  Data Protector 联机帮助已替换为当前发布的整个文档的脱机捆绑包。保留上下文敏感性。除了查看帮助主题之外，您现在还可以脱机浏览整个文档。有关最新文档，请参阅 https://docs.microfocus.com/?DP。
- 本地化：
  Data Protector 文档已本地化为法语、日语和简体中文。可用的本地化内容将始终处于上一发行版级别。例如，Data Protector 2019.02 文档包含 Data Protector 2018.11 的本地化内容。要访问已本地化的文档，请使用相应的语言 URL：
  - 法语: https://docs.microfocus.com/itom/Data_Protector:2019.02/Home/fr
  - 日语: https://docs.microfocus.com/itom/Data_Protector:2019.02/Home/ja
  - 简体中文: https://docs.microfocus.com/itom/Data_Protector:2019.02/Home/zh-cn
- 从业人员备注：
  ITOM 从业人员门户中的从业人员备注是一个节点，公司内外的产品专家可以在该节点中共享有关 ITOM 产品的信息。创建该节点是为了维护补充产品文档的技术信息。此处包含的信息将不时进行审核，并整合到产品文档中以提高其质量和准确性。
  请注意，从业人员备注中的内容由产品用户提供。产品开发人员尚未对其进行测试。
  通过单击左侧导航栏中的“从业人员备注”链接来访问从业人员备注。

Data Protector 2018.11 中的新增功能

Data Protector 2018.11 引入了以下新增功能:

VMware 6.7 U1 支持

Data Protector 现在支持 VMware vSphere 6.7 U1 以及最新 vddk 版本。通过新的 vddk 集成，支持以下代理主机: Windows Server 2008 R2 (x64)、Windows Server 2012、2012 R2 (x64)、Windows Server 2016、CentOS7.4 (x64)、RHEL 6.7、6.8、7.2、7.3 (x64) 和 SLES 12.1 (x64)。从 Data Protector 2018.11 (10.20) 开始，VMware vSphere 5.5.x 已过时。

高级版和精简版均支持该功能。

EMC 数据域系统高级 VMware 操作

EMC 数据域系统设备现在支持“粒度恢复”、“启动”和“实时迁移”等高级 VMware 操作。VMware vSphere 6.7 U1 环境中的虚拟机也支持该功能。

高级版和精简版均支持该功能。

EMC 数据域系统库升级

Data Protector 现在与最新的 EMC 数据域系统库 v3.4 集成并支持 DDOS 6.1。

适用于 H3C CAS 的虚拟环境集成

Data Protector 与 H3C CAS 版本 5.0 (适用于 H3C 基础架构即服务 (IaaS) 的云管理平台) 集成，支持备份和还原托管在 H3C CAS 环境上的虚拟机。

高级版和精简版均支持该功能。

许可容量计算 – 90 天

容量计算算法已修改，仅将最近 90 天备份且处于活动保护下的数据计入许可范围。这仅适用于 Data Protector 高级版许可证和基于容量的许可证。任何超过 90 天仍受保护的数据将不计入许可范围 (TB)。

REST API 桥

Data Protector 引入了新的 REST API 桥。此桥提供了新的 REST 端点，以 RESTful 方式提供 Data Protector CLI，在新旧环境之间架起一座桥梁。使用 REST API 解锁 Data Protector 的高级功能 (以 CLI 形式提供)。

安装/升级环境

Data Protector 安装和升级流改进为全新安装和升级提供了更好的体验。

调度程序改进

在 Data Protector 10.20 (2018.11) 中，基本调度程序可供使用。对于从 Data Protector 8.1x 和 9.0x 升级的环境，不执行计划迁移。但是，可以使用 omnidbutil 命令将计划迁移到基于 Web 的调度程序。有关更多详细信息，请参阅 omnidbutil -help CLI 选项。

对于已经使用基于 Web 的调度程序的环境，提供了用于恢复基本计划的选项。有关更多详细信息，请参阅 omnidbutil –help CLI 选项。

报告

Data Protector 现在包含许多新报告，以便更深入地了解 Data Protector 环境。此发布附加了以下报告:

- “配置报告”下的“IDB 详细信息报告”
- “配置报告”下的“客户机备份报告”
- “高级报告”下的“退款报告”

Data Protector 还引入了一个新类别:“自定义报告”，用于创建满足企业需求的报告。

Data Protector 2018.09 中的新增功能

Data Protector 发布 2018.09 (10.10) 引入了两个新版本的 Data Protector: Data Protector Express 和 Data Protector Premium。

Data Protector Express

Data Protector Express 是基于套接字许可模式的虚拟专用产品。Data Protector Express 包含以下功能:

- 引入基于套接字的许可，包括对软件加密的支持
- 支持现有虚拟化环境 (VMware 和 Hyper-V)。
- 支持虚拟机和 Data Protector 内部数据库 (IDB) 的备份和恢复。但是，不支持文件系统备份、应用程序集成等。
- 支持各种高级虚拟化功能，如粒度恢复 (GRE)、开机、实时迁移和零宕机时间 (ZDB) 集成。
- 恢复当前和先前备份的数据 (升级前)。
- 许可详细信息提供有关已耗用套接字和可用套接字的信息。
- 可以仅使用 Data Protector GUI 添加其他套接字的许可证。可以在导入 vCenter/Hyper-V 或 ESXi 服务器期间或导入之后应用许可证。不支持通过 CLI 管理许可证，例如添加或删除套接字。
- 支持从 Data Protector 8.1x、9.x和 10.0x 版本升级到 Data Protector 10.10。

在独立环境或 Manager-of-Manager 环境中，不支持具有基于套接字和基于容量的许可的混合模式环境。如果安装了 Data Protector Express 和 Data Protector Premium 许可证，则仅限使用 Data Protector Premium 许可证。

Data Protector Premium

Data Protector Premium 许可基于受保护的容量大小。如果安装了 Data Protector Express 和 Data Protector Premium 许可证，则仅限使用 Data Protector Premium 许可证。Data Protector Premium 包含以下功能:

- 支持软件加密。
- 支持 Data Protector 的全部功能。
- 支持文件系统备份、应用程序集成、虚拟化等。
- 支持使用 Data Protector Premium 许可证的具有多个 Cell Manager 的 MoM 环境。
- 支持从 Data Protector 8.1x、9.x和 10.0x 版本升级到 Data Protector 10.10。
- 只需更改许可证密钥，即可轻松从 Data Protector Express 升级到 Data Protector Premium。

Data Protector 报告

Data Protector 现在提供各种报告，可帮助您管理和计划备份环境。这些报告可使用 Data Protector GUI 中的“主页”上下文 >“报告”选项进行访问。Data Protector 报告可自定义，并提供有关上次备份状态、对象复制、对象合并或对象验证、介质池中介质消耗、设备状态等信息。您可以下载 PDF、PNG、 CSV 或 JSON 格式的报告。您也可以在“报告”>“高级设置”选项中进行配置，以通过电子邮件发送这些报告。要使用报告功能，请在不用作 Data Protector Cell Manager 的 Linux 或 Windows 服务器上安装报告组件。Data Protector 报告仅适用于容量、试用 (精简版) 或试用 (高级版) 许可证。

Windows 本机 NTFS 重复数据删除卷的备份

备份对象摘要中引入了新选项“重复数据删除卷备份”，用于保护 Windows 本机 NTFS 重复数据删除卷。选择此选项后，可以使用 Windows 本机重复数据删除卷的更改日志提供程序来运行增量备份，增强型增量备份或增量备份。

Data Protector Premium 中基于容量的许可证改进

现在，Data Protector 仪表板将在主机/对象级别显示为基于容量的许可证计算而保护和计数的数据量。改进了基于容量的许可，以避免在更改主机名、IP 地址或 vCenter 名称时重复计算容量。

90 天试用许可证

Data Protector 试用许可证现在延长到可使用 90 天。

安装程序改进

Data Protector 安装程序的主要改进包括：在安装和升级过程中进行自动检查。这将验证主机名兼容性，并且满足其他先决条件。简化证书重新生成。支持短主机名和长主机名。

调度程序改进

Data Protector 调度程序包含以下增强功能: 扩展 omnidbutil 命令以获得高级调度程序选项。接受用于导入/导出操作的非默认路径。导出/导入 JSON 中调度程序的所有选项（例如：网络负载、保护和优先级）。在命令输出中列出是启用还是禁用计划。

CLI 更改

Data Protector 2018.09 (10.10) 包括以下 CLI 更改:

- **omnicc** 命令包含一个新选项 **schedule_info**。

Data Protector 10.04 中的新增功能

Data Protector 10.04 引入了以下新增功能:

IBM Power Systems 上的 SUSE Linux Enterprise Server 支持

Data Protector 10.04 支持将 IBM Power Systems 上的 SUSE Linux Enterprise Server 作为磁盘代理平台。

非根用户安装 Data Protector 客户机

Data Protector 10.04 允许非根用户安装 Data Protector 客户机。非 root 用户必须是 SUDO 用户组的成员才能安装 Data Protector 客户机。

NDMP 增强功能

Data Protector 10.04 支持将 EMC Isilon 和 VNX DMP Server 备份到 StoreOnce Catalyst 和文件库设备。

Operation Orchestration 集成

Data Protector 与 Operations Orchestration (OO) 10.80 集成在一起，在一个称为流的结构化序列中创建和使用操作。这些结构化序列用于对 IT 资源进行维护、故障诊断、修复和配置。

调度程序增强功能

调度程序中包括以下主要增强功能：

- 增强的日期视图界面。
- 改进的维护作业功能。

用户管理—LDAP 组

通过下列 LDAP 组功能增强了用户管理：

- 支持 Active Directory。
- LDAP_GROUP 中所有用户将被允许访问 Data Protector。

Cell Manager 身份验证

连接到特定的 Cell Manager 时，Data Protector 仅提示一次输入用户凭据。无需对该 VSphere 会话中的同一 Cell Manager 再次进行身份验证。

装载代理选择

使用 Data Protector，可以在连接到 vCenter GRE 插件进行初始配置时选择安装代理。

CLI 更改

Data Protector 10.04 包括以下 CLI 更改:

- **omniusers** 命令包含一个新选项 **ldap_config**。

Data Protector 10.03 中的新增功能

Data Protector 10.03 引入了以下新增功能:

直接升级到 Data Protector 10.03

Data Protector 10.03 是完整版本，现在可以从 Data Protector 版本 8.1x、9.0x 或 10.0x 直接升级到 Data Protector 10.03。

例如，如果您的环境中正在运行 Data Protector 9.09，则可以直接将环境升级到 10.03，而无需安装 Data Protector 10.00。

更名的 Data Protector

Data Protector 10.03 已更名并使用 Micro Focus 名称和主题进行了更新。现在，您可以在我们的 GUI 和 CLI 中拥有相同的体验。

调度程序增强功能

在 Data Protector 10.03 中，调度程序包括以下主要增强功能：

- 现在，您可以使用调度程序UI创建，编辑和删除一次性维护作业。
- 您现在可以通过调度程序 UI 禁用或启用计划。默认情况下，计划会在添加时启用。现在，您可以禁用它，保留计划设置不变以供以后使用。禁用计划不会影响当前正在运行的会话。
- 您现在可以在月视图和日视图中查看假期。
- 现在，您可以使用 omnidbutil 命令创建、修改、列出、导出、导入和删除计划。

用户管理

Data Protector 10.03 中的新用户管理提供以下功能：

- 将为所有用户提供 Web 访问权限。现有用户将被迁移以具有 Web 访问权限。
- 用户可以将其 Web 用户名和密码用于 REST API。
- 可以通过 GUI 和 CLI 命令执行用户和组操作（例如添加、修改、删除和列出）。
- 可以通过 GUI 和 CLI 命令重置或清除密码。只有具有管理员权限的用户才能完成此操作。

在 Data Protector 10.03 中，不支持 LDAP_GROUP，并且在迁移后，将从用户列表文件中删除具有 LDAP_GROUP 的用户。

安装和升级改进

现在，您可以在本地将 UNIX 客户机升级到 Data Protector 10.03。不属于 Cell Manager 的客户机也可以分别使用发行包和补丁程序升级到最新发行版和补丁程序级别。使用新的 omnisetup.sh 命令选项，您可以：

- 将 Cell Manager、安装服务器或客户机升级到最新发行本或补丁包。
- 从发行版和补丁包中提取并安装特定的组件数据包
- 在 Cell Manager、安装服务器和客户机上安装 Data Protector 补丁包。
- 在安装服务器和客户机上安装 Data Protector 补丁 (仅升级客户机中安装的组件)。
- 从 Data Protector 安装包中提取数据包。这些包然后用于安装可安装在客户机主机上的组件。

更新 INET 端口

现在，您可以在安装过程中指定 INET 端口（仅UNIX）或在本地更新它。

- 在 UNIX 上安装 Data Protector 10.03 时，更新 INET 端口。现在，您可以在 omnisetup.sh 命令中将 INET 端口指定为选项。INET 端口的默认值为 5565。在安装或升级补丁包期间，无法更改 INET 端口值。
- 安装后在本地系统上更新 INET 端口号。使用新的 omnicc 命令选项 update_local_port 和 InetPort 来更改 INET 端口。即使客户机不是 Cell Manager 的一部分，也可以更改 INET 端口。

Amazon S3 支持

Data Protector 10.03 支持将 Amazon S3（与 API 兼容）作为新的“备份到磁盘”(B2D) 设备。Amazon S3 API 兼容对象类型包括 Amazon S3、Ceph 和 Scality 设备。您可以直接备份到这些云目标，也可以将对象复制到这些云目标。

NDMP 备份到 StoreOnce Catalyst

使用 Data Protector 10.03，您可以向/从 StoreOnce Catalyst 和文件库设备执行 NDMP 数据的 3 向备份和还原（仅限 NetApp）。

下一代 StoreOnce 集成

从 Data Protector 10.03 和下一代 StoreOnce Systems 起，将无法创建 Catalyst 存储。向客户支持咨询下一代 StoreOnce Systems 的上市日期。

数据不变性

Data Protector 10.03 现在具有数据不变性功能，组织可以使用它来保护 StoreOnce Catalyst 备份和备份副本，避免备份管理员使这些数据从备份应用程序中过期。在 StoreOnce Catalyst 设备上启用了数据不变性后，如果未达到定义的保留期限，则任何删除 Catalyst 项的尝试都将失败。

转变了信息体验

从 Data Protector 10.03 开始，该文档可在新的客户信息门户上找到，网址为 https://docs.microfocus.com/?DP。该门户网站由搜索引擎索引，您无需登录即可查看内容。您可以随时访问此门户以访问最新文档。您还可以为整个文档集或此门户中的选定部分生成 PDF 文件，以供离线使用。

Data Protector 10.02 中的新增功能

Data Protector 10.02 引入了以下新增功能。

调度程序增强功能

在 Data Protector 10.02 中，添加了以下调度程序增强功能：

- 分钟和小时: 现在，您可以按分钟或小时的频率模式递归计划作业。
- 调试：添加了新的调试选项，该选项允许为特定日程创建调试日志。

为确保调度程序在升级后正常工作，请确保在升级到 Data Protector 10.02 后立即清除 IE 缓存。

Recovery Manager Central (RMC) 支持

在 Data Protector 10.02 中，支持 Recovery Manager Central (RMC) 4.0 和 4.1。

支持 GRE 与 Microsoft Exchange 2016

在 Data Protector 10.02 中，现在支持 Microsoft Exchange 2016 与 Granular Recovery Extension (GRE)。

Data Protector 10.01 中的新增功能

Data Protector 10.01 引入了以下新增功能。

网络多宿主支持

在 Data Protector 中，多宿主环境指连接到多个网络的系统。如果客户机具有多个网络接口（主机名），则 Data Protector 将使用已导入到单元中的主机名传输数据。

NetApp 群集支持

支持驻留在群集环境中的 NetApp 存储。

调度程序改进

在 Data Protector 10.01 中，以下新功能添加到调度程序中：

- 每月视图：显示当前月份的日历视图，其中列出了每个日期的每日计划数。
- 过滤选项: 可用来根据规范类型过滤计划。
- 搜索：可用来在每日视图中运行自由文本搜索。
- 性能改进: 下表显示了每天 1300 个计划的计划呈现时间：

	Data Protector 10.00	Data Protector 10.01
每日视图	12 秒	0.5 秒
每月视图	21 秒	2.7 秒

MS SharePoint 2013 GRE 对 SQL 可用性组的支持

在 10.01 之前的 Data Protector 版本中，SharePoint 2013 Granular Recovery Extension (GRE) 不支持将 SQL 可用性组与可用性组侦听器结合使用。无法导入数据库操作，数据库还原操作失败。在 Data Protector 10.01 中，SharePoint 2013 Granular Recovery Extension (GRE) 支持 SQL 可用性组，在 SharePoint 场使用可用性组侦听器配置的情况下，它能够导入数据库并执行项目恢复。

自动删除失败对象

在 Data Protector 10.01 中，引入了每日维护任务，如果成功恢复了失败的会话，则该任务将删除失败的会话对象。因此，报告现在不会错误地显示失败对象的计数。还引入了新命令 `omnidbutil -delete_obsolete_resumed_versions` ，该命令使用户可以手动删除失败的对象。

Linux 和 AIX 操作系统上的直接 I/O 支持

Data Protector 磁盘代理引入了新的 omnirc 变量 `OB2ODIRECT_BACKUP` 、 `OB2ODIRECT_RESTORE` 和 `OB2ODIRECT_RESTORE_MINIMUM_SIZE` 来在 Linux 和 AIX 操作系统上启用直接 I/O。但是，如果基础文件系统不支持直接 I/O 操作，则将应用旧行为。

VMware 6.5 Update 1 和 VMFS 6 支持

Data Protector 10.01 提供对新备份代理、虚拟磁盘开发工具包 (VDDK) 6.5 Update 1 的支持，以及对 VMFS 6 的全面支持。

Oracle 12c SYSBACKUP 兼容性

当前，Data Protector Oracle 集成使用 SYSDBA 作为请求的用户特权来连接到数据库。在新的 Oracle 12c 版本中，提供了新的 SYSBACKUP 用户特权以及所有用于备份、还原和恢复功能的必需特权。通过此增强功能，SYSBACKUP 用户特权可以连接到 12c Oracle 版本的 Oracle 数据库。较早的 Oracle 版本将像以前一样继续具有 SYSDBA 用户特权。

SAP 存档备份会话成功

在 10.01 之前的版本中，如果不备份任何存档日志，则 SAP 存档日志备份状态将标记为“失败”。在 版本10.01 中，引入了新的全局选项 SessSuccessfulWhenSAPNoArchiveLogsBackedUp ，启用该选项后，即使备份了 0 个存档日志，该选项也将 SAP 备份会话标记为成功。

DD OS 6.1 和 DDboost 3.4 支持

Data Protector 现在与 Data Domain OS 6.1 和 DDBoost 3.4 库兼容。

Data Protector 10.00 中的新增功能

Data Protector 10.00 引入了以下新增功能。

Data Protector 中的安全性增强功能

Data Protector 10.00 提供以下安全增强功能：

安全通信

在 Data Protector 10.00 中，默认情况下，Cell Manager 和客户机之间的所有通信均受到保护。使用带证书锁定的自签名证书代替根 CA。

集中式命令执行

借助 Data Protector 10.00，当通过安全 TLS 1.2 通道发送时，Data Protector 客户机上的 Inet 进程只接受来自 Cell Manager 的连接。所有命令都通过 Cell Manager 路由。

新管理上下文（主页）

Data Protector GUI 中的新“主页”上下文为访问“仪表板”、“遥测”UI 和基于 Web 的“调度程序”提供了统一的方式。

新仪表板视图

仪表板清晰地显示了您的 Data Protector 环境收集的数据。使用仪表板，您可以快速查看已配置客户机的总数，Cell Manager 上保护的总数据、已安装许可证的数量以及所有存储设备的列表。“仪表板”视图中的不同图表提供了 Data Protector 环境的高层次图。

基于 Web 的新遥测 UI

遥测是一种用于获取客户洞察力的服务，旨在改善支持、产品最佳实践和客户管理。客户数据将传输到支持后端供进一步分析以增强顾客体验。Data Protector 10.00 引入了新的遥测 UI，允许您订阅/取消订阅遥测服务。

基于 Web 的新调度程序

借助 Data Protector 10.00，基本调度程序和高级调度程序已过时，被基于 Web 的新调度程序所替代。新的调度程序具有细化的用户界面、简单且易于使用的 Web 控件，便于轻松管理调度。您现在可以使用单个调度程序向导设置调度优先级、数据保护、重复模式和修复冲突。

新的 OVKEY4 许可证密钥

升级或全新安装 Data Protector 10.00 后，新的 OVKEY4 许可证必须从许可门户下载。

REST API

Data Protector 10.00 引入了公开 REST API 端点的安全方法，允许使用 REST 操作 Data Protector 的特定元素。通过这些 API，您可以将 Data Protector 工作流集成到您自己的解决方案中，如 Web 门户和部署工具。借助 Data Protector 10.00，将发布以下 API：

- 验证 API 适用于 Java“胖客户机”和 Web 浏览器，允许到 Cell Manager 的入站 REST API 查询。
- 浏览和还原 API，使合作伙伴和客户能够自动执行 Data Protector 还原操作。使用这些 API，您可以启用文件系统、SQL、SAP、Oracle、VEPA（VMware、Hyper-V）、IDB、磁盘映像和 NDMP 备份的自服务还原。
- 调度程序 API，使您能够在 Data Protector 中管理所有计划任务。

DDBoost 3.3.1.1 支持

Data Protector 现在与 DDBoost 3.3.1.1 库兼容。

快速入门

本节提供有关以下任务的信息：

Data Protector 简介

Data Protector 是备份解决方案，用于为快速增长的业务数据提供可靠的数据保护和高度可访问性。Data Protector 具有专门为整个企业和分布式环境特别定制的综合备份和还原功能。

Data Protector 的主要功能

- 可扩展和高度灵活的体系结构
- 支持混合环境
- 方便的集中管理
- 高性能备份
- 轻松还原
- 数据和控制通信安全性
- 支持高可用性
- 自动或无人看管操作
- 监视、报告和通知
- 服务管理
- 与联机数据库应用程序集成
- 与其他产品集成

Data Protector 组件

Data Protector 可用于从多个站点上的一个系统到数千个系统的各种环境。基本管理单元是 Data Protector 单元。

Data Protector 单元是由 Cell Manager 系统、一个或多个安装服务器、客户机系统和设备组成的网络环境。

Cell Manager 和 Installation Server 可位于相同的系统上（这是默认选项），或位于不同的系统上。

Cell Manager

Cell Manager 是从中心点控制 Data Protector 单元的主要系统，其中安装了 Data Protector 核心软件和 IDB。Cell Manager 运行多种 Session Manager，后者控制备份和还原会话，并将会话信息写入 IDB。IDB 跟踪备份文件以及 Data Protector 单元的配置。

安装服务器

Installation Server 是存储 Data Protector 软件存储库的计算机。对 UNIX 和 Windows 环境至少各需要一个 Installation Server，以便可以通过网络执行远程安装，以及将软件组件分发给单元中的客户机系统。

客户机系统

在 Cell Manager 系统上安装 Data Protector 软件之后，可以在单元中的每个系统上安装 Data Protector 组件。这些系统将成为 Data Protector 客户机。客户机的作用取决于已在此系统上安装的 Data Protector 软件。

- 要备份的系统

  要备份的客户机系统必须装有 Data Protector 磁带客户机（DA 也称为备份代理）。磁盘代理会从系统上的磁盘中读取数据或将数据写入磁盘，并将数据发送到介质代理或从介质代理接收数据。磁带客户机还安装在 Cell Manager 上，从而可以备份 Cell Manager 上的数据、Data Protector 配置和 IDB。

- 带备份设备的系统

  连接了备份设备的客户机系统必须装有 Data Protector 介质代理 (MA)。介质代理从设备中的介质读取数据或向其写入数据，并将数据发送到磁带客户机或从其接收数据。备份设备不仅可以与 Cell Manager 相连，还可以与任何系统相连。具有备份设备的客户机系统也称为驱动器服务器。具有多个备份设备的客户机系统称为多驱动器服务器。

报告服务器
报告服务器是 Data Protector 的组件，您可以使用它查看用于管理和计划备份环境的集成报告。报告服务器必须安装在非 Data Protector Cell Manager 的服务器上。

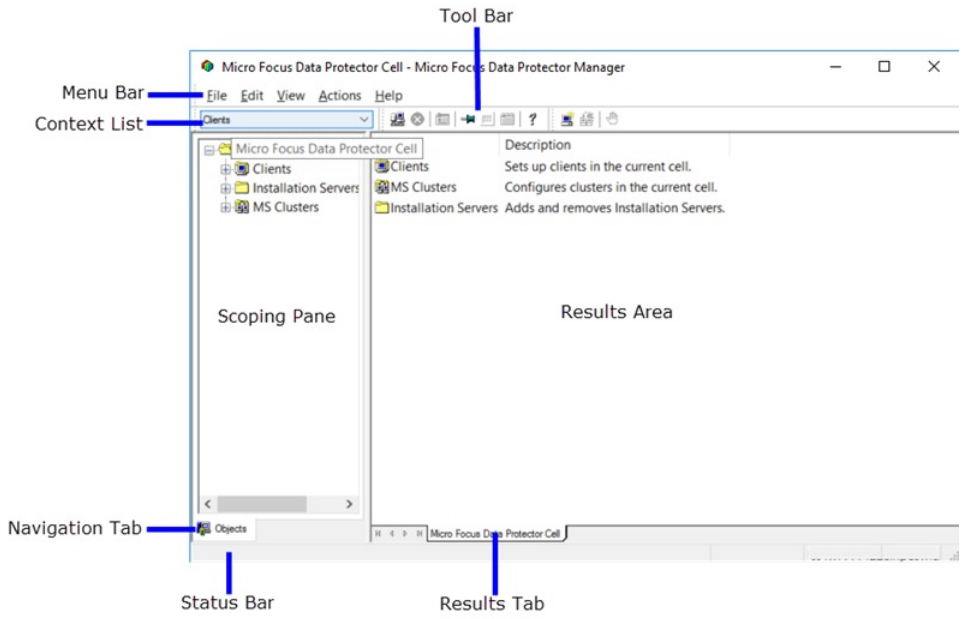
相关主题

- Data Protector GUI 的元素
- Data Protector 版本

Data Protector GUI 的元素

Data Protector GUI 的元素包括：

Data Protector 图形用户界面



上下文列表

上下文列表是一个下拉列表，用于在不同的管理上下文或视图之间进行移动。例如，从下拉列表中选择“用户”将更改菜单栏、工具栏、范围窗格和结果区域的内容，以反映用户管理器中可使用的功能。

根据用户权限，可访问全部上下文或仅访问其中的某些。

客户机

管理 Data Protector 单元中的客户机系统。例如，添加和删除客户机。

用户

管理用户、用户组及其权限。

设备和介质

配置和维护单元内的设备和介质。

备份

控制备份哪些数据和备份数据的方式。

对象操作

控制复制、合并或验证哪些备份对象以及操作方法。

监控

监视正在进行中的会话。

还原

控制还原什么数据以及还原方法。

内部数据库

管理 IDB。

即时恢复

控制如何在以下设备上执行即时恢复：

- P4000 SAN 解决方案
- P9000 XP 磁盘阵列系列
- 3PAR StoreServ Storage

使用此功能需要持有一种特殊的许可证。

范围窗格

范围窗格列出了可供选择的若干视图。它类似于浏览目录树；在范围窗格中选择某个项目时，结果区域中将显示有关所选项目的信息。底部的两个选项卡（对象和任务）提供了其他视图。根据所选的上下文，只能出现一种视图。

对象

默认视图。此视图以层次结构的形式表示数据，类似于 Microsoft 资源管理器中的目录树。例如，在“设备和介质”上下文中，“范围窗格”将显示使用 Data Protector 配置的设备和介质列表。

任务

其中列出可执行的任务。单击任务将显示一个向导，引导您完成整个任务（如备份文件）。

结果区域

结果区域显示与范围窗格中所选项目相对应的信息。例如，如果在上下文列表中选择了“客户机”，并在范围窗格中单击“客户机”项目，则结果区域中将显示单元内所有客户机的列表。

结果选项卡

结果选项卡上的名称对应于范围窗格中当前所选项目的名称。单击工具栏上的大头针图标，使此视图“固定”，从而使其可供将来使用。如果需要使用 GUI 查找其他信息，但希望以后继续使用上一个视图，则可通过选择“固定的”选项卡访问该视图。通过右键单击选项卡所在区域并选择删除选项卡或删除其他选项卡，可删除这些选项卡。

状态栏

状态栏显示 Cell Manager 名称、有关当前操作的信息以及 GUI、Cell Manager 和 IDB 之间通信的进度。

Data Protector 版本

从 DP 10.10 (2018.09) 版本开始，Data Protector 提供以下两个版本:

- **Data Protector Express:** 此版本是以基于套接字的许可 模型为基础的虚拟专用产品。
- **Data Protector Premium:** 此版本使用基于容量的许可 模型。

有关传统的基于功能的 许可模型和其他许可的详细信息，请参阅许可。

注意:

- 对于 **Express** 版本，您只能使用 Data Protector GUI 为其他套接字添加许可证。您可以在导入支持的服务器期间或之后应用许可证。您不能使用命令行界面执行许可证管理任务，例如添加或删除套接字。许可详细信息显示有关已耗用套接字和可用套接字的信息。
- 不支持具有基于套接字的许可和基于容量的许可 的混合模式环境。如果您安装 **Data Protector Express** 和 **Data Protector Premium** 许可证，Data Protector 仅使用 **Premium** 许可证。
- 如果您使用的是传统的基于功能的许可模型，您可以继续使用相同的许可模型，或通过更改许可证密钥将许可升级到 **Premium**。
- 通过更改许可证密钥，可以将许可证轻松从 **Data Protector Express** 升级到 **Data Protector Premium**。

下表比较了 **Express** 版和 **Premium** 版的 DP 功能支持:

功能	Express 版	Premium 版	备注
虚拟化环境支持	✓	✓	• 支持虚拟化环境，例如 **VMware**、 **Hyper-V** 和 **H3C CAS**。 • 支持高级虚拟化功能，例如: ◦ Granular Recovery Extension (GRE) ◦ 启动 ◦ 实时迁移 ◦ 零宕机时间备份 (ZDB) 集成。 注意: **Express** 版仅支持适用于 VMware 的 ZDB。
Data Protector 全功能支持	X	✓	**Express** 版仅支持虚拟化环境。 除了虚拟化环境支持，**Premium** 版还支持源的备份和还原，例如: • 数据库 • 集成 • 除 Cell Manager 之外的主机上的文件系统数据 • 网络数据管理协议 (NDMP)。
Cell Manager 文件系统备份	✓	✓	
客户机文件系统备份	X	✓	
vProtect 备份支持	X	✓	
软件加密 (高级加密标准 256 位加密)	✓	✓	
Data Protector 内部数据库 (IDB) 的备份和恢复	✓	✓	
应用程序集成的备份和恢复	X	✓	
从以前的 DP 版本升级	✓	✓	从 Data Protector 8.1*x*、9.*x* 和 10.0*x* 版本升级到 Data Protector 10.20 及更高版本。
支持具有多个 Cell Manager 的 MoM 环境	X	✓	

视频库

要了解有关 Data Protector 的更多信息，请观看以下视频:

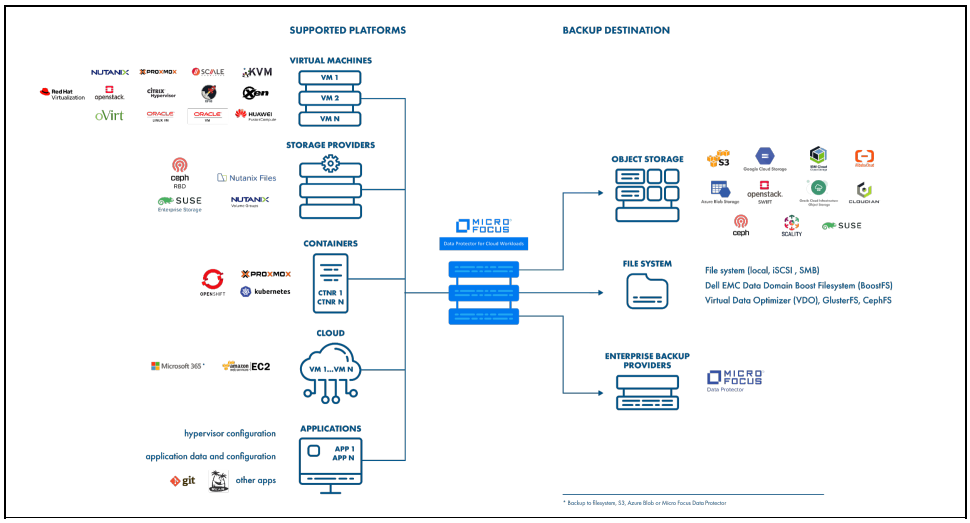
Data Protector 简介
使用 Micro Focus 数据保护套件保护 SAP HANA 环境: 概述和演示
使用 Micro Focus 数据保护套件备份到云端: 概述和演示
Micro Focus 数据保护套件新的 GUI 和调度程序: 概述和演示
对 NetApp 存储阵列的 Micro Focus 数据保护套件三向 NDMP 备份: 概述和演示
适用于 HPE StoreOnce Cloud Bank Storage 的 Micro Focus 数据保护套件支持: 概述和演示

适用于云工作负载的 Data Protector 简介

在 Data Protector 11.01 中，Micro Focus 引入了适用于云工作负载的 Data Protector (DP4CW)，以增强或扩展对以下范围的备份和还原支持:

- 云数据存储库，例如 Microsoft 365 (Exchange、SharePoint、Teams、OneDrive)
- 虚拟化环境，例如 Citrix XenServer、KVM、Nutanix
- 其他数据平台，例如 OpenShift、OpenStack

适用于云工作负载的 Data Protector 是一个稳定的无代理备份和快照管理解决方案套件，适用于虚拟环境和云。
它使您能够可靠地提高和自动化备份性能，自动化恢复测试，显著节省资源、时间和资金。
Data Protector 和适用于云工作负载的 Data Protector 现在一起提供混合企业备份和恢复任务的全面覆盖。有关设置 DP4CW 的信息，请参阅设置适用于云工作负载的 Data Protector。



关键概念

本节介绍 Data Protector 的概念。请阅读本节内容以充分了解 Data Protector 的基础知识和模型。

目标读者

本节的目标读者是有兴趣了解 Data Protector 操作的概念的用户，以及计划公司备份策略的人员。

关于备份和 Data Protector

本主题概述备份和还原的概念，并介绍 Data Protector 架构、介质管理、用户界面、备份设备和其他功能。本主题概述 Data Protector 配置以及设置 Data Protector 所需执行的其他任务。

关于 Data Protector

Data Protector 是一款为快速增长的业务数据提供可靠的数据保护和高度可访问性的备份解决方案。Data Protector 具有专门为整个企业和分布式环境特别定制的综合备份和还原功能。以下列出的几点是对 Data Protector 主要特点的描述:

- **可扩展和高度灵活的体系结构**

  Data Protector 可用于从多个站点上的一个系统到数千个系统的各种环境。由于 Data Protector 的网络组件概念，备份基础架构的元素可以根据用户需求置于拓扑中。借助若干用于设置备份基础结构的备份选项和备用选项，可以实施您所需的几乎所有配置。Data Protector 还能够使用合成备份和磁盘分段等高级备份概念。

- **方便的集中管理**

  Data Protector 通过易于使用的图形用户界面 (GUI) 使用户能够从单个系统管理整个备份环境。为了方便操作，GUI 可安装在多种系统上，这样多个管理员就可以通过各自本地安装的控制台访问 Data Protector。甚至可以从一个系统管理多个备份环境。Data Protector 命令行界面 (CLI) 支持您使用脚本管理 Data Protector。

- **高性能备份**

  Data Protector 支持您同时将数据备份到数百个备份设备。它以大型库支持高端设备。备份功能多样，如本地备份、网络备份、联机备份、磁盘映像备份、合成备份和对象镜像备份；通过并行数据流内置支持功能可以使备份完全满足用户需求。

- **数据安全性**

  为增强数据安全性，Data Protector 允许用户对备份进行加密，以阻止其他人访问数据。Data Protector 提供两种数据加密技术：基于软件的技术和基于驱动器的技术。

  安全通信

  在 Data Protector 中，默认情况下，Cell Manager 和客户机之间的所有通信均受到保护。使用带证书锁定的自签名证书代替根 CA 概念。新安全模型的主要特点包括：

  - 不同 Data Protector 实体之间的所有通信均通过安全的 TLS 1.2 通道。
  - 在 Windows 客户机上推送安装 Data Protector 代理时，现在使用会话消息块 (SMB) 签名。签名的 SMB 流量提供数据完整性，因为在安装期间向客户机提供的是安全数据，而且攻击者无法更改数据。
  - 在 Linux/Unix 客户机上推送安装 Data Protector 代理时，现在使用 SSH 协议。如果安装服务器和客户机之间未预先配置 SSH 密钥，则会根据客户机提示密码。
  - Data Protector 客户机和 Cell Manager 现在使用安全对等方式进行配置，并且在客户机（在本地安装时）上运行命令，以使用 Cell Manager 进行身份验证。

  集中式命令执行

  Data Protector 采用客户机/服务器模型来执行备份、还原和恢复操作。为了支持这些操作，一个主机上的 Data Protector 代理通过 INET 连接，并与相同或不同主机上的 Data Protector 代理进行通信。在某些情况下，一个主机上的代理与另一个主机上的 INET 进行通信来执行命令，从而对被入侵的客户机导致的漏洞执行远程命令。

  当通过安全 TLS 1.2 通道发送时，Data Protector 客户机上的 Inet 进程只接受来自 Cell Manager 的连接。所有命令都通过 Cell Manager 路由。集中化命令执行可确保控制和数据都通过安全的 TLS 通道发送，从而保证数据完整性。此外，Data Protector 客户机现在只侦听并接受来自受信任且经验证的 Cell Manager 的指令和脚本，这样可显著降低安全漏洞的风险。

- **支持混合环境**

  Data Protector 支持异构环境，大多数功能对 UNIX 和 Windows 平台都通用。UNIX 和 Windows Cell Manager 可以控制所有支持的客户机平台。从 Data Protector 用户界面可以访问所有受支持平台上的全部 Data Protector 功能。有关支持的平台的列表，请参见最新支持矩阵。

- **在混合环境中轻松实现安装**

  安装服务器概念简化了安装和升级过程。要远程安装 UNIX 客户机，需要适用于 UNIX 的安装服务器。要远程安装 Windows 客户机，需要适用于 Windows 的安装服务器。远程安装可以从安装了 Data Protector GUI 的任何客户机执行。有关安装服务器所支持的平台，请参阅最新支持矩阵。

- **高可用性支持**

  Data Protector 能够满足客户对昼夜不停地持续业务操作的需求。在当今的全球分布式业务环境下，公司范围的信息资源和客户服务应用程序必须始终可用。Data Protector 可以通过以下方式满足高可用性需求：

  - 与群集集成，确保防故障操作以及能够备份虚拟节点。有关支持的群集的列表，请参见最新支持矩阵。
  - 使 Data Protector Cell Manager 本身能够在群集上运行。
  - 支持所有常用的联机数据库应用程序编程接口。
  - 与 NetApp 存储或 Dell-EMC 存储等高级高可用性解决方案集成。
  - 提供适用于 Windows 和 UNIX 平台的多种灾难恢复方法。
  - 提供备份期间或备份之后复制备份数据的方法，以提高备份容错能力或用于冗余目的。

- **备份对象操作**

为了灵活选择备份和存档策略，提供了可对单个备份对象执行操作的高级技术。这些技术包括将对象从一个介质复制到另一个介质（对磁盘分段和存档很有用）、将来自增量备份的多个对象版本合并为一个完整备份版本。为了支持这样的功能，还需要能够验证原始的和复制的或合并的备份对象。

- **轻松还原**

  Data Protector 包含一个可持续跟踪数据的内部数据库，例如某个特定介质上保留了哪个系统的哪些文件。用户只需浏览文件和目录即可还原系统中任何部分的数据。这加快并方便了对要还原数据的访问。

- **自动或无人看管操作**

  Data Protector 借助内部数据库保存有关每个 Data Protector 介质的信息以及介质上的数据。Data Protector 具有先进的介质管理功能。例如，它可持续跟踪特定备份需要为还原保留多久，以及哪些介质可以用于或重新用于备份。

  大型库支持可弥补其中不足，使数天甚至数周的无人看管操作（自动介质循环）得以实现。此外，当新磁盘连接到系统时，Data Protector 能够自动检测到（或发现）磁盘并进行备份。这样就不必手动调整备份配置。

- **监控、报告和通知**

  通过各种通知功能，您可以轻松查看备份状态、监视活动的备份操作和自定义报告。报告可通过 Data Protector GUI 或 CLI 生成。

  新的调度程序具有细化的用户界面、简单且易于使用的 Web 控件，便于轻松管理调度。您现在可以使用单个调度程序向导设置数据保护、重复模式和修复冲突。

  此外，Data Protector 审计功能还支持您收集备份会话信息的子集并提供备份操作的概述。

  有关配置详细信息，请参阅“管理”。

- **与联机应用程序集成**

  Data Protector 提供对 Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint Server、Oracle、Informix Server、SAP R/3、SAP MaxDB、Lotus Notes/Domino Server、IBM DB2 UDB、Sybase 数据库对象、SAP HANA、VMware vSphere 和 Hyper-V 对象的联机备份。

- **与其他产品集成**

  此外，Data Protector 还可与 Dell EMC Unity、Microsoft Cluster Server、Serviceguard 和其他产品集成。

有关说明 Data Protector 功能的详细文档，包括集成信息以及最新的平台和集成支持信息，请查询最新支持矩阵。

介绍备份和还原

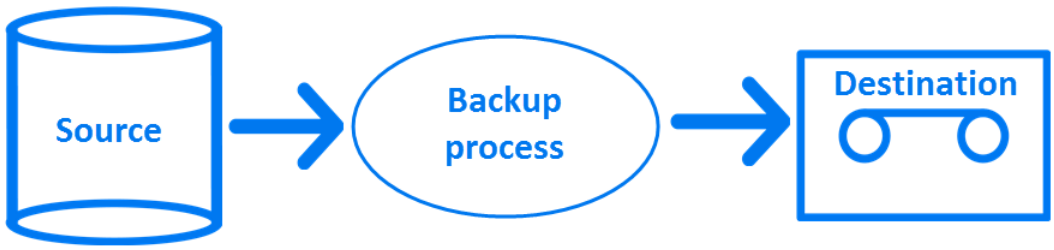
本节将介绍备份和还原的基本概念。

什么是备份？

备份是在备份介质上创建数据副本的过程。该副本的存储和保留是供将来万一发生原始数据损坏时使用。

备份过程中显示了备份的高级表示。

备份过程



在大多数情况下，**源**是指磁盘上的数据，如文件、目录、数据库和应用程序。如果备份的目的是为了用于灾难恢复，则备份需要保持一致。

备份应用程序是实际将数据复制到目标的软件。**目标**是指通过介质将数据副本写入其中的备份设备，如磁带驱动器或磁盘设备。

什么是还原？

还原是从备份副本重新创建原始数据的过程。该过程由数据准备及实际还原和一些还原后的操作组成，执行还原后操作是为了使还原的数据可用。

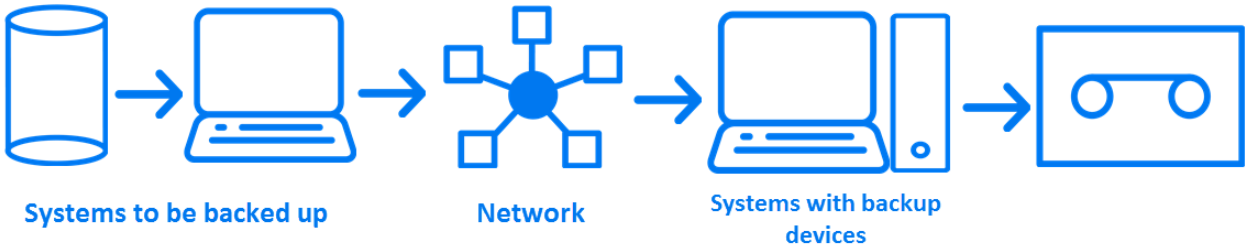
还原过程

源是指备份复本。还原应用程序是实际将数据写入目标的软件。**目标**通常是指将原始数据写入其中的磁盘。

备份网络环境

备份网络环境期间，数据会从要备份的系统通过网络传送到带有备份设备的系统介质上，数据便存储在那里。

网络备份



要实现网络环境备份，需要应用程序具备以下功能：

- 将备份设备连接到网络中的任何系统

  这样就可以对数据量庞大的系统进行本地备份和网络备份，以降低备份设备成本。
- 将备份数据流路由到任何网络路径
- 在数据量或网络流量使 LAN 传输效率低下时，将备份数据从 LAN 路由到 SAN
- 从任何系统管理备份活动
- 集成到 IT 管理框架
- 支持要备份的各种类型的系统

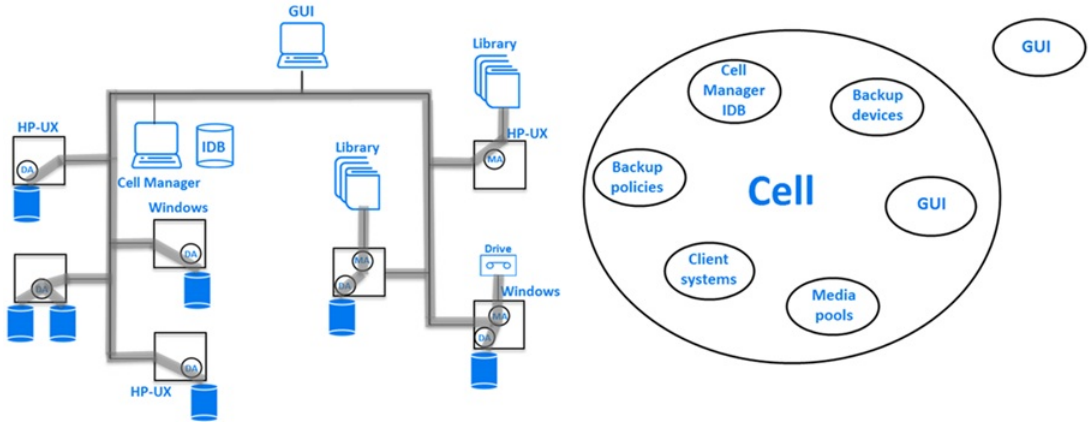
Data Protector 体系结构

Data Protector 单元 (物理视图和逻辑视图) 中所示的 Data Protector 单元是一种包含 “Cell Manager”、“客户机系统”和“设备”的网络环境。Cell Manager 是安装有 Data Protector 软件的中央控制点。安装 Data Protector 软件后，可以添加要备份的系统。这些系统将成为属于单元一部分的 Data Protector 客户机系统。Data Protector 在备份文件时，会将文件保存到备份设备中的介质上。

“Data Protector 内部数据库 (IDB)”会持续跟踪备份文件，以便您可以浏览和轻松恢复整个系统或单个文件。

Data Protector 使备份和还原作业变得简单。您可以使用 Data Protector 用户界面进行即时（或交互）备份。也可以安排备份在无人看管的情况下运行。

Data Protector 单元（物理视图和逻辑视图）



注意Data Protector Cell Manager 和 Data Protector 图形用户界面系统不需要运行相同的操作系统。有关特定 Data Protector 组件所支持操作系统的列表，请参阅支持矩阵。

Cell Manager

Cell Manager 是单元中的主系统。Cell Manager:

- 从中央点管理单元
- 包含 IDB

  IDB 包含备份详细信息（如备份持续时间、介质 ID 和会话 ID）
- 运行核心 Data Protector 软件
- 运行可启动和停止备份及还原会话并将会话信息写入 IDB 的会话管理器

要备份的系统

要备份的客户机系统必须装有 Data Protector 磁盘代理 (DA) (也称为“备份代理”)。要备份联机数据库集成，请安装**应用程序代理**。在本文档以下部分中，“磁盘代理”一词指上述两种代理。磁盘代理会从系统上的磁盘中读取数据或将数据写入磁盘，并将数据发送到介质代理或从介质代理接收数据。

虽然 Cell Manager 安装本身可提供内部数据库和相关配置数据的备份和还原方法，要能够备份和还原位于 Cell Manager 上的非 Data Protector 数据，还必须安装磁盘代理。

带备份设备的系统

连接有备份设备的客户机系统必须安装了 Data Protector“驱动器服务器”。备份设备不仅可以与 Cell Manager 相连，还可以与任何系统相连。介质代理会从设备的介质中读取数据或将数据写入介质，并将数据发送到磁盘代理或从磁盘代理接收数据。

带用户界面的系统

您可以从安装了 Data Protector 图形用户界面 (GUI) 的任何系统通过网络管理 Data Protector。因此，您可以在从桌面系统管理 Data Protector 的同时在机房中使用 Cell Manager 系统。

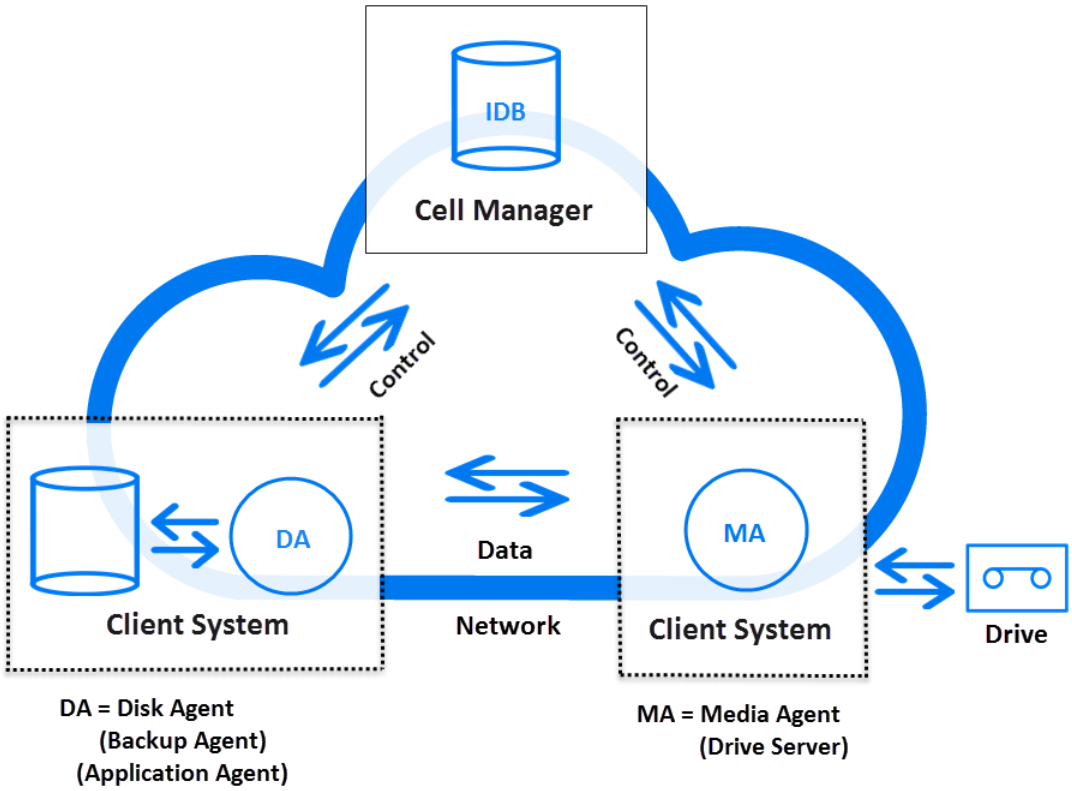
安装服务器

“安装服务器”是特定体系结构下的 Data Protector 安装包存储库。Cell Manager 默认情况下也是安装服务器。混合环境至少需要两台安装服务器: 一台用于 UNIX 系统，一台用于 Windows 系统。

单元中的操作

Data Protector Cell Manager 可控制分别执行备份或还原所有必需操作的备份和还原会话，如备份或还原操作所示。

备份或还原操作



备份会话

什么是备份会话？

备份会话是在存储介质上创建数据副本的过程，如备份会话所示。它可以使用 Data Protector 用户界面由操作员交互启动，也可以使用 Data Protector 调度程序以无人看管的方式启动。

如何工作？

Backup Session Manager 进程将启动介质代理和磁盘代理、控制会话，并将生成的消息存储到 IDB 中。磁盘代理会读取数据并将数据发送到介质代理，由介质代理将数据保存到介质。

备份会话

典型的备份会话比备份会话中显示的会话更为复杂。许多磁盘代理会从多个磁盘并行读取数据，然后将数据发送到一个或多个介质代理。有关复杂备份会话的详细信息，请参阅如何操作 Data Protector。

还原会话

什么是还原会话？

还原会话是将数据从之前的备份中还原到磁盘的过程，如还原会话所示。还原会话可以由操作员通过 Data Protector 用户界面交互启动。

如何工作？

从之前的备份中选择要还原的文件后，即会调用实际的还原进程。Restore Session Manager 进程将启动所需的介质代理和磁盘代理、控制会话，并将消息存储到 IDB 中。介质代理会读取数据并将数据发送到磁盘代理，由磁盘代理将数据写入磁盘。

还原会话

还原会话比还原会话中显示的会话更为复杂。有关还原会话的详细信息，请参阅如何操作 Data Protector。

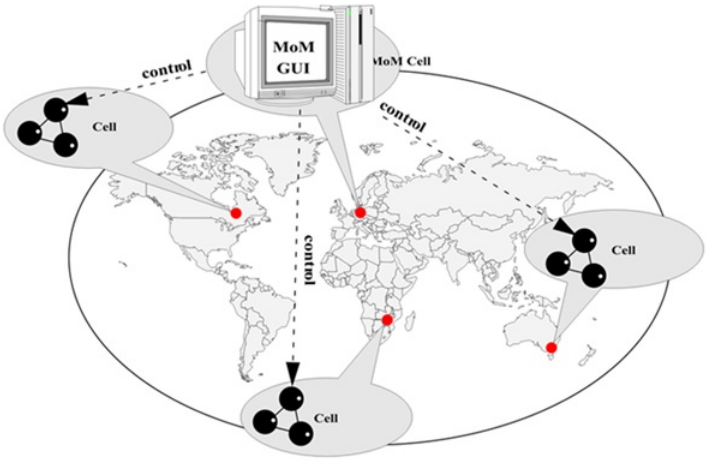
企业环境

典型的企业网络环境由来自不同供应商、安装了不同操作系统的许多个系统组成，如大型 Data Protector 企业环境所示。这些系统可能位于不同的地理区域和时区。所有系统都接入 LAN 或 WAN 网络，以各种通信速度运转。

何时使用企业环境

如果多个在地理位置上分散的站点需要使用通用“备份策略”，则可以使用此解决方案。也可以在同一站点的所有部门想要共享相同的备份设备集时使用。

大型 Data Protector 企业环境



配置和管理此类异构环境的备份是一个挑战。Data Protector 功能旨在高度简化此任务。有关 Manager of Managers (MoM) 的信息，请参阅 "MoM"。

将环境拆分成多个单元

您可能出于多种原因决定将大环境拆分成多个单元：

为何要将大环境拆分成多个单元？

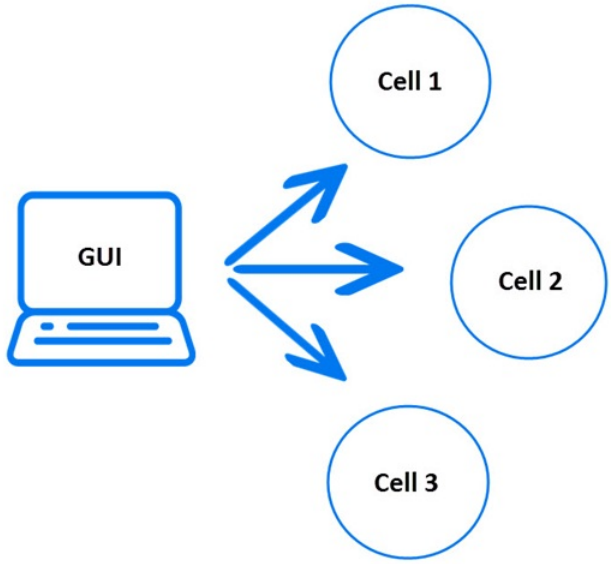
- 按地域对系统进行分组。
- 对系统进行逻辑分组，例如，按部门。
- 某些系统间的连接速度较慢。
- 出于性能考虑。

- 使管理控制分开。

有关规划环境的注意事项列表，请参阅计划备份策略。

Data Protector 允许您从单点管理多个单元。

多个单元的单点管理

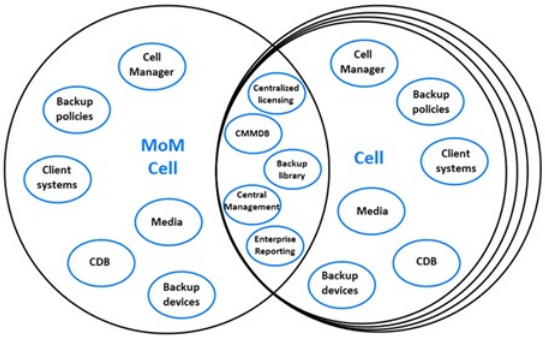


MoM

Data Protector 可提供 Manager-of-Managers，用于管理包含多个单元的大型环境。使用 MoM 可以将多个单元归为一个可从单点管理的大单元 (称为 MoM 环境)，如多个单元的单点管理所示。MoM 允许备份环境虚拟地无限增长。可以添加新单元或拆分现有单元。

MoM 环境不要求 Data Protector 单元与 MoM 中央单元之间有可靠的网络连接，因为备份是在每个 Data Protector 单元内本地执行的，只有控制信息才通过远距离连接进行发送。然而，这是基于每个单元都有自己的 Media Management Database 的假设。

Manager-of-Managers 环境



Manager-of-Managers 提供以下功能：

- **集中式许可存储库**

  这简化了许可证管理。这是可选的，但对大环境非常有用。

- **Centralized Media Management Database (CMMDB)**

  通过 CMMDB，可以在 MoM 环境中的若干单元之间共享设备和介质。这样，一个单元（使用 CMMDB）的设备就可供其他使用 CMMDB 的单元访问。CMMDB（如果使用）必须驻留在 Manager of Managers 上。在这种情况下，MoM 单元和其他 Data Protector 单元之间需要有可靠的网络连接。请注意，集中 Media Management Database 是可选的。

- **共享带库**

  通过 CMMDB，可以在多单元环境中的若干单元之间共享高端设备。其中一个单元可以控制机械手，为连接到其他单元中的系统的多个设备

提供服务。甚至磁带客户机到介质代理的数据路径也可以跨单元边界。

- **企业报告**

  Data Protector Manager-of-Managers 可以生成基于单个单元的报告，也可以生成基于整个企业环境的报告。

介质管理

Data Protector 可提供强大的介质管理功能，使您能够按以下方式轻松、有效地管理环境中的大量介质：

介质管理功能

- 将介质分为若干个逻辑组，即**介质池**，这样您就可以考虑较大的介质集，而不必担心各个单独的介质。
- Data Protector会持续跟踪所有介质及每个介质的状态、数据保护到期时间、介质的备份可用性以及已备份到每个介质中的数据的编目。
- 完全自动操作。如果 Data Protector 控制着带库设备中的足够介质，则可以使用介质管理功能在无操作员干预的情况下运行备份会话。
- 自动的介质循环策略，它允许自动执行备份介质选择。
- 对支持条形码的大型带库设备和 silo 设备提供条形码识别及支持功能。
- 识别、跟踪、查看和处理 Data Protector 用于大型带库设备和 silo 设备中的介质。
- 将介质信息集中于某个中央位置，并在 Data Protector 单元间共享。
- 在介质上交互或自动创建其他数据副本。
- 支持介质保管。

什么是介质池？

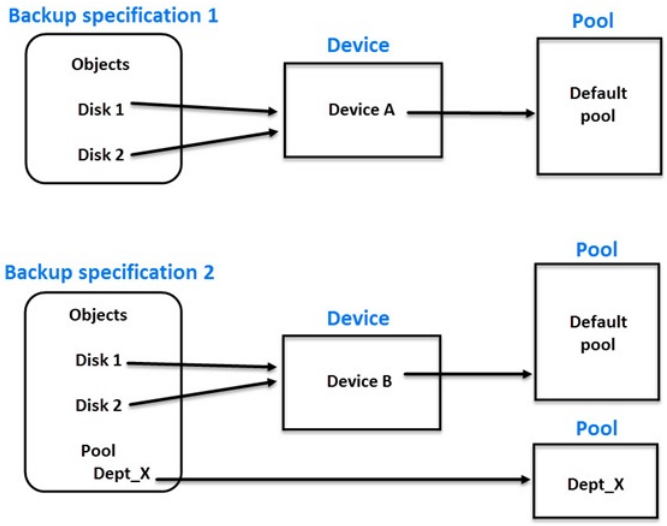
Data Protector使用介质池管理大量介质。介质池是物理类型**相同**、具有公用使用策略（属性）的介质的逻辑集合。其用途取决于介质上的数据。介质池的结构和数量以及哪个池在介质上包含哪类数据，则完全取决于用户偏好。

配置设备时，会指定默认介质池。该介质池在备份规范中未定义任何其他介质池时使用。

备份设备

Data Protector 将每个设备定义并构建为具有其各自使用属性（如默认池）的物理设备。使用这一设备概念是因为这样能够轻松、灵活地配置设备，并且能够结合备份规范使用这些设备。设备的定义存储在 Data Protector 介质管理数据库中。

备份规范、设备和介质池之间的关系



备份规范、设备和介质池之间的关系显示了备份规范、设备和介质池之间的关系。在备份规范中会引用设备。每个设备又与介质池相链接，介质池可以在备份规范中进行更改。例如，备份规范 2 引用了 Dept_X 介质池，而不是默认介质池。

Data Protector 支持各种设备。有关更多信息，请参阅最新支持矩阵。

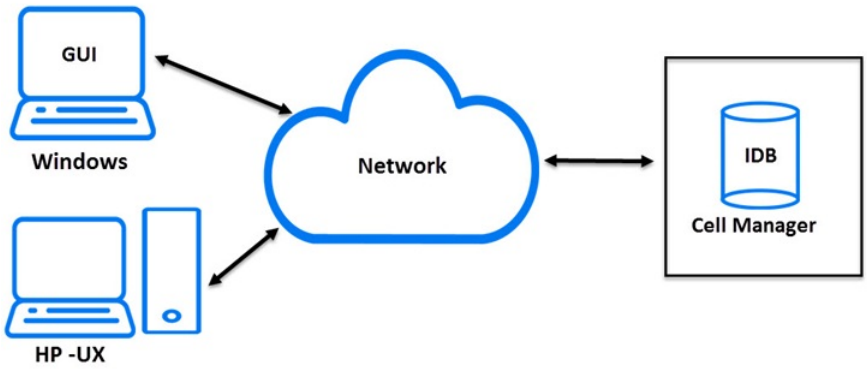
用户界面

用户可通过 Data Protector 使用 Windows 平台上的 Data Protector GUI 轻松访问所有配置和管理任务。此外，在 Windows 和 UNIX 平台上还可以使用命令行界面 (CLI)。

通过 Data Protector 体系结构可以灵活安装和使用 Data Protector 用户界面。不必从 Cell Manager 系统中使用用户界面，可以将其安装在桌

面系统上。如使用 Data Protector 用户界面所示，用户界面还允许用户在所有支持的平台上使用 Cell Manager 对 Data Protector 单元进行透明管理。

使用 Data Protector 用户界面



提示在典型的混合环境中，将 Data Protector 用户界面安装在环境中的多个系统上，这样就可以从多个系统访问 Data Protector。

Data Protector GUI

Data Protector GUI 是一个简单好用且功能强大的界面，可提供以下功能:

- 提供包含所有配置向导、属性和列表的结果选项卡。
- 易于配置和管理在 Windows 环境（如 Microsoft SQL Server、Microsoft Exchange Server、SAP R/3 和 Oracle Server）和 UNIX 环境（如 SAP R/3、Oracle Server 和 Informix Server）下运行的联机数据库应用程序的备份。
- 包含帮助主题和上下文相关帮助的综合帮助系统。

要设置的任务的概述

本节将概述设置 Data Protector 备份环境的全局任务。根据环境的大小和复杂程度，可能不必完成以下所有步骤。

1. 分析网络和组织结构。确定需要备份的系统。
2. 检查是否有任何特殊的应用程序和数据库要备份，如 Microsoft Exchange、Oracle、IBM DB2 UDB、SAP R/3 等等。Data Protector 提供与这些产品的特定集成功能。有关详细信息，请参阅对应的“集成”。
3. 确定 Data Protector 单元的配置，如：
   - 要作为 Cell Manager 的系统
   - 安装用户界面的系统
   - 本地备份和网络备份
   - 控制备份设备和库的系统
   - 连接类型，LAN 和/或 SAN
4. 根据设置购买所需的 Data Protector 许可证。

   这样即可获得安装所需的密码。

   或者，您也可以使用即开即用密码运行 Data Protector。但是，这种密码仅在安装之日起 60 天内有效。有关详细信息，请参阅“Data Protector 安装”部分。
5. 考虑安全方面：
   - 分析安全注意事项。请参阅“安装”。
   - 考虑需要配置的用户组。
   - 通过将数据以加密格式写入介质增强安全性。
6. 确定如何构建备份：
   - 需要有哪些介质池以及作何用途？
   - 将使用哪些设备，以及如何使用？

- 每个备份需要多少个副本？
- 需要多少种备份规范，如何分组？
- 如果计划备份到磁盘，请考虑高级备份策略，如合成备份和磁盘分段。

7. 安装和配置 Data Protector 环境。
   - 安装 Data Protector Cell Manager 系统，并使用 Data Protector 用户界面为其他系统分配 Data Protector 组件。
   - 连接设备（磁盘驱动器）和用于控制设备的系统。
   - 配置备份设备。
   - 配置介质池并准备介质。
   - 配置备份规范，包括 IDB 备份。
   - 配置报告（如果需要）。
8. 熟悉以下任务：
   - 处理失败的备份
   - 执行还原
   - 复制已备份数据和保管介质
   - 准备灾难恢复
   - 维护 IDB

关于报告服务器

报告服务器是 Data Protector (DP) 的组件，您可以使用它查看用于计划和管理备份环境的高级集成报告。可从 DP UI 的主页上下文 (“主页”上下文 **>**“报告”) 获取集成报告。
报告服务器可帮助 DP 管理员和操作员高效地管理日常任务。虽然在 DP GUI 的“报告”上下文中将基于文本的基本报告作为传统报告提供，但是报告服务器允许更广泛和智能地显示资源信息。它可以帮助您在环境中的问题变得严重之前找出这些问题。报告服务器还可以通过提供历史信息和预测信息来帮助微调备份过程。因此，报告服务器的集成报告不仅提供基本报告，还可以作为有效的工具进行分析和优化。

MoM 环境中的报告服务器

报告服务器支持 Manager of Manager (MoM) 配置。您可以配置一个具有多个 Cell Manager 的报告服务器。您可以在相应的 Cell Manager 上查看单个报告，也可以在 MoM Cell Manager 上查看合并报告。

许可

您可以将报告服务器与传统许可的 DP 安装以及 Data Protector 的 Express 和 Premium 版本一起使用。如果更改许可证，请取消注册报告服务器软件，然后重新注册，以使新许可证生效。
有关更多信息，请参阅报告服务器许可证。

安装

要查看报告服务器提供的集成报告，您必须在专用 Windows 或 Linux 计算机上安装报告服务器，然后将其导入 Cell Manager。有关更多信息，请参阅安装报告服务器。

相关主题

有关设置报告服务器以查看和生成集成报告的信息，请参阅设置集成报告。
有关生成集成报告的信息，请参阅使用报告服务器。
有关与报告服务器相关的故障诊断信息，请参阅对报告服务器进行故障排除。

Data Protector 的运行方式

本节介绍 Data Protector 的操作，并解释 Data Protector 进程 (在 UNIX 上) 和服务 (在 Windows 上)、备份和还原会话以及介质管理会话。

Data Protector 进程或服务

Data Protector 运行多个后台进程 (在 UNIX 上) 和服务 (在 Windows 上)，使其能够运行备份和还原会话。它提供必需的通信路径、激活备份和还原会话、启动磁盘代理和介质代理、存储有关已备份内容的信息、管理介质，以及执行类似功能。

进程或服务

进程（服务）	描述
CRS	单元请求服务器 (CRS) 进程 (服务) 在 Data Protector Cell Manager 上运行。它将启动和控制备份与还原会话。该服务会在 Data Protector 安装到 Cell Manager 系统上时立即启动，并在每次重新启动系统时重新启动。
MMD	介质管理后台程序 (MMD) 进程 (服务) 在 Data Protector Cell Manager 上运行，负责控制介质管理和设备操作。该进程由 Cell Request Server 进程（服务）启动。
Inet	Data Protector Inet 服务在 Data Protector 单元中的每个 Windows 系统上运行。Inet 负责单元中的系统之间的通信，并负责启动备份和还原所需的其他进程。Data Protector Inet 服务会在 Data Protector 安装到系统上时立即启动。在 UNIX 系统上，系统 inet 后台程序 (INETD) 将启动 Data Protector Inet 进程。
KMS	密钥管理服务器 (KMS) 进程 (服务) 在 Cell Manager 上运行，负责为 Data Protector 加密功能提供密钥管理。Cell Manager 上安装 Data Protector 后启动该进程。
hpdp-idb	Data Protector 内部数据库服务 (hpdp-idb) 是用于运行 IDB 的服务。此服务可供需要内部数据库中的信息的进程在 Cell Manager 上以本机方式进行访问。仅在将有关传输的介质管理信息从 Cell Manager 上的 IDB 传输到 Manager-of-Manager (MoM) 上的 IDB 上时，才能远程访问此服务。
hpdp-idb-cp	Data Protector 内部数据库连接池程序 (hpdp-idb-cp) 服务提供了一系列到 hpdb-idb 的开放连接，可以根据需要使用这些连接，而无需为每个请求打开一个新连接，从而确保 hpdp-idb 连接的可扩展性。服务在 Cell Manager 上运行，仅可供本地进程访问。
hpdp-as	Data Protector 应用程序服务器 (hpdp-as) 服务用于通过 HTTPS 连接 (Web 服务) 将 GUI 连接到 IDB。在 Cell Manager 上运行，具有到 hpdp-idb-cp 服务的本地连接。

备份会话

本节将介绍如何启动备份会话，备份会话期间会执行哪些操作，以及涉及的进程和服务。

当备份规范启动时，该备份规范就称为备份会话。备份会话会将源数据（通常来自硬盘）复制到目标（通常为磁带介质）。备份会话的结果是备份介质（即介质集）上出现数据副本。

安排的和交互的备份会话

- 安排的备份会话

  安排的备份会话由 Data Protector 调度程序在指定的时间启动。您可以在 Data Protector 监视器中查看计划的备份会话的进度。

- 交互式备份会话

  交互式备份会话从 Data Protector 用户界面直接启动。此时会立即启动 Data Protector 监视器，您可以在其中查看备份会话的进度。请注意，多位用户可以监控同一备份会话。可能要通过从会话断开用户界面的连接以停止监视。会话随后将在后台继续运行。

备份会话数据流和进程

在备份会话中会执行哪些操作？

备份会话的信息流如备份会话信息流 (1)所示。请注意，这里介绍的数据流和进程是针对标准网络备份而言的。有关其他类型备份（如分割镜像备份）特定的数据流和进程，请参见相关章节。

启动备份会话时，将执行以下操作：

1. 备份会话管理器 (BSM) 进程在 Cell Manager 系统上启动并控制备份会话。该进程读取备份规范，以了解有关备份内容、备份选项、备份介质和备份设备的信息。
2. BSM 会打开 IDB 并写入有关备份会话的 IDB 信息，如生成的消息、备份数据的详细信息以及会话中所用的设备和介质。
3. BSM 会在有设备配置用于备份的系统上启动介质代理 (MA)。为每个并行使用的驱动器启动新的介质代理。单元中可启动的介质代理的数目受单元配置和购买的许可证数目的限制。

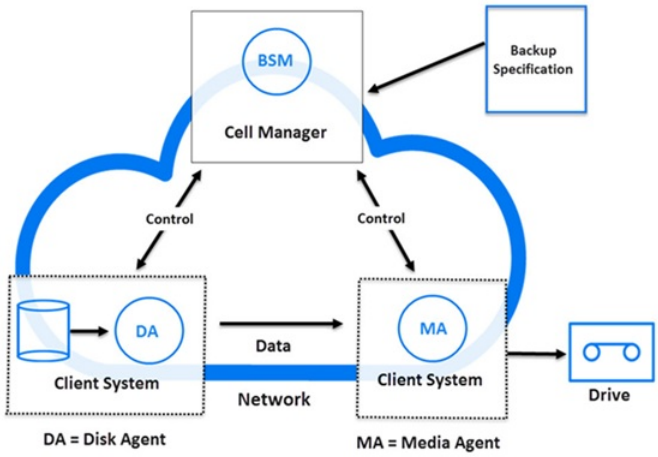
   在使用对象镜像的备份会话中，BSM 还会启动用于镜像的介质代理。
4. BSM 为每个需要并行备份的磁盘启动磁盘代理 (DA)。启动的磁盘代理的实际数目取决于备份规范中配置的磁盘代理的并发数。并发数是指可启动的磁盘代理数目，以将数据并行发送到介质代理，从而使设备能够传送数据。
5. 磁盘代理从磁盘中读取数据，将数据发送到介质代理，再由介质代理将数据写入介质。

   在使用对象镜像的备份会话中，用于写入镜像对象的介质代理以菊花链的形式进行连接。每个介质代理将接收到的数据写入介质，然后将其

转发给菊花链中的下一个介质代理。

6. BSM 监视会话进度，并根据需要启动新的磁盘代理和新的介质代理。
7. 备份会话完成时，BSM 即关闭会话。

备份会话信息流

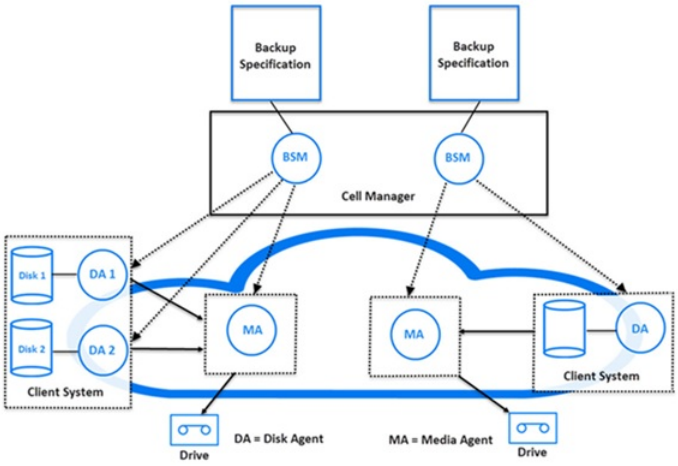


可以并发运行多少个会话？

多个备份会话可以同时在单元中运行。此数目受单元中的资源 (如设备可用性) 和 Cell Manager 配置 (如处理器速度、主内存大小等) 的限制。为避免 Data Protector 进程超出系统容量，对并发备份会话的最大数目作了限制。该限值是可配置的。

备份会话信息流 - 多个会话显示了并发运行的多个会话。

备份会话信息流 - 多个会话



pre-exec 和 post-exec 命令

通过 Data Protector pre-exec 命令，可以在备份或还原会话之前执行某些操作。通过 Data Protector post-exec 命令，可以在备份或还原会话之后执行某些操作。典型的 pre-exec 操作将关闭数据库以使数据处于一致的状态。

可以为备份规范设置 pre-exec 和 post-exec 命令，并且可以在 Cell Manager 系统上执行，或者可以指定这些命令作为备份对象选项，并在运行各个磁盘代理的客户机系统上执行。

pre-exec 和 post-exec 脚本命令可作为可执行文件或 shell 脚本写入。Data Protector 不提供这些命令，必须由备份操作员等相关人员分别写入。

命令的启动和位置

分别在备份会话前后启动备份会话的 pre-exec 和 post-exec 命令。默认情况下在 Cell Manager 上执行这些命令，但可以选择其他系统。

Windows 系统

在 Cell Manager 上执行时，pre-exec 和 post-exec 脚本由 Data Protector CRS 启动；而在远程执行时，以 Data Protector Inet 服务帐户 (默认情况下为本地系统帐户) 执行这些脚本。

Cell Manager 和其他系统上的脚本必须位于 Data_Protector_home\bin 目录中，用户必须只指定文件名或相对路径名。

对于位于 Data_Protector_home\bin 目录中的脚本，请仅指定文件名，否则要指定脚本的完整路径名。

对于 pre-exec 和 post-exec 命令，仅支持 .bat、.exe 和 .cmd 扩展名。要运行扩展名不受支持的（例如 .vbs）脚本，请创建用于启动该脚本的批处理文件。然后配置 Data Protector，将批处理文件作为 pre-exec 或 post-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

如果使用引号 ("") 指定路径名，请勿使用反斜杠和引号的组合 (\\")。如果需要在路径名末尾使用尾随的反斜杠，则要使用双反斜杠 (\\)。

> **注意**禁止直接使用 perl.exe。

UNIX 系统

Pre-exec 和 post-exec 脚本由备份会话所有者启动，除非备份会话所有者具有 Backup as root 权限；那么，将以 root 启动这些命令。

在 Cell Manager 或远程 UNIX 客户机上，备份规范的 exec 命令必须位于如下位置：

- Solaris 和 Linux 系统: /opt/omni/lbin
- 其他 UNIX 系统： /usr/omni/bin

对于位于 /opt/omni/lbin 或 /usr/omni/bin 目录中的命令，可仅指定文件名，否则要指定完整的路径名。

备份会话列队等待

超时

当备份会话启动时，Data Protector 会尝试分配所有必需资源，如设备。会话将列队等待直到所需的最少资源变得可用为止。如果资源在超时后仍不可用，则将中止会话。

备份会话中的装载请求

当 Data Protector 需要新的介质用于备份而该介质不可用时，便会出现备份会话中的装载请求。

Data Protector 发出装载请求的原因如下：

发出装载请求

- 备份介质空间不够，且无新的介质可用。
- Data Protector 的备份介质分配策略所要求的介质在设备中不可用。
- 预分配列表中定义了介质用于备份的顺序，但相应顺序中的介质不可用。

响应装载请求

响应装载请求包括提供所需的介质并指示 Data Protector 继续备份。

在 Data Protector 中可以配置发出装载请求时应如何响应:

向操作员发送通知

您可以配置 Data Protector 通知，以向操作员发送电子邮件，通知其有装载请求。操作员可以执行相应操作，如手动装载所需介质或中止会话。

自动化装载请求

可以配置处理装载请求的自动化操作。为此，请写入执行所需操作的脚本或批处理程序。

使用磁盘发现进行备份

在使用磁盘发现进行备份的过程中，Data Protector 会在启动备份会话时在目标系统上创建一个详细的磁盘列表，并备份所有磁盘。因此，系统上的所有本地磁盘即使在配置备份时不在系统上，也会对它们进行备份。通过磁盘发现进行备份在配置变化迅速的动态环境中尤其有用。它支持您在备份中选择或排除特定目录。

磁盘发现与标准备份相比如何？

在标准备份中，您可以通过在备份规范中进行相应配置明确配置用于备份的特定磁盘、目录或其他对象。因此，将仅对这些对象进行备份。如果向

系统中添加了新磁盘或想要备份一些其他对象，必须手动编辑备份规范和这些新对象。您可以在配置备份时选择要使用的方法 —磁盘发现或标准备份。

恢复备份会话

如果备份会话没有成功完成（例如，由于一些网络问题）或被中止，可以使用 Data Protector 继续会话功能继续进行备份。恢复失败的备份会话时，Data Protector 会继续进行备份，正好从失败的会话停止之处开始。

还原会话

本节将介绍如何启动还原会话，还原会话期间会执行哪些操作，以及涉及的进程和服务。

在恢复会话中，数据将从备份副本（通常在磁带介质上）复制回磁盘。

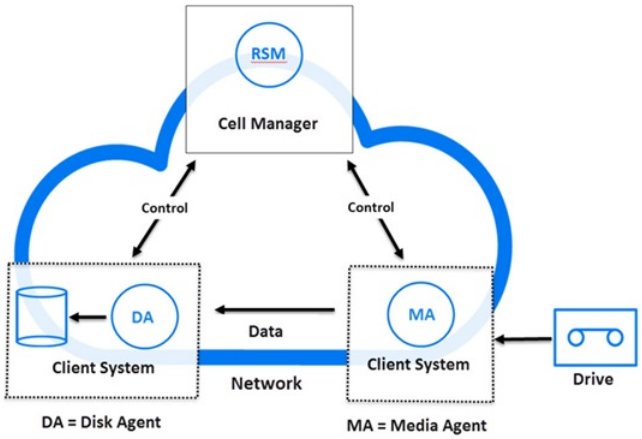
还原会话交互启动。指示 Data Protector 要恢复的对象，让 Data Protector 确定所需介质、选择一些选项并启动恢复。您和其他用户可以监视会话进度。

还原会话数据流和进程

当还原会话启动时 (如还原会话信息流所示)，会执行以下操作:

1. 在 Cell Manager 系统上启动还原会话管理器 (RSM) 进程。该进程控制还原会话。
2. RSM 将打开 IDB，读取有关还原所需介质的信息，并将还原会话信息（如生成的消息）写入 IDB。
3. RSM 会在有设备用于还原的系统上启动介质代理 (MA)。为每个并行使用的驱动器启动新的介质代理。
4. RSM 为每个并行还原的磁盘启动磁带客户机 (DA)。启动的磁带客户机实际数目取决于选择进行还原的对象。
5. 介质代理从介质中读取数据，将数据发送到磁带客户机，再由磁带客户机将数据写入磁盘。RSM 监视会话进度，并根据需要启动新的磁带客户机和新的介质代理。
6. 还原会话完成时，RSM 即关闭会话。

还原会话信息流



可以并发运行多少个恢复会话？

多个还原会话可以同时在单元中运行。此数量受单元中的资源 (如 Cell Manager) 和带有连接设备的系统的限制。

恢复会话列队等待

超时

当还原会话启动时，Data Protector 会尝试分配所有必需资源，如备份设备。只要所需的最少资源尚不可用，会话将一直列队等待。Data Protector 尝试在特定时段（超时）内分配资源。用户可以配置超时时间。如果资源在超时后仍不可用，则将中止会话。

还原会话中的装载请求

如果设备中没有恢复所需的介质，则恢复会话中将显示装载请求。Data Protector 可用于配置显示装载请求时应发生的所需操作。

响应装载请求

响应装载请求包括提供所需介质或任意介质副本并指示 Data Protector 继续还原。

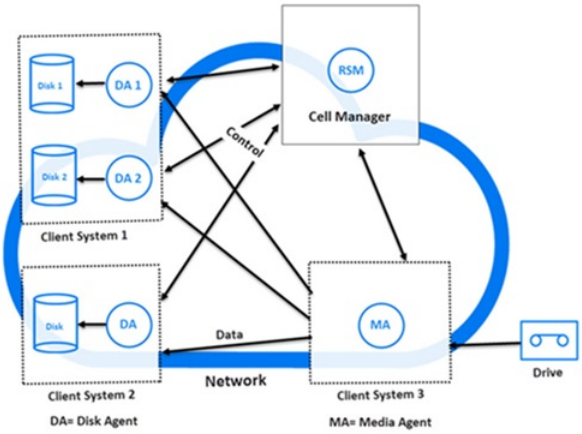
并行恢复

在并行还原时，从单路径的介质中并发读取和还原来自多个对象的交叉存取数据。并行还原大大提高了从同一介质还原多个对象时的还原性能。

并行还原与标准还原相比如何？

来自多个磁带客户机的数据（大多数情况下）复用并存储在介质上。执行标准恢复时，Data Protector 会从介质中读取多路复用的数据，并仅收集所选对象需要的部分。假设两个对象位于同一介质上，并使用复用写入，则还原下一个对象时，Data Protector 必须回绕介质并读取另一对象所需的部分。

并行还原会话流



在并行还原中，Data Protector 会读取所有选定对象的复用数据，动态收集所有对象需要的部分，然后将正确的数据发送给正确的磁盘代理。这提高了从介质读取数据的性能。如果所选对象要写入不同的物理磁盘，在这种情况下数据将被同时复制到多个磁盘，则还会进一步提高性能。

快速恢复多个单一文件

Data Protector 使用不连续的对象还原提高还原性能。还原特定文件或树后，Data Protector 会直接重新定位到介质中的下一个文件或树，如果文件或树之间至少有一个段，则继续还原。

在单个还原对象内，您可以启动多个磁带客户机。这样，恢复分布在整个介质中的多个单一文件比 Data Protector 遍历介质要快得多。

恢复还原会话

如果还原会话没有成功完成 (例如，由于一些网络问题)，可以使用 Data Protector 恢复会话功能继续进行还原。恢复失败的会话时，Data Protector 将在新会话中继续还原，从失败的会话停止处继续。

对象复制会话

本节将介绍如何启动对象复制会话，会话期间会执行哪些操作，以及涉及的进程和服务。

对象复制会话是在其他介质集上创建已备份、已复制或已合并数据的副本的过程。在对象复制会话期间，选定的已备份、已复制或已合并对象从源介质复制到目标介质。

> **注意**默认情况下启用**重新连接**功能。

自动的和交互的对象复制会话

自动的对象复制会话

自动的对象复制会话可以安排，也可以在备份、对象复制或对象合并后立即启动。安排的对象复制会话使用 Data Protector 调度程序在指定的时间启动。备份后、复制后或合并后的对象复制会话在指定会话结束后启动。您可以在 Data Protector 监视器中查看自动的对象复制会话的进度。

交互的对象复制会话

交互的对象复制会话从 Data Protector 用户界面直接启动。此时会立即启动 Data Protector 监视器，您可以在其中查看会话的进度。多位用户可以监视同一对象复制会话。可能要通过从会话断开用户界面的连接以停止监视。会话随后将在后台继续运行。

对象复制会话数据流和进程

对象复制会话的信息流如对象复制会话信息流所示。启动对象复制会话时，将执行以下操作：

1. 在 Cell Manager 系统上启动复制和合并会话管理器 (CSM) 进程。该进程读取对象复制规范，以了解有关要复制的对象、复制选项、复制介质和复制设备的信息。它还控制对象复制会话。

2. CSM 将打开 IDB，读取有关复制所需介质的信息，并将对象复制会话的信息（如生成的消息）写入 IDB。
3. CSM 锁定设备。会话将列队等待直到所有读取介质代理和所需的最少写入介质代理都锁定为止，超时时间与备份相同。如果资源在超时后仍不可用，则将中止会话。
4. CSM 会在有设备配置用于复制的系统上启动介质代理。介质代理按备份策略的分配方式加载源和目标介质。
5. 介质代理从源介质读取数据，并连接到随目标介质一起加载的介质代理。

   如果目标设备未按对象指定，则 Data Protector 将按照以下优先级标准从在对象复制规范中选定的那些设备中自动进行选择:

   - 先选择块大小与源设备相同的目标设备，再选择那些块大小与源设备不同的设备
   - 先选择本地连接的设备，再选择网络连接的设备
6. 随目标介质一起加载的介质代理接受随源介质一起加载的介质代理的连接请求，并开始将对象副本写入目标介质。

   如果源设备的块大小小于目标设备的块大小，则在对象复制会话的此阶段会对块进行重新包装。
7. CSM 根据指定的复制会话选项更新所有复制成功的对象的 IDB 保护条目。

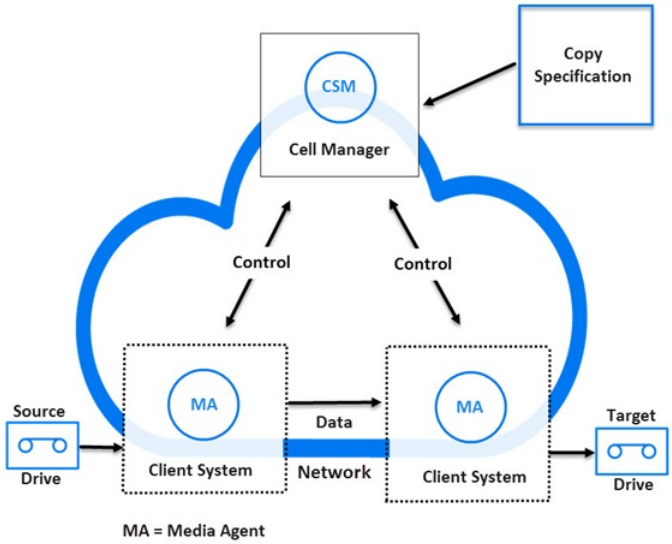
   同时还会更新所有失败的源对象的保护，以便在为会话指定了循环选项的情况下进行循环。
8. 对象复制会话完成时，CSM 即关闭会话。

可以并发运行多少个会话？

多个对象复制会话可以同时在单元中运行。此数量受单元中的资源 (如 Cell Manager) 和带有连接设备的系统的限制。

但是，不允许从同一对象复制规范中并行运行两个或两个以上的对象复制会话。

对象复制会话信息流



对象复制会话列队等待

超时

对象复制会话启动时，Data Protector 会尝试分配所有必需资源。会话将列队等待直到所需的最少资源变得可用为止。如果资源在超时后仍不可用，则将中止会话。

对象复制会话中的装载请求

当对象复制操作所需的源或目标介质不可用时，将发出对象复制会话中的装载请求。

响应装载请求

响应装载请求包括提供所需介质和确认装载请求。如果所需源介质有介质副本，则可以提供副本来代替原始介质。

复制会话

本节将介绍如何启动复制会话，会话期间会执行哪些操作，以及涉及的进程和服务。

复制会话是在其他能够执行复制的备份到磁盘 (B2D) 设备上创建已备份、已复制或已合并数据的其他复本的过程。在复制会话期间，选定的已备

份、已复制或已合并对象将从源设备复制到目标设备，直接从一个设备复制到另一个设备，而不用通过介质代理客户机传输数据。另外，由于只有唯一（重复）数据才通过网络进行传输，这样也减轻了网络负载。

自动的和交互的复制会话

自动的复制会话

自动复制会话可以安排，也可以在备份、对象复制或对象合并后立即启动。在指定的时间使用 Data Protector Scheduler 启动安排的复制会话。备份后、复制后或合并后的复制会话在指定会话结束后启动。可以在 Data Protector 监视器中查看自动复制会话的进度。

交互的复制会话

交互的复制会话直接从 Data Protector 用户界面启动。此时会立即启动 Data Protector 监视器，您可以在其中查看会话的进度。多个用户可以监视同一个复制会话。可能要通过从会话断开用户界面的连接以停止监视。会话随后将在后台继续运行。

复制会话数据流和进程

显示了复制会话的信息流。启动复制会话时，将执行以下操作：

1. 在 Cell Manager 系统上启动复制和合并会话管理器 (CSM) 进程。该进程读取复制规范（启用了复制选项），以了解有关要复制的对象、要使用的复制选项和复制设备的信息。它还控制复制会话。
2. CSM 将打开 IDB，读取有关复制所需设备的信息，并将复制会话的信息（如生成的消息）写入 IDB。
3. CSM 锁定设备。如果资源在超时后仍不可用，则将中止会话。
4. CSM 将在针对复制配置的设备间启动复制过程。
5. CSM 根据指定的复制会话选项更新所有复制成功的对象的 IDB 保护条目。

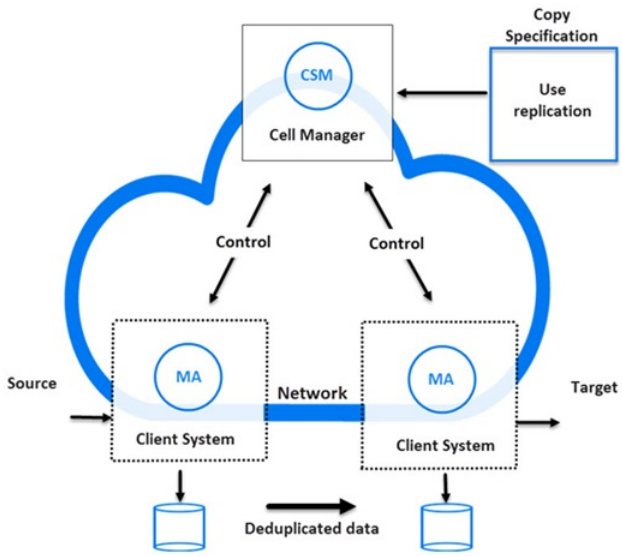
   同时还会更新所有失败的源对象的保护，以便在为会话指定了循环选项的情况下进行循环。
6. 复制会话完成时，CSM 即关闭会话。

可以并发运行多少个会话？

多个复制会话可以同时在单元中运行。此数量受单元中的资源 (如 Cell Manager) 和带有连接设备的系统的限制。

但是，不允许从同一复制规范中并行运行两个或两个以上的复制会话。您也不能并行运行两个或两个以上的交互式复制会话。

复制会话信息流



复制会话列队等待

超时

当替换会话启动时，Data Protector 会尝试分配所有必需资源。会话将列队等待直到所需的最少资源变得可用为止。如果资源在超时后仍不可用，则将中止会话。

对象合并会话

本节将介绍如何启动对象合并会话，会话期间会执行哪些操作，以及涉及的进程和服务。

对象合并会话是将包含一个完整备份和至少一个增量备份的备份对象还原链合并为该对象的新合并版本的过程。在对象合并会话期间，Data

Protector 会从源介质读取备份的数据，合并数据，并将合并后的数据版本写入目标介质。

自动的和交互的对象合并会话

自动的对象合并会话

自动的对象复制会话可以安排，也可以在备份后立即启动。计划的对象合并会话使用 Data Protector 调度程序在指定的时间启动。

备份后的对象合并会话在指定备份会话结束后启动。您可以在 Data Protector 监视器中查看自动的对象合并会话的进度。

交互的对象合并会话

交互的对象合并会话从 Data Protector用户界面直接启动。此时会立即启动 Data Protector 监视器，您可以在其中查看会话的进度。多位用户可以监视同一对象合并会话。可能要通过从会话断开用户界面的连接以停止监视。会话随后将在后台继续运行。

对象合并会话数据流和进程

启动对象合并会话时，将执行以下操作：

1. 在 Cell Manager 系统上启动复制和合并会话管理器 (CSM) 进程。该进程读取对象合并规范，以了解有关要合并的对象、合并选项、合并介质和合并设备的信息。它还控制对象合并会话。
2. CSM 将打开 IDB，读取有关所需介质的信息，并将对象合并会话的信息（如生成的消息）写入 IDB。
3. CSM 锁定设备。会话将列队等待直到所有读取介质代理和所需的最少写入介质代理都锁定为止，超时时间与备份相同。如果资源在超时后仍不可用，则将中止会话。
4. CSM 在有设备用于会话的系统上启动介质代理。介质代理按备份策略的分配方式加载源和目标介质。

   如果目标设备未按对象指定，则 Data Protector 将按照以下优先级标准从在对象合并规范中选定的那些设备中自动进行选择:

   - 先选择块大小与源设备相同的目标设备，再选择那些块大小与源设备不同的设备
   - 先选择本地连接的设备，再选择网络连接的设备
5. 一个介质代理可读取完整的对象版本，将数据发送到另一个介质代理，然后由另一个介质代理读取增量对象版本。第二个介质代理执行实际的合并操作，然后将数据发送给第一个介质代理，由第一个介质代理将数据写入目标介质。

   如果完整备份和增量备份位于同一文件库或 B2D 设备（智能缓存除外）中，则由同一介质代理读取所有备份并进行合并。

   如果源设备的块大小小于目标设备的块大小，则会对块进行重新包装。
6. 对象合并会话完成时，CSM 即关闭会话。

可以并发运行多少个会话？

多个对象合并会话可以同时在单元中运行。对象合并会话与备份会话类似，限制其数目的因素也与备份会话相同。

对象合并会话列队等待

超时

对象合并会话启动时，Data Protector 会尝试分配所有必需资源。会话将列队等待直到所需的最少资源变得可用为止。如果资源在超时后仍不可用，则将中止会话。

对象合并会话中的装载请求

当对象合并操作所需的源或目标介质不可用时，将发出对象合并会话中的装载请求。

响应装载请求

响应装载请求包括提供所需介质和确认装载请求。如果所需源介质有介质副本，则可以提供副本来代替原始介质。

对象验证会话

本节将介绍如何启动对象验证会话，会话期间会执行哪些操作，以及涉及的进程和服务。

对象验证会话是对分配给一个或多个指定对象的介质段进行验证的过程，检查头段中的信息并读取数据段中的数据块验证其格式。如果在原始备份中执行了循环冗余校验 (CRC)，它还会重新计算 CRC 并将其与原始备份中的 CRC 进行比较。

Data Protector 可以作为备份源的主机上执行验证，有效验证另一主机上还原路径中的 Data Protector 组件，验证还原到其他位置的能力，也可以直接在涉及的介质代理主机上执行验证，但仅验证数据。

自动的和交互的对象验证会话

自动的对象验证会话

可以使用 Data Protector 调度程序让自动的对象验证会话在指定的时间运行，也可以在指定的备份、对象复制或对象合并会话完成后让其作为备份后的对象验证会话立即运行。您可以在 Data Protector 监控器中查看这些会话的进度。

交互的对象验证会话

交互的对象验证会话可以从 Data Protector用户界面直接启动。此时会立即启动 Data Protector 监视器，您可以在其中查看会话的进度。多位用户可以监视同一对象验证会话。使用用户界面还可以执行其他操作，如果需要，可以让会话在后台继续运行。

对象验证会话数据流和进程

当启动对象验证会话时，基本处理流程如下：

1. 在 Cell Manager 系统上启动还原会话管理器 (RSM) 进程，该进程由以下对象触发:
   - Data Protector 调度程序 (针对计划的会话)
   - End of Session 事件（备份后的会话）
   - GUI 或 CLI 中的用户（交互会话）

   此进程控制验证会话。
2. RSM 将打开 IDB，读取有关要验证的对象的信息，并将验证会话的信息（如生成的消息）写入 IDB。
3. RSM 在与验证有关的源系统上启动介质代理 (MA)。为每个并行使用的驱动器启动新的介质代理。
4. 数据验证由目标主机上的磁带客户机 (DA) 执行，因此 RSM 会为每个并行的目标磁盘启动磁带客户机。启动的磁带客户机实际数目取决于选择进行验证的对象。该进程与还原会话的进程类似。
5. 介质代理从介质中读取对象数据，并将数据发送给执行验证的磁带客户机。RSM 监视会话进度，并根据需要启动新的磁带客户机和新的介质代理。
6. 对象验证会话完成时，RSM 即关闭会话。

对象验证处理流程的变化

从请求还原数据到数据到达目标主机的这一过程中，对象验证进程与还原进程类似。在数据到达目标主机之后，验证进程不会写入任何数据，对于应用程序集成对象，也不会与应用程序集成进行通信。

介质管理会话

介质管理会话用于对介质执行一些操作，比如对介质进行初始化、扫描内容、验证介质上的数据和复制介质等。

记录到 IDB

有关介质管理会话的信息（如生成的消息）存储在 IDB 中。

Data Protector 监视器与介质管理会话

在监视器窗口可以查看介质管理会话。如果关闭 Data Protector GUI，会话将继续在后台运行。

介质管理会话数据流

启动介质管理会话时，将执行以下操作：

1. 在 Cell Manager 系统上启动介质会话管理器 (MSM) 进程。该进程控制介质会话。
2. MSM 在有设备用于介质管理会话的系统上启动介质代理 (MA)。
3. 介质代理执行请求的操作，并将生成的消息发送到 Data Protector 用户界面，在那里可以跟踪其进度。该会话也存储在 IDB 中。
4. 会话完成时，MSM 即关闭会话。

可以并发运行多少个会话？

如果介质管理会话不使用相同的资源（如设备或介质），则多个介质管理会话可以同时在单元中运行。

复制会话管理器的重新连接功能

在运行合并或复制会话时，Data Protector 将尝试重新连接介质代理（BMA、RMA 或 MMA）与 CSM 之间已断开的连接。

默认情况下启用“Data Protector 重新连接已断开的连接”功能。

要禁用“重新连接已断开的连接”功能，请在 Cell Server 上将 omnirc 选项 OB2_CSM_NORECON 设置为 1。

默认情况下，Data Protector 尝试重新连接 20 分钟。要修改此超时时段，请在 Cell Server 和客户机上设置 omnirc 选项 OB2RECONNECT_RE

TRY 。单元服务器和客户机值必须同步。

> **注意**客户机上的 OB2RECONNECT_RETRY 选项指客户机尝试在出现错误后重新连接所持续的时间。服务器上的 OB2RECONNECT_RETRY 选项指服务器等待客户机重新连接所持续的时间。

关于跨 Cell Manager 复制的限制

执行跨 Cell Manager 复制时，MSM 与 CSM 之间的连接上未启用重新连接。只能修复 MA 与 CSM 之间的连接。

计划备份策略

本主题介绍备份策略计划，并集中讨论以下计划：Data Protector 单元、性能和安全性，以及备份和还原数据。本主题还将讨论基本备份类型、自动备份操作、群集和灾难恢复。

备份策略计划

Data Protector 的配置和管理都很简单。但是，如果您工作于有着不同客户机系统的大环境中，有海量数据需要备份，就必须预先计划。计划可简化后续配置步骤。

什么是备份策略计划？

备份策略计划是包含以下步骤的过程：

1. 定义备份的要求和限制，例如，您的数据需要多久备份一次、是否需要在其他介质集上存储已备份数据的更多副本。
2. 了解影响备份解决方案的因素，例如网络和备份设备的持续数据传输速率。这些因素可以影响 Data Protector 的配置方式和选择的备份类型 -- 例如网络备份或直接备份。例如，如果备份到磁盘，就可以利用合成备份和磁盘分段等高级备份策略。
3. 制定支持您的备份概念的备份策略及其实现方式。

本节将展开叙述上述步骤。本主题的其余部分提供了可以帮助您计划备份解决方案的重要信息和注意事项。

定义备份策略的要求

定义备份策略的目标和约束包括回答如下问题：

- 贵公司关于备份和恢复的**公司策略**是什么？

  一些公司已经定义了有关存档和存储数据的政策。您的备份策略应符合以下方针。

- 需要备份哪些类型的数据？

  列出网络中现有的所有数据类型，例如用户文件、系统文件、Web 服务器和大型关系数据库。

- 恢复所需的最长宕机时间有多久？

  允许的宕机时间会对网络基础架构投资和备份所需设备产生重大影响。对于每种类型的数据，列出恢复所需的最长宕机时间，即从备份恢复特定数据前允许这些数据有多长时间不可用。例如，用户文件可以在两天内还原，而大型数据库中的某些业务数据需要在两小时内还原。

  还原时间主要由访问介质所需时间以及将数据实际还原到磁盘所需时间组成。完整的系统恢复需要更多时间，因为还需要执行一些额外的步骤。

- 特定类型的数据应保留多久？

  对于每种类型的数据，列出数据必须保留多久。例如，用户文件可能只需要保留三周，但有关公司员工的信息则可能需要保留五年。

- 应如何存储和维护带备份数据的介质？

  对于每种类型的数据，列出存储数据的介质必须在保管库（一个安全的外部位置）保存多久（如果使用保管库）。例如，用户文件可能无需存储在保管库中，而订单信息可能需要保存五年，并且两年后需要验证每个介质的可用性。

- 备份过程中需要将数据写入多少个介质集？

  可考虑在备份过程中将关键数据写入多个介质集，以提高此类备份的容错能力，或使用多个地点的保管库保存介质。对象镜像增加了备份所需时间。

- 有多少数据需要备份？

  对于每种类型的数据，列出估计的需要备份的数据量。这会影响备份所需时间，并帮助您选择正确的备份设备和备份介质。

- 预计的未来数据量的增长情况如何？

  对于每种类型的数据，估计未来的增长。这有助于提出不会很快过时的备份解决方案。例如，如果公司计划雇佣 100 名新员工，用户数据和客户机系统数据的总量会相应增长。

- 备份可能需要多久？

  估计每次备份所需的时间。这会直接影响数据的可用时间。用户文件可以在用户未使用它们的任何时候备份，而某些交易数据库可能只有几小时可以用于备份。

  备份所需时间取决于备份类型，是完整备份还是增量备份。Data Protector 还备份某些常用的联机数据库应用程序。

  如果备份到磁盘，则可以利用合成备份和磁盘分段功能。

  如果要在较慢的设备上备份很快很大的磁盘，可以考虑通过多个并行磁带客户机来备份一个硬盘。在同一磁盘上启动多个磁带客户机可以显著提升备份性能。

- 数据需要多久备份一次？

  对于每种类型的数据，列出数据需要多久备份一次。例如，用户工作文件可以每日备份，系统数据需要每周备份，而某些数据库事务则需要

每天备份两次。

影响备份策略的因素

有许多因素可能会影响备份策略的实现方式。在制定备份策略前要了解这些因素。

- 公司的备份及存储策略和要求。
- 公司的安全策略和要求。
- 物理网络配置。
- 公司不同地方的计算机和人力资源。

制定备份策略计划

计划的结果是制定一个涉及以下方面的备份策略：

- 系统可用性（和备份）对公司有多重要
  - 发生灾难时将备份数据保存在远程位置的需求。
  - 业务持续性水平

    这包括所有关键客户机系统的恢复和还原计划。
  - 备份数据的安全性

    防止未授权人员进入数据存储场所的需求。这也包括使用物理访问防护和电子密码保护技术防止所有相关数据遭受未授权的访问。
- 需要备份的数据类型

  列出公司的数据类型，以及希望在备份规范中将它们组合起来的方式，包括可用于备份的时间范围。公司数据可分为各种类别，例如：公司业务数据、公司资源数据、项目数据和个人数据，每种数据都有其特定要求。
- 备份策略的实现
  - 如何进行备份和使用的备份选项

    这定义了完整备份和增量备份的频率，也定义了使用的备份选项、是否永久保护备份数据，以及是否将备份介质存储在保障公司。
  - 如何对客户机系统进行备份规范分组

    考虑一下最好如何对备份规范进行分组。比如，可以按照部门、数据类型或备份频率进行分组。
  - 如何调度备份

    考虑使用交错排列方法，在不同日期为不同客户机（备份规范）安排完整备份，以规避网络负载、设备负载和时间窗口问题。
  - 保留介质上的数据和关于备份的信息

    考虑保护数据在指定时间内不被较新的备份所覆盖。这一保护称为数据保护，是以会话为基础的。

    定义 Catalog Database 存储以下信息的时间长度：备份版本信息、备份文件数和目录数的信息以及数据库中存储的消息。因为只要该编目保护尚未到期，所备份的数据就易于访问。
- 设备配置

  确定用于备份的设备，以及它们所连接到的客户机系统。将备份设备与数据量最大的客户机系统相连接，以便尽可能在本地备份数据而不是通过网络进行备份。这可提高备份速度。

  如果需要备份大量数据：
  - 考虑使用带库设备。
  - 考虑备份到基于磁盘的设备。除了其他优点外，备份到磁盘还可缩短备份所需时间，使用户能使用合成备份和磁盘分段等高级备份策略。
- 介质管理

  确定要使用的介质类型、如何将介质分组到介质池，以及如何在介质上放置对象。

  确定如何将介质用于备份策略。
- 保管

  确定是否要将介质存储到安全的地方（保管库），并在那里保存一段时间。为此，考虑在备份过程中或备份后复制已备份的数据。
- 备份管理员和操作员

  确定可管理和操作存储产品的用户权限。

计划单元

计划备份策略时，最重要的决定之一是确定单元环境是单个还是多个。本节将介绍以下内容：

- 计划单元时应考虑的因素

- 单元如何与典型的网络环境相关联
- 单元如何与 Windows 域相关联
- 单元如何与 Windows 工作组环境相关联

一个单元还是多个单元？

当确定在环境中拥有单个单元还是多个单元时，请考虑以下事项：

- 备份管理问题

  使用多个单元可提高每个单元内的管理自由度。您可以对每个单元应用完全独立的介质管理策略。如果有多个管理组，出于安全考虑，您可能不希望一个单元跨越这些组。拥有多个单元的缺点是可能需要执行更多管理工作，甚至每个单元都需要独立的管理员。

- 每个单元的大小

  Data Protector 单元的大小会影响备份性能和管理单元的能力。如果某个特定单元超过了建议的大小，则此单元可能不易于管理。

- 网络注意事项

  一个单元中的所有客户机系统都应部署在同一局域网上，以最大程度地提高性能。有关其他网络注意事项（如网络配置）的详细信息，请参见后面的章节。

- 地理位置

  如果要备份的客户机系统在地理位置上很分散，从单一单元管理它们可能就很困难，在客户机系统之间可能存在联网问题。此外，数据安全性也可能成问题。

- 时区

  每个单元都应在同一时区内。

- 数据安全性

  Data Protector 提供基于单元级别的安全性。所有 Data Protector 管理工作在单一单元的环境中完成：介质、备份设备和备份数据属于一个单元。请注意，Data Protector 允许您共享设备或在单元之间移动介质，因此对介质的物理访问必须限于授权人员。

- 混合环境

  Data Protector 允许在单一单元内备份不同平台的客户机系统。但是，根据平台对单元内的客户机系统进行分组，可能较为方便。例如，您可以让一个单元是 Windows 客户机系统，另一个单元是 UNIX 客户机系统。如果您对 UNIX 和 Windows 环境有不同的管理员和策略，这就特别有用。

- 部门和场所

  可以将每个部门或场所分组到独立的单元中。例如，您可以将会计部门作为一个单元，将 IT 部门作为一个单元，将制造部门作为一个单元。即使选择拥有多个单元，也可以通过 Data Protector 方便地在单元之间配置通用策略。

安装和维护客户机系统

如果有多个 UNIX 和 Windows 客户机系统，用有效的机制安装 Data Protector 就变得尤为重要。在大环境中，在每个客户机上进行本地安装是不可行的。

安装服务器和 Cell Manager

Data Protector 单元中的主系统是 Cell Manager。为了便于从一个中央位置将 Data Protector 组件分配 (远程安装) 给客户机系统，需要可保存 Data Protector 软件存储库的系统。该系统称为 Data Protector 安装服务器。Cell Manager 默认情况下也是安装服务器。

每次执行远程安装时，都需要访问安装服务器。使用安装服务器的优势在于远程安装、更新、升级和删除 Data Protector 软件所需的时间大大缩短，特别是在企业环境中。

开始安装该软件之前，安装服务器和 Cell Manager 必须满足特定的硬件和软件要求。专用端口（通常是端口 5555/5565）必须在整个单元内可用。

Cell Manager 和安装服务器直接从下载的软件包 (zip/tar) 中安装。安装 Cell Manager 和安装服务器后，就可以用 Data Protector 安装图形用户界面 (GUI) 在不同客户机系统上安装组件。

第一次安装 Data Protector 时，它以即开即用许可证 (有效期为 60 天) 运行，让您可以在获取永久许可证之前使用 Data Protector。在此期间，请购买所需许可证。

同样在此期间，您应设置和配置 Data Protector 环境，并请求永久许可证。要请求永久性密码字符串，您需要知道客户机系统属于哪个 Data Protector 单元、连接到该客户机系统的设备数，以及是否需要使用任何 Data Protector 集成。

在 UNIX 环境中创建单元

在 UNIX 环境中创建单元非常简单。根据本主题中的注意事项，确定要向单元添加哪些客户机系统，并定义 Cell Manager 系统。在安装过程中，需要对每个客户机系统具有 root 访问权限。很重要的先决条件是具有清晰的节点名称解析设置，这样就可以使用同一完全限定节点名称从其他客户机系统访问每个客户机系统。

在 Windows 环境中创建单元

由于可用配置的不同 (域和工作组)，对 Windows 管理员提供的支持程度也不同，这可能会影响安装过程中对 Data Protector 的设置。

> **重要说明**很重要的先决条件是具有清晰的节点名称解析设置，这样就可以使用同一完全限定节点名称从其他客户机系统访问每个客户机系统。

Windows 域

Windows 域很容易映射到 Data Protector 单元。在单一 Windows 域内，如果域大小未超过 Data Protector 单元的建议大小，则使用一对一映射。否则，会将域分割为两个或多个单元，用 Data Protector Manager-of-Managers 管理这些单元。

将 Data Protector 单元映射到 Windows 域

将 Data Protector 单元映射到 Windows 域也会方便 Data Protector 本身的管理。为便于管理，分配软件时，要考虑到让所有客户机系统都能用域组织内的中央 Windows 帐户安装。但是，其他操作并不限于 Windows 域组织，因为所有操作和安全确认都由 Data Protector 内部协议来执行，而非由 Windows Security 保证。

通常，对于如何安装 Data Protector 及其安装位置并无限制。但是，由于 Windows 的结构以及最通用的配置是域环境，将 Data Protector 映射到单一域或多域模式（其中一个域是主域，允许单个用户管理环境中的所有客户机系统，即软件分配和用户配置）时，某些操作会比较容易。

在具有 Manager-of-Managers 的多单元环境中，这个问题就更为显著，因为配置的所有单元都需要有能访问整个备份环境的中央管理员。配置具有主域的单一域或多域时，同一全局主域用户可以是所有单元和 Manager-of-Managers 环境的管理员。如果使用多个独立域，则需要配置多个用户来管理环境。

Windows 工作组

由于不像域中那样有全局用户，在某些情况下部分配置任务需要更多步骤。软件分配要求您对在其上安装该软件的每个客户机系统进行唯一登录。这意味着要在工作组环境中安装 100 个客户机系统，就需要进行 100 次登录。在这种情况下就需要使用域环境，因为安装与许多其他非 Data Protector 相关管理任务对于大环境而言更为容易。

在这样的环境中使用 MoM，要求您为每个单元单独配置管理员，以便从任何单元管理 MoM 环境。

同样，Data Protector 并不限于 Windows 域组织。但是，在需要用户认证的环节（安装、用户管理）中，它能利用并简化管理步骤。

在混合环境中创建单元

在混合环境中，要考虑在 UNIX 环境中创建单元中所述的因素。环境分为越多个域和越多个工作组，分配软件及准备环境以便管理时需要考虑的帐户和步骤就越多。

远程单元

通过 Data Protector 可轻松管理地理上远程的单元。

远程单元的注意事项

配置远程单元时，请记住以下事项：

- 数据不通过 WAN 发送。

  要备份的设备和客户机系统是本地配置的。

- 单元是在 MoM 中配置的。

  要以集中方式管理远程单元，需要在 MoM 环境中配置单元。

- 考虑用户配置。

  这里提到的有关单一域、多域和工作组配置的所有注意事项都要考虑在内。

可以通过远程位置配置单一单元。在这种情况下，您需要确保数据从每个客户机系统传输到对应设备不是通过 WAN 实现的。因为 WAN 是不稳定的连接，可能会中途断开连接。

MoM 环境

MoM 环境不要求单元与 MoM 中央单元之间有可靠的网络连接，因为备份是在每个 Data Protector 单元内本地执行的，只有控制信息才通过远距离连接进行发送。然而，这是基于每个单元都有自己的 Media Management Database 的假设。

在这种情况下，请使用 Data Protector“重新连接已断开的连接”备份选项，以便在连接断开后重新建立连接。

了解和计划性能

在业务关键环境中，发生数据库损坏或磁盘灾难时应尽可能缩短数据恢复所需的时间，这是关键要求。因此，了解和计划备份性能至关重要。如何缩短备份连接在不同网络和不同平台上的众多客户机系统和大数据库所需的时间，是富有挑战性的任务。

以下章节将概述最常见的影响备份性能的因素。由于变量众多，不可能明确给出满足所有用户需要的建议。

基础架构

基础架构对备份和还原的性能有很大影响。最重要的方面是数据路径的并行性和高速设备的使用。

网络备份和本地备份

通过网络发送数据会引入额外的开销，因为网络也成为性能考虑因素之一。对于以下情况，Data Protector 处理数据流的方式有所不同：

- 网络数据流：从磁盘到源系统存储器、到网络、到目标系统存储器再到设备
- 本地数据流：从磁盘到存储器再到设备

要使性能最大化，请对高容量数据流使用本地备份配置。

设备

设备性能

由于设备向磁带写入数据（或从中读取数据）时可保持的速度不同，设备类型和型号会影响性能。

数据传输率还取决于是否使用硬件压缩。可以达到的压缩率取决于要备份的数据的性质。在大多数情况下，使用带硬件压缩的高速设备能提高性能。但是，仅在设备流畅通无阻时才使用此类高速设备。

在备份会话的开始和结束时，备份设备需要些时间以执行回绕介质和装载或卸载介质等操作。

由于库能够快速自动地访问许多介质，就提供了额外的优势。备份时，需要加载新的或可重用的介质，恢复时需要快速访问包含要还原的数据的介质。

基于磁盘的设备中的数据访问起来比传统设备中的更快，因为无需加载和卸载介质。这就缩短了备份和还原所需时间。此外，基于磁盘的设备能使用合成备份和磁盘分段等高级备份策略，这也可缩短备份和还原时间。

不同于设备的高性能硬件

计算机系统的性能

计算机系统本身的速度会直接影响性能。系统是在备份中通过读取磁盘、处理软件压缩等加载的。

除了 I/O 性能和网络类型外，磁盘读取数据的速率和 CPU 使用率也是系统本身的重要性能条件。

高级高性能配置

Data Protector 零宕机时间备份解决方案提供了缩短应用程序宕机时间或备份模式时间和减少网络管理成本的途径，这是通过使用本地连接的备份设备而非网络备份设备来实现的。应用程序宕机时间或备份模式时间限于创建数据复本所需的时间，数据副本随即从备份系统备份到本地连接的设备。

并行使用硬件

并行使用多个数据路径是提高性能的基本方法和有效方法。其中包括网络基础架构。并行性技术在以下情况中能大幅提高性能:

何时使用并行性

- 多个客户机系统可以本地备份，即使用同一客户机系统上连接的磁盘和相关设备。
- 多个客户机系统可以通过网络备份。在这里网络流量的路由设置必须使得数据路径不重叠，否则会影响性能。
- 多个对象（磁盘）可以备份到一个或多个（磁带）设备。
- 可以在特定的客户机系统之间使用多个专用网络链接。例如，如果 system_A 有 6 个对象（磁盘）需要备份，而 system_B 有 3 个快速磁带设备，可考虑在 system_A 和 system_B 之间使用 3 个专用网络链接。
- 负载均衡

  使用该 Data Protector 功能，Data Protector 就可以动态判断哪个对象应备份到哪个设备。特别是要备份动态环境中的大量文件系统时，请启用该功能。

  请注意，您无法预测特定对象会写入哪个介质。

配置备份和还原

任何给定的基础架构都必须有效使用，以尽可能提高性能。Data Protector 可提供能适应环境的灵活途径和操作备份与还原的理想方式。

软件压缩

软件压缩是在从磁盘读取数据时由客户机 CPU 完成的。这可减少通过网络发送的数据，但需要占用客户机大量的 CPU 资源。

默认情况下，软件压缩处于禁用状态。只对这样的备份使用软件压缩：许多计算机通过较慢的网络连接，这种情况下在通过网络发送数据之前可以先压缩数据。如果使用了软件压缩，就会禁用硬件压缩，因为试图压缩数据两次实际上会使数据膨胀。

硬件压缩

硬件压缩是由一台从驱动服务器接收原始数据并以压缩后模式将这些数据写入介质的设备完成的。硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数据较少。

默认情况下，硬件压缩处于启用状态。在 UNIX/Linux 系统上，可选择硬件压缩设备文件来启用硬件压缩。在 Windows 系统上，可在设备配置期间启用硬件压缩。请谨慎使用硬件压缩，因为*无法*使用未压缩的设备读取写入压缩模式下的介质，反之亦然。

完整备份和增量备份

提高性能的基本途径就是减少要备份的数据量。要小心地计划完整备份和增量备份。请注意，可能无需同时执行所有客户机系统的所有完整备份。

如果备份到磁盘，则可以利用合成备份和磁盘分段等高级备份策略。

磁盘映像备份和文件系统备份

过去，备份磁盘映像比备份文件系统效率更高。在某些情况下仍然如此，例如负载较重的系统或包含大量小文件的磁盘。但通常建议使用文件系统备份。

向介质分配对象

下面是 Data Protector提供的对象/介质备份配置示例：

- 一个对象（磁盘）备份到一个介质

  优点是对象和对象所在介质之间存在已知的固定关系。这对于还原过程可能有好处，因为只需访问一个介质。

  网络备份配置的缺点是由于网络原因可能限制性能，导致设备不能实现流式传送。

- 多个对象备份到几个介质，每个介质有来自多个对象的数据，一个对象备份到一台设备

  这样做的优点是备份时数据流具有灵活性，有助于优化性能，特别是在网络配置中。

  该策略基于这样的假设：设备接收了足够实现流式传送的数据，因为每台设备会从多个源并行接收数据。

  缺点是在还原单一对象时，必须跳过（来自其他对象）的数据。此外，也无法准确预测哪个介质会接收来自哪个对象的数据。

磁盘性能

Data Protector 备份的所有数据都位于系统内的磁盘上。因此，磁盘的性能会直接影响备份性能。磁盘实际上是一种顺序设备，即可以读取或写入数据，但不能同时读写。另外，您可以一次读取或写入一个数据流。Data Protector 按顺序备份文件系统，以减少磁头运动。它也是以顺序方式还原文件的。

有时这不可见，因为操作系统将最常用的数据存储在**缓存内存**中。

磁盘碎片

磁盘上的数据不是以您浏览文件和目录时看到的逻辑顺序保存的，而是以遍布整个物理磁盘的小块形式分散分布。因此，要读取或写入文件，磁盘头就必须在整个磁盘区域上移动。请注意，这随着操作系统的不同而异。

提示碎片很少的大文件的备份效率最高。

压缩

如果数据是压缩在磁盘上的，Windows 操作系统会先解压缩数据，再通过网络进行发送。这样可降低备份速度并占用 CPU 资源。

磁盘映像备份

通过 Data Protector 也可将 UNIX 和 Windows 磁盘备份为磁盘映像。通过磁盘映像备份，将整个磁盘的映像进行备份，而不跟踪文件系统结构。磁盘头在磁盘表面线性移动。因此，磁盘映像备份要比文件系统备份快得多。

基于块的备份

基于块的备份使您能够在块级别执行文件系统备份。 所有操作系统 (OS) 都有一个称为“文件系统”的专用组件。例如 Windows 上的NTFS。文件系统将硬盘、卷或 RAID 阵列（软件和硬件 RAID）分成固定的字节组，这些字节组称为块。

常规文件系统备份类型使用 OS 上的文件系统来读取磁盘或卷上的数据。基于块的备份直接从磁盘或卷中读取块，而无需跟踪文件系统结构。块按它们在磁盘上保存的顺序读取，而不是按文件中显示的顺序读取。系统仅备份已使用的块，从而减少了备份时间。

Windows 系统上的磁盘代理性能

Windows 文件系统备份的磁盘代理性能可以通过启用异步读取来提高。在磁盘阵列上备份数据时，异步读取可以提高磁盘代理的性能，特别是备份大文件时。建议执行测试备份，以判断在您的特定环境中，异步读取能否提高性能，并确定最优的异步读取设置。

SAN 性能

如果需要在一个会话中备份大量数据，传输数据所需时间就变得至关重要了。数据传输时间即将数据通过连接（LAN、本地或 SAN）移到备份设备所需的时间。

联机数据库应用程序性能

备份数据库和应用程序（例如 Oracle、SAP R/3、Sybase 和 Informix Server）时，备份性能还取决于应用程序。提供数据库联机备份，以便在数据库应用程序保持联机时进行备份。尽管此功能有助于最大限度地提高数据库正常运行时间，但可能影响应用程序的性能。Data Protector 集成了所有常用的联机数据库应用程序以优化备份性能。

有关如何提高备份性能的详细信息，请参见联机数据库应用程序随附的文档。

计划安全性

计划备份环境时，要考虑安全性。一个深思熟虑后实施和更新的安全计划，可防止未授权的访问、复制或修改数据。在 Data Protector 10.00 版本之前，客户可以选择通过启用加密控制通信 (ECC)，保护 Cell Manager 和客户机之间的通信。启用 ECC 后，客户机生成 CRS 请求，该请求由 Cell Manager 上托管的 CA 进行签名。此处，通过检查证书中的 CA 和主机名，建立信任。在 Data Protector 10.00 中，默认情况下，Cell Manager 和客户机之间的所有通信均受到保护。此外，从 Data Protector 2019.08 (10.50) 开始，默认情况下还保护客户机之间的所有通信。使用带证书锁定的自签名证书代替根 CA 概念。

什么是安全性？

在备份上下文中，安全性通常是指：

- 谁可以管理和操作备份应用程序 (Data Protector)。
- 谁可以实际访问客户机系统和备份介质。
- 谁可以还原数据。
- 谁可以查看已备份数据的信息。

Data Protector 可提供所有级别的安全解决方案。

Data Protector 安全功能

以下功能允许和限制对 Data Protector 及已备份数据的访问。以下章节将详细介绍该列表中的项目。

- 单元
- Data Protector 用户帐户
- Data Protector 用户组
- Data Protector 用户权限
- 备份数据的可见性和访问权限
- 数据加密

单元

启动会话

Data Protector 安全性基于单元。除非有 Data Protector Manager-of-Managers 功能，否则只能从 Cell Manager 启动备份和还原会话。这就确保了其他单元的用户不能从本地单元的系统备份和还原数据。

从特定 Cell Manager 进行访问

此外，通过 Data Protector 还可以显式配置能从哪个 Cell Manager 客户机系统进行访问，即配置受信任者。

限制预执行和后执行

出于安全方面的原因，可以为 pre-exec 和 post-exec 脚本配置不同程度的限制。通过这些可选脚本可以为备份准备客户机系统，例如通过关闭应用程序获得一致的备份。

Data Protector 用户帐户

使用 Data Protector 功能、管理 Data Protector 或还原个人数据的任何人都必须有 Data Protector 用户帐户。这可限制 Data Protector 和已备份数据遭受未授权访问。

谁定义用户帐户？

管理员创建此帐户时将指定用户登录名、用户登录用的系统，以及定义用户权限的 Data Protector 用户组成员资格。

何时检查帐户？

用户启动 Data Protector 用户界面时，Data Protector 会检查用户权限。用户执行特定任务时也会检查用户权限。

Data Protector 用户组

什么是用户组？

创建新的用户帐户时，用户就成为指定用户组的成员。每个用户组都包含所定义的 Data Protector 用户权限。所有的组成员都具有为该组设置的用户权限。

为什么要使用用户组？

Data Protector 用户组可简化用户配置。管理员根据用户所需访问权限对他们进行分组。例如，最终用户组只允许成员将个人数据还原到本地系统，而操作员组则允许成员启动和监视备份，但不能创建备份。

Data Protector 用户权限

什么是用户权限？

Data Protector 用户权限定义用户可以通过 Data Protector 执行的操作。用户权限应用于 Data Protector 用户组级别，而非逐个应用于每个用户。添加到用户组的用户会自动获得分配给该用户组的用户权限。

为什么要使用用户权限？

Data Protector 可提供灵活的用户和用户组功能，使管理员能够有选择地定义谁可以使用特定的 Data Protector 功能。慎重应用 Data Protector 用户权限非常重要：备份数据和还原数据实际上与复制数据相同。

备份数据的可见性

备份数据意味着创建新副本。因此，处理机密信息时，限制对原始数据和备份副本本身的访问很重要。

对其他用户隐藏数据

配置备份时，您可以决定还原过程中数据对每个人都可见（公开），还是只对备份的所有者可见（私有）。

什么是备份所有权？

谁拥有备份会话？

每个备份会话和在会话中备份的所有数据都会指定有一个所有者。所有者可以是启动交互式备份的用户、运行 CRS 进程时使用的帐户，或在备份规范选项中指定为所有者的用户。有关如何指定备份所有者的说明，请参阅《Data Protector 帮助》索引：“所有权”。

备份所有权和还原

备份所有权会影响用户查看和还原数据的能力。除非该对象标记为“公开”，否则只有介质集所有者或管理员才能看到该介质集中保存的数据。查看和还原私有对象的权限也可以授予 *admin* 以外的组。有关谁可以查看和还原私有对象以及如何应用该操作的说明，请参阅《Data Protector 帮助》索引：“所有权”。

数据加密

开放式系统和公共网络使得数据安全性是大型企业不可或缺的功能。通过 Data Protector 可以对备份数据进行加密，以使其与其他数据相比受到保护。Data Protector 提供两种数据加密技术：基于软件的技术和基于驱动器的技术。

Data Protector 软件加密，又称为“AES 256 位加密”，基于使用 256 位长度的随机密钥的 AES-CTR (Advanced Encryption Standard in Counter Mode) 加密算法。加密和解密都使用同一密钥。基于 AES 256 位加密，数据在通过网络传输之前和写入介质之前先进行加密。

Data Protector“基于驱动器的加密”使用驱动器的加密功能。具体实现和加密强度取决于驱动器的固件。Data Protector 仅启用该功能并管理加密密钥。

密钥管理功能由位于 Cell Manager 上的“密钥管理服务器 (KMS)”提供。所有加密密钥都集中存储在 Cell Manager 上的密钥库中，由 KMS 管理。

您可以在备份规范中加密全部对象或所选对象，也可以在同一介质上结合使用加密会话和未加密会话。

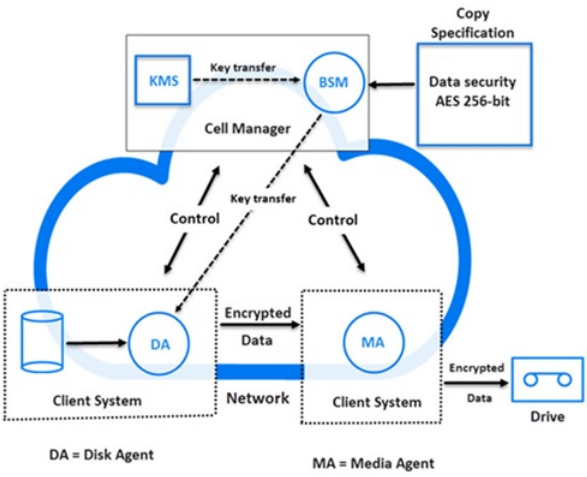
除了加密功能外，Data Protector 还为此提供使用无密钥内置算法的编码功能。

Data Protector AES 256 位加密的工作原理

Backup Session Manager (BSM) 会读取选择了 **AES 256 位**加密选项的备份规范，并从密钥管理服务器 (KMS) 请求活动的加密密钥。该密钥将传输到磁盘代理 (DA)，后者会加密数据。这样，已备份数据将先加密，再通过网络传输并写入介质。

使用 AES 256 位加密的备份会话显示与选择了 **AES 256 位 (AES 256-bit)** 加密选项的加密备份会话的基本交互。

使用 AES 256 位加密的备份会话



Data Protector 基于驱动器的加密原理

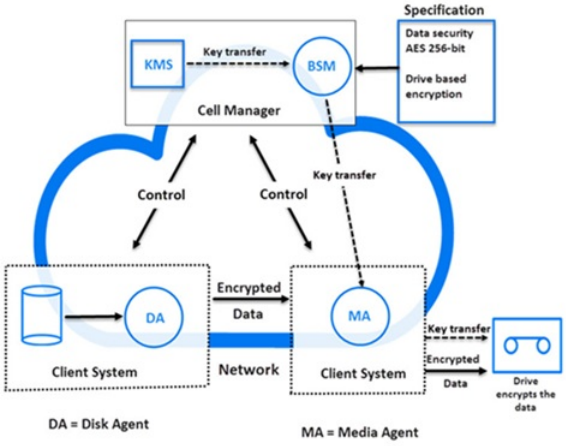
BSM 会读取选择了**基于驱动器的加密**选项的备份规范，并从 KMS 请求活动的加密密钥。该密钥将传输到介质代理 (MA)，后者为加密配置驱动器并将加密密钥设置到驱动器内。驱动器会同时对写入介质的数据和元数据进行加密。

从加密的备份执行对象复制或对象合并操作时，数据由源驱动器解密，通过网络传输，再由目标驱动器加密。

如果自动介质复制会话中涉及的源介质存储了加密及未加密数据，写入对应目标介质的所有数据也会加密或未加密，这取决于基于驱动器的加密的当前设置。

使用 AES 256 位加密和基于驱动器加密的备份会话显示在已选择 **AES 256 位 (AES 256-bit)** 加密选项和**基于驱动器的加密 (Drive-based encryption)** 的选项的加密备份会话的基本交互。

使用 AES 256 位加密和基于驱动器加密的备份会话



从加密的备份还原

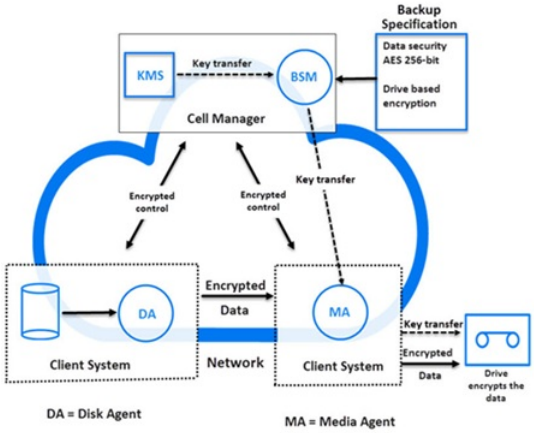
还原加密的备份时，无需额外的加密相关准备工作，因为 Data Protector 会自动获取相应的解密密钥。

Data Protector 中的数据加密与默认安全通道通信

通过将数据加密与默认安全通道通信相结合，可以轻松实现对系统最大限度的保护：

- 软件（AES 256 位）加密可在数据通过网络传输并写入介质之前对其进行加密。
- 对备份进行硬件（基于驱动器）加密可阻止介质存储和传输期间对数据进行未经授权的访问。
- 默认安全通道通信可在单元的客户机之间提供安全通信。

默认安全通道通信和数据加密显示了加密备份会话期间 Data Protector 单元中的基本交互，其中已选择“AES 256 位”加密和“基于驱动器的加密”的选项，而且启用了默认安全通道通信。



默认安全通道通信与数据加密

数据通道加密

默认情况下，通道通信以及磁盘代理与介质代理之间的通信都是加密的。因此，全局选项 **EnableSecureDataCommunication** 默认情况下设置为 1。这样，Data Protector 的代理之间的数据流便通过 SSL 传输。此全局选项使单元中的每个代理数据通信都使用 SSL，但来自未配置安全通信和不支持安全通信的主机的代理除外。
您可以通过将 **EnableSecureDataCommunication** 全局选项设置为 0 来禁用代理之间的安全数据通信。

将硬件 (基于驱动器) 加密与安全数据通道通信相结合，可以轻松实现最高的系统安全性。

通过线路启用数据加密时，请确保:

- 已启用硬件加密
- 具备多核 CPU

> **注意**使用单核并且没有硬件加密时，完成备份所需时间将比平时更长。

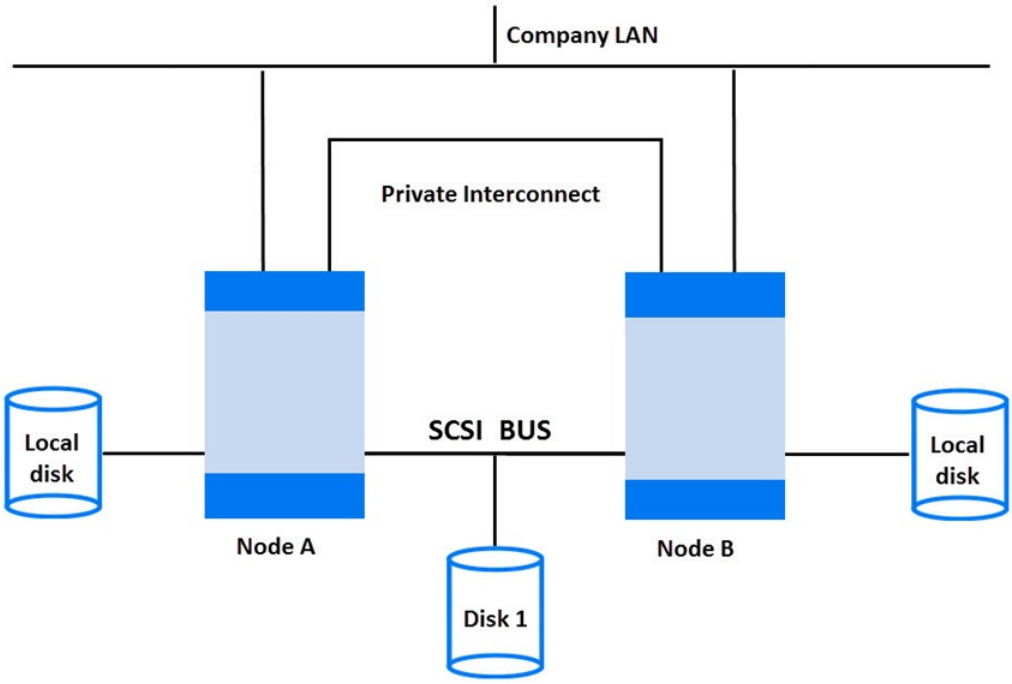
群集

“群集”是两台或更多计算机作为一个系统出现在网络上所构成的组。这组计算机作为单个系统进行管理，并且旨在：

- 确保任务关键型应用程序和资源具有尽可能高的可用性
- 容许组件故障
- 支持增删组件

Data Protector 支持群集以实现高可用性。有关更多详细信息，请参阅支持矩阵下的“平台和集成支持矩阵”。

典型群集



组件：

- 群集节点（两个或更多）
- 本地磁盘
- 共享磁盘（节点之间共享）

群集节点

“群集节点”是组成群集的多台计算机。这些计算机以物理方式连接到一个或多个共享磁盘。

共享磁盘

“共享磁盘卷”(MSCS) 或“共享卷组”(MC/SG、Veritas Cluster) 包含任务关键应用程序数据以及运行群集时所需的特定群集数据。在 MSCS 群集中，共享磁盘一次只在一个群集节点上处于活动状态。

群集网络

群集网络是连接所有群集节点的私有网络。它传输称为**群集波动信号**的内部群集数据。波动信号是一个带有时间戳的数据包，它分配在所有群集节点中。每个群集节点都会比较该数据包，并判断仍可用的群集结点，以便您正确判断“数据包”(MC/SG、Veritas Cluster) 或“组”(MSCS) 的所有权。

什么是数据包或组？

数据包 (MC/SG、Veritas Cluster) 或组 (MSCS) 是运行特定“群集感知”应用程序所需资源的集合。每个群集感知应用程序会声明各自的关键资源。

以下资源必须在每个组或数据包内定义：

- 共享磁盘卷 (MSCS)
- 共享卷组（MC/SG、Veritas Cluster）
- 网络 IP 名称
- 网络 IP 地址
- 群集感知应用程序服务

什么是虚拟服务器？

磁盘卷和卷组代表共享的物理磁盘。网络 IP 名称和网络 IP 地址是定义群集感知应用程序的“虚拟服务器”的资源。其 IP 名称和地址通过群集软件进行缓存，并映射到当前正在运行特定数据包或组的群集节点。由于组或数据包可以从一个节点切换到另一个节点，虚拟服务器可以在不同时段存在于不同计算机上。

什么是故障转移？

每个数据包或组都有其通常运行的“首选”节点。此类节点称为“主节点”。数据包或组可以移到其他群集结点（**辅助节点**之一）。将数据包或组从主群集节点传输至辅助节点的过程称为“故障转移”或切换。辅助节点在主节点故障时接受数据包或组。许多原因都可能导致故障转移：

- 主节点上的软件故障
- 主节点上的硬件故障
- 由于主节点维护，管理员有意转移所有权

在群集环境中，可以有多个辅助节点，但只能有一个主节点。

负责运行 IDB 和管理备份与还原操作的群集感知 Data Protector Cell Manager 和非群集版本相比具有诸多重要优点:

Data Protector Cell Manager 的高可用性

所有 Cell Manager 操作始终可用，因为 Data Protector 服务在群集中被定义为群集资源，并在发生故障转移时自动重新启动。

备份的自动重新启动

可以对定义备份步骤的 Data Protector 备份规范进行轻松配置，以便在 Data Protector Cell Manager 发生故障转移时重新启动其对应的会话。重新启动参数可使用 Data Protector GUI 来定义。

发生故障转移时的负载均衡

可提供一种用于操作的特殊命令行实用程序，允许在不同于 Data Protector 的应用程序执行故障转移时中止备份会话。通过 Data Protector Cell Manager 可以定义这种情况下的行为。如果备份不如该应用程序重要，Data Protector 可中止运行会话。如果备份更重要或即将结束，Data Protector 可继续会话。有关如何定义条件的详细信息，请参阅《Data Protector 帮助》索引: “群集, 管理备份”。

群集支持

Data Protector群集支持意味着：

- Data Protector Cell Manager 安装在群集内。这样的 Cell Manager 具有容错功能，并可以在故障转移后自动在单元内“重新启动”操作。

  > **注意**如果 Cell Manager 安装在群集内，其群集关键资源需要在同一群集包或组中配置为要备份的应用程序，才能自动重新启动由于故障转移而“失败备份会话”。否则，失败的备份会话必须手动重新启动。

- Data Protector 客户机安装在群集内。在这种情况下，Cell Manager (如果未安装在群集内) 不允许出现故障；单元中的操作必须手动重新启动。

至于“备份会话”(由于故障转移而失败)，故障转移后 Cell Manager 的行为是可以配置的。失败的会话可以:

- 整体重新启动
- 仅对失败对象重新启动
- 从不重新启动

有关 Data Protector Cell Manager 故障转移时备份会话行为选项的详细信息，请参阅《Data Protector 帮助》索引: “群集, 备份规范选项”。

群集环境示例

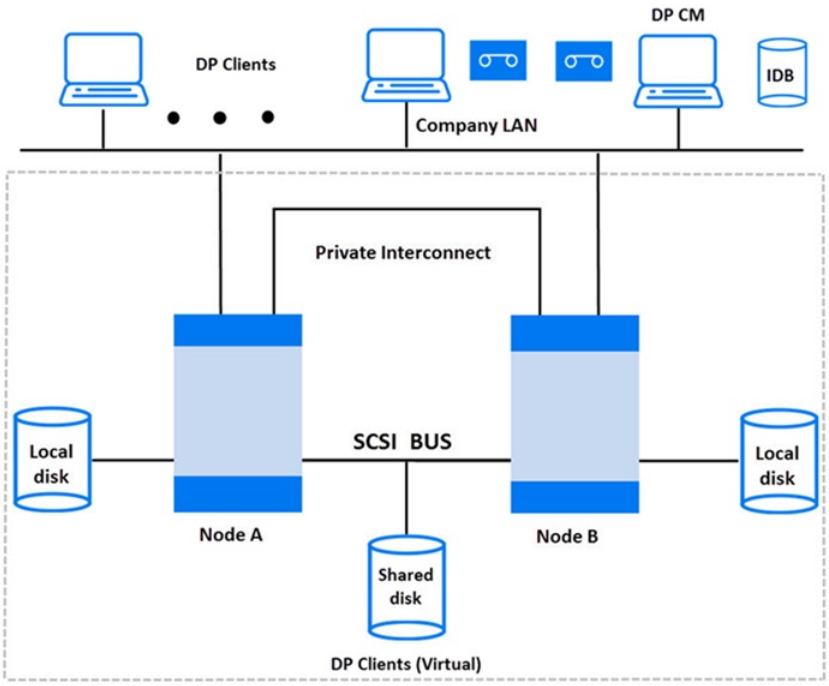
本节将给出三个群集配置示例。

安装在群集外部的 Cell Manager

在下述环境中：

- 安装在群集外部的 Cell Manager
- 连接到 Cell Manager 或 (非群集) 客户机之一的备份设备

安装在群集外部的 Cell Manager



创建备份规范时，可以查看能在群集中备份的三个或更多系统。

- 物理节点 A
- 物理节点 B
- 虚拟服务器

虚拟服务器备份

如果在备份规范中选择虚拟服务器，则备份会话将备份所选的活动虚拟主机/服务器，无论包或组当前在哪个物理节点上运行都是如此。

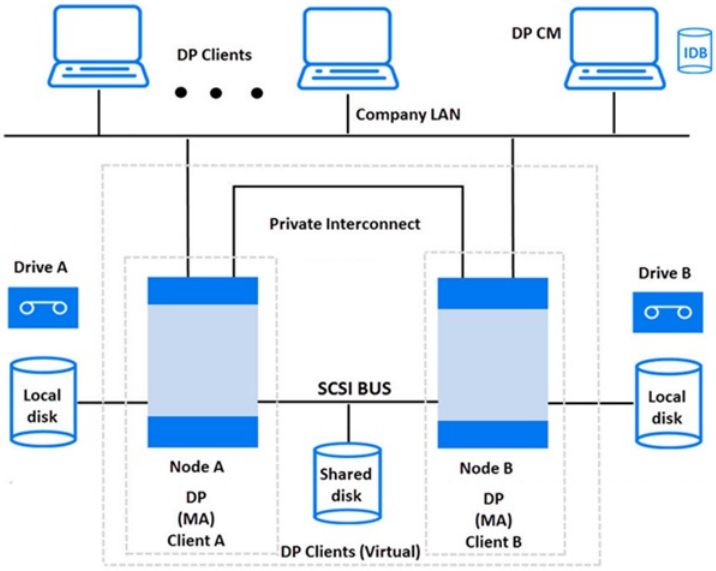
有关如何定义这些选项的详细信息，请参阅《Data Protector 帮助》索引：“群集，备份规范选项”。

Cell Manager 安装在群集外，设备连接到群集节点

在下述环境中：

- 安装在群集外部的 Cell Manager
- 备份设备连接到群集节点

Cell Manager 安装在群集外，设备连接到群集节点



创建备份规范时，可以查看能在群集中备份的三个或更多系统。

- 物理节点 A
- 物理节点 B
- 虚拟服务器

虚拟服务器备份

如果在备份规范中选择虚拟服务器，则备份会话将备份所选的活动虚拟主机/服务器，无论包或组当前在哪个物理节点上运行都是如此。

> **注意**与上一示例的区别是，每个群集结点都安装了 Data Protector 介质代理。此外，您需要使用 Data Protector 负载均衡功能。备份规范中两个设备都要包括。当负载均衡设置为 min=1 和 max=1 时，Data Protector 只使用第一台可用设备。

Cell Manager 安装在群集内，设备连接到群集节点

在下述环境中：

- Cell Manager 安装在群集内。

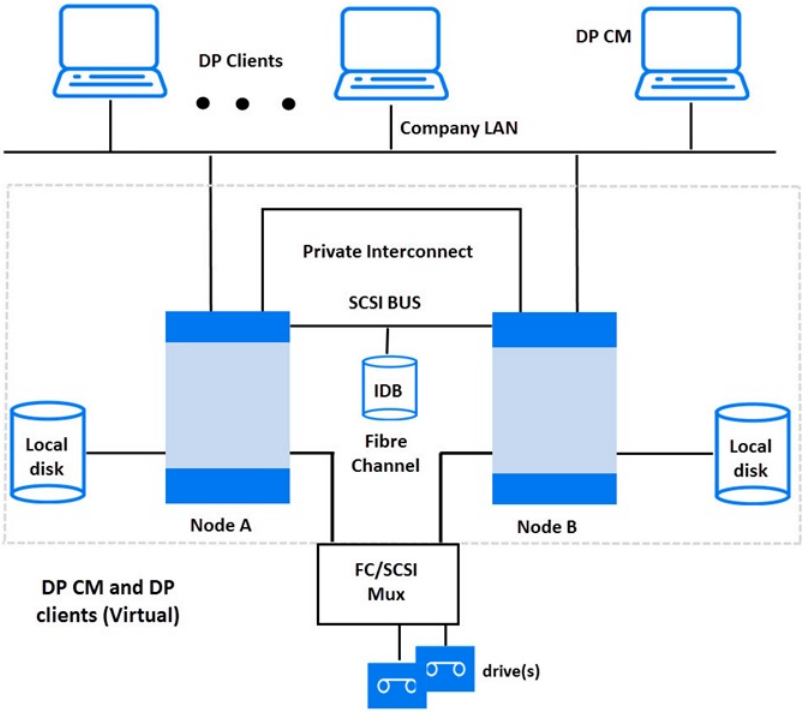
  关于 Data Protector 应用程序集成，有两种可能的方式可以用来配置 Data Protector 和此类配置下的应用程序:

  - Data Protector Cell Manager 配置为与应用程序运行于同一节点上 (无论正常操作还是故障转移中) - Data Protector 群集关键资源与应用程序群集关键资源在同一包 (Serviceguard) 或组 (Microsoft 群集服务器) 中定义。

    > **重要说明**只有在此类配置中，才可能定义在故障转移期间中止 Data Protector 会话的自动操作。

  - Data Protector Cell Manager 配置为与应用程序运行于不同节点上 (无论正常操作还是故障转移中) - Data Protector 群集关键资源与应用程序群集关键资源在不同包 (Serviceguard) 或组 (Microsoft 群集服务器) 中定义。
- 通过 FC/SCSI MUX 连接到群集共享光纤通道总线的备份设备。

Cell Manager 安装在群集内，设备连接到群集结点



创建备份规范时，可以查看能在群集中备份的三个或更多系统。

- 物理节点 A

- 物理节点 B
- 虚拟服务器

虚拟服务器备份

如果在备份规范中选择虚拟服务器，则备份会话将备份所选的活动虚拟主机/服务器，无论包或组当前在哪个物理节点上运行都是如此。

> **注意**群集不支持包含共享磁带的 SCSI 总线。要使介质代理也具有高可用性，可以使用“光纤通道”技术作为设备的接口。设备本身在此配置下不具有高可用性。

该配置允许使用以下功能：

- 可自定义在 Cell Manager 发生故障转移时自动重新启动备份。

  Data Protector 备份规范可配置为在 Cell Manager 发生故障转移时重新启动。重新启动参数可使用 Data Protector GUI 来定义。

- 故障转移时的系统负载控制。

  可提供用于定义 Data Protector 在故障转移时的行为的复杂控制功能。对于该目的，提供了特殊命令 omniclus 。Cell Manager 允许管理员定义这种情况下的行为。

  - 如果备份不如刚切换到备份系统的应用程序重要，Data Protector 可中止运行会话。
  - 如果备份更重要或即将结束，Data Protector 可继续会话。

此外，Data Protector 群集 Cell Manager/客户机可以与 P9000 XP 磁盘阵列系列环境集成，实现具备极高可用性的备份环境。

完整备份、增量备份与合成备份

Data Protector 提供两种基本的文件系统备份类型：完整备份和增量备份。

完整备份保存文件系统中选择备份的所有文件。增量备份只保存自上次完整备份或增量备份以来更改过的那些文件。本节将提示如何选择备份类型，并说明备份类型对备份策略的影响。

完整备份与增量备份的比较

	完整备份	增量备份
资源	需要比增量备份更多的时间，并且需要更多介质空间。	仅备份自上次备份以来发生的更改，这样需要的时间和介质空间较少。
设备处理	如果使用只有一个驱动器的独立设备，则在备份不适合单个介质时需要手动更换介质。	但备份不大可能需要额外的介质。
还原	可实现简单且快速的还原。	由于所需的介质较多，因此还原需要较长时间。
对 IDB 的影响	占据 IDB 中的更多空间。	占用 IDB 中的空间较少。

Data Protector 还可以对联机数据库应用程序进行增量/差异备份。这些随应用程序的不同而异。例如，在 Sybase 上，此类备份称为事务备份（自上次备份以来对修改过的事务日志的备份）。

请注意，增量备份概念与日志级别概念无关，后者定义写入 IDB 的信息量。

> **注意**对于 Data Protector 应用程序集成，有许多其他类型备份（如分割镜像备份、快照备份和数据移动器备份）可用。

完整备份

完整备份始终会备份所有选中对象，即使自上次备份以来没有更改过这些对象。

合成备份

合成备份是一种高级备份解决方案，无需运行定期的完整备份。而是运行增量备份，然后与完整备份合并成新的合成完整备份。

增量备份

增量备份备份自上次仍受保护的（完整或增量）备份以来的更改。必须存在某对象的完整备份（相同的客户机名、装载点和描述），才能对该对象进行增量备份。

增量备份取决于上次完整备份。如果您指定某增量备份，而无受保护的完整备份，则将执行完整备份。

传统增量备份

运行特定备份对象的增量备份前，Data Protector 会将备份对象中的树与该对象的有效还原链中的树进行比较。如果树不匹配（例如，选中了备份对象中上次备份时尚不存在的其他目录进行备份，或者存在备份对象相同、树不同的多个备份规范），将自动执行完整备份。这就确保备份了自上次相关备份以来更改过的所有文件。

对于传统的增量备份，确定某文件自上次备份以来有没有更改的主要标准是该文件的修改时间。但是，如果文件被重命名、移到新位置或改变了部分属性，其修改时间并不会变化。因此，该文件在传统的增量备份中不一定会被备份。而是在下次完整备份中备份此类文件。

增强型增量备份

增强型增量备份能可靠检测和备份重命名过的、移动过的和属性更改过的文件。

部分选择备份的树变更时，使用增强型增量备份就无需对整个备份对象进行完整备份。例如，如果自上次备份以来选择了其他目录进行备份，则将执行该目录（树）的完整备份，而对剩余部分进行增量备份。

使用增强型增量备份是合成备份的先决条件。

使用更改日志提供程序的增量备份

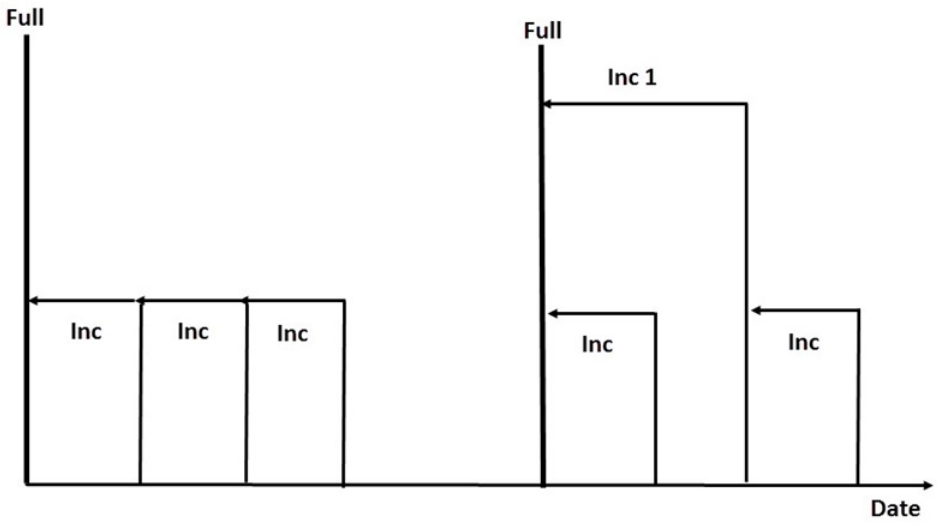
可以使用 Windows NTFS 更改日志提供程序执行增强型增量备份或传统的增量备份。更改日志提供程序在 Windows 更改日记中搜索更改过的文件列表，而不是执行费时的文件树遍历。因为更改日记检测和记录 NTFS 卷上对文件和目录所作的全部更改，Data Protector 可将它用作跟踪机制，以生成自上次完整备份以来修改过的文件的列表。这可提高增量备份速度，特别是在包含上百万个文件、其中只有少数文件被修改过的环境中，可以消除不必要的完整备份。

增量备份的类型

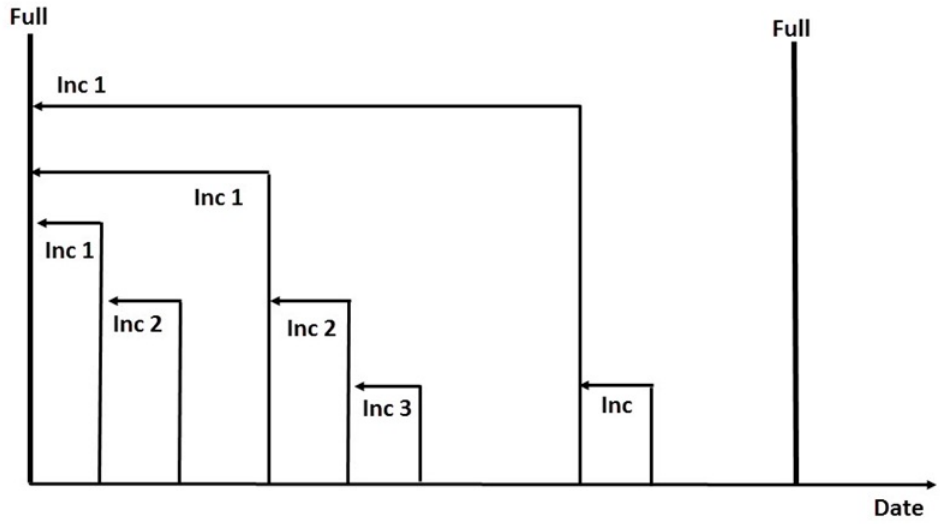
Data Protector可提供不同类型的增量备份：

增量	简单的增量备份，如增量备份所示，是基于仍受保护的上次备份，后者可以是完整备份或增量备份。
增量1-9	“分级增量备份”，如分级增量备份中所示，取决于低一级别仍受保护的上一次备份。例如，1 级增量备份保存自上次完整备份以来的所有更改，而 5 级增量备份保存自上次 4 级增量备份以来的所有更改。1-9 级增量备份永不引用现有增量备份。

增量备份



分级增量备份



备份运行的相对引用显示了各种备份类型的备份运行的相对引用。有关完整说明，请参见该表后的文字。

备份运行的相对引用

1	完整	<----	增量 1				
2	完整	<----	<----	<----	2 级增量备份		
3	完整	<----	增量 1	<----	2 级增量备份		
4	完整	<----	增量				
5	完整	<----	增量 1	<----	增量		
6	完整	<----	增量 1	<----	2 级增量备份	<----	增量
7	完整	<----	增量 1	<----	增量	<----	增量
8	完整	<----	增量 1	<----	3 级增量备份		
9	完整	<----	增量 1	<----	2 级增量备份	<----	3 级增量备份
10	完整	<----	<----	<----	2 级增量备份	<----	3 级增量备份
11	完整	<----	<----	<----	<----	<----	3 级增量备份

如何理解备份运行的相对引用

- 备份运行的相对引用中的行彼此独立，显示不同的情况。
- 备份的老化程度从右到左递增，因此最左边的备份是最旧的，最右边的备份是最近的备份。
- 完整备份和 X 级增量备份代表同一所有者的仍受保护对象。未保护的任何现有 X 级增量备份都可用于还原，但不视为后续备份运行的引用。

示例

- 在第二行中，有一个完整备份（仍受保护）和 2 级增量备份正在运行。没有 1 级增量备份，因此备份执行为 1 级增量备份。
- 在第五行中，有一个完整备份（1 级增量备份）和另一个增量备份正在运行。Data Protector 将当前运行的备份引用到上一个增量备份，即 1 级增量备份。
- 在第八行中，3 级增量备份执行为 2 级增量备份，在第十一行中，3 级增量备份执行为 1 级增量备份。

备份生成

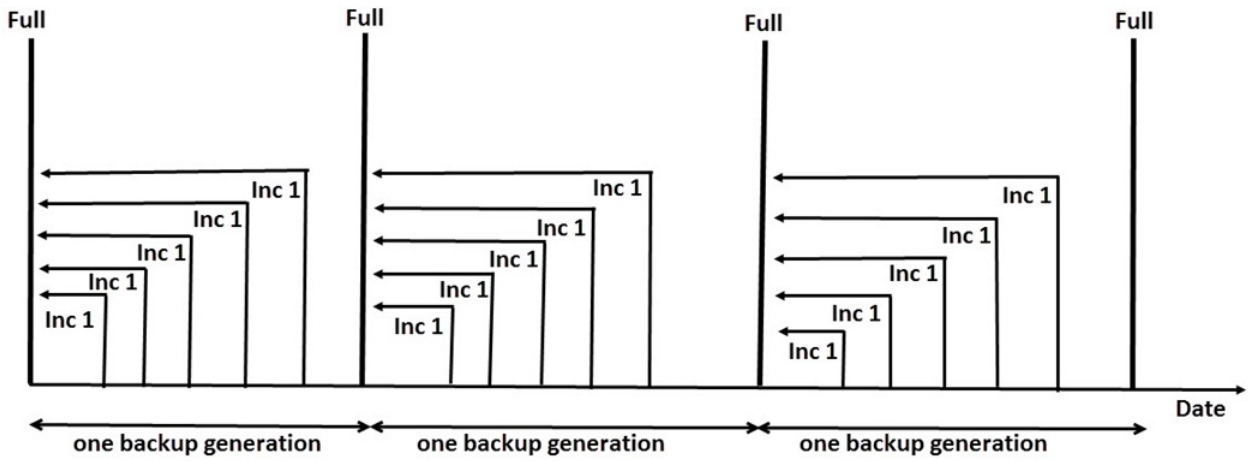
Data Protector 提供时间/日期相关的保护模型。如果已进行定期备份，则很容易将基于生成的备份模型映射到基于时间的模型。

什么是备份生成？

备份生成（如备份生成所示）代表完整备份以及基于该完整备份的所有增量备份。完成下次完整备份时，将创建新的备份生成。

备份生成可帮助您了解备份的数据有多少版本。为成功进行时间点还原，需要至少一个备份生成（完整备份以及到该时间点为止的所有增量备份）。根据贵公司的数据保护政策，保留多个备份生成（例如三个）。

备份生成



配置 Data Protector 以自动保留所需的备份生成数，这是通过以下操作实现的：选择适当的数据和编目保护持续时间，并安排无人看管备份（完整和增量）。

例如，如果有每周的完整备份和每日的分级增量备份，则要保持三个备份生成，请将数据保护指定为 7*3+6=27 天。备份生成代表完整备份以及到下次完整备份之前的所有增量备份：因此，公式中的 6 代表属于第三次备份生成的下次，第四次，备份生成之前的增量备份。

可以通过适当的池使用概念设置自动介质循环（对于保护时间已到期的介质）。

合成备份

本节将介绍合成备份的概念并说明 Data Protector 提供的合成备份解决方案。

概述

随着数据量的增加和备份时间窗口的缩短，执行完整备份往往会在时间和存储空间方面遇到问题。另一方面，许多增量备份也经常出现问题，因为每个增量备份都会增加执行还原所需的时间。

由于性能高、容量大以及逐步下降的磁盘价格，备份到磁盘日渐普及，这促使新的机会随之出现。业界的要求是尽可能缩短备份的时间窗口，最小化生产服务器和网络上的负载，并且能够快速还原。合成备份可满足这些要求。

合成备份是一种高级备份解决方案，它将生成“合成完整备份”，在数据方面与传统的完整备份别无二致，但不会对生产服务器或网络造成压力。合成完整备份是从之前的完整备份和任意数量的增量备份中创建的。

执行合成备份，就无需运行常规的完整备份。而是运行增量备份，然后与完整备份合并成新的合成完整备份。此过程可以无限重复，不再需要运行完整备份。

在还原速度方面，合成完整备份与传统的完整备份相当。还原链只由一个元素构成，因此还原做到了尽可能快速简单。

合成备份的优点

合成备份具有以下优点：

- 无需进行完整备份。进行初始的完整备份后，只需执行增量备份，从而显著缩短了备份所需的时间。
- 备份对象的合并将在设备服务器上执行，对生产服务器或网络不会造成压力。
- 有一种称为虚拟完整备份的合成备份甚至更为高效。虚拟完整备份用指针合并数据，消除了不必要的数据复制。
- 从合成完整备份还原与从传统完整备份还原一样快，因为都无需从增量备份获取数据。这样，就无需在还原链中从每个增量备份读取数据，如果用的是磁带设备，也就无需装载和卸载多个介质以及寻找对象版本。

Data Protector 合成备份的工作原理

您可以通过 Data Protector合成备份将完整备份与任意数量的增量备份合并成新的合成完整备份。

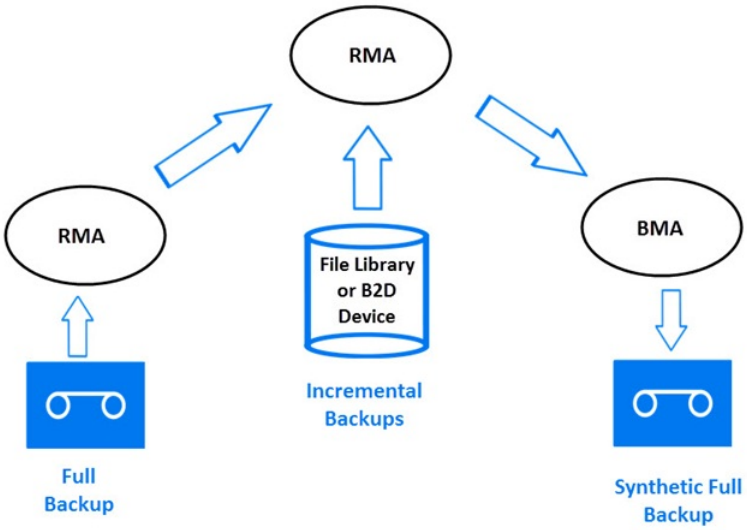
为进行合成备份，需要使用增强型增量备份。执行完整备份和增量备份之前，必须打开增强型增量备份。

合成完整备份可以从写入磁盘或磁带设备的完整备份与写入基于磁盘的设备、Data Protector文件库或 B2D 设备 (智能缓存除外) 的增量备份创建，例如 StoreOnce 或数据域设备。合成完整备份可以再次写入磁盘或磁带设备。

如果所有备份 (完整和增量) 都写入使用分布式文件介质格式的同一文件库，就可以使用一种称为“虚拟完整备份”的更高效的合成备份。此解决方案用指针合并数据，而非复制数据。因此，合并所用时间更短，并且避免了对数据不必要的复制。

下图说明了合成备份和虚拟完整备份的概念。其中显示了如何从完整备份和任意数量的增量备份中创建合成完整备份或虚拟完整备份。

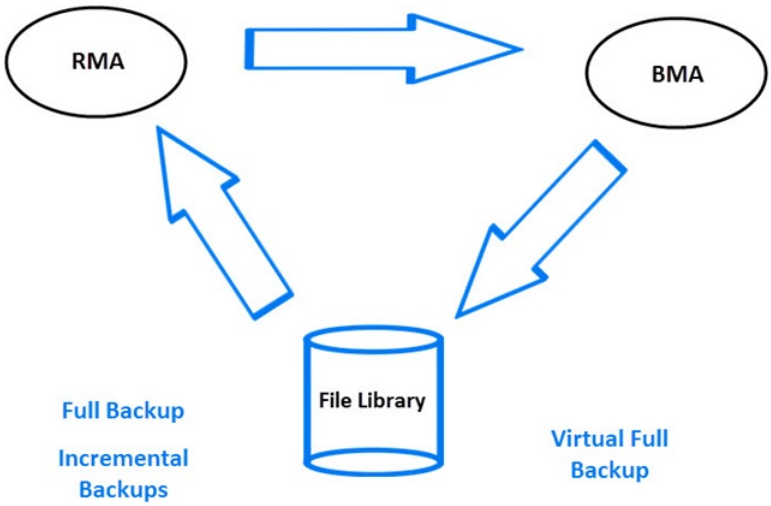
合成备份



合成备份显示了如何创建合成完整备份。还原介质代理 (RMA) 从备份介质（可以是磁带或磁盘）读取完整备份。然后将数据发送到其他 RMA，后者将从文件库或 B2D 设备（Smart Cache 除外）读取增量备份并合并数据。合并后的数据将随机发送到备份介质代理 (BMA)，备份介质代理将合成完整备份写入备份介质（可以是磁带或磁盘）。

随后，合成完整备份通常将与后续增量备份合并，以形成新的合成备份。该过程可以在每次增量备份后或按所需时间间隔无限次重复。

虚拟完整备份



虚拟完整备份显示了如何创建虚拟完整备份。对于此类备份，所有备份都位于使用分布式文件介质格式的单一文件库中。还原介质代理 (RMA) 将读取完整备份和增量备份的信息，并生成虚拟完整备份的数据。生成的数据会发送到备份介质代理 (BMA)，后者将在文件库中创建虚拟完整备份。

合成备份和介质空间消耗

如果频繁执行合成备份并保留源文件，这通常意味着会消耗备份介质上可观的空间。但是，如果执行虚拟完整备份，则可将备份介质空间消耗最小化。

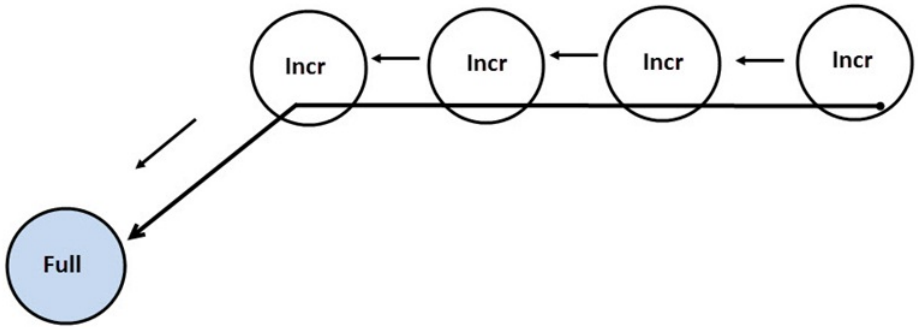
对于虚拟完整备份，空间消耗主要取决于要备份的文件的大小。如果文件明显大于所用的块大小，则虚拟完整备份与普通的合成备份相比可以最大

限度地节省空间。如果文件小于块大小，则节省的空间就很少了。

还原和合成备份

从合成完整备份进行还原等同于从传统完整备份进行还原。下图显示了不同的情况（假设您需要将数据还原到最近的可用状态）。在所有示例中，对于备份对象都存在一个完整备份和四个增量备份。区别在于如何使用合成备份。

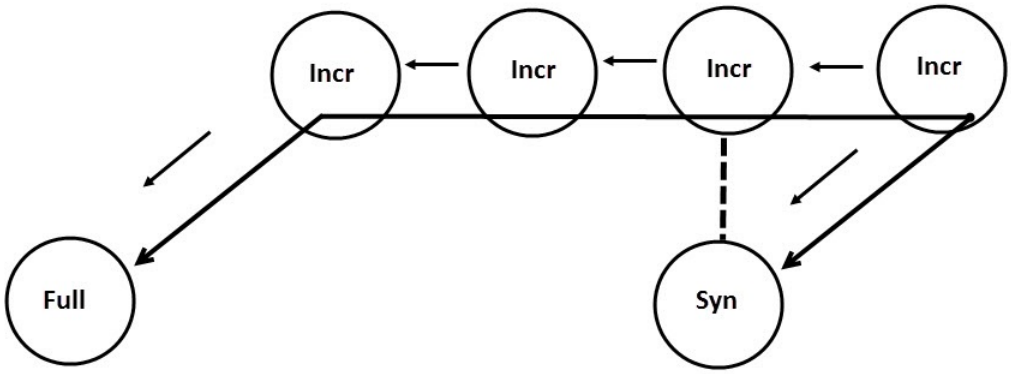
完整备份和增量备份



在完整备份和增量备份中，执行了传统备份。要还原到最近的可用状态，需要完整备份和全部的四个增量备份。还原链由五个元素组成，它们通常位于不同的介质上。

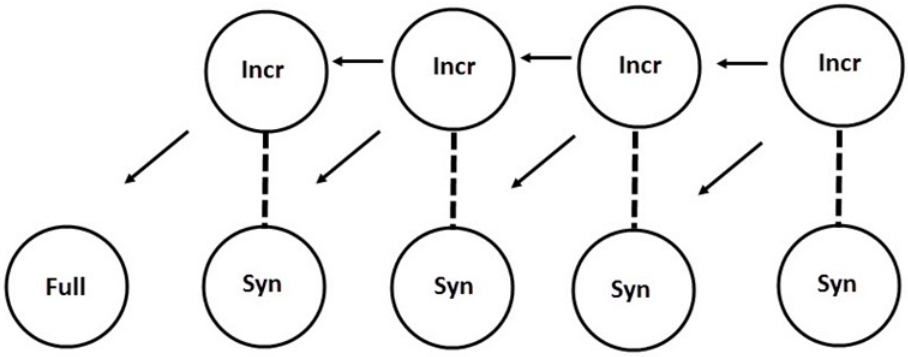
此类还原可能需要耗费可观的时间，因为必须读取每个增量备份。如果使用磁带设备，则时间将用在装载和卸载若干介质以及寻找要还原的对象版本上。

合成备份



在合成备份中，存在合成完整备份，默认情况下用它进行还原。还原链只由两个元素组成，即合成完整备份和后续增量备份。与不用合成完整备份相比，该还原过程大为简化且更快了。图中显示了两种可能的还原链。

定期合成备份



定期合成备份显示了在每次增量备份后执行合成备份的情况。通过该策略可以使用最简单、最快速的方式将数据还原到最近的可用状态，或者将其还原到已备份的任何较早时间点。还原只需一个元素，即所需时间点的合成完整备份。

合成备份和对象复制

DP202005_synthetic and object copy.png

在合成备份和对象复制中，将执行合成备份，然后进行复制。这可增强安全性。要将数据还原到最近的可用状态，可使用所示的三种不同还原链中的任意一个。默认情况下，Data Protector 选择最优还原链，它通常包括合成完整备份或其副本。如果缺少介质、发生介质错误或类似情况，则将使用备用还原链。

数据保护周期如何影响从合成备份还原

传统完整备份的数据保护和合成完整备份前的所有增量备份并不会妨碍成功的还原。

默认情况下，将使用备份链中最近一次的合成完整备份进行还原，不考虑之前的备份是否仍有效，也不考虑其保护是否已过期以及对象是否已从 IDB 中删除。

为增强安全性，请将数据保护设置为永久，这样就不会意外覆盖介质上的数据。

考虑还原

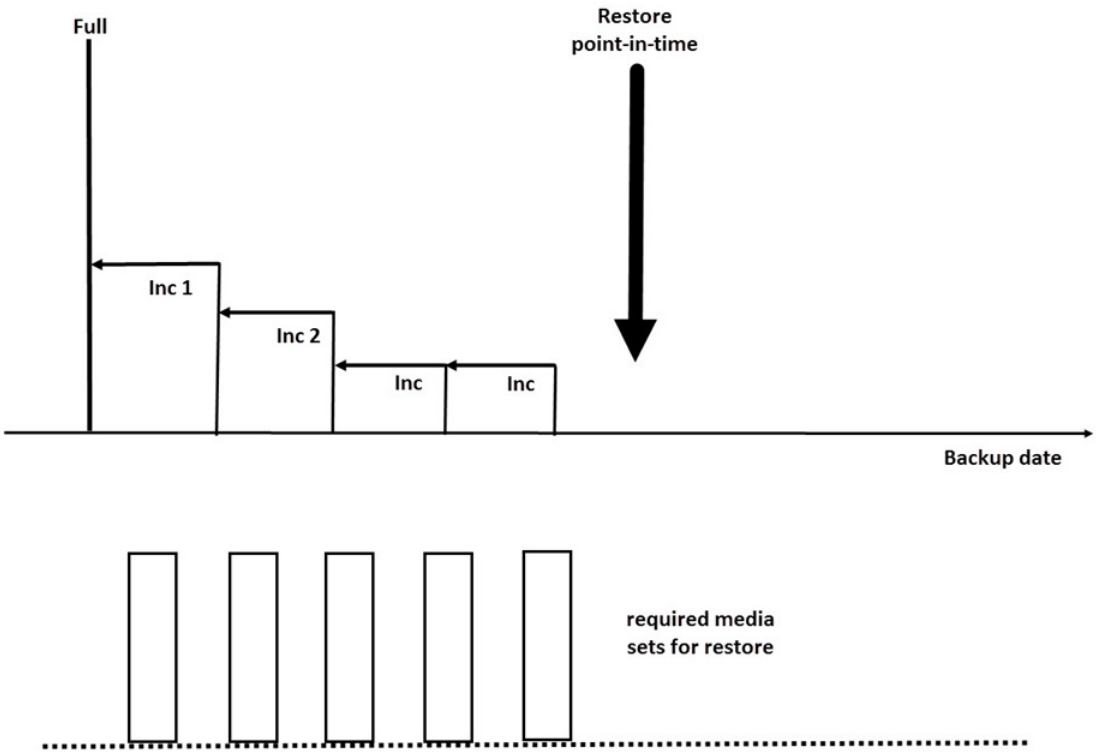
要还原最新数据，您需要来自上次完整备份和后续增量备份的介质。因此，拥有的增量备份越多，需要处理的介质也越多。此时使用独立设备就不方便，并且还原过程可能持续较长时间。

如从简单和分级增量备份还原所需的介质所示，使用简单和分级增量备份，需要访问以前完成的全部五个**介质集**，最多可达到并包括完整备份。这里所需的介质空间最小，但还原起来很复杂。所需的一组介质集也称为“还原链”。

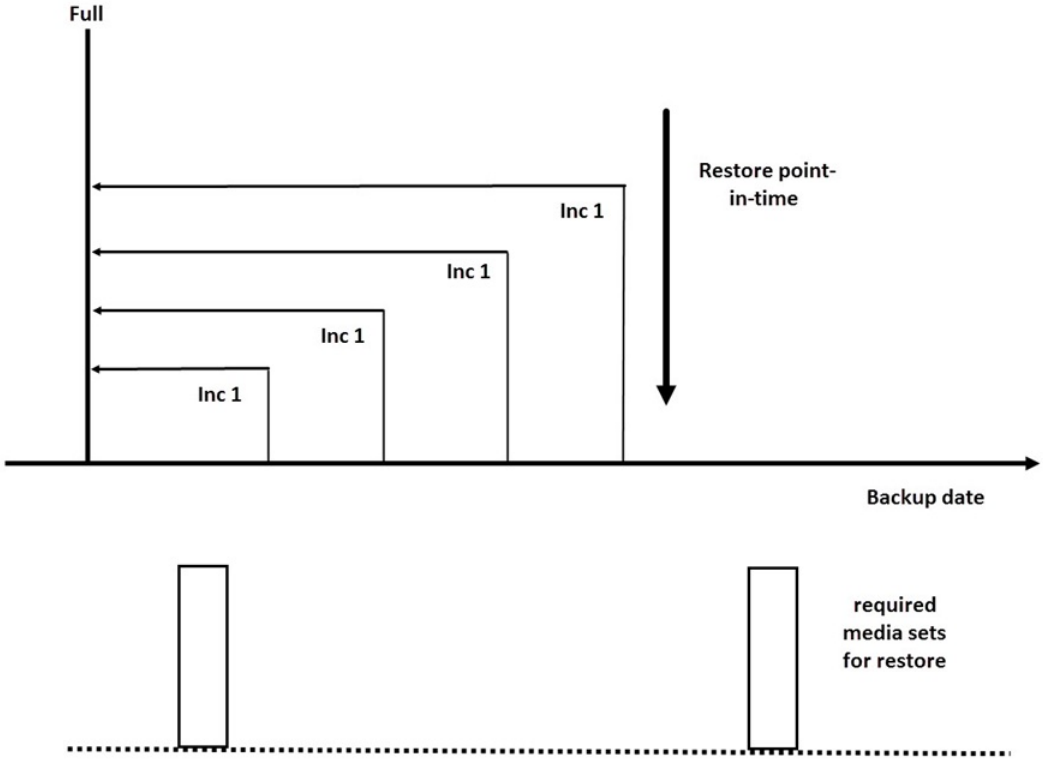
> **提示**使用 Data Protector“只可追加增量”选项保存来自同一介质集上的完整备份和增量备份 (符合同一备份规范) 中的数据。

从分级增量备份还原所需的介质指出了增量备份概念的另一常见用途。这里介质上需要的空间略大。还原至所需时间点只需要访问两个介质集。请注意，此类还原不依赖任何先前的 1 级增量备份介质集，除非移动了所需的还原时间点。

从简单和分级增量备份还原所需的介质



从分级增量备份还原所需的介质



请注意，您必须设置适当的数据保护，以便获取还原所需的所有完整备份和增量备份。如果未正确设置数据保护，可能会得到破损的还原链。

保留备份数据和有关数据的信息

通过 Data Protector 可指定已备份数据在介质上保留多久（数据保护）、关于已备份数据的信息在 IDB 中保留多久（编目保护），以及 IDB 中保留的信息级别（日志记录级别）。

您可以在 IDB 中为已备份数据和这些数据的备份信息单独设置保护。复制介质时，可以为副本指定不同于原始介质的保护期限。

Data Protector 内部数据库

还原的性能部分取决于能多快找到还原所需的介质。默认情况下，这些信息存储在 IDB 中，以实现最佳还原性能，同时便于浏览要还原的文件和目录。但是，把所有备份的全部文件名放在 IDB 中并保存很久，会使 IDB 变大到无法管理的程度。

通过 Data Protector 可在 IDB 增长与恢复的方便性之间进行权衡，这是通过让您指定独立于数据保护的编目保护来实现的。例如，您可以将编目保护设置为 4 周，以实现一种能够方便快速地还原备份后 4 周内的数据的策略。此后，仍可用不太方便的方法进行还原，直到数据保护到期，比如说 1 年后。这就显著减小了 IDB 中所需的空间。

数据保护

什么是数据保护？

通过 Data Protector 可指定一段时间，在此期间，介质上的数据不会被 Data Protector 覆盖。您可以用绝对日期或相对日期来指定保护。

可以在 Data Protector 的不同部分中指定数据保护。有关详细信息，请参阅《Data Protector 帮助》索引: “数据保护”。

如果配置备份时不更改**数据保护**备份选项，就会永久保护这些数据。请注意，如果不更改这一保护，备份需要的介质数就会持续增加。

编目保护

Data Protector 在 IDB 中保存有关已备份数据的信息。由于有关已备份数据的信息在每次备份完成时都会写入 IDB，IDB 会随着备份次数和备份大小的增加而变大。在 Data Protector 中，通过编目保护指定有关已备份数据的信息在恢复期间可供用户浏览的时间长度。编目保护过期后，Data Protector 会在一次后续备份中覆盖 IDB 中（而非介质上）的这些信息。

您可以用绝对日期或相对日期来指定保护。

如果配置备份时不更改**编目保护**备份选项，则有关已备份数据的信息与数据保护具有相同的保护持续时间。请注意，如果不更改这一保护，IDB 会随着每次备份时添加的新信息而不断变大。

有关编目保护设置如何影响 IDB 增长和性能的详细信息，请参阅《Data Protector 帮助》。

日志记录级别

日志记录级别决定在备份期间写入 IDB 的关于文件和目录的详细信息量。无论备份期间使用何种日志记录级别，您始终可以恢复数据。

Data Protector 提供了 4 种日志记录级别，用于控制写入 IDB 的文件和目录详细信息的总量。。

浏览要还原的文件

IDB 保存着有关已备份数据的信息。通过这些信息可以使用 Data Protector 用户界面浏览、选择和启动文件的还原。只要介质仍可用，没有这些信息也可以还原数据，但您必须知道要使用哪些介质以及需要还原的内容，例如准确的文件名。

IDB 还保存了有关介质上的实际数据多久以内不会被覆盖的信息。

数据保护、编目保护和日志记录级别策略影响还原时数据的可用性和访问时间。

启用文件浏览和快速还原

要快速还原文件，编目中已备份数据和介质上受保护数据的信息都必须存在。通过编目中的信息可以使用 Data Protector 用户界面浏览、选择和启动文件的还原，并且可以通过 Data Protector 快速定位备份介质上的数据。

启用文件还原但不启用浏览

编目保护过期但数据保护仍有效时，您不能在 Data Protector 用户界面中浏览文件，但如果知道文件名和介质，仍可恢复数据。恢复会比较慢，因为 Data Protector 不知道所需数据在介质上的位置。您也可以把介质导入回 IDB，从而重新在编目中建立已备份数据的信息，然后开始还原。

用新数据覆盖已备份的文件

数据保护到期后，介质上的数据会在一次后续备份中被覆盖。在此之前，您仍可以从该介质还原数据。

> **提示**将数据保护设置为必须保存数据的总时间，例如 1 年。
>
> 将编目保护设置为希望能用 Data Protector 用户界面浏览、选择和快速恢复文件的总时间。

从单元导出介质

从 Data Protector 单元导出介质会从 IDB 删除介质上与已备份数据有关的所有信息和介质本身。您不能使用 Data Protector 用户界面从导出的介质浏览、选择或还原文件。需要将介质重新读取回（或添加回）Data Protector 单元。该功能是将介质移到其他单元所必需的。

在导出介质过程中，与介质相关的加密信息也会导出并以 .csv 文件的形式置于导出目录中。将任何加密备份重新导入或导入其他单元后，需要该文件才能对其进行还原。

将 WORM 介质导入到单元

将介质导入到 Data Protector 单元会将介质上与已备份数据有关的所有信息和介质本身添加到 IDB。您可以使用 Data Protector 用户界面从导入的介质浏览、选择或还原文件。将其上的数据保护已过期的介质导入 Data Protector 单元时，该介质上的数据会在一次后续备份会话中被覆盖。

如果是 WORM 介质，则不允许覆盖介质上的数据且该介质将变为不可附加。要允许 Data Protector 向 WORM 介质附加数据，请将数据保护日期设置为向介质写入新数据的日期之后以防止覆盖现有数据。

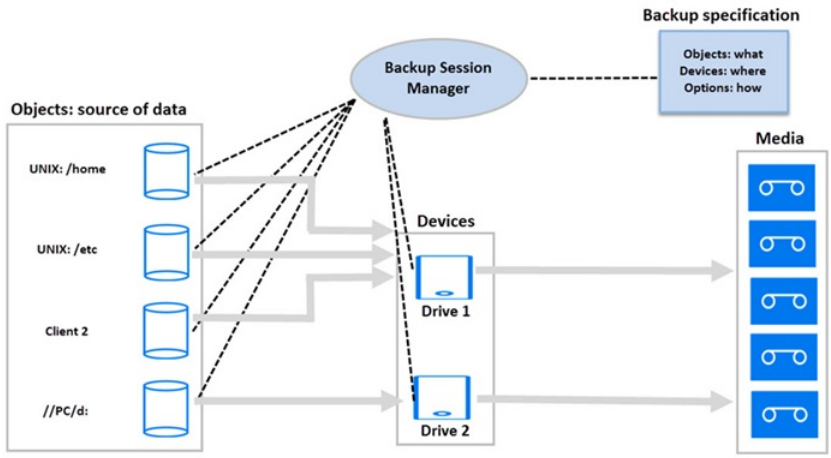
备份数据

备份数据由以下若干步骤或全部步骤组成：

- 选择要从哪个客户机系统备份什么 - 数据源。
- 选择备份到哪里 - 目标。
- 选择将同一批数据写入其他介质集 - 镜像。
- 选择如何备份 - 备份选项。
- 为自动操作安排备份。

您可以在创建备份规范时指定所有这些设置。

备份会话



在指定时，Data Protector 会根据备份规范启动备份会话。数据源指定为对象列表（例如 UNIX 上的文件系统或 Windows 系统上的磁盘驱动器），目标是指定的（磁带）设备。在备份会话期间，Data Protector 会读取对象，通过网络传输数据，并将数据写入设备中的介质。备份规范会命名要使用的设备。它还可以指定介质池。如果未指定介质池，则将使用默认介质池。备份规范可以简单定义成将磁盘备份到独立 DDS 驱动器，或复杂定义成将 40 个大型服务器备份到带有 8 个驱动器的 Silo 磁带库。

创建备份规范

通过备份规范，您可以将要备份的对象分组到具有相同特征（例如使用的设备、备份类型和备份会话选项）的组内。

可以使用 Data Protector 用户界面配置备份规范。您需要知道要备份的内容、要创建的镜像数，以及要用于备份的介质和设备，还可以选择所需的特定备份行为。Data Protector 提供的默认行为在绝大多数情况可以满足使用要求。您可以使用 Data Protector 备份选项自定义备份行为。

Data Protector 可通过在备份时发现磁盘，在所有磁盘连接到客户机时备份该客户机。

> ⚠ **警告**仅应使用 Data Protector **GUI 或 CLI 命令**修改备份规范。不支持手动修改备份规范文件。

选择备份对象

Data Protector 使用术语“备份对象”作为备份单位，它包含从一个磁盘卷 (逻辑磁盘或装载点) 选择备份的所有项目。所选项目可以是任意数量的文件、目录、整个磁盘或装载点。此外，备份对象也可以是数据库实体或磁盘映像。

备份对象由以下各项定义：

- 客户机名称：备份对象所在的 Data Protector 客户机的主机名。
- 装载点：备份对象所在的客户机目录结构中的访问点（Windows 上的驱动器，UNIX 上的装载点）。
- 说明：使用相同的客户机名称和装载点唯一地定义备份对象。
- 类型：备份对象类型，例如文件系统或 Oracle。

定义备份对象的方式，对于理解增量备份如何完成很重要。例如，如果备份对象的描述变了，就视为新的备份对象，因此将自动执行完整备份而非增量备份。

备份选项示例

您可以指定每个备份对象的备份选项来自定义该对象的备份行为。下面是可以指定的备份选项的示例：

- 信息的日志记录级别记录在 IDB 中。

  Data Protector 提供了 4 种级别，用于控制 IDB 中存储的文件和目录详细信息的总量：

  - 全部记录
  - 记录文件
  - 日志目录
  - 不记录任何内容

  请注意，更改所存储信息的级别，会影响还原时使用 Data Protector 用户界面浏览文件的能力。

- 自动负载均衡

  来自指定列表的动态设备分配。

  Data Protector 会动态判断哪个对象（磁盘）应备份到哪个设备。

- Pre-exec 和 post-exec 脚本

  为实现一致备份对客户机执行的操作。

- 数据安全性

  应用于数据的安全性级别。

  Data Protector为已备份数据提供三种安全性级别：

  - 无
  - AES 256 位
  - 编码

您还可以指定要从备份排除的目录，或只备份特定目录。也可以在添加磁盘时进行备份。因此，备份是完全可配置而动态的。

备份会话

备份会话是从客户机系统将数据备份到介质的过程。备份会话始终在 Cell Manager 系统上运行。备份会话是基于备份规范的，在备份运行时启动。

在备份会话期间，Data Protector 会用默认或自定义行为备份数据。

对象镜像

对象镜像是在备份会话期间创建的备份对象的其他副本。创建备份规范时，您可以选择创建一个或多个特定对象的镜像。使用对象镜像可提升备份的容错能力，并实现多地点保管。但是，备份会话中的对象镜像会增加备份所需的时间。

介质集

备份会话的结果就是在介质或介质集上备份数据。每个备份会话都会生成一个或多个介质集，这取决于您是否使用对象镜像执行备份。根据介质池的使用，几个会话可以共享同一介质。还原数据时，您需要知道要从哪个介质中还原数据。Data Protector 将此信息保存在编目数据库中。

备份类型和安排的备份

计划策略定义备份何时开始，以及备份类型 (完整或增量)。考虑完整备份与增量备份的区别。

您可以在配置安排的备份时，结合使用完整备份和增量备份。例如，可以在每个星期日运行完整备份，在每个工作日运行增量备份。要备份大量数据并避免完整备份导致的高容量峰值冲击，请使用交错排列方法。

安排备份、备份配置和会话

备份配置

计划备份时，该备份规范中指定的所有对象都会在计划的备份会话中备份。

对于每个单次或定期安排的备份，可以指定以下选项：**备份类型 (Backup type)**（完整或增量）、**网络负载 (Network load)** 和**备份保护 (Backup protection)**。使用分割镜像或快照备份时，如果是 ZDB 到磁盘或 ZDB 到磁盘 + 磁带（启用了即时恢复），则需指定**分割镜像/快照备份**选项。对于 ZDB 到磁盘，将忽略备份类型（执行完整备份）。

在一种备份规范内，您可以安排 ZDB 到磁盘和 ZDB 到磁盘 + 磁带的备份，并为每个单次或定期安排的备份指定不同数据保护期限。

备份会话

当备份会话启动时，Data Protector 会尝试分配所有必需资源，如设备。只要所需的最少资源尚不可用，会话将一直列队等待。Data Protector 尝试在特定时段（超时）内分配资源。用户可以配置超时时间。如果资源在超时后仍不可用，则将中止会话。

优化备份性能

为优化 Cell Manager 的负载，Data Protector 在默认情况下会同时启动五个备份会话。如果同时安排的会话数目超出负载，超出的会话会列队等候，等待其他会话完成后再启动。

计划建议和技巧

“完整备份、增量备份与合成备份”和“保留备份数据和有关数据的信息”两节介绍了备份生成、数据保护和编目保护的概念。

本节将通过几个示例说明备份安排，并给出有效安排备份的一些建议，将这些概念结合起来。

何时安排备份

一般将备份安排在用户活动最少时进行，通常是在夜里。完整备份所需时间最久，因此将其安排在周末。

可以考虑将不同客户机（备份规范）的完整备份安排在不同日子，如交错排列完整备份所示。

> **注意**Data Protector 提供的报告显示了从设备使用的观点来看可用的时间空档。这样您就可以选择一个时间，在这段时间内，要使用的设备不太可能因为用于现有备份而被占用。

交错排列完整备份

在同一天执行所有系统的完整备份可能会导致网络负载和时间窗口方面的问题。为避免这些问题，请对完整备份采用交错排列方法。

交错排列方法

	星期一	星期二	星期三	...
system_grp_a	完整	增量 1	增量 1	...
system_grp_b	增量 1	完整	增量 1	...
system_grp_c	增量 1	增量 1	完整	...

为还原而优化

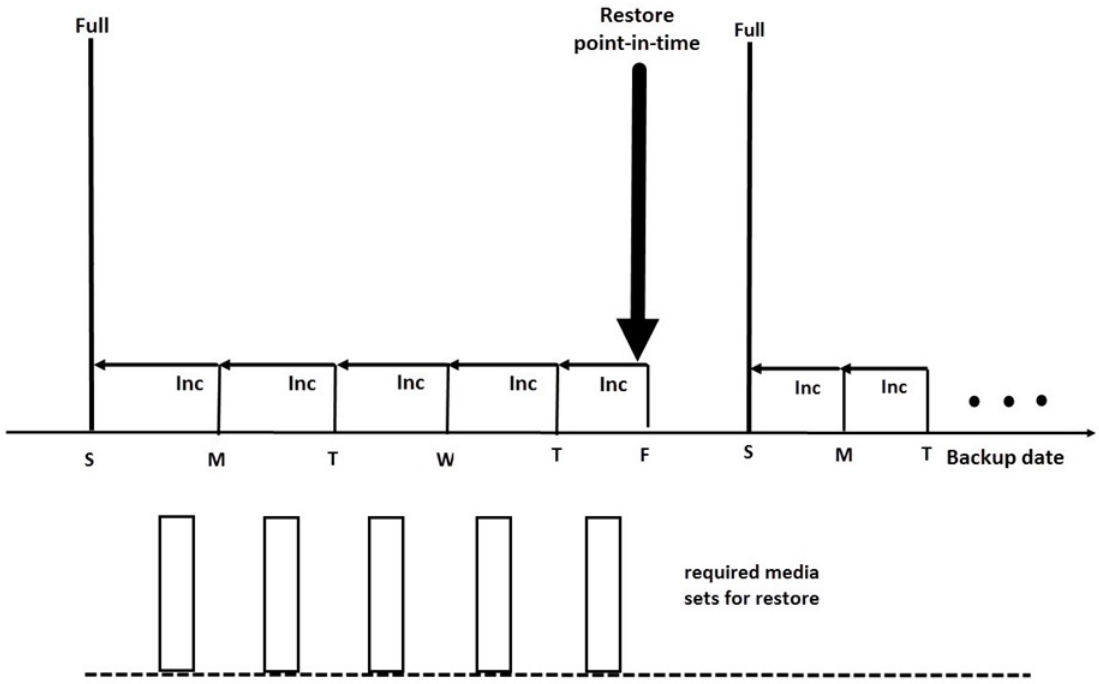
调度策略以及完整备份和增量备份，会深深影响还原数据所需的时间。这将通过本节的三个示例来说明。

对于时间点还原，需要完整备份以及到所需时间点为止的所有增量备份。由于完整备份和增量备份通常不在同一介质上，您可能需要为完整备份和每个增量备份加载不同的介质。

示例 1

完整备份加上每日增量备份描述了基于完整备份和简单增量备份的计划策略。

完整备份加每日简单增量备份

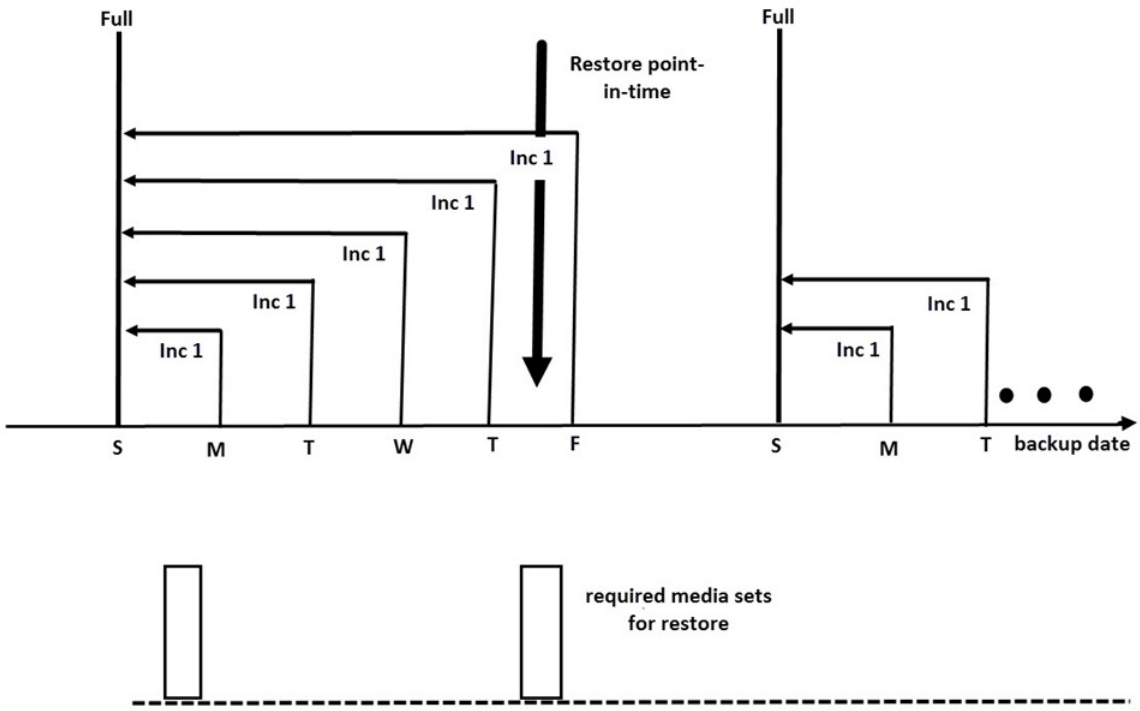


此策略可减少备份所需的介质空间和时间，因为只备份前一天以来的更改。但是，为了从星期四的备份还原文件，您需要提供完整备份和到星期四为止的每个增量备份，即五个介质集。这会使还原过程复杂化，并减慢还原速度。

示例 2

完整备份加上每日的 1 级增量备份描述了基于完整备份和一级增量备份的调度策略。

完整备份加上每日的 1 级增量备份

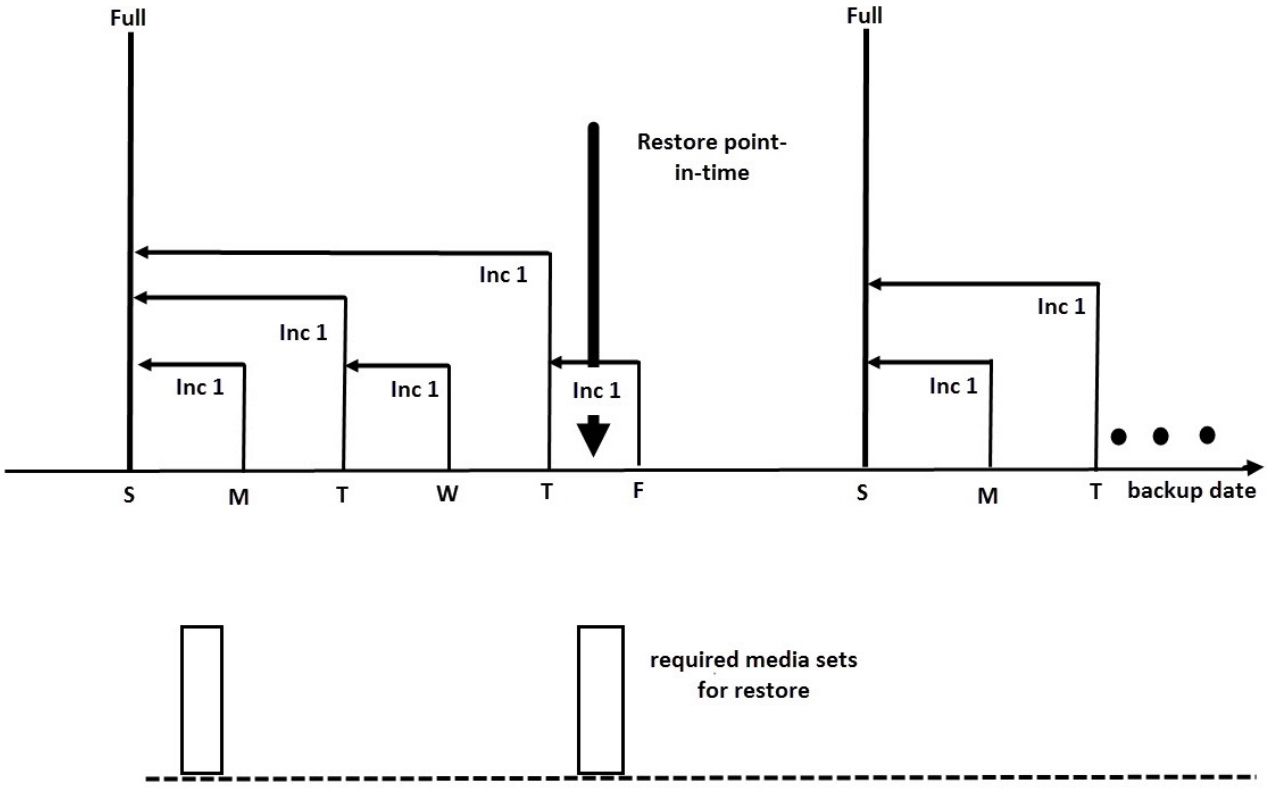


该策略需要的备份时间和介质空间略多，因为您每天要备份自上次每日完整备份以来的所有更改。要从星期四的备份还原文件，您需要提供完整备份的介质和星期四增量备份的介质，即只需两个介质集。这就显著简化并加速了还原过程。

示例 3

根据您的环境和需求，最佳解决方案应介于两者之间。例如，您的调度策略可能如下：

完整备份加上混合增量备份



此策略将周末更改不多的情况考虑在内。数据用简单增量备份与 1 级增量（差别）备份的组合进行备份，以优化备份性能。要从周四的备份还原文件，需要提供完整备份的介质和第二个增量 1 备份的介质，即两个介质集。

自动或无人看管操作

为简化操作和操作员对备份过程的干预，Data Protector 提供了支持熄灯时无人看管或自动备份的诸多功能。本节将介绍如何计划调度策略、这些策略如何影响备份行为，并提供调度策略示例。本节将集中讨论长期无人看管操作，时间跨度从数天到数周不等，而非单次备份中的无人看管操作。

无人看管备份的注意事项

Data Protector 可提供调度备份的简单方法。由于调度策略的有效性取决于环境，您需要事先计划，才能找到最佳调度策略。

- 何时系统使用和用户活动最少？

  通常是在夜里，大多数备份都安排在晚上运行。Data Protector 可以生成有关用于备份的设备的报告。

- 您有哪类数据？您希望多久安排一次对此类数据的备份？

  经常变化且对公司很重要的数据（如用户文件、事务和数据库）必须定期备份。系统特定数据（如不经常更改的程序文件）就无需那么频繁地备份。

- 您希望在多大程度上简化还原过程？

  根据您对完整备份和增量备份的安排，将需要完整备份和增量备份的介质以还原最新版本的文件。这可能需要较长时间，如果没有自动带库设备甚至需要手动处理介质。

- 您需要备份多少数据？

  完整备份比增量备份需要的时间更长。备份通常必须在有限的时间范围内完成。

- 需要多少介质？

  定义介质循环策略。这会显示您是否能够在计划的带库内保留足够的介质用于所需时段的操作，而无须手动处理介质。

- 装载提示处理如何?

  考虑使用一个带库还是多个带库。这样就可以进行自动操作，因为 Data Protector 可访问全部或大多数介质，由此可显著减少手动处理介质的需要。

- 如何处理不可用的设备？

  使用动态负载均衡或设备链，并在创建备份规范时提供多个设备。这样，当设备未打开或设备连接的系统故障时，就可避免备份失败。

- 备份全部数据需要多久？

  由于备份必须在网络使用率低且用户不使用其系统时完成，请考虑恰当安排备份，以分散备份造成的网络负载，尽可能提高备份会话的效率。这可能需要使用交错排列方法。

  如果您需要备份大量数据而备份时间窗口存在问题，请考虑备份到基于磁盘的设备，并使用合成备份和磁盘分段等高级备份策略。

- 如果准备运行应用程序进行备份？许多应用程序都会使文件打开，因此运行备份会导致备份不一致。

  这可以通过使用 pre-exec 和 post-exec 脚本来避免，pre-exec 和 post-exec 脚本可用于将应用程序的状态与备份活动同步。

复制已备份数据

复制已备份数据有一些好处。可以复制数据以提高其安全性和可用性，或为了操作原因而这样做。

Data Protector 可提供以下方法来复制已备份数据：对象复制、对象镜像和介质复制。

Data Protector 数据复制方法

	对象复制	复制	对象镜像	介质复制
复制什么	来自一个或多个备份、对象复制或对象合并会话的任意对象版本组合	来自备份会话、对象复制会话或对象合并会话的对象集	备份会话中的一组对象	整个介质
复制时间	完成备份后的任何时间	完成备份后的任何时间	备份期间	完成备份后的任何时间
源和目标介质的介质类型	可以不同	仅能将数据复制到相同类型的 B2D 设备	可以不同	必须相同
源和目标介质的大小	可以不同	目标设备必须具备足够的空间用于删除了重复数据后的数据	可以不同	必须相同
是否可追加目标介质	是	不适用	是	否
操作的结果	包含所选对象版本的介质	存储在目标 B2D 设备上的完全相同的副本	包含所选对象版本的介质	与源介质相同的介质

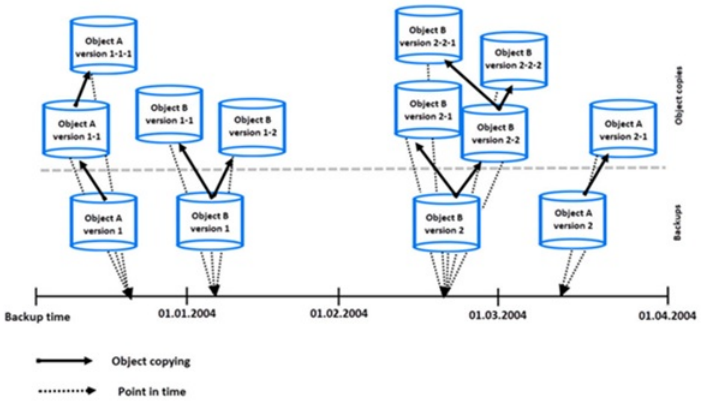
复制对象

Data Protector 对象复制功能使您能将所选对象版本复制到特定介质集。您可以从一个或几个备份、对象复制或对象合并会话中选择对象版本。在对象复制会话中，Data Protector 会从源介质读取备份的数据，传输数据，并将其写入目标介质。

对象复制会话可以得到包含指定对象版本副本的介质集。

对象复制的概念显示了如何在特定时间点以后复制当时已备份的数据。您可以从包含备份的介质或包含对象复制的介质中复制任何备份对象。

对象复制的概念



在图中，有一个来自对象 A 的备份的对象版本（版本 1），和同一对象版本的两个额外副本。版本 1-1 是通过复制备份所生成的对象版本得到的，版本 1-1-1 是通过复制对象版本的副本得到的。这些对象版本中的任何一个都可以用于还原同一对象版本。

启动对象复制会话

可以用交互形式启动对象复制会话，或指定自动启动会话。Data Protector 提供两种类型的自动对象复制: **备份后对象复制**和**安排的对象复制**。

备份后对象复制

备份后对象复制以及（备份后对象复制的子集）复制后和合并后对象复制，发生在自动对象副本规范中指定的会话完成之后。它们复制根据该特定会话中写入的自动对象复制规范选择的对象。

计划的对象复制

计划的对象复制发生在用户定义的某个时间。在一个计划的对象副本会话中可以复制不同会话中的对象。

设备的选择

您需要将要使用的设备与源介质和目标介质分开。目标设备的块大小可以大于源设备。但是，为避免影响性能，建议目标设备和源设备具有相同的块大小，且连接到同一系统或 SAN 环境。

默认情况下对于对象复制要进行负载均衡。Data Protector 通过使用尽可能多的设备，最优地利用可用的设备。

源设备的选择

默认情况下，Data Protector 根据设备配置内设置的设备策略，自动选择用于对象复制的源设备。这样能确保可用资源的最佳利用率。如果要使用原始设备或选择特定设备，可以禁用自动设备选择功能：

- 自动设备选择（默认）：

  Data Protector 会自动使用可用的源设备。该设备选择用于对象复制，来自同一带库，具有与所替换的原始设备相同的介质类型（例如 LTO）。

  Data Protector 会首先尝试使用用于写入对象（原始设备）的设备。如果没有选择用于对象复制的原始设备，则考虑全局选项。要优先使用备用设备或干脆不用原始设备，请修改全局选项 AutomaticDeviceSelectionOrder。

  您可以通过指定设备标记，将设备分为不同用途的设备组。具有相同标记的设备认为是兼容的，可以相互替换。不可用的原始设备可以替换为设备标记相同并来自同一带库的备用设备。默认情况下，不定义设备标记。

  请注意，如果删除了原始设备，则来自同一带库、具有相同介质类型的设备会替换原始设备。将不会检查是否选择该设备用于对象复制，也

不会检查该设备是否与原始设备具有相同的设备标记。

与备份期间相比，对象复制可以用较少的设备开始。

- 原始设备的选择：

  Data Protector 将使用原始设备作为对象复制的源设备，如果该设备不可用，则将等待。

目标设备的选择

如果目标设备未按对象指定，则 Data Protector 将按照以下优先级标准从在对象复制规范中选定的那些设备中自动进行选择：

- 先选择块大小与源设备相同的目标设备，再选择那些块大小与源设备不同的设备
- 先选择本地连接的设备，再选择网络连接的设备

会话开始的时候锁定设备。那时不可用的设备就不能用于会话中，因为会话开始后即无法锁定设备。如果发生介质错误，则该复制会话中将避免使用出错的设备。

复制源介质集的选择

如果要复制的对象版本存在于多个介质集（用 Data Protector 数据复制方法之一创建的）上，则任何介质集都可用作复制源。通过指定介质位置的优先级可以影响介质集的选择。

介质选择的总体过程与还原相同。

对象复制会话的性能

设备块大小和设备连接等因素都会影响对象复制的性能。如果对象复制会话中所用设备具有不同的块大小，数据会在会话期间重新打包，这就要占用额外的时间和资源。如果通过网络传输数据，则将增加网络负载并消耗更多时间。如果对操作进行了负载均衡，就能最小化此影响。

为什么使用对象副本？

出于多种目的创建已备份、已复制或已合并数据的额外副本：

- 保管

  您可以制作已备份、已复制或已合并对象的副本，并将其保存在多个位置。

- 释放介质

  要只保存介质上受保护对象的版本，您可以复制此类对象版本，然后释放介质以便覆盖。

- 取消复用介质

  您可以复制对象以消除数据的交叉存取。

- 合并还原链

  您可以复制还原到一个介质集所需的所有对象版本。

- 迁移到其他介质类型

  您可以将备份复制到不同类型的介质。

- 支持高级备份概念

  您可以使用磁盘分段等备份概念。

保管

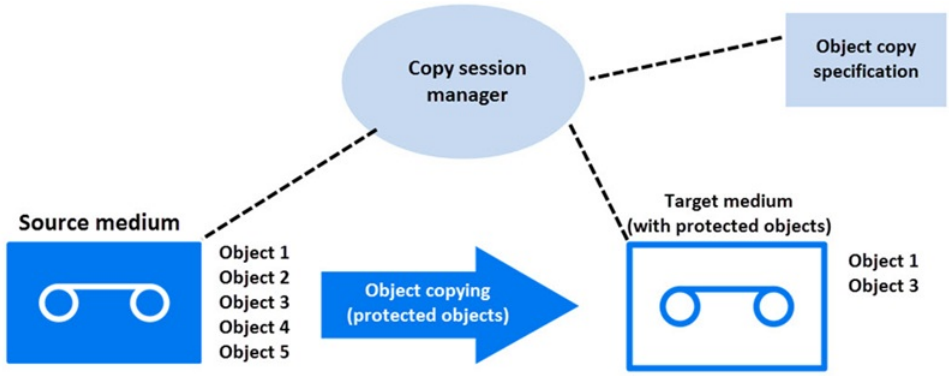
保管就是将介质放在安全位置保存一段时间的过程，这个安全位置通常称为保管库。

建议制作现场所备份数据的副本，以便还原。要获得更多副本，您可以根据需要使用对象复制、对象镜像或介质复制功能。

释放介质

您可通过只保留受保护的备份并覆盖未受保护的备份，尽可能减少介质空间的占用。由于单个介质可能同时包含受保护和不受保护的备份，因此可以将受保护对象复制到新介质集，以便覆盖原有介质。

释放介质

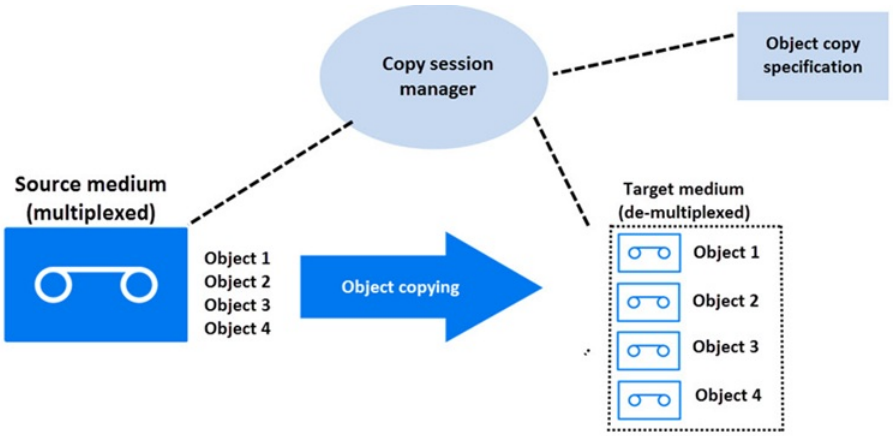


取消复用介质

多路复用的介质包含多个对象的交错数据。此类介质可能由于多个并行设备的备份会话而产生。复用介质会削弱备份的隐私安全，而且需要更多时间才能还原。

Data Protector 提供了取消复用介质的可能性。将复用介质中的对象复制到指定的多个介质。

取消复用介质



合并还原链

您可以将对象版本的还原链 (恢复所需的全部备份) 复制到新的介质集。从这种介质集可以更快更方便地还原，因为不需要加载多个介质和寻找所需的对象版本。

迁移到其他介质类型

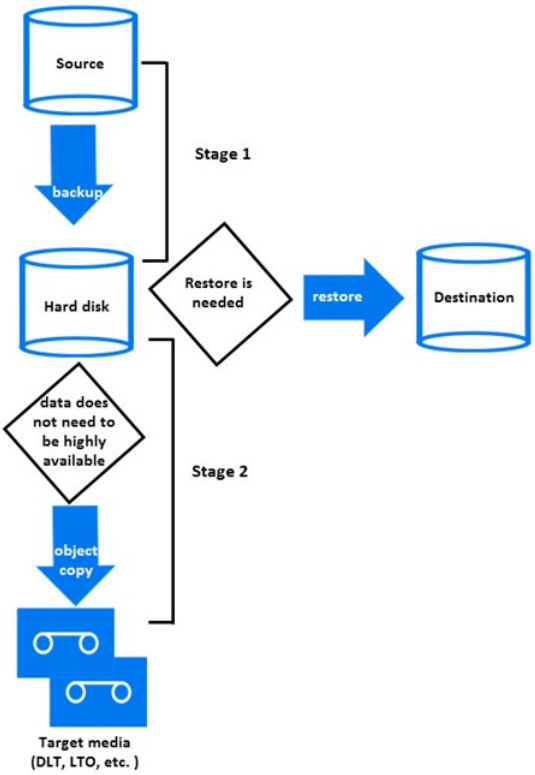
可以将备份数据迁移到其他介质类型。例如，可以从文件设备将对象复制到 LTO 设备，或者从 DLT 设备将对象复制到 LTO 设备。

磁盘分段

磁盘分段的概念基于在多个分段备份数据，以提高备份和还原的性能，降低恢复所备份数据的成本，提高数据可用性和还原可访问性。

备份阶段由以下部分组成：将数据备份到某种介质，然后将数据移入另一种介质。将数据备份到具有高性能、高可访问性但容量有限的介质（例如，系统磁盘）。这些备份通常保持可访问状态一段时间，以便进行还原，这段时间正是最有可能进行还原的时间段。经过这段特定时间后，使用对象复制功能将数据移到性能和可访问性较低但容量较大的介质中进行存储。

磁盘分段的概念



该过程可作为自动操作执行。

考虑以下示例，其简要描述了一种实施简单、可用作标准操作的方法，同时还可提供额外的数据安全性。它使用独立设置源保护和目标保护的选项。要求是前 15 天内能快速从磁盘还原，此后 30 天能从磁带执行标准还原。

- 初始备份使用文件库执行到磁盘的备份，数据和编目保护设置为总共需要的 45 天。
- 然后执行备份后复制操作，将备份对象复制到磁带，把初始备份留在文件库上。如果成功复制到磁带，则将其数据和编目保护设置为 45 天。
- 成功创建副本后，磁盘备份的保护时间就可以缩短为 15 天，即需要快速还原的时间段。此后，可以删除它，通过磁带副本提供长期的安全性。此时，磁带副本在磁盘副本损坏时可提供额外的安全性。

磁盘分段也消除了将大量小对象频繁备份到磁带的必要。由于要频繁装载和卸载介质，此类备份很不方便。使用磁盘分段，可节约备份时间，避免了介质退化。

复制

通过 Data Protector 复制功能，可以在两个具有复制功能的备份到磁盘 (B2D) 设备之间复制对象，而无需通过介质代理传输数据。

您可以选择一个或几个备份会话、对象复制会话或对象合并会话。在复制会话期间，Data Protector 会从一个备份会话中读取对象，并启动从源 B2D 设备到目标设备的复制。复制会话的结果为来自指定会话的所有对象的副本。

通过选择能够执行复制的设备并在对象复制规范中选择相应的选项，可以在创建对象复制规范时启用复制。

以下先决条件适用:

- 选择用于复制的设备必须具备复制功能。
- 源设备和目标设备类型必须相同。
- 在 StoreOnce 库内，源设备和目标设备必须属于不同存储。
- 必须在至少一个备份规范中配置源设备。

复制会话的启动

可以用交互方式启动复制会话，也可以指定自动启动会话。Data Protector 提供两种类型的自动复制: **备份后复制**和**安排的复制**。

备份后复制

备份后复制以及复制后和合并后替换 (均为备份后替换的子集)，发生在自动替换规范中指定的会话完成之后。它们会根据该特定会话中写入的自动复制规范复制选定对象。

安排的复制

安排的复制在用户定义的时间发生。不同的会话可以在单个安排的复制会话内复制。

设备的选择

您需要将要使用的设备与源设备和目标设备分开。只有 B2D 设备才能用于复制。

为何使用复制？

在需要使用对象复制的许多情况下（例如保管等）都可以使用复制，除了涉及到介质的操作以外。此外，与对象复制相比，B2D 设备间的复制具备以下优点：

- 直接在 B2D 设备间复制数据。这样可减轻介质代理客户机上的负载。
- 只会复制唯一（重复的）数据。这样可减轻网络负载。

对象镜像

通过 Data Protector 的对象镜像功能，可以在备份会话期间将同一数据同时写入多个介质集。您可以将全部或部分备份对象镜像到一个或多个其他介质集。

使用对象镜像的成功执行备份会话的结果是得到一个包含已备份对象的介质集以及包含镜像对象的其他介质集。这些介质集上的镜像对象被视为对象副本。

对象镜像的优点

使用对象镜像功能可以达到以下目的：

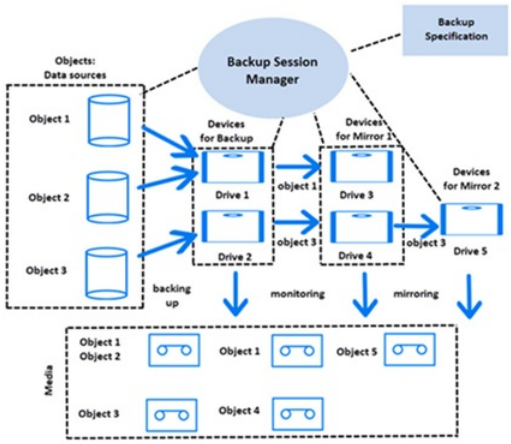
- 由于存在多个副本，它可提高已备份数据的可用性。
- 它使得多地点保管介质变得更加容易，因为已备份数据可以镜像到远程站点。
- 由于相同数据写入到若干介质上，因此它提高了备份的容错能力。一个介质上的介质故障不会影响创建其他镜像。

对象镜像操作

在具有对象镜像的备份会话中，将备份每个所选的对象，同时按照备份规范中指定的镜像次数进行镜像。

我们以图中的对象 3 为例。磁带客户机会从磁盘读取数据块，并将数据发送给负责备份对象的介质代理。此介质代理随后将数据写入驱动器 2 的介质，并将数据转到负责镜像 1 的磁盘代理。此介质代理反过来将数据写入驱动器 4 的介质，并将数据转到负责镜像 2 的磁盘代理。此介质代理将数据写入驱动器 5 的介质。会话结束时，三个介质中都可以使用对象 3。

对象镜像



设备的选择

默认情况下对于对象镜像进行负载均衡。Data Protector 通过使用尽可能多的设备，最优地利用可用的设备。会根据以下条件（按优先级顺序）选择设备：

- 选择相同块大小的设备（如果可用）
- 先选择本地连接的设备，再选择网络连接的设备

从命令行执行对象镜像操作时，负载均衡不可用。

备份性能

对象镜像对备份性能有影响。在 Cell Manager 和介质代理客户机上，写入镜像的影响与备份额外对象的影响相同。在这些系统中，备份性能的降低将取决于镜像数。

在磁盘代理上，镜像对性能无影响，因为备份对象只读取一次。

备份性能还取决于设备块大小和设备连接等因素。如果备份和对象镜像所用设备的块大小不同，则将在会话期间将镜像数据重新打包，此过程会占用额外的时间和资源。如果通过网络传输数据，则将增加网络负载并消耗更多时间。

复制介质

Data Protector 介质复制功能使您能够在执行备份后复制介质。介质复制是创建包含备份的介质的精确副本的过程。您可以用它复制介质，以达到存档或保管目的。复制介质后，可以将原始介质或副本移到非现场保管库。

除了手动启动介质复制外，Data Protector 还提供了自动介质复制功能。

如何复制介质

您需要具有相同介质类型的两台设备，一台用作源介质，另一台用作目标介质。源介质是要复制的介质，目标介质是要将数据复制到的介质。

复制有多个驱动器的库内的介质时，可以用一个驱动器作为源，另一个驱动器用于复制。

结果如何？

复制介质的结果是两个完全相同的介质集 — 原始介质集和副本。其中任何一个都可用于还原。

复制源介质后，Data Protector 把它标记为不可附加，以避免附加新备份（这会导致原始介质与其副本不同）。随后将副本也标记为不可追加。副本的默认保护与原始保护相同。

您可以制作原始介质的多个副本。但不能制作副本的副本，也称为二次生成副本。

自动介质复制

自动介质复制是为包含备份的介质创建副本的自动化过程。该功能对带库设备可用。

Data Protector 提供两种自动介质复制：备份后介质复制和排定介质复制。

备份后介质复制

备份后介质复制发生在完成备份会话之后。它复制该特定会话中使用的介质。

计划的介质复制

计划的介质复制发生在用户定义的某个时间。不同备份规范中使用的介质可以在单个会话中复制。创建自动介质复制规范来定义要复制的介质。

自动介质复制如何工作？

首先，创建自动介质复制规范。自动介质复制会话开始时，Data Protector 会根据自动介质复制规范中指定的参数生成介质列表，作为源介质。对于每个源介质，都会选择要将数据复制到的目标介质。目标介质从源介质所在的同一介质池、自由池或库内的空白介质中选择。

对于每个源介质，Data Protector 都会从您在自动介质复制规范中指定的设备中选择一对设备。自动介质复制功能提供其自己的负载均衡。Data Protector 通过利用尽可能多的设备和选择本地设备（如果其可用），尝试充分利用可用的设备。

自动介质复制功能不处理装载请求或清除请求。如果收到装载请求，则中止相关的介质对，但会话将继续。

有关使用的示例，请参阅《Data Protector 帮助》。

验证备份介质和备份对象

作为备份管理员，仅仅定期备份重要数据是不够的。能够在发生问题时成功还原已备份数据，特别是用现在可用的一些更复杂的备份技术，也同样重要。借助 Data Protector 备份介质和备份对象验证，您可以用不同的置信水平检查还原能力。

什么是介质验证？

通过 Data Protector 介质验证可检查任何介质的数据格式是否有效，并更新 IDB 中的介质信息。您可以使用该功能交互地检查任何完整的单个 Data Protector 驻留介质。在以下情况下，可能需要使用介质验证：

- 您复制了用于存档的介质，并想在将它置于保管库之前检查副本的有效性。
- 备份介质已满，您想检查其上所有对象后再送去长期保管。

介质验证的目的是什么？

运行介质验证时，Data Protector 会：

- 检查 Data Protector 头中的介质 ID、描述和位置信息
- 读取介质上的所有块，并验证块格式
- 如果在备份期间执行了循环冗余校验 (CRC)，则重新计算 CRC，并将它与介质上存储的值进行比较

前两项检查如果成功，就确认磁带的硬件状态良好，所有数据都可以从中成功读取，从而提供从该介质进行还原的中等置信水平。

第三项检查如果成功，就确认每个块内的备份数据本身是一致的，从而提供从该介质进行还原的较高置信水平。

什么是对象验证？

通过 Data Protector 对象验证可检查备份对象相对于备份介质的有效性。可以使用该功能来检查：

- 单个或多个对象
- 在单个或多个介质上
- 以交互方式，还是在安排的会话或操作后会话中

在以下情况下，可能需要使用对象验证：

- 在对象复制到其他介质后
- 在增量备份的对象的还原链上执行对象合并后
- 要检查备份设备更改后指定时间范围内生成的所有备份对象

对象验证的目的是什么？

运行对象验证时，Data Protector 可提供与介质验证级别相同的数据验证。尽管对于介质验证它只能检查完整的单个介质，但是对于对象验证则可以检查如下对象：

- 单个备份对象，无需检查整个介质，对于大的备份介质可能会节约很多时间
- 跨多个介质的大对象
- 几个介质上的几个对象
- 特定对象版本（仅交互式）

此外，您可以对以下对象执行验证：

- 介质代理主机，不会增加任何网络流量
- 影响网络效率的其他主机

有关对象验证规范和会话的信息，请参见各种“会话规范和时间框架中的会话”报告。

还原数据

还原数据的策略是公司总体备份策略的关键部分。请记住以下几点：

- 备份和还原文件本质上与复制文件相同。因此，要确保只有授权人员才有权还原机密数据。
- 确保未授权人员不能还原其他人的文件。

本节将介绍使用 Data Protector 的还原策略的一些可行实现方式。您可以浏览还原对象或还原会话来还原文件系统数据。默认情况下，数据将恢复到其原始位置。但是，您可以指定任何位置作为还原数据的目标位置。

恢复持续时间

数据丢失后，只有在完成恢复过程后才可能访问数据。尽可能缩短还原持续时间，以便用户能够执行日常工作，这至关重要。因此，要计划还原特定数据所需的时间。

影响还原持续时间的因素

还原持续时间取决于多个因素，例如:

- 要还原的数据量。这也会直接影响以下所有项目。
- 完整备份和增量备份的组合。
- 用于备份的介质和设备。
- 网络和系统的速度。
- 要恢复的应用程序，例如 Oracle 数据库文件。
- 并行还原的使用。可以通过单次读取操作还原多个对象，这取决于数据是如何备份的。
- 选择要还原的数据的速度和方便程度，这取决于备份中所用的日志记录级别设置和编目保护时间。

介质集的选择

如果要恢复的对象版本存在于多个介质集（使用 Data Protector 数据复制方法之一创建）上，则任何介质集都可用于恢复。默认情况下，Data Protector 会自动选择要使用的介质集。通过指定介质位置的优先级可以影响介质集的选择。除非是还原集成对象，否则您还可以手动选择要用于还原的介质集。

介质集选择算法

默认情况下，Data Protector 会选择具有最佳可用性和质量的介质集。例如，Data Protector 会避免使用缺少介质或质量低劣的介质集；它会考虑对象的完整状态、用于某些介质集的设备的可用性和位置等。先使用位于带库内的介质集，再使用独立设备中的介质集。

还原链的选择

如果使用合成备份，那么对于同一对象时间点，经常有多个还原链。默认情况下，Data Protector 会选择最方便的恢复链以及所选恢复链内最合适的介质。

介质位置优先级

要影响介质集的选择，请指定介质位置优先级。如果使用多地点存储的概念，这很重要。如果将介质存放在不同地点，则可以指定更适合于特定还原的位置。如果多个介质集符合选择算法的条件，则 Data Protector 将使用优先级最高的介质集。

您可以设置全局介质位置优先级，也可以为特定还原会话设置介质位置优先级。

设备的选择

默认情况下，Data Protector 会根据设备配置中设置的设备策略，自动选择用于恢复的设备。这样能确保可用资源的最佳利用率。如果要使用原始设备或选择特定设备，可以禁用自动设备选择功能：

- 自动设备选择（默认）：

  Data Protector 会自动使用可用的设备。该设备选择用于还原，来自同一带库，具有与所替换的原始设备相同的介质类型（例如 LTO）。

  Data Protector 会首先尝试使用用于写入对象（原始设备）的设备。如果没有选择用于还原的原始设备，则考虑全局选项。要优先使用备用设备或干脆不用原始设备，请修改全局选项 AutomaticDeviceSelectionOrder。

  您可以通过指定设备标记，将设备分为不同用途的设备组。具有相同标记的设备认为是兼容的，可以相互替换。不可用的原始设备可以替换为设备标记相同并来自同一带库的备用设备。默认情况下，不定义设备标记。

  请注意，如果删除了原始设备，则来自同一带库、具有相同介质类型的设备会替换原始设备。将不会检查是否选择该设备用于还原，也不会检查该设备是否与原始设备具有相同的设备标记。

  与备份期间相比，还原可以用较少的设备开始。

- 原始设备的选择：

  Data Protector 将使用原始设备进行恢复，如果该设备不可用，则将等待。这是 Data Protector SAP MaxDB 和 DB2 UDB 集成的首选选项。此类数据库通常用相互依赖的数据流备份，因此，还原过程必须使用备份中所用的相同数量的设备启动。

允许操作员执行还原

常用的还原策略就是只有专门的备份操作员或网络管理员才有权还原文件或执行灾难恢复。

何时使用该策略

在以下情况下可使用该策略：

- 在大型网络环境中，最好有专职人员从事此类工作。
- 在最终用户没有还原文件所必需的计算机知识的环境中，可由受信任的操作员还原敏感数据。

需要做什么

需要执行以下操作来实现该策略：

- 将备份操作员或网络管理员添加到 Data Protector**operators** 或 **admin** 用户组，他们将为其他用户还原失且无法恢复控制文数据。

  无需将其他人员（例如要恢复到自己系统的用户）添加到任何 Data Protector 用户组。

- 安装过程中，不要在最终用户的系统上安装 Data Protector 用户界面。安装允许 Data Protector 备份这些系统的磁带客户机。
- 制定处理还原请求的策略。该策略应涵盖最终用户如何请求文件还原，例如通过这样一封电子邮件，其中包含能让操作员找到并将文件还原回最终用户的系统所需的全部详细信息。最终用户还应通过某种途径了解这些文件何时能够还原完成。

允许最终用户执行还原

另一个可能的还原策略是允许所有或所选最终用户还原自己的数据。该策略可以提供足够的安全性，并且可以减轻备份操作员执行许多还原操作。

何时使用该策略

在以下情况下可使用该策略：

- 最终用户拥有足够知识来处理还原时。可能需要对用户提供基本概念和还原操作方面的培训。
- 对于最近备份的介质，使用带库备份设备。默认情况下，Data Protector end user 用户组不允许最终用户处理所需介质的装载请求。如果需要处理装载请求，最终用户仍需备份操作员的协助。可以通过使用大型带库来避免这一情况。

需要做什么

需要执行以下操作来实现该策略：

- 向 Data Protector end users 用户组添加允许还原自己的数据的最终用户。为增强安全性，可以将这些用户的 Data Protector 访问权仅限于特定系统。
- 在最终用户正在使用的系统上安装 Data Protector 用户界面。Data Protector 自动检查用户权限并仅允许恢复功能。
- 配置最终用户系统的备份时，可通过设置 Data Protector“公共”选项使备份对最终用户可见。

灾难恢复

本节只是简短介绍一下灾难恢复的概念。有关详细的灾难恢复概念、计划、准备和过程，请参阅 Data Protector 灾难恢复一节。

“计算机灾难”是指任何导致计算机系统无法启动的事件，无论是由于人为错误、硬件或软件故障，还是自然灾害等。在此类情况下，很可能无法使用系统的引导或系统分区，必须先还原环境才能开始标准的还原操作。这包括重新分区和/或重新格式化引导分区，用定义环境的所有配置信息恢复操作系统。*必须完成该步骤，才能恢复其他用户数据。*

计算机灾难发生后，系统 (称为“目标系统”) 通常处于不能引导的状态，Data Protector 灾难恢复的目标是将该系统还原到其原始系统配置。受影响系统与目标系统的区别在于目标系统已更换了所有故障硬件。

灾难通常都很严重，但以下因素可能使情况更为严峻：

- 系统必须尽快、尽可能高效率地恢复到联机状态。
- 管理员不熟悉执行灾难恢复过程所需的步骤。
- 执行恢复的可用人员只有基础系统知识。

灾难恢复是一项复杂的任务，在执行前涉及广泛的计划和准备工作。为了准备和执行灾难恢复，您需要有定义明确的逐步恢复过程。

灾难恢复过程由 4 个阶段组成：

1. **阶段 0**（计划/准备）是成功实施灾难恢复的先决条件。

   > ⚠ **警告**灾难发生后再准备灾难恢复就太晚了。

2. 在**阶段 1** 中，安装并配置 DR OS，此过程通常包括对引导分区进行重新分区和重新格式化，这是因为系统的引导或系统分区并非一直可用而环境需要在常规还原操作再次继续之前得到恢复。

3. 阶段 2 中，将用 Data Protector (按原样) 还原带有定义环境的所有配置信息的操作系统。
4. 只有在完成阶段 2 后，才可能进行应用程序和用户数据的还原 (阶段 3)。

   必须遵循明确定义的逐步过程，以确保快速有效还原。

灾难恢复方法

Data Protector 支持以下灾难恢复方法：

- 手动灾难恢复

  这是基本的，也是很灵活的灾难恢复方法。您需要安装和配置 DR OS。然后使用 Data Protector 还原数据（包括操作系统文件），用还原后的操作系统文件替换还原前的操作系统文件。

- 自动灾难恢复

  自动系统恢复 (ASR) 是 Windows 系统上的自动系统，它可以在发生灾难时将磁盘重新配置为其原始状态（或者，如果新磁盘比原始磁盘大，则调整分区大小）。这样，ASR 允许使用 Data Protector drstart.exe 命令安装活动 DR OS，以提供 Data Protector 磁盘、网络、磁带和文件系统访问。

- 磁盘传送灾难恢复

  在 Windows 客户机上，受影响系统的磁盘（或物理损坏磁盘的替换磁盘）会临时连接到托管系统。还原后，就可以将它连接到故障系统并进行引导。在 UNIX 系统上，使用具有最小操作系统、网络连接并装有 Data Protector 代理的辅助磁盘执行磁盘传递灾难恢复。

- 增强型自动灾难恢复 (EADR)

  增强的自动灾难恢复 (EADR) 是针对 Windows 客户机和 Cell Manager 的完全自动的 Data Protector 恢复方法，只需极少的用户干预。该系统从灾难恢复 CD ISO 映像进行引导，并且 Data Protector 会自动安装和配置 DR OS，格式化磁盘并进行分区，最后用 Data Protector 恢复备份时的原始系统。

- 一键式灾难恢复 (OBDR) 是针对 Windows 客户机和 Cell Manager 的完全自动的 Data Protector 恢复方法，只需极少的用户干预。该系统从 OBDR 磁带引导并自动恢复。

有关特定操作系统支持的灾难恢复方法的列表，请参阅最新支持矩阵。

其他灾难恢复方法

本节将比较 Data Protector灾难恢复概念与其他供应商的灾难恢复概念。本节仅指出其他恢复概念的重要方面。

讨论了两种备用恢复方法：

操作系统供应商支持的恢复方法

大多数供应商都提供自己的方法，但对于还原，通常需要执行以下步骤：

1. 从头开始重新安装操作系统。
2. 重新安装应用程序。
3. 还原应用程序数据。

需要对操作系统和应用程序进行大量手动的重新配置和自定义工作，才能重建灾难前的状态。这是一个很复杂、很费时、很容易出错的过程，需要使用各种不同工具，这些工具并没有彼此集成。它无法从操作系统、应用程序及其配置的整体备份中获益。

使用第三方工具恢复（适用于 Windows 系统）

该方法通常由一种特殊工具组成，它将系统分区备份为快照，后者可以快速还原。该方法概念上需要执行以下步骤：

1. 还原系统分区（使用第三方工具）。
2. 如果需要，用标准备份工具还原任何其他分区（可能有选择性）。

很明显，必须用不同工具从两种不同备份进行恢复。如果要定期执行恢复，这是一项困难的任务。如果在大公司实施这个概念，就必须考虑管理来自两个工具的不同版本的数据（每周备份）带来的管理成本。

另一方面，Data Protector 则代表了强大的集成式跨平台企业解决方案，可快速有效地进行包括备份和还原的灾难恢复，并支持群集。它可提供方便的中央管理和还原、高可用性支持、监视和报告及通知功能，有助于大公司内系统的管理。

基于块的备份、还原和恢复

Data Protector 允许您在块级别为受支持的 Windows 和 Linux 设备执行数据的完整备份和增量备份。要还原备份，可以执行以下操作:

- 基于块的还原**:** 将整个备份卷作为一个整体进行还原。
- 基于块的恢复**:** 允许您选择要恢复的单个文件和文件夹。

注意**:** 以下内容适用于 完整 和 增量基于块的备份 :

- 不支持重新启动失败对象的功能。
- (适用于 Windows 客户机上的升级场景) 为了成功浏览和恢复文件及文件夹，必须确保 Data Protector INET 和 Data Protector 过滤侦听程序 服务都在同一用户帐户下运行。
- 不支持在 Linux 客户机上备份未装载的磁盘。
- 不支持从基于块的备份还原、浏览和恢复到混合设备类型，例如:
  - 具有原始设备和镜像设备属于不同类型的镜像设备配置的完整备份。
    例如，原始设备属于 StoreOnce catalyst 类型，镜像设备属于 DD Boost 类型，反之亦然。
  - 到不同目标设备类型的增量备份。
    例如，两个增量备份，其中一个备份到 StoreOnce catalyst 设备，另一个备份到 DD Boost 设备。

  使用同一设备类型来备份数据以实现成功的还原、浏览和恢复操作。
- 考虑使用“还原为” 选项将备份还原到装有 XFS 文件系统的同一主机上的其他卷。由于同一 UUID 同时应用于原始备份设备和 XFS 文件系统的还原设备，此还原卷的装载失败并显示错误。要解决此问题，请参阅装载还原到同一主机上的其他卷的卷时出错。

基于块的备份

通过基于块的备份 ，您可以在块级别执行文件系统备份。所有操作系统 (OS) 都有一个称为“文件系统”的专用组件。例如，Windows 上的新技术文件系统 (NTFS)。文件系统将硬盘、卷或 RAID 阵列（软件和硬件 RAID）分成固定的字节组，这些字节组称为块。

常规文件系统备份类型使用 OS 上的文件系统来读取磁盘或卷上的数据。 基于块的备份 直接从磁盘或卷中读取块，而无需跟踪文件系统结构。它按块在磁盘上保存的顺序读取块，而不是按文件中显示的顺序读取。系统仅备份已使用的块，从而减少了备份时间。

基于块的备份 容量计算是基于常规文件系统备份容量进行的。

并行备份

您可以并行执行多个 基于块的备份 。要执行卷的并行备份，请使用以下方法之一配置备份规范:

- 每个 DA 客户机系统将所有卷配置为一个规范的一部分。
- 根据备份规范配置单个卷。
- 在一个规范中跨 DA 客户机配置卷。

注意**:** Micro Focus 建议您不要运行已经属于当前运行备份的卷的备份。

增量备份

它允许备份与上次备份相比发生更改的数据。它使用更改后的块驱动程序 软件，获取与上次备份会话相比已更改的块。更改后的块驱动程序 是内核过滤器驱动程序，用于监视 DA 客户机系统上新技术文件系统 (NTFS) 卷的已修改或已更改的块。

在增量备份期间，Data Protector 备份代理 (磁盘代理) 与更改后的块驱动程序 进行交互以获取已更改的块。增量备份包括与上次完整备份或增量备份相比的增量更改。增量数据大小的计算依赖于与上次备份相比在卷上发生的数据更改。在备份会话期间，将显示一条消息，指示备份类型是完整还是增量。

有关安装或卸载更改后的块驱动程序的信息，请参阅安装或卸载更改后的块驱动程序。

注意**:**以下操作仅适用于增量 基于块的备份 **:**

- 在升级 Data Protector 或重新配置“更改后的块驱动程序” 后立即执行增量 基于块的备份 时，增量备份将退回到完整备份。
- 对于成功的 基于块的增量 备份，如果 DA 客户机 (具有针对增量备份选择的卷) 上的 INET 服务以内置 '**NT AUTHORITY/Local System**' 帐户以外的用户帐户运行，则将用户帐户添加到 Cell Manager 的 **Admin** 用户组中。
- 不支持镜像增量备份数据的还原、浏览和恢复。
- 增量备份要求最小文件系统块大小为 1 KB 或更大。
  在对 **XFS** 文件系统进行增量备份之前，必须确保最小文件系统块大小为 1 KB 或更大

增量备份的好处

- 还原期间优化了块访问，可提供单一还原操作
- 减少每次备份移动的数据，并减少作业的运行时间。

基于块的备份限制

请考虑 基于块的备份 的以下限制:

- 仅支持带有 NTFS 文件系统的 Windows x64 系统。
- 仅支持 SUSE Linux Enterprise Server (SLES) 15.x 和 Red Hat Enterprise Linux (RHEL) 8.x.x 64 位平台。
- 仅支持具有 Ext3 、 Ext4 和 XFS 文件系统的 SLES 和 RHEL 平台。
- 支持 Logical Volume Manager (LVM) 2.0。
- 仅支持 StoreOnce 和 DDBoost 域目标备份设备。
- 不支持 VHD/VHDX 设备上创建的卷在目标主机上显示为文件。仅当代理在来宾操作系统中运行时，它才支持 VHD/VHDX 设备上的 Hyper-V VM。
- 不支持卷装载点。
- 不支持对设备执行对象复制操作，因为从这些对象复制会话进行备份、还原和恢复可能不起作用。

基于块的还原

通过基于块的还原 ，您可以还原在块级别备份的数据。磁盘代理 (DA) 从存储设备读取备份数据，并将该数据还原到还原位置，而无需涉及介质代理 (MA)，从而提高了还原性能。DA 使用备份期间生成的块映射文件来标识备份块的位置，然后将其还原。通过基于块的还原，您可以还原备份的整个卷。

先决条件

- 确保可以备份到 StoreOnce 或 DDBoost 设备。

注意事项和限制

- 仅支持带有 NTFS 文件系统的 Windows x64 系统。
- 仅支持 SUSE Linux Enterprise Server (SLES) 15.*x* 和 Red Hat Enterprise Linux (RHEL) 8.x.x 64 位平台。
- 仅支持具有 Ext3 、 Ext4 和 XFS 文件系统的 SLES 和 RHEL 平台。
- 支持 Logical Volume Manager (LVM) 2.0。
- 不支持将 StoreOnce 软件作为备份设备。
- 不支持在单个还原会话中触发基于块的还原和文件系统还原。但是， 基于块的还原 和文件系统还原可以由不同的还原会话管理器并行触发。

基于块的恢复

通过基于块的恢复 ，您可以浏览 基于块的备份 ，在树结构中选择各个文件和目录并进行恢复。仅恢复您选择的文件和文件夹的属性和数据。

- 选择供恢复的文件**:** 仅在文件级别恢复数据和属性。它不包括选定文件的父文件夹层次结构。
- 选择供恢复的文件夹**:** 恢复选定文件夹及其子文件夹或文件的数据和属性。它不包括选定文件夹的父文件夹层次结构。

增量备份支持

浏览**:** 允许您浏览备份的 NTFS 文件系统以恢复选择性文件或文件夹，而不是还原完整的 NTFS 卷。允许选择特定的时间点备份会话进行浏览。NTFS 文件系统的文件或文件夹列表将作为浏览的一部分显示在选定的时间点备份会话还原链的浏览中。要选择其他时间点备份会话，请执行以下操作:

1. 在浏览中右键单击根文件夹 (“/”)，然后选择“还原版本” 选项卡。
2. 将显示“还原会话选择向导”。选择适当的时间点备份会话，然后单击“确定” 。
3. 展开根文件夹进行浏览。将显示属于所选还原会话链的文件和文件夹的列表。
4. 选择要恢复的文件和文件夹，然后执行恢复。

> 注意**:** 每个文件夹扩展显示的最大元素数限制为 64K。Micro Focus 建议您将文件夹中的文件或子文件夹限制为小于 64K。

恢复**:** 允许将所选文件或文件夹恢复到所选目标位置。

注意事项和限制

- 不支持将 StoreOnce 软件作为备份设备。
- 为了成功浏览和恢复文件和文件夹， Data Protector INET 和 Data Protector 过滤侦听程序 服务必须在同一用户帐户下运行。
- 如果通过本地系统帐户执行还原或恢复，已还原文件夹的加密用户帐户将从“管理员”更改为“系统”加密。如果通过“管理员”帐户执行还原或恢复，加密用户帐户将保持“管理员”加密。
- 不支持使用 Data Protector 2019.12 (10.60) 进行备份来恢复文件和文件夹的浏览选项。
- 当文件夹展开时，恢复上下文中的树展开视图最多只能显示 64000 个文件和文件夹。
- 为了成功浏览和恢复文件和文件夹，必须确保要浏览的文件或文件夹的绝对路径不超过 1024 字节。

相关主题

- Block-based backup 步骤
- Block-based restore 步骤
- Block-based recovery 步骤
- 有关安装或卸载更改后的块驱动程序的信息，请参阅安装或卸载更改后的块驱动程序。

设备和介质管理

本主题介绍 Data Protector 介质和设备管理的概念，并讨论设备、介质池和大型带库。

设备

Data Protector 支持的许多设备在市场上都可以买到。有关受支持设备的最新列表，请参阅最新支持矩阵。

设备类型

设备可分为以下几类：

- 磁带设备：
  - 独立设备。
  - 小型盒设备。
  - 大型库。
- 基于磁盘的设备。
- 云备份设备。

将设备与 Data Protector 结合使用

要将设备与 Data Protector 结合使用，必须在 Data Protector 单元中配置该设备。配置设备时，需要指定设备名称、一些设备特定的选项 (如条形码或磁头清洗磁带支持) 和一个介质池。设备配置过程可通过使用向导得到简化，它会指引您完成所有步骤，甚至可以自动检测和配置设备。在 Data Protector 中可以使用不同的 (逻辑) 设备名称对具有不同使用属性的同一物理设备进行多次定义，例如，一个设备无硬件数据压缩，另一个设备有硬件数据压缩。

下面介绍一些特定的设备功能，以及 Data Protector 如何操作各种设备。

库管理控制台支持

许多现代磁带库都提供管理控制台，可通过该控制台从远程系统配置、管理或监视库。可远程执行的任务范围取决于管理控制台的实施，它独立于 Data Protector。

Data Protector 方便了对库管理控制台界面的访问。管理控制台的 URL（Web 地址）可以在库配置或重新配置过程中指定。选择 GUI 中的专用菜单项时，系统即会调用 Web 浏览器，并将控制台界面自动加载到浏览器中。

有关支持该功能的设备类型的列表，请参阅最新支持矩阵。

> **重要说明**使用库管理控制台之前，请考虑某些可通过控制台执行的操作可能会妨碍介质管理操作和/或备份和还原会话。

TapeAlert

TapeAlert 是磁带设备状态监视和消息发送实用程序，有助于检测可能会影响备份质量的问题。从使用磨损的磁带到设备硬件缺陷，TapeAlert 可第一时间报告各种易于理解的警告或错误，并提出一系列建议的操作以修复问题。

只要连接的设备也提供此功能，Data Protector 即完全支持 TapeAlert 2.0。

设备列表和负载均衡

多个备份设备

配置备份规范时，可以指定多个独立设备或在库设备中指定多个设备，用于备份操作。在这种情况下，操作速度更快，因为数据将并行备份到多个设备 (驱动器) 中。

均衡使用设备

默认情况下，Data Protector 会自动均衡设备的负载 (使用)，从而平均地使用它们。这称为“负载均衡”。负载均衡通过均衡备份到每个设备的对

象数量来优化设备使用。负载均衡在备份时自动完成，您无需管理会话中所用设备的对象分配；只需指定要使用的设备即可。

何时使用负载均衡

在下列情况中使用负载均衡：

- 要备份大量对象。
- 使用带多个驱动器的库（自动更换器）设备。
- 不知道对象要备份到哪些介质。
- 网络连接良好。
- 您希望提高备份的稳定性。Data Protector 自动将备份操作从故障设备重定向到设备列表中的其他设备。

何时不使用负载均衡

在下列情况中不使用负载均衡：

- 只需备份少量大对象。在这种情况下，Data Protector 一般无法有效均衡设备间的负载。
- 希望明确选择每个对象要备份到的设备。

负载均衡的原理

例如，假设有 100 个对象配置为备份到四个设备，并发数设置为 3，负载均衡参数 MIN 和 MAX 均配置为 2。如果至少有两个设备可用，则会话开始时会将 3 个对象并行备份到最先可用的两个设备中的任何一个设备。其他 94 个对象将暂挂，这时不会分配给特定设备。

特定对象备份执行完毕时，下一个暂挂对象开始进行备份，并分配给不足三个并发备份对象的设备。负载均衡可确保，只要仍有要备份的暂挂对象，两个设备就将并行运行。如果设备在备份期间出现故障，将会使用备用的两个设备中的其中一个设备。正在备份到故障设备的对象将会中止，而接下来的三个暂挂对象会分配给新设备。这意味着，如果有其他设备可供备份会话继续，每个设备的每次故障都可能导致最多三个对象被中止。

设备链

通过 Data Protector 可将连接到同一系统且类型相同的多个独立设备配置为一个设备链。当一个设备中的介质变满时，备份会自动在设备链的下一个设备中的介质上继续进行。

设备流式传送和并发

什么是设备流式传送？

要最大程度地提高设备性能，必须保持设备流式传送。如果设备可以向介质输送足够的数据，使介质保持持续前移，则表示设备在进行流式传送。否则，设备会等待更多的数据，而磁带介质不得不停止移动。也就是说，如果数据写入磁带的速率小于等于计算机系统向设备提供数据的速率，那么表示设备在进行流式传送。在以网络为中心的备份基础架构中，设备流式传送值得关注。对于磁盘和设备都连接到同一系统的本地备份，如果磁盘速度够快，将并发数配置为 1 就可以了。

如何配置设备流式传送

要使设备可以进行流式传送，必须向设备发送足够数量的数据。Data Protector 会为将数据写入设备的每个介质代理启动多个磁盘代理。

磁盘代理并发

为每个介质代理启动的磁盘代理数量称为“磁盘代理 (备份) 并发”，使用设备的“高级”选项或在配置备份时可以修改此项。Data Protector 提供的默认数量足以满足大多数情况。例如，在标准 DDS 设备上，两个磁盘代理可以发送设备流式传送所需的足够数据。对于带有多个驱动器、每个驱动器受一个介质代理控制的库设备，可以单独设置每个驱动器的并发数目。

提高性能

如果设置正确，则备份并发可提高备份性能。例如，如果您的库设备有四个驱动器，每个驱动器受一个介质代理控制，每个介质代理从两个磁盘代理并发地接收数据，来自八个磁盘的数据同时进行备份。

设备流式传送也取决于其他因素，比如，网络负载和写入设备的数据块的大小。

多个数据流

通过 Data Protector 可将磁盘的几个部分并发备份到多个设备。此功能对于将数据容量大、速度快的磁盘备份到相对较慢的设备很有用。多个磁盘代理从磁盘并行读取数据，并将数据发送到多个介质代理。此方法可加快备份速度，但需要考虑以下情况：

如果一个装载点通过多个磁盘代理进行备份，数据将包含在多个对象中。要还原整个装载点，必须在单个备份规范中定义各个装载点部分，然后还原整个会话。

设备过滤

什么是设备过滤？

设备过滤是一种基于群集设置的活动节点选择用于备份的设备目标的机制。

设备过滤器可用于将备份目标分配到附近的客户机以减少网络流量。例如，Oracle RAC Metro 群集可能跨越两个数据中心。设备过滤是一种用于识别数据来源节点并将其分配给该节点本地目标的机制。

设备过滤的工作原理是什么？

在群集设置中，每个节点由被称为主机标记的唯一名称标识。相同名称被分配给可能为潜在目标的设备。在备份规范中选择目标设备时，请选择与所有节点主机标记匹配的设备。在基于数据流入的节点进行备份时，将使用匹配设备。

如何设置设备过滤器标记？

可以采用两种方法之一设置设备过滤器标记：

必须在单元服务器主机以下位置提供的设备过滤器文件中设置设备过滤器标记：

<DP configuration>/server/cell/devfilters

设备过滤器文件在一行中涵盖各个逻辑设备。以下为行格式：

<Logical Device Name><filter tag>[,<filter tag>]*

> **注意**如果 Logical Device Name 包含空格，则必须将整个名称括在引号 (") 中。建议将所有逻辑设备名称括在引号中，最大限度减少出错的可能性。此外， 与 omnirc 变量相似，过滤器标记必须用逗号隔开。

或

可以在 Data Protector GUI 中使用设备属性来配置设备过滤器标记。此外，可以使用 Data Protector GUI 来设置主机标记。可以为每个客户机分配任意数量的过滤器标记。过滤器标记的默认值可以为空，并且可包含任意字母数字字符。不允许空格字符。

设备在备份会话期间进行过滤，并且对照设备过滤器文件来检查 datalist 或 barlist 中的所有设备。主机标记中的所有过滤器标记都必须与适用于特定主机的备份会话的设备的设备过滤器标记相匹配。如果某个设备在设备过滤器文件中不可用，则假定没有为该设备分配任何过滤器标记。因此，如果为客户机设置了过滤器标记，则无法使用该设备。

设备过滤仅适用于驱动器，因此没有必要在设备过滤器文件中添加库（机械手）。

也可以使用以下全局变量来控制设备过滤功能：

- EnableDeviceFilters = 0|1 (默认情况下， EnableDeviceFilters 设置为 0)

  如果将 EnableDeviceFilters 全局变量设为 1 ，则过滤器标记为定义的主机标记和设备过滤器文件。

  如果 EnableDeviceFilters 全局变量设置为 0 ，则即便已经设置过滤器标记，Data Protector 也会将其忽略。

- DeviceFilterMatch = 0|1 (默认情况下， DeviceFilterMatch 设置为 0)

  如果 DeviceFilterMatch 全局变量设置为 0 ，则设备过滤器将以 AND 方式匹配。

  如果 DeviceFilterMatch 全局变量设置为 1 ，则设备过滤器将以 OR 方式匹配。

例如，假设 devfilters 文件和客户机上的主机标记包含以下内容：

devfilters 文件和客户机上的主机标记

devfilters 文件	客户机上的主机标记
"HP:Ultrium 1" tag1	<hostname A> tag1
"HP:Ultrium 2" tag2	<hostname B> tag2
"HP:Ultrium 3" tag1,tag2	<hostname C> tag1,tag2

当 DeviceFilterMatch=0 时，以下设备可用于特定主机上的对象：

来自主机 A 的对象：“HP:Ultrium 1”和“HP:Ultrium 3”设备符合条件

来自主机 B 的对象：“HP:Ultrium 2”和“HP:Ultrium 3”设备符合条件

来自主机 C 的对象：仅“HP:Ultrium 3”设备符合条件

当 DeviceFilterMatch=1 时，以下设备可用于特定主机上的对象：

来自主机 A 的对象：“HP:Ultrium 1”和“HP:Ultrium 3”设备符合条件

来自主机 B 的对象：“HP:Ultrium 2”和“HP:Ultrium 3”设备符合条件

来自主机 C 的对象：“HP:Ultrium 1”、“HP:Ultrium 2”和“HP:Ultrium 3”设备符合条件

以下限制适用:

- Data Protector 文件系统、Data Protector Oracle Server 集成、Data Protector Microsoft Exchange Server 2010 集成和 Data Protector Microsoft SQL Server 集成支持在备份会话期间进行设备过滤。
  通过将全局选项 EnableDeviceFilters 设置为 1，可以启用设备过滤。

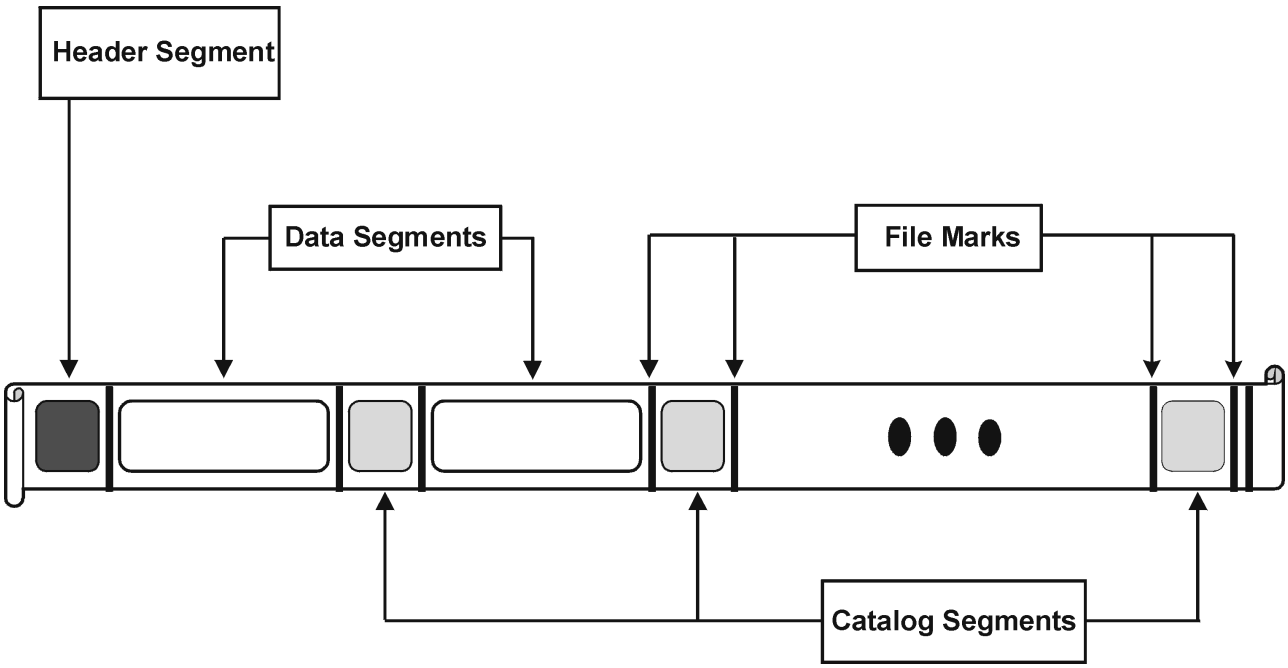
如果您是为设备过滤器功能使用 omnirc 变量 OB2DEVICEFILTER 的现有客户，则需要使用 omnicc -migrate_devfilter [HostName] [-delete_old_devfilter] 命令迁移过滤器标记。

段大小

介质可划分为数据段、编目段和头段。头信息存储在头段中，大小与块大小相同。数据存储在数据段的数据块中。每个数据段的信息存储在相应的编目段中。这些信息先存储在介质代理内存中，然后写入介质的编目段和 IDB。所有段按文件标记划分，如数据格式。

> **注意**某些磁带技术对每个介质的文件标记数目有所限制。确保您的段大小不要过小。

数据格式



段大小（以 MB 为单位度量）是数据段的最大大小。如果要备份大量小型文件，可以通过编目段的最大大小限制实际段大小。用户可以对每个设备的段大小进行配置。段大小会影响还原速度。段大小较小会减少介质上存储数据的空间，因为每个段的文件标记都会占用介质空间。但是，文件标记数目越多还原速度越快，因为介质代理可以更快地找到包含要还原数据的段。最佳段大小取决于设备中使用的介质类型和要备份的数据种类。例如，默认情况下 DLT 介质的段大小为 150 MB。

块大小

段并不作为完整单位，而是分为更小的子单位，称为块。设备的硬件以设备类型特定的块大小为单位处理数据。使用 Data Protector 可以调整发往设备的块大小。大部分设备的默认块大小值是 256 kB。

增加块大小可提高性能。更改块大小应该在格式化磁带*之前*完成。例如，采用默认块大小写入数据的磁带不能附加使用其他块大小的数据。

> ⚠ **警告**为由在特定操作系统上运行的 Data Protector 介质代理控制的设备增加块大小之前，请确保所需块大小不会超过该操作系统支持的默认最大块大小。如果超过限制，则 Data Protector 无法从这类设备还原数据。有关是否可以调整最大支持块大小以及如何调整的信息，请参见操作系统文档。

> **注意**针对可与不同设备类型结合使用的介质使用相同的块大小。Data Protector 只能使用相同的块大小将数据附加到介质。

磁盘代理缓冲区的数量

Data Protector 介质代理和磁盘代理使用内存缓冲器保存等待传输的数据。该内存分为许多个缓冲区（每个磁盘代理对应一个缓冲区，具体取决于设备并发数）。每个缓冲区由 8 磁盘代理缓冲器组成（大小与配置的设备块大小相同）。虽然几乎没有必要更改此值，但是您可以将其更改为 1 和 32 之间的任意值。更改此设置有两个根本原因：

- 内存不足

  介质代理所需的共享内存可以按如下方法计算：

  DAConcurrency * NumberOfBuffers * BlockSize

  比如，将缓冲器数目从 8 个更改为 4 个，可以减少 50% 的内存消耗，但会影响性能。

- 流式传送

  如果可用网络带宽在备份期间变化很大，则介质代理有足够的可供写入的数据对于保持设备流式传送变得更加重要。在这种情况下，需要增加缓冲器数目。

设备锁定和锁名称

设备名称

配置与 Data Protector 结合使用的设备时，可以使用不同特性对同一物理设备进行多次配置，只需在 Data Protector 中使用不同的设备名称配置同一物理设备即可。例如，简单、独立的 DDS 设备可以配置为压缩设备，然后再将其配置为未压缩设备，但不建议进行后一种配置。

物理设备冲突

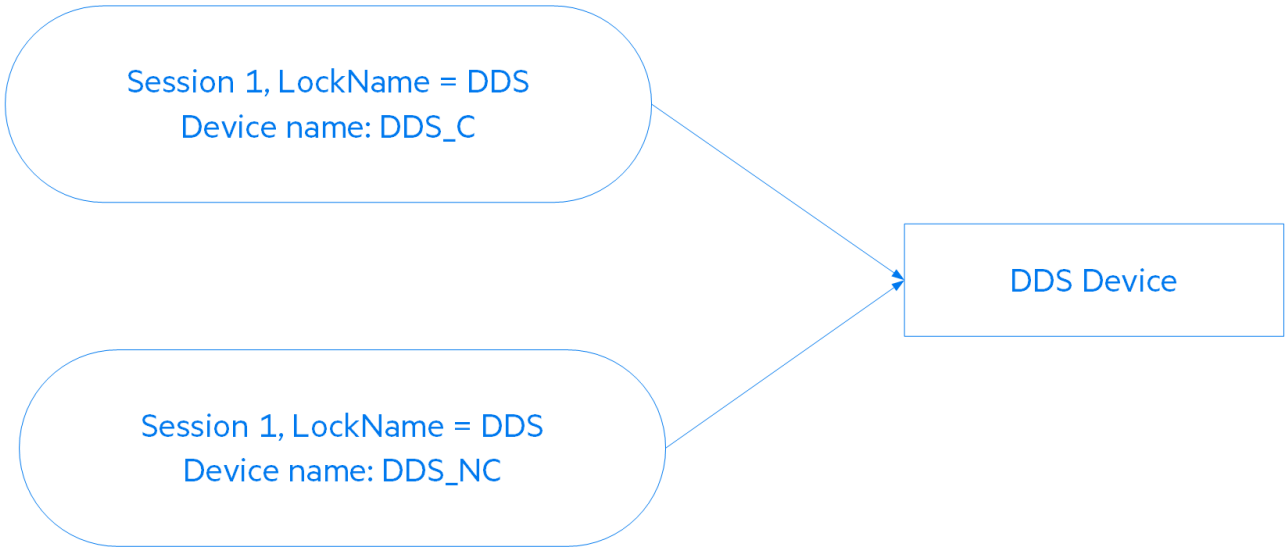
指定用于备份的设备时，可以在一个备份规范中指定一个设备名称，在另一个备份规范中为同一物理设备指定另一个设备名称。根据备份计划，这样可能会导致 Data Protector 在多个备份会话中尝试同时使用同一物理设备，从而产生冲突。

防止冲突

为防止发生此冲突，可在两种磁盘配置中指定一个虚拟锁名称。Data Protector 会检查设备的锁名称是否相同，以防止发生冲突。

例如，将 DDS 设备配置成名为 DDS_C 的压缩设备和名为 DDS_NC 的非压缩设备，如设备锁定和设备名称。为这两种设备指定相同的锁名称 DDS。

设备锁定和设备名称



独立设备

独立设备是指含一个驱动器的设备，该驱动器一次读取/写入到一个介质。

独立设备用于小规模的备份或特殊备份。当介质已满时，操作员必须手动更换新介质以继续备份。

Data Protector 和独立设备

设备连接到系统后，使用 Data Protector 用户界面可以配置与 Data Protector 结合使用的设备。为此，必须先在已连接设备的系统上安装 Data Protector 介质代理。Data Protector 可以检测并自动配置大多数独立设备。

备份期间，当设备中的介质已满时，Data Protector 会发出装载请求。操作员必须更换介质才能继续备份。

什么是设备链？

通过 Data Protector 可将多个独立设备配置为一个设备链。当一个设备中的介质变满时，备份会自动在设备链的下一个设备中的介质上继续进行。

借助设备链，可以使用多个独立设备运行无人看管备份，介质已满时也不必手动插入/弹出介质。

堆栈器设备

堆栈器设备与设备链类似，包含许多按顺序使用的介质。当介质变满时，将加载下一个介质用于备份。

小型盒设备

箱盒设备将许多介质组成一个单元，称为箱盒。Data Protector 将箱盒视为单个介质。盒的容量比单个介质大，处理起来比多个单个介质容易。有关支持的设备的列表，请参阅最新支持矩阵。

Data Protector 和箱盒设备

Data Protector 允许对单个介质执行介质管理任务，也允许对作为集合的箱盒执行介质管理任务，方法是通过提供箱盒视图和介质视图来模拟单个介质。

或者，您可以将箱盒设备用作常规库，而无需使用 Data Protector 箱盒支持。Data Protector 可以检测并自动配置箱盒设备。

清洁脏驱动器

使用磁头清洁磁带功能，Data Protector 可以在箱盒设备和其他设备变脏时自动进行清洁。

大型库

什么是库设备？

库设备是自动化设备，也称为自动加载器、交换器或介质库。在 Data Protector 中，大多数库都配置为 SCSI 库。它们在设备存储库中包含许多介质盒，可以具有若干可一次写入多个介质的驱动器。

典型库设备中的每个驱动器都有一个 SCSI ID，在插槽和驱动器之间来回移动介质的库机械手装置也有一个 SCSI ID。例如，一个由四个驱动器组成的库拥有五个 SCSI ID，其中四个用于驱动器，一个用于机械手装置。

Data Protector 还支持 Silo 库，例如 Libraries、StorageTek/ACSLS 和 ADIC/GRAU AML。有关受支持设备的列表，请参阅最新支持矩阵。

介质处理

Data Protector 用户界面提供特殊的库视图，简化了库设备的管理。

大型库设备中的介质可以都属于一个 Data Protector 介质池，也可以拆分到多个池。

配置库

配置设备时，请配置想要分配给 Data Protector 的插槽范围。这样就可以与其他应用程序共享库。分配的插槽可能包含空白 (新) 介质，Data Protector 或非 Data Protector 介质。Data Protector 检查插槽中的介质，并以库视图显示介质的相关信息。这样，您不仅可以查看 Data Protector 所使用的介质，还可以查看各种介质。

库大小

以下信息有助于您估计所需的库大小：

- 确定需要将介质分散到多个地点还是存放在一个中央位置。
- 获取所需的介质数。

与其他应用程序共享库

可与设备中将数据存储至介质的其他应用程序共享库。

您可以决定将库中的哪些驱动器与 Data Protector 一起使用。例如，在库的四个驱动器中，可以选择仅将其中两个驱动器与 Data Protector 一同使用。

您可以决定库中的哪些插槽用 Data Protector 进行管理。例如，在库的 60 个插槽中，可以将 1-40 个插槽与 Data Protector 一起使用。那么，剩余的插槽就可以由其他应用程序使用和控制。

与其他应用程序共享库对于大型库和 silo 库而言尤其重要，比如 StorageTek/ACSLS 或 ADIC/GRAU AML 设备。

插入/弹出邮件插槽

库设备提供专门的插入/弹出邮件插槽，操作员可以用其将介质插入设备或从设备中弹出介质。根据设备，可以提供多个插入/弹出插槽。如果只有一个邮件插槽，则需逐个插入介质；如果有多个邮件插槽，则在一次插入/弹出操作中可以使用特定数量的插槽。

Data Protector 允许一步插入/弹出多个介质。例如，您可以在设备中选择 50 个插槽，然后通过一次操作弹出所有介质。Data Protector 将自动按正确的顺序弹出介质，以便操作员从插入/弹出邮件插槽取出介质。

有关详细信息，请参见您的设备文档。

条形码支持

Data Protector 通过条形码读取器支持库设备。在这些设备中，每个介质都有一个唯一标识介质的条形码。

条形码的优点

使用条形码显著提高了 Data Protector 识别介质、标记介质和检测磁头清洁磁带的能力。

- 加快了扫描设备存储库中介质的条形码的速度，因为 Data Protector 无需实际向驱动器加载介质和读取介质头。

- Data Protector 会自动读取条形码用于识别介质。
- 如果磁头清洁磁带含有 CLN 条形码前缀，将自动检测该磁头清洁磁带。
- 条形码是介质在 IDB 中的唯一标识符。环境中不能有重复的条形码。

> **提示**在初始化介质时可以选择使用条形码作为介质标签。

磁头清洁磁带支持

Data Protector 使用磁头清洗磁带自动清洗大多数设备。如果 Data Protector 检测到设备驱动器变脏事件，将自动使用该介质进行清洁。

- 对于 SCSI 库，可以定义哪个插槽将用于保存磁头清洁磁带。
- 对于带有条形码读取器的设备，如果磁头清洁磁带含有 CLN 前缀，Data Protector 会自动识别该磁带的条形码。
- 对于不带磁头清洁磁带的设备，检测到脏驱动器会导致在会话监视器窗口显示清洁请求。操作员必须手动清洁设备。

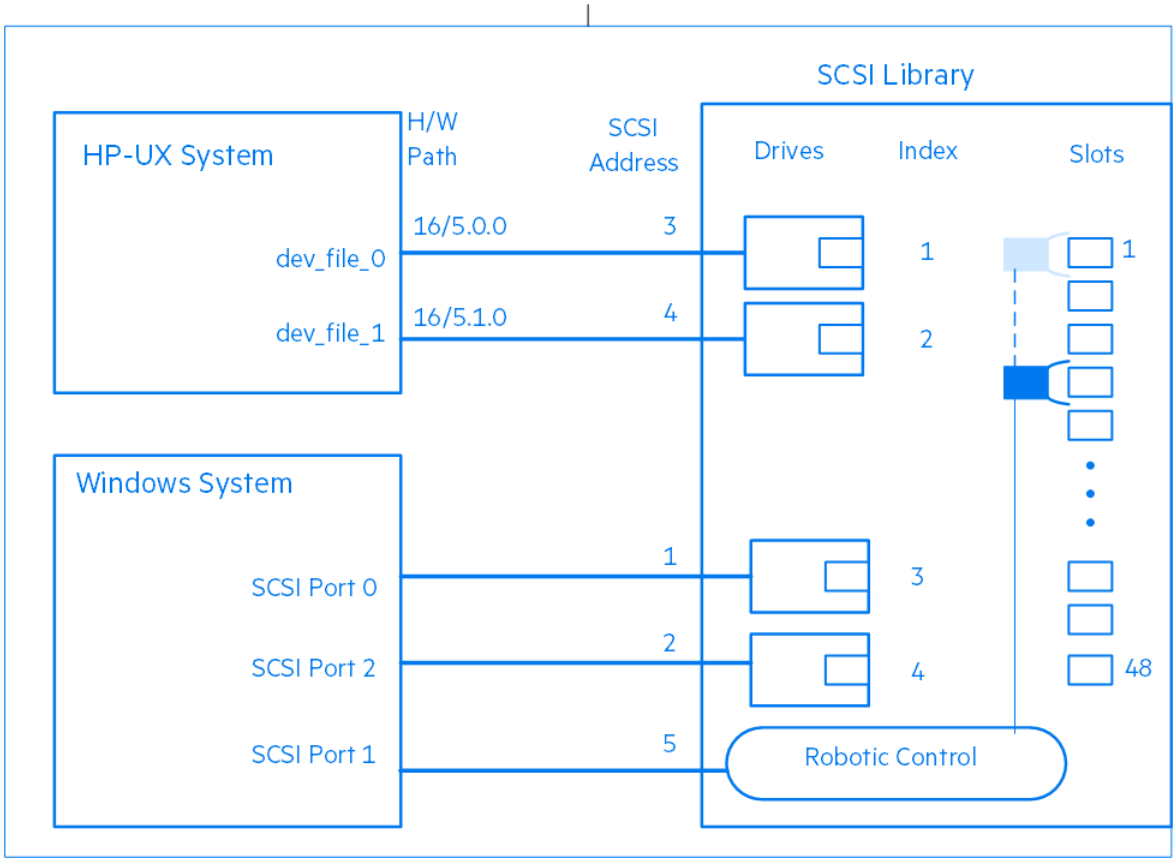
  不清洁设备则无法继续备份，因为备份可能会因数据未正确写入并存储在介质上而告失败。

与多个系统共享库

什么是库共享？

通过设备共享可以将物理库的不同驱动器与不同的系统相连接。这些系统就可以执行到库的本地备份。其结果是大大提高了备份性能，减少了网络流量。要实现库共享，库中的驱动器必须能够接入单独的 SCSI 总线。这一点对于高性能库尤其有用，使驱动器能够以持续的流式传送形式从多个系统接收数据，从而进一步增强性能。Data Protector 将机械手命令内部重定向到管理机械手的系统。

将驱动器与多个系统相连接



控制协议和 Data Protector 介质代理

库中的驱动器必须能够物理连接到已安装 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理) 的不同系统。

对于 Data Protector，有两种用于控制驱动器的协议:

- SCSI — 适用于以 SCSI 或光纤通道连接的驱动器。

  在常规介质代理和 NDMP 介质代理中均可履行此协议。

- NDMP — 用于 NDMP 专用驱动器。

  仅在 NDMP 介质代理中可履行此协议。

另一方面，有四种用于控制库机械手的协议：

- ADIC/GRAU — 适用于 ADIC/GRAU 库机械手
- StorageTek ACS — 适用于 StorageTek ACS 库机械手
- SCSI — 适用于其他库机械手
- NDMP — 适用于 NDMP 机械手

在常规介质代理和 NDMP 介质代理中均可履行所有四种库机械手控制协议。

驱动器控制

任何配置为控制库中驱动器的 Data Protector 客户机系统 (无论使用何种驱动器控制协议和平台) 均可与任何配置为控制库中机械手的 Data Protector 客户机系统 (无论使用何种机械手控制协议和平台) 建立通信。因此，在各种平台上使用各种机械手和驱动器协议均可在 Data Protector 客户机系统之间共享任何受支持库的驱动器。只有在控制 NDMP 服务器备份的客户机系统上才需要 NDMP 介质代理（在为 NDMP 专用驱动器配置的客户机系统上）。在所有其他客户机系统上，两个 Data Protector 介质代理可以互换。

驱动器控制所需的 Data Protector 介质代理显示了配置为控制库驱动器的客户机系统所需的 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)，这里的库是指在多个客户机系统之间实现了驱动器共享的库。

驱动器控制所需的 Data Protector 介质代理

	驱动器控制协议	
NDMP	SCSI	
机械手控制协议 (ADIC/GRAU、StorageTek ACS、SCSI、NDMP)	NDMP 介质代理	NDMP 介质代理或常规介质代理

机械手控制

无论库驱动器使用何种驱动器协议 (NDMP 或 SCSI)，控制库机械手的 Data Protector 客户机系统都可以安装常规介质代理或 NDMP 介质代理。

机械手控制所需的 Data Protector 介质代理显示了配置为控制库机械手的客户机系统所需的 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)，这里的库是指在多个客户机系统之间实现了驱动器共享的库。

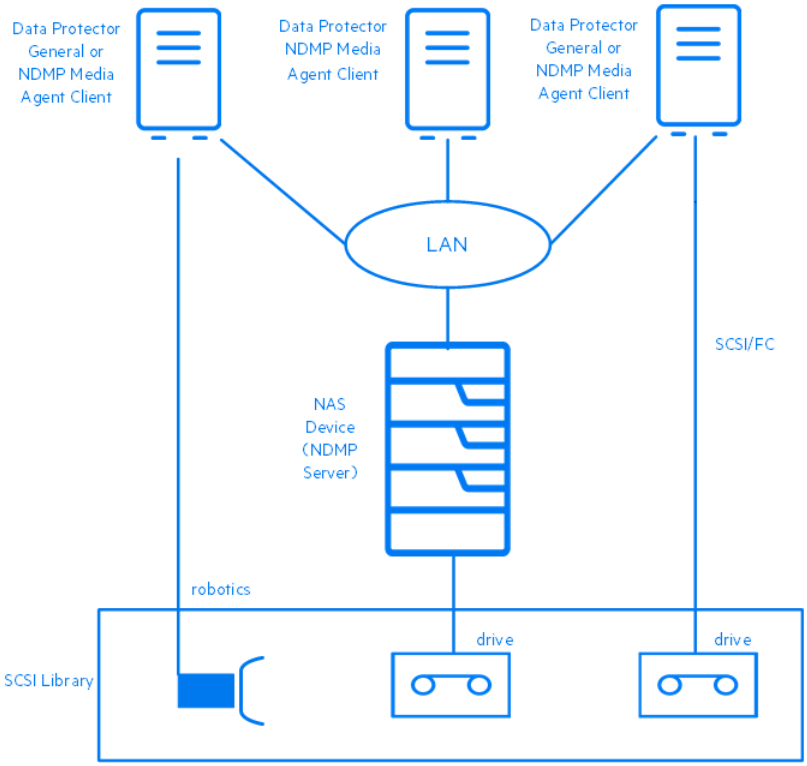
机械手控制所需的 Data Protector 介质代理

	驱动器控制协议			
ADIC/GRAU	StorageTek ACS	SCSI	NDMP	
驱动器控制协议 (NDMP、SCSI)	NDMP 介质代理或常规介质代理	NDMP 介质代理或常规介质代理	NDMP 介质代理或常规介质代理	NDMP 介质代理或常规介质代理

典型配置

共享 SCSI 库 (机械手与 Data Protector 客户机系统相连接) 到共享 ADIC/GRAU 或 StorageTek ACS 库显示了库中共享驱动器的典型配置以及这些配置中的 Data Protector 介质代理分布。

共享 SCSI 库 (机械手与 Data Protector 客户机系统相连接)

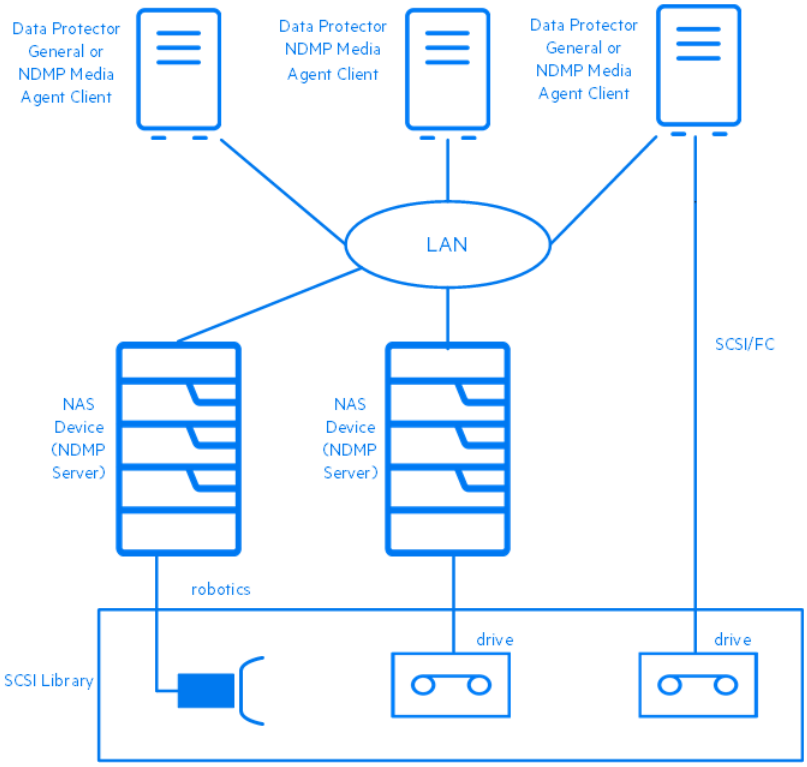


“共享 SCSI 库 (机械手与 Data Protector 客户机系统相连接)”显示的是一个 SCSI 库，其机械手与安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统相连接，并配置在该客户机系统上。客户机上的常规介质代理或 NDMP 介质代理使用 SCSI 机械手控制协议。连接了机械手的 Data Protector 客户机系统同时也连接有一个或多个驱动器。

库中的 NDMP 专用驱动器配置在安装了 NDMP 介质代理的 Data Protector 客户机系统上。客户机上的 NDMP 介质代理使用 NDMP 驱动器控制协议。

另一个库驱动器与安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统相连接，并配置在该系统上。客户机上的常规介质代理或 NDMP 介质代理使用 SCSI 驱动器控制协议。

共享 SCSI 库（机械手与 NDMP 服务器相连接）



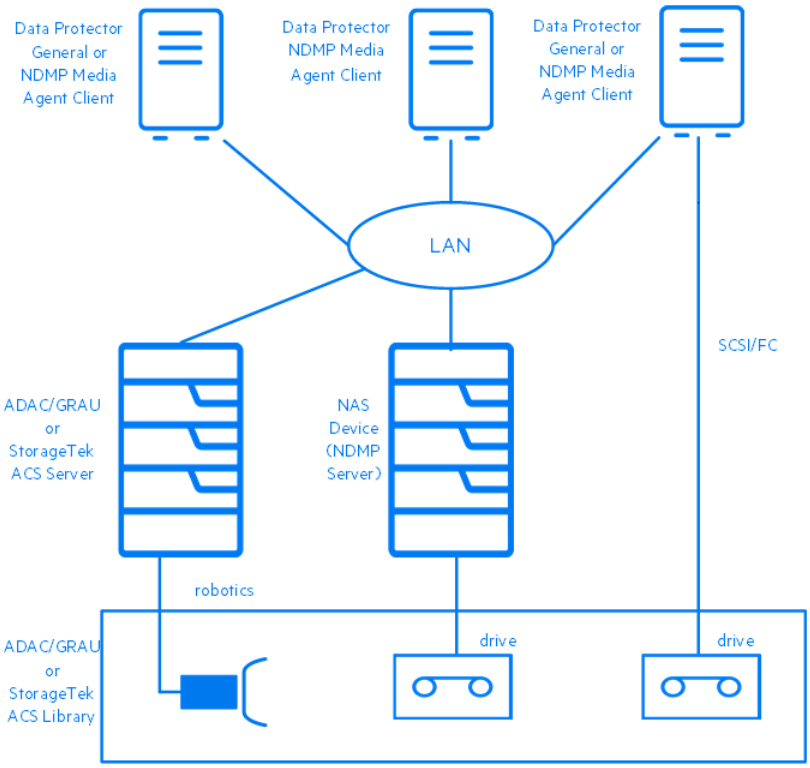
“共享 SCSI 库 (机械手与 NDMP 服务器相连接)”显示的是一个 SCSI 库，其机械手与 NDMP 服务器相连接，并配置在安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统上。客户机上的常规介质代理或 NDMP 介质代理使用 SCSI 机械手控制协议。连接了机械手的 NDMP 服务器同时也连接有一个或多个驱动器。

重要说明如果连接了机械手的 NDMP 服务器同时也连接有 NDMP 专用驱动器，那么在其上配置了机械手和 NDMP 专用驱动器的 Data Protector 客户机系统只能安装 NDMP 介质代理，因为 NDMP 专用驱动器使用 NDMP 驱动器控制协议。

库中的 NDMP 专用驱动器配置在安装了 NDMP 介质代理的 Data Protector 客户机系统上。客户机上的 NDMP 介质代理使用 NDMP 驱动器控制协议。

另一个库驱动器与安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统相连接，并配置在该系统上。客户机上的常规介质代理或 NDMP 介质代理使用 SCSI 驱动器控制协议。

共享 ADIC/GRAU 或 StorageTek ACS 库



“共享 ADIC/GRAU 或 StorageTek ACS 库”显示的是一个 ADIC/GRAU 或 StorageTek ACS 库，其机械手与 ADIC/GRAU 或 StorageTek ACS 服务器相连接，配置在安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统上。客户机上的常规介质代理或 NDMP 介质代理使用 ADIC/GRAU 机械手控制协议。ADIC/GRAU 或 StorageTek ACS 服务器也连接有一个或多个驱动器。

库中的 NDMP 专用驱动器配置在安装了 NDMP 介质代理的 Data Protector 客户机系统上。客户机上的 NDMP 介质代理使用 NDMP 驱动器控制协议。

另一个库驱动器与安装了常规介质代理或 NDMP 介质代理的 Data Protector 客户机系统相连接，并配置在该系统上。客户机上的常规介质代理或 NDMP 介质代理使用 SCSI 驱动器控制协议。

基于磁盘的备份设备

本节将介绍与将数据备份到磁盘相关联的概念及其实现技术，还将讨论 Data Protector 支持的磁盘到磁盘备份配置。

在整个工作日中，许多应用程序和数据库会频繁对现有文件进行小的更改，或生成包含业务关键数据的许多新文件。这些文件必须立即备份，以确保其中数据不会丢失。这种要求意味着需要一种能够存储大量数据且无需中断就能工作的快速介质来存储数据。

磁盘设备的好处

在许多情况下，执行备份时使用基于磁盘的设备更具优势。基于磁盘的设备实际上就是特定文件或指定目录，您可以将数据备份到这些文件或目录中，作为备份到磁带的替代方法或补充。以下列表指出了基于磁盘的设备特别有用的某些场合：

- 许多应用程序和数据库会连续生成或更改大量文件，这些文件包含业务关键数据。在上述情况下，必须连续备份相关文件，以确保能够还原它们而不丢失数据。

  在这些环境下，磁带设备通常必须处于停止/启动模式，因为它们并不接收连续的数据流。这会导致磁带设备限制对相关文件的访问。此外，备份设备的寿命也会大大缩短。

  作为替代方法，可以在任何基于磁盘的设备上执行备份，以克服上述局限性。作为短期备份解决方案，这就足够了。如果需要长期备份解决方案，可定期将基于磁盘的设备中的数据移到磁带，以释放磁盘空间。该过程也称为**磁盘暂存**。

- 在具有高速大容量磁盘驱动器和低速磁带驱动器的环境中，您可以通过先执行备份到基于磁盘的设备，然后再把数据移到磁带，来缩短备份的时间窗口。
- 使用基于磁盘的设备进行备份时，可以利用**合成备份**等高级备份策略。
- 基于磁盘的设备在为最近备份的数据提供快速还原功能方面很有用。例如，备份数据可以 24 小时保留在基于磁盘的设备中，以提供快速方便的还原功能。
- 从机械结构来看，基于磁盘的设备使用起来比磁带快。使用基于磁盘的设备时，无需装入和取出磁带。备份或还原少量数据时，基于磁盘的设备更快，因为它无需磁带驱动器所需的初始化时间。使用基于磁盘的设备，无需装载和卸载介质，后者在小规模备份或还原时会耗费大量时间。从增量备份进行还原时，使用基于磁盘的设备的优势更为明显。
- 介质出问题的风险（如磁带故障、磁带装入失败）也降至最低。由于可以使用 RAID 磁盘配置，在发生磁盘故障时数据也能得到保护。
- 由于无需处理磁带，管理成本也相应降低。
- 总体来说，即使与基于磁带的存储相比，基于磁盘的存储空间也越来越便宜。

Data Protector 基于磁盘的设备

Data Protector 具有以下基于磁盘的设备:

- 独立文件设备
- 文件介质库设备
- 文件库设备
- StoreOnce 设备
- 数据域设备

独立文件设备

独立文件设备是最简单的基于磁盘的备份设备。它由可用于备份数据的单个插槽组成。配置后，其属性就不能更改了。文件设备的最大容量是 2 TB，前提是运行设备的操作系统支持该文件大小。

文件介质库设备

文件介质库设备是 Data Protector 介质库设备的特殊版本。介质库设备可配置为备份光学介质或文件介质。用于备份文件介质的介质库设备称为文件介质库设备。介质库要备份的介质类型在设备配置时指定。

文件介质库设备由可用于备份数据的多个插槽组成。配置过程分为两个阶段，第一阶段是创建文件介质库设备，第二阶段是为其配置一个或多个驱动器。配置完设备后，即可更改其属性。文件介质库设备中每个插槽的最大容量为 2 TB。设备的最大容量等于：

```
Number of slots * 2 TB
```

文件库设备

文件库设备是最复杂的基于磁盘的备份设备。它有多个称为**文件仓库**的插槽，您可以将数据备份到其中。文件库设备的配置只需一步即可完成。可以随时更改文件库设备的属性。设备的最大容量等于设备所驻留文件系统上可保存的最大容量。每个文件仓库的最大容量最多为 2 TB。将根据需要自动创建文件仓库。

文件库设备具有智能磁盘空间管理功能。保存数据时，它会预测可能发生的问题。如果剩余磁盘空间量接近设备工作所需的配置最低量，则将在事件日志中写入警告消息。这样，您就可以在设备状况良好时释放更多磁盘空间，以继续保存数据。如果分配给文件库设备的所有空间完全用尽，屏幕上将出现警告消息，并指示如何解决该问题。

如果特定备份所需空间大于单个文件仓库的可用空间，则文件库设备会自动创建更多文件仓库。

推荐的磁盘备份设备

建议使用文件库设备作为首选的基于磁盘的备份设备。文件库设备在这组基于磁盘的备份设备中，是最灵活、最智能的。它可以在使用中随时重新配置，与任何其他基于磁盘的备份设备相比，它能执行更为复杂的磁盘空间处理任务。此外，它还能够使用高级备份策略，如合成备份。

有关文件库设备功能的说明，请参阅《Data Protector 帮助》索引: “文件库设备”。

数据格式

基于磁盘的设备的数据格式以磁带数据格式为基础。Data Protector 先将要备份的数据转换为磁带格式，然后再将数据写入基于磁盘的设备。智能缓存设备以本机格式保存数据，并将实际数据与元数据分开。

使用用于**虚拟完整备份**的文件库时，必须采用分布式文件介质格式。在设备的属性中选择该格式。

备份到磁盘设备

备份到磁盘 (B2D) 设备提供更高级的功能，如重复数据删除、云存储和增强的 Vmware 特定功能。

Data Protector 集成了备份到磁盘设备和重复数据删除功能。通过支持重复数据删除，Data Protector 引入了多个新概念，包括一种新的设备类型 — 备份到磁盘设备，以及四种接口类型: StoreOnce 软件重复数据删除、StoreOnce 备份系统、智能缓存和 EMC 数据域提升。本文档将详细讨论备份到磁盘设备和重复数据删除。

*备份到磁盘设备*是将数据备份到物理存储磁盘并支持多主机配置的设备。这些设备支持不同的后端，如 HP StoreOnce 软件重复数据删除、StoreOnce 备份系统、智能缓存或 EMC 数据域提升。本文档还介绍了*重复数据删除技术*背后的基本原理。

Data Protector 支持以下重复数据删除后端：

- “Data Protector 软件重复数据删除”能够在几乎任何行业标准硬件上部署目标端重复数据删除功能。因其能够部署更广泛的硬件设置，所以提供了比现有解决方案更强的灵活性，并且还提供了企业级的可扩展性。

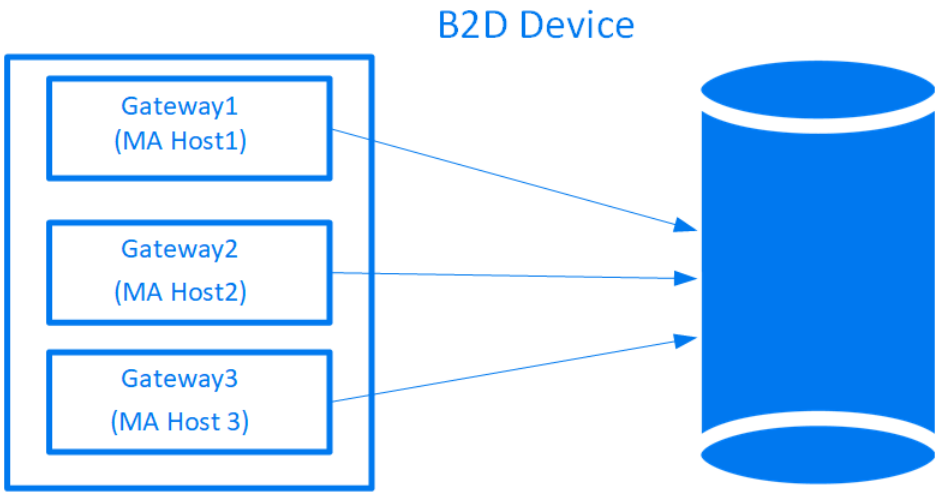
  由于 Data Protector 使用了非常高效的 StoreOnce 引擎，因此 Data Protector 软件重复数据删除可非常有效地使用内存。因此，您可以在应用程序或备份服务器上部署重复数据删除，而不会降低应用程序性能。Data Protector 软件重复数据删除甚至可以部署在虚拟机上。此外，Data Protector 软件重复数据删除还具有非常高的吞吐量。

- “StoreOnce 备份系统”设备是支持重复数据删除的磁盘到磁盘 (D2D) 备份设备。
- 智能缓存设备是备份到磁盘设备，允许从 VMware 备份进行恢复。
- *EMC 数据域提升*设备是支持重复数据删除的 D2D 备份设备。

B2D 设备的操作和详细信息

备份到磁盘 (B2D) 设备可将数据备份到物理存储磁盘。B2D 设备支持多主机配置。这表示可以通过多个主机（称为网关）访问单个物理存储磁盘。每个网关都代表一个安装有介质代理组件的 Data Protector 客户机。B2D 设备是一种逻辑设备，由多个网关和一个存储区组成。下图显示了具有多个网关的通用 B2D 设备与存储区之间的关系。

B2D 设备（逻辑视图）

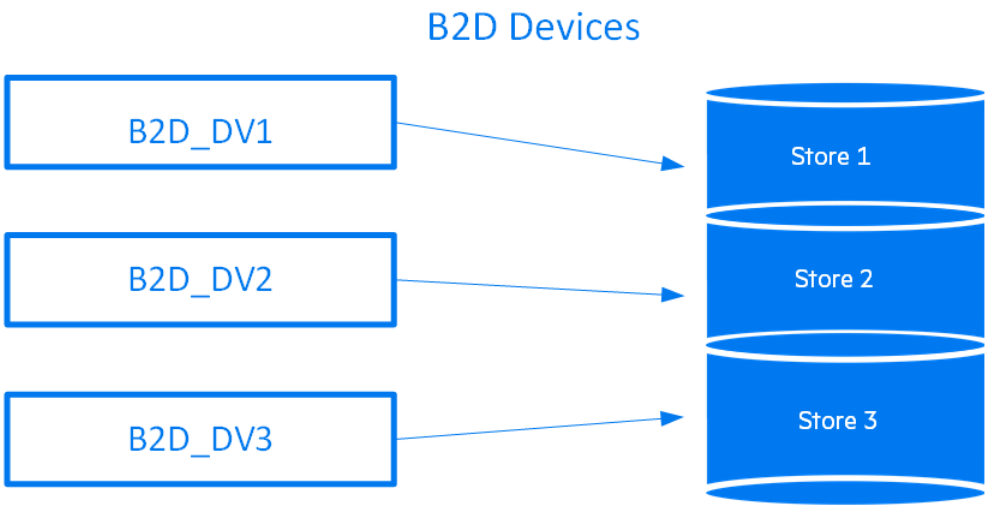


物理存储区还可以划分为表示特定存储部分的各个存储区，这类似于对硬盘进行分区。 存储区由网络路径表示，并由备份应用程序使用。这些参数以及任何其他设备配置信息都存储在 IDB 的设备配置中。

物理存储磁盘上的每个存储区只能通过一个 B2D 设备进行访问。但是，多个 B2D 设备可以访问相同物理存储上的不同存储区。

> **注意**某些物理磁盘限制不适用于基于云的设备。

访问同一物理磁盘上三个单独存储区的三个单独 B2D 设备



配置 B2D 设备时，请注意以下事项：

- 可以在单个重复数据删除服务器节点上配置多个存储区。这些存储区共享资源，例如 CPU、内存、磁盘 I/O 以及每个重复数据删除系统的连接数。但是，每个存储区代表各自的重复数据删除域。重复数据删除不会发生在不同的存储区。
- 每个存储区必须配置各自的专用 B2D 设备。无法将两个存储区配置到同一个 B2D 设备。
- 每个 B2D 设备必须独占使用一个存储区。不支持多个 B2D 设备访问同一个存储区。

可以在特定网关上启动的介质代理数由以下各项定义：

- 网关限制。每个 B2D 网关都受限于最大数量的并行流。此限制已在 GUI 中指定。
- 存储区的连接限制。每个 B2D 设备受限于每个存储区的最大连接数。此限制已在 GUI 中指定。如果该值未被选中，Data Protector 将使用可用的最大值。
- 物理存储磁盘的物理连接限制。此值从物理存储区检索得到（见下文）。
- 根据当前操作，每个 Session Manager 会尝试针对以下输入参数平衡网关上的介质代理数：
  - 要备份的对象数
  - 对象位置
  - 物理连接限制。
- 对象位置
- 物理连接限制。

会话期间验证物理连接限制（物理上可能的最大数量）。GUI 中输入的值根据可用连接数进行检查。如果输入的值超过物理限制，则使用物理限制。物理连接限制无法在 GUI 中配置。(注意: 要使用最大数量，请取消选中该选项)。当没有数据连接处于活动状态时，物理连接限制为 100。达到此限制后进行的数据连接将无法成功。

如果大型物理存储已经被分区成较小的存储区（存储区 1、存储区 2、存储区 3，如前所述），则这些存储区中的每个存储区都有连接数限制。

以下限制适用:

- 如果源和目标存储不具备相应证书，则不支持备份到硬盘 (B2D) 间的复制。复制会话失败，并显示以下错误消息：

```
权限被拒
```

如果具有源存储的原始客户机没有访问目标存储的权限，则将客户机信息导入到其他客户机时无法更改写入源存储的信息。即使新客户机有权访问目标存储，此问题也无法解决。源主机上的原始信息写入重要存储中。

设备锁定

锁定的用途是确保一次只有一个系统与在若干系统之间共享的设备进行通信。对于 B2D 设备，必须遵循某些连接限制。这些连接限制是每个网关的并行流的最大数量和每个存储区的最大连接数。Data Protector 为这两个资源保留锁定计数。达到限制时，锁定将被拒绝。如果锁定请求成功，则网关和存储区的锁定计数将增加。网关解锁时，锁定计数将减少。这可确保 B2D 连接限制被视为存在于整个 Cell Manager 范围内，而不仅仅是在特定会话期间。

对象合并

为了适应网关和网关/存储区/设备连接限制，对象复制和合并功能可确保：

- 当 B2D 设备用作源时，至少有一个连接可用于对象复制，至少 n 个连接用于对象合并，其中 n 是用于合并的源介质数量（详见下一段落）。
- 当 B2D 设备用作目标时，至少 m 个连接必须可用，其中 m 是复制/合并规范中的最小设备设置。如果并行使用其他类型的设备，则 CSM（复制和合并会话管理器）会尝试平衡这些设备，以便达到最小设置，否则将终止会话。

合并备份数据（完整备份和增量备份）时，请确保到存储区有足够的可用连接。通过考虑一个含六个增量的合并会话示例，这一点可更容易地得到解释。在这种情况下，连接数 = 1（完整）+ 6（增量）+ 1（目标）= 8 个连接。建议每周对 6 到 10 个增量运行一次合并会话。

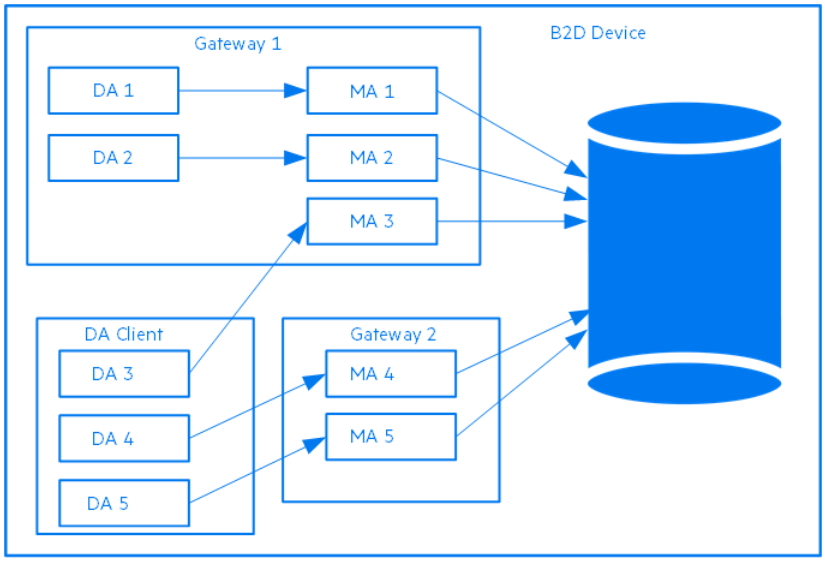
使用 B2D 设备备份数据

备份到 B2D 设备类似于备份到基于磁带的设备。显著的区别是会话管理器在定义的网关上动态生成介质代理，介质代理通过特定于设备的 API 与设备进行通信。

以下是使用具有两个网关（网关 1 和网关 2）的一个 B2D 设备的备份会话示例。五个对象（DA 1 ... DA 5）正在进行备份，其中两个对象是第一个网关的本地对象，另外三个对象是两个网关的远程对象。到物理存储的连接数为 6。备份规范配置为：

- 负载均衡（最大）参数设置为 5（表示在此会话期间最多可以使用 5 个介质代理）
- B2D 设备的连接限制设置为 10。
- 两个网关的连接限制为 5。

使用两个网关（本地和远程对象）的备份配置示例



会话管理器根据上述配置动态启动五个介质代理。由于涉及两个网关，五个介质代理分布在两个网关之间。负载均衡算法在介质代理之间分布磁盘代理，使网关 1 的本地磁盘代理分配给该网关上的介质代理。其他磁盘代理在两个网关之间进行负载均衡，因为它们对于所有介质代理而言是远程代理。

创建备份规范时，可以选择 B2D 设备作为目标。也可以选择特定的网关。如果选择 B2D 设备作为目标设备，则在备份过程中将使用最新的设备配置信息选择所有网关。但是，这仅适用于负载均衡备份。配置静态备份（非负载均衡）时，只能将每个对象分配给网关，而不能分配给 B2D 设备。

B2D 设备使用特殊数据格式进行快速读/写访问，以及提高重复数据删除比率。该格式将元数据从要备份的实际数据中分割出来。选择 B2D 设备时将自动设置数据格式，并且此数据格式仅用于 B2D 设备。

网关

备份到磁盘 (B2D) 设备必须配置为访问预定义的网关。网关或*网关客户端*是安装了介质代理组件的客户端（客户端必须是 64 位系统，请参见下文）。与单元中的任何其他客户端一样，它可以进行备份。网关由唯一的名称标识。网关名称包括将设备指向物理存储的网络路径名。默认命名约定类似于文件库：*DeviceName_gwnumber*。从 GUI 中的下拉列表中选择网关。无法充当网关的客户机未被列出。

可以验证（检查）网关连接来确保设备能够与网关通信。如果网关因任何原因而不可用，将显示错误状态。此外，网关属性和功能包括：

- 网关属性（如网关名称和高级选项）可以在“网关属性”对话框中修改。多个网关的属性可以同时修改。
- 可以启用或禁用网关。要启用或禁用网关，请右键单击要在“设备”列表中启用或禁用的网关，然后相应地选择“启用网关”或“禁用网关”。
- 介质代理组件只能安装在 64 位客户机系统上。这意味着如果要将客户机指定为网关，则它必须是 64 位系统。
- 每个网关表示一个主机，在该主机上可以同时启动多个介质代理（采用单个会话或多个会话）。为此，网关有时被称为介质代理主机。
- 如果您熟悉基于库的设备，B2D 设备相当于库，网关相当于库中的驱动器。

源端网关

您还可以为每个设备配置一个源端网关。如果启用源端重复数据删除，则此（虚拟）网关将在备份系统上自动扩展。这些网关的默认命名约定为 *DeviceName*_Source_side。

StoreOnce 库（重复数据删除存储区）

StoreOnce 库 (或重复数据删除存储区) 是由 StoreOnce 软件重复数据删除接口使用的物理存储磁盘 (StoreOnce 软件重复数据删除使用 StoreOnce 备份系统技术)。物理磁盘支持的容量为 20 TB（删除重复的数据）。通常，重复数据删除比率为 20:1，相当于备份 400 TB 的数据。如果使用多个存储区，支持的总容量仍为 20 TB。

一个 StoreOnce 软件重复数据删除系统可以托管多个重复数据删除存储区，前提是这些存储区共享相同的根目录。尽管 Data Protector 每卷最多支持 32 个存储区，但只有一个存储区可实现最佳性能（就重复数据删除比率而言）。配置重复数据删除存储区只需一步即可完成。

启动 SOS 服务/后台程序后启动存储区时，会发生以下过程:

- 运行维护作业。
- 删除回收文件夹中的详细说明数据。
- 检查每个存储区中是否存在 s.dirty 标记文件。如果存在此文件，则进行恢复过程。

以下限制适用：

- 在备份失败不久后重建断开的介质失败，并显示以下错误消息：

```
无法加载或打开介质。
```

StoreOnce 或 EMC 数据域提升备份系统设备上会出现此问题。因此，必须等待一段时间再触发重建。

StoreOnce 软件重复数据删除的等待时间为 2 个小时，EMC 数据域提升设备的等待时间为 3 个小时。

- 在连接断开时，StoreOnce Catalyst 不支持重新连接到 Data Protector 介质代理。

从重复数据删除存储区中删除过期的备份数据

Data Protector 定期自动触发清理会话来删除物理存储区中的备份数据。可采用多种方法来删除不受保护的数据。

- 手动删除不受保护的 B2D 备份对象

  Data Protector 会对存储区中不受保护的备份对象构建列表。Data Protector 首先将其从存储区中删除，然后从 Data Protector 数据库中删除介质（对象）信息。请注意，从存储区中删除介质不会释放磁盘空间；它只是指示存储区将数据视为已过时。

- 自动删除不受保护的 B2D 备份对象

  此方法与上述方法相同，但由 Data Protector 定期自动执行。该间隔可以在全局选项文件中进行配置。

- 删除插槽时立即删除

  删除插槽将从 IDB 中删除插槽和插槽中的对象，插槽本身也将从存储区中删除。这与回收和删除操作相同。

删除不受保护的 B2D 备份对象会立即删除关联的插槽。删除项目不会立即释放磁盘空间。在下一个内务管理作业中，将删除过期的文件和未引用的区块，并可能释放一些磁盘空间。

> **注意**冗余数据是存储区中不再引用的数据。对于过期的数据，保护日期已过期。

清除重复数据删除存储区中的冗余数据

Data Protector 提供空间管理（内务管理）实用程序来优化存储空间。内务管理实用程序默认启动，并在后台运行。

当数据区块不再被索引表引用时，则变得冗余。数据不会自动从存储区中删除。这仅在内务管理实用程序运行并释放磁盘空间时才会发生。

StoreOnce 软件存储区的稳定性

StoreOnce 软件重复数据删除具有内置机制来验证存储区的完整性。为了最大限度地减少或防止数据丢失，请注意以下事项：

- 使用不间断电源 (UPS)。它可增强 StoreOnce 软件重复数据删除系统的容错能力。当主电源丢失时，UPS 可让您的计算机在短时间内保持运行。它还可防止电涌。
- 存储区必须配置为 RAID 阵列。由于重复数据删除存储区的目录结构，如果一个磁盘损坏，整个存储区将变得不可用。首选硬件 RAID。
- 对于关键数据，建议从重复数据删除存储区到磁带执行对象复制操作。备份时不要写入存储区。

重复数据删除统计信息

对于使用重复数据删除的备份会话，Data Protector 会在每个对象版本完成后显示备份统计信息，例如：

Source-side Deduplication Statistics for dd2.company.com:/C "C:".

Using device: "b2d_Source_side [GW 13148:3:649335383]@dd2.company.com":

Mbytes Total: ..... 35 MB

Mbytes Written to Disk: ..... 1 MB

Deduplication Ratio: ..... 35.0 : 1

统计信息包括：

- The type of the deduplication (source-side, target-side, and server-side)
- Information about the device.
- Mbytes Total: 对象版本的原始大小（要备份的数据）。
- Mbytes Written to Disk: 重复数据删除后写入磁盘的实际大小。（如果小于 1 MB，则显示 1 MB）。
- Deduplication Ratio: “总计 (MB)”除以“已写入磁盘的数据 (MB)”。（见下面的备注。）

在解释重复数据删除比率时，请注意以下事项：

- 如果“已写入磁盘的数据 (MB)”的值小于 1 MB，则舍入为 1 MB（否则计算会产生不切合实际的结果）。
- 通常，您可以预期 10 - 20:1 的重复数据删除比率。忽略错误比率（例如，4435:1）。当分母（已写入磁盘的数据 (MB)）非常小时，可能会发生这种情况。

备份统计信息中显示的比率适用于当前会话。CLI 中显示的比率适用于整个存储区。

重复数据删除比率

使用重复数据删除功能节省的存储容量通常以比率表示。所有预先删除重复的备份数据的总和与删除重复的数据所需的实际存储量进行比较。例如，10:1 的比率表示，与没有使用重复数据删除相比，多存储了 10 倍数据。

影响重复数据删除比率的最重要因素是：

- 数据保留期。
- 备份之间的更改量。
- 文件大小：小文件可能导致较低的重复数据删除比率。

但是，许多因素会影响在特定环境中节省的存储空间。此比率在设备上下文 (“设备”>“存储区”) 中的摘要屏幕 (添加设备后) 以及备份操作后的备

份统计信息中进行报告 (有关典型的输出，请参阅重复数据删除统计信息)。

建议将 B2D 设备配置为使用 256 KB 的块大小来实现更高的重复数据删除比率。

以下限制适用：

- 重复数据删除不适合存档数据。
- 群集环境不支持 StoreOnceSoftware 代理。
- 不支持多个 B2D 设备访问同一个存储区。这意味着每个 B2D 设备必须配置为专用存储区。不要配置第二个设备来使用相同的存储区。
- 如果合并备份数据（完整备份和增量备份）所需的连接数超过最大连接数，则无法合并的还原链将终止。另见对象合并。
- 具有本地网关的磁盘代理客户机支持灾难恢复。要对具有本地网关的磁盘代理客户机执行灾难恢复，必须在“灾难恢复”设置中选择“使用原始网络设置”选项。
- 源端重复数据删除不支持对象镜像。
- B2D 设备不支持自动介质复制。
- 在 B2D 设备之间启用复制时，必须将所选目标设备上每个存储区的最大连接数设置为大于或等于备份规范中配置的负载均衡的最大限制。
- 您不能选择源端网关进行对象合并。对于完整备份，Data Protector 会自动选择另一个网关。对于增量备份，您需要手动选择另一个网关。网关必须与源端网关属于相同的 B2D 设备。
- 您不能选择源端网关进行对象复制。您可以：
  - 手动将读取源设备替换为非源端网关。网关必须与源端网关属于相同的 B2D 设备。
  - 在非源端网关的“属性”窗口中，转到“策略”选项卡，并选择“网关可用作进行对象副本的源网关”。Data Protector 会自动将源端网关替换为此网关。
- 启用加密控制通信时，不支持排除。运行 StoreOnce 软件后台程序的单元成员一旦受到保护，后台程序将只处理安全连接。
- 为其运行的系统（单元成员）启用加密控制通信后，必须手动重新启动 StoreOnce 软件服务/后台程序。
- 只有在已连接至 FC 的系统上，才可对使用光纤通道 (FC) 配置的 StoreOnce 备份系统设备执行源端重复数据删除备份。因此，在执行此备份之前，必须确保系统符合以下要求：
  - 已安装 Data Protector 磁盘代理。
  - 已安装 Data Protector 介质代理。
  - 已配置光纤通道连接。

  备份期间，您可使用“系统已准备好源端重复数据删除”选项，过滤出那些不支持源端重复数据删除的系统。但是，此选项并不会过滤出那些没有 FC 连接的系统，而 FC 连接是对使用 FC 配置的 StoreOnce 备份系统设备执行源端重复数据删除备份的要求之一。

  要验证系统是否具有 FC 连接，请单击“检查”以验证网关，同时添加 StoreOnce 备份系统设备。
- 选择用于复制的设备必须具备复制功能。
- 选择用于复制的源设备和目标设备类型必须相同。
- 在 StoreOnce 库内，源设备和目标设备必须属于不同存储。
- 必须在至少一个备份规范中配置源设备。
- 在数据域设备上执行交互复制时，只能选择一个会话进行复制。
- 必须在源和目标数据域设备上安装相同版本的数据域操作系统 (DDOS)。有关详细信息，请参见您的数据域文档。
- 在连接断开时，StoreOnce Catalyst 不支持重新连接到 Data Protector 介质代理。

智能缓存

智能缓存是备份到磁盘设备，允许从 VMware 备份进行恢复。智能缓存设备可在以下装载点之一上操作：

- NAS 共享（CIFS 和 NFS）
- 使用文件系统格式化的磁盘（SAN、iSCSI、本地）

智能缓存设备使用 GUI 进行配置。有关详细信息，请参阅《Data Protector 帮助》中的“配置备份到磁盘设备”。

> **注意**只有 Windows x64 和 Linux x64 操作系统支持 Smart Cache 设备。

注意Smart Cache 磁盘只能作为 VMware 备份的目标设备。

重要说明不支持编码或 AES 256 位加密 VMware 备份和将对象复制到 Smart Cache 设备。但是支持在具有硬件加密的磁带设备中进行对象复制。

Data Protector 和存储区域网络

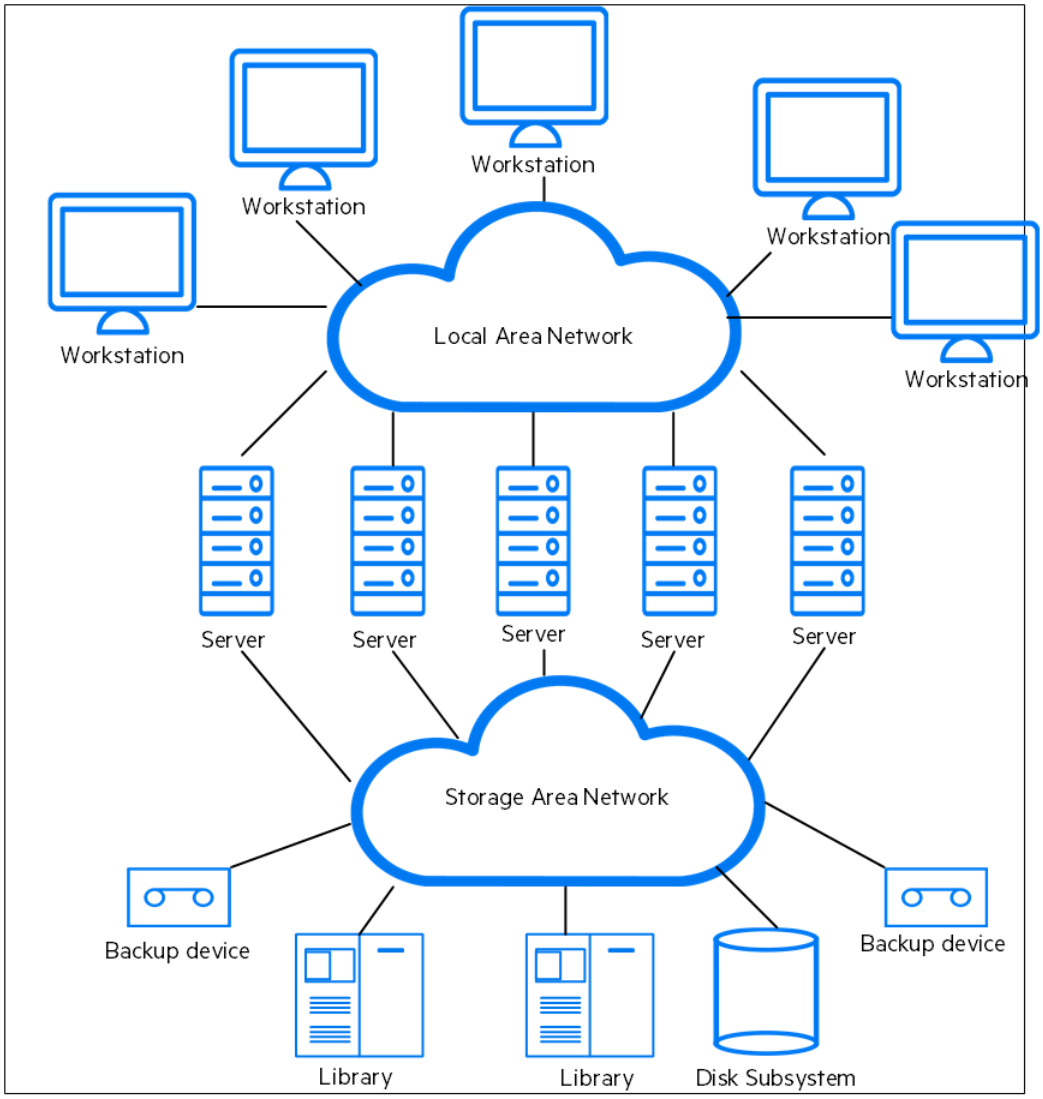
在您企业的什么地方以及如何存储数据将会对企业业务产生重大影响。信息对于大多数公司而言变得日益重要。如今，千兆字节的数据必须通过网络供用户访问。Data Protector 基于 SAN 的光纤通道技术的实现为您提供了所需的数据存储解决方案。

存储区域网络

存储区域网络 (SAN) 为所有网络资源提供“任意互连”，因而能够在多个客户机系统之间实现设备共享，增强数据流量性能和设备可用性。

使用 SAN 概念可以在多个数据存储设备和服务器之间交换信息。服务器可以从任意设备直接访问数据，无需通过传统的 LAN 传输数据。SAN 由服务器、备份设备、磁盘阵列和其他节点构成，各部分通过快速的网络连接（通常是光纤通道）进行连接。这种附加的网络提供从传统 LAN 到单独网络的卸载存储操作。

存储区域网络



光纤通道

光纤通道是高速计算机互联的 ANSI 标准。它使用光缆或铜缆，支持双向传输大型数据文件。光纤通道是目前最可靠、最高效的信息存储、传输和检索方法。

光纤通道使用 3 种物理拓扑连接节点，可以有以下几种变式:

- 点对点拓扑
- 环拓扑
- 交换式拓扑

点对点拓扑、环拓扑和交换式光纤通道拓扑可以混合使用，以便最好地满足您的连接和增长需求。

有关支持的配置的列表，请参阅最新支持矩阵。

点对点拓扑

这种拓扑允许在两个节点（通常是服务器和备份设备）之间进行连接。最主要的优点是提高性能，拉长节点之间的距离。

环拓扑

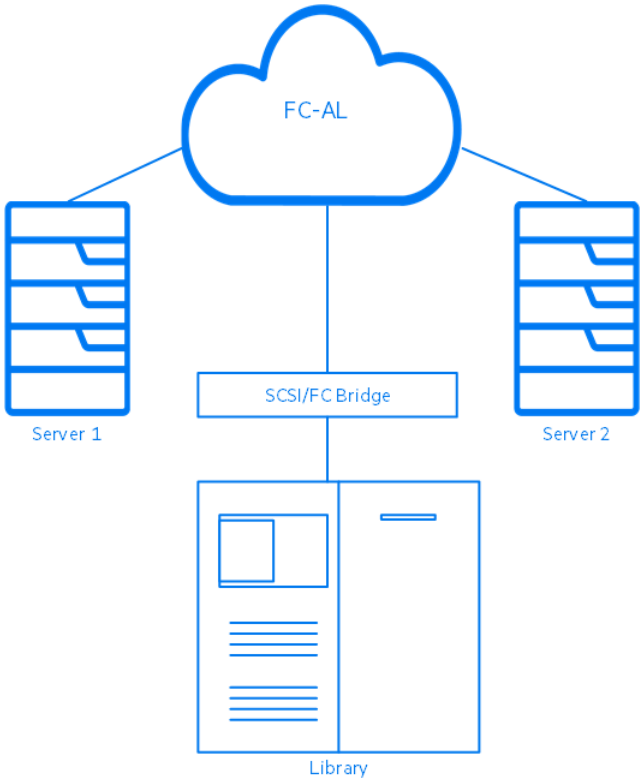
环拓扑基于 Fibre Channel Arbitrated Loop (FC-AL) 标准。节点包括服务器、备份设备、集线器和交换机。环中的任意节点都可以与环中的任何其他节点进行通信，所有节点享有相同的带宽。FC-AL 环一般使用具有自动端口旁路的 FC-AL 集线器来实现通信。自动端口旁路支持在环中热插入节点。

LIP

触发 LIP 的原因很多，最常见的是引入新设备。新设备可以是已开启的现有参与设备，也可以是从一个交换机端口移到另一个交换机端口的活动设备。LIP 的出现可能会导致意外中断 SAN 上正在进行的操作过程，例如，磁带备份操作。它会重置连接 SCSI/FC 桥和节点（SCSI 设备）的 SCSI 总线。请参见环路初始化协议。

如果是备份或还原，SCSI 总线重置会记录为写入错误。Data Protector 会在出现写入错误时中止所有操作。如果是在备份，建议重新格式化介质（先复制已备份到介质上的信息），然后重新启动备份。

环路初始化协议



交换式拓扑

交换式拓扑在连接到交换机的所有节点之间提供任意连接。交换机易于安装、使用，因为光纤通道协议具有自我配置和自我管理功能。交换机自动

检测连接的对象（节点、FC-AL 集线器或其他 FC 交换机），并对自身进行相应的配置。交换机对连接的节点按比例提供带宽。交换式拓扑具有真正的热插入节点功能。

> **注意**热插入是指重置、重新建立通信等协议功能。请注意，热插入时会中断正在进行的数据传输，一些设备（比如，磁带设备）会无法处理此行为。将节点接入环路或从环路中断开节点，很可能会中断备份或还原过程，导致操作失败。只有当系统没有在使用相关硬件运行备份或还原操作时，才可以在环路中接入或断开节点。

SAN 中的设备共享

Data Protector支持 SAN 概念，使多个系统能够共享 SAN 环境中的备份设备。从多个系统可以访问同一物理设备。因此，任何系统都可以对一些设备或任何其他设备执行本地备份。数据通过 SAN 传输，备份无需任何传统的 LAN 带宽。这种类型的备份有时被称为“无 LAN”备份。备份性能也得到了改善，因为基于 SAN 的光纤通道技术在吞吐量方面往往比 LAN 技术要高。

您需要防止多个计算机系统同时将数据写入同一设备。当从多个应用程序使用设备时，这种情况会变得甚至更加复杂。所有相关系统访问设备时都需要同步。使用锁定机制实现这一点。

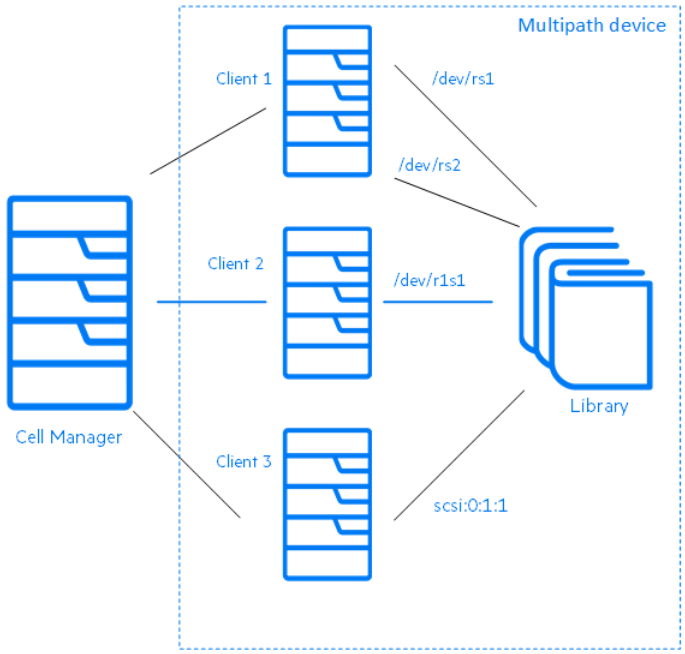
SAN 技术为从多个系统管理机械手提供一种极好的方式。这样就可以选择从一个系统管理机械手（典型），如果在所有相关系统中能够同步向机械手发出的请求，还可以让每个使用库的系统直接访问机械手。

配置多条物理设备路径

SAN 环境中的设备通常连接到若干客户机，因此可以通过若干路径访问该设备，这些路径包括客户机名称和 SCSI 地址（UNIX 中的设备文件）。Data Protector 可以使用这些路径中的任意一种。您可以将所有物理设备路径配置为单个逻辑设备 — **多路径设备**。

例如，设备连接至 client1 并配置为 /dev/rs1 和 /dev/rs2，在 client2 上为 /dev/r1s1，在 client3 上为 scsi1:0:1:1。因此，可以通过四条不同的路径访问该设备： client1:/dev/rs1 、 client1:/dev/rs2 、 client2:/dev/r1s1 和 client3:scsi1:0:1:1。因此，多路径设备包含指向此磁带设备的所有四个路径。

多路径配置



为何使用多条路径？

如果使用以前版本的 Data Protector，只能从一个客户机访问设备。为解决此问题，必须为使用锁名称的物理设备配置多个逻辑设备。因此，如果使用锁名称来配置从不同系统对单个物理设备的访问，就不得不在每个系统上配置所有设备。例如，如果有 10 台客户机与单个设备连接，则必须用相同的锁名称配置 10 台设备。而使用当前版本的 Data Protector 简化了这一配置过程，您可以为所有路径配置单个多路径设备。

多路径设备可提高系统的复原能力。Data Protector 将尝试使用所定义的第一个路径。如果某台客户机上的所有路径都不可访问，Data

Protector 会尝试使用下一台客户机上的路径。只有当所有列出的路径都不可用时，才会中止会话。

路径选择

在备份会话期间，设备路径一般按配置设备时定义的顺序来选择，在备份规范中选择了首选客户机的情况除外。在这种情况下，首先使用首选客户机上的路径。

如果全局变量 LANfree 设置为 1（默认值为 0），而不使用首选主机或不遵循配置的路径顺序，则备用会话管理器 (BSM) 将使用本地路径（如果多路径配置中提供）。

在还原会话期间，设备路径按以下顺序来选择：

1. 还原对象的目标客户机上的路径，如果*所有*对象都还原到同一目标客户机
2. 过去用于备份的路径
3. 其他可用路径

如果启用了直接库访问功能，则无论配置了什么顺序，都会首先使用本地路径（目标客户机上的路径）进行库控制。

向后兼容

升级期间不会重新配置使用先前版本的 Data Protector 配置过的设备，无需任何更改即可与在先前版本的 Data Protector 中一样使用这些设备。但是，为了利用新增的多路径功能，必须将设备重新配置为多路径设备。

设备锁定

锁定设备的前提条件是: 多个应用程序使用同一设备，且只有 Data Protector 能够通过从多个系统向其发送数据和命令的方式来使用设备。锁定的用途是确保一次只有一个系统与在若干系统之间共享的设备进行通信。

多个应用程序的设备锁定

如果 Data Protector 和至少另一其他应用程序都想要从多个系统使用同一设备，则每个应用程序必须使用相同 (通用) 的设备锁定机制。该机制需要在多个应用程序中都起作用。Data Protector 目前不支持此模式。如果需要此模式，操作规则必须确保一次只有一个应用程序能够独占访问所有设备。

Data Protector 中的设备锁定

如果 Data Protector 是唯一使用驱动器的应用程序，但有多个系统需要使用同一设备，则必须运用设备锁定。

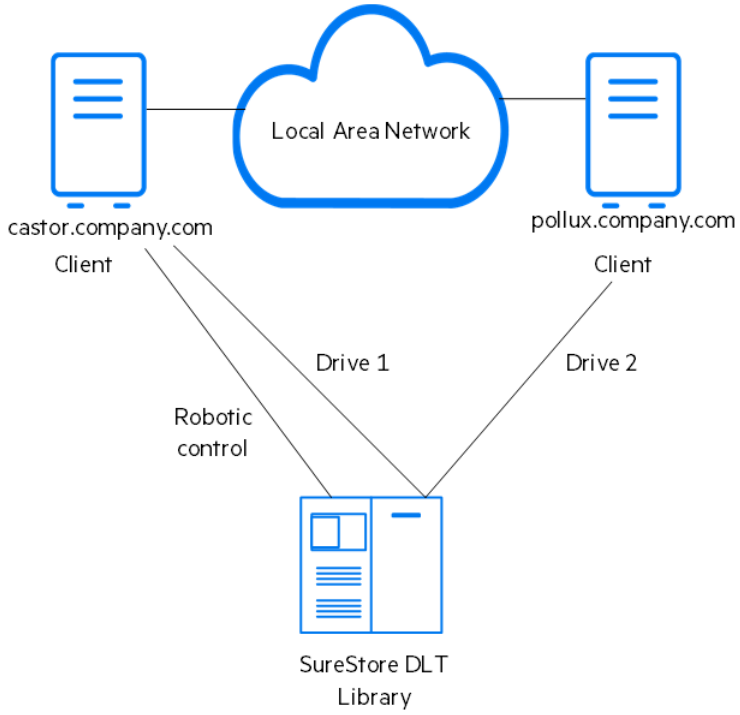
如果 Data Protector 是唯一从多个系统使用机械手控制的应用程序，且库控制与需要控制库的所有系统位于同一单元中，则 Data Protector 会在内部处理此行为。在这种情况下，通过 Data Protector 内部控制管理对设备访问的所有同步过程。

间接和直接库访问

使用 SCSI 库设备配置 Data Protector 后，客户机系统可以有两种方式访问库机械手: 间接库访问和直接库访问。

间接库访问

此配置可以在 SAN 与传统的 SCSI 直接连接的环境中使用。多个系统可以将访问请求转发给具有直接访问库机械手权限的客户机系统来访问库机械手。这称为间接库访问。在间接库访问中描述的示例中，两个客户机系统连接到 DLT 多驱动器库。客户机系统 castor 控制机械手和第一个驱动器，而客户机系统 pollux 控制第二个驱动器。 pollux 上的 Data Protector 介质代理与运行在 castor 上的进程进行通信，以操作机械手。当库和驱动器的主机名不同时，自动使用此 Data Protector 库共享功能。



请注意，如果控制机械手的客户机系统（在本例是 castor ）发生故障，则不能使用共享的库。

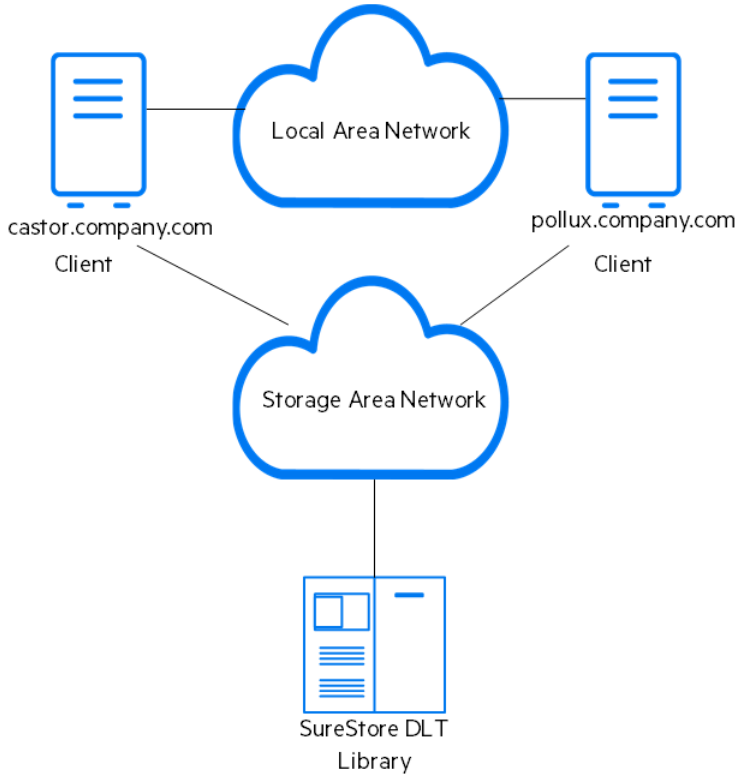
直接库访问

运用 SAN 概念时，可以使用 SCSI 库配置 Data Protector，这样每个客户机系统都拥有自己的库机械手和驱动器的访问权限。这称为直接库访问。

机械手没有单独的“控制客户机系统”：一旦控制机械手的系统发生故障，使用库的任何其他系统都不能幸免。此操作无需重新配置即可执行。您可以使用多个客户机系统来控制机械手。

直接库访问显示的是通过 SAN 连接到两个客户机系统的 DLT 多驱动器库。两个客户机系统都可以访问库和两个驱动器。它们使用 SCSI 协议与库通信。

直接库访问



群集中的设备共享

群集概念通常与 SAN 概念结合使用，它是基于节点之间共享的网络资源（例如，网络名称、磁盘和磁带设备）的。

群集感知应用程序随时可以在群集中的任何节点上运行（它们可以在虚拟主机上运行）。要对这些应用程序执行本地备份，需要用虚拟主机而不是真实的节点名称配置设备。如果使用锁名称设备锁定机制，可以根据需要为每个物理设备配置多个设备。有关详细信息，请参阅设备锁定。

静态驱动器

静态驱动器是配置在群集中的真实节点上的设备。使用静态驱动器可以不具有共享磁盘的系统备份数据。但是，它们对备份群集感知应用程序不起作用，因为此类应用程序可以在群集中的任何节点上运行。

浮动驱动器

浮动驱动器是用虚拟系统名称配置在虚拟主机上的设备。配置浮动驱动器是为了备份群集感知应用程序。这可确保，无论应用程序目前在群集中的哪个节点上运行，Data Protector 始终能够在该节点上启动介质代理。

用户和用户组

本主题讨论 Data Protector 的安全性、用户、用户组和用户权限。

为用户提供增强型安全性

Data Protector 提供了高级安全功能，可防止未经授权备份或还原数据。Data Protector安全性涉及以下方面: 对未授权的用户隐藏数据、数据编码以及根据用户职责对用户进行限制性分组。

本节将介绍与使用 Data Protector 备份数据、恢复数据或监控备份会话进度有关的安全性问题。

访问备份数据

备份并还原数据本质上与复制数据是相同的。因此，将这些数据的访问仅限于授权用户很重要。

Data Protector提供了以下与用户相关的安全:

- 所有要使用任何 Data Protector 功能的用户，都必须配置为 Data Protector 用户。

备份数据的可见性

- 备份数据对于备份所有者以外的其他用户而言都是隐藏的。其他用户甚至看不到已经备份数据。例如，如果备份操作员配置了某备份，则只有备份操作员或系统管理员能够看到和还原备份数据。可以使用 Data Protector“公共”选项使数据对其他用户可见。有关说明，请参阅《Data Protector 帮助》。

用户和用户组

要使用 Data Protector，您必须作为具有特定特权的 Data Protector 用户添加到 Data Protector 用户配置中。请注意，添加新用户并不是备份该用户所用系统的必备条件。

将根据特定用户权限（例如监视单元中的会话、配置备份，以及还原文件）将用户分为不同的用户组。

预定义用户组

为简化备份的配置，Data Protector 提供了具有访问 Data Protector 功能的特定权限的预定义用户组: 例如，只有 admin 用户组的成员能够访问所有 Data Protector 功能。默认情况下，操作员可以启动和监视备份。有关详细信息，请参阅《Data Protector 帮助》索引: “用户组”。

> **提示**在较小的环境中，执行所有备份任务只需要一个人。此人必须是 Data Protector admin 用户组的成员。在这种情况下，无需向 Data Protector 配置添加其他用户。

自定义用户组

可以根据您的环境决定是使用默认的 Data Protector 用户组、修改用户组还是创建新组。

默认管理员

在安装过程中，以下用户会自动添加到 Data Protector admin 用户组中：

- Linux Cell Manager 系统上的 Linux 根用户
- Windows Cell Manager 系统上安装 Data Protector 的用户

这样，他们就可以配置和使用完备的 Data Protector 功能。有关详细信息，请参阅《Data Protector 帮助》索引: “用户组, admin”。

Data Protector 用户权限

Data Protector 用户具有其所属用户组的 Data Protector 用户权限。

从运行于 Linux Cell Manager 上的 Data Protector 中的 Windows 域配置用户时，必须用域名或通配符组 “*”配置用户。

此外，可以在 Data Protector 用户组提供的用户安全性层中加入一些限制，来限制用户对单元的某些系统执行操作。

Data Protector 内部数据库

本主题介绍 Data Protector 内部数据库 (IDB) 的体系结构及其用法和操作。还将说明数据库的各部分及其记录，并提出如何管理数据库增长和性能的建议（包括计算其大小的公式）。利用这些信息，可以有效地管理数据库配置和维护。

IDB 概述

IDB 是位于 Cell Manager 上的嵌入式数据库，存储的信息包括备份数据、数据所处备份介质，备份、还原、对象复制、对象合并、对象验证和介质管理会话的结果，以及配置的备份设备和库。

为何使用 IDB？

IDB 中存储的信息有以下用途：

- 快速、方便的还原：可以使用 IDB 中存储的信息迅速找到还原所需的备份介质，从而大大加快了还原速度。它还可方便查找要还原的文件和目录。
- 备份管理：可以使用 IDB 中存储的信息验证备份方式。也可以使用 Data Protector 报告功能配置各种报告。
- 介质管理：可以使用 IDB 中存储的信息在备份、对象复制和对象合并会话期间分配介质、跟踪介质属性、将介质分组到不同的介质池，以及跟踪磁带库中的介质位置。
- 加密/解密管理：Data Protector 可以使用 IDB 中存储的信息为加密备份或对象复制会话分配加密密钥，并提供还原加密备份对象所需的解密密钥。

IDB 大小和增长注意事项

IDB 可以变得非常庞大，其大小会对备份性能和 Cell Manager 系统产生影响。因此，Data Protector 管理员必须了解 IDB，并根据需要决定在 IDB 中保留哪些信息以及保留多长时间。管理员一方面要平衡还原时间和功能，另一方面要平衡 IDB 大小和增长。Data Protector 提供了两个关键参数帮助平衡您的需求：“日志记录级别”和“编目保护”。

IDB 位置和所用内部编码

IDB 位置

IDB 位于 Cell Manager 上的以下目录中:

Windows 系统： Data_Protector_program_data\server\db80

UNIX 系统： /var/opt/omni/server/db80

IDB 中的内部文本编码

IDB 以 Unicode 双字节格式或 UTF-8 格式存储所有文本信息。这些格式可完全支持本地化为其他语言的文件名和消息。

Manager-of-Managers 环境下的 IDB

在 Manager-of-Managers (MoM) 环境中，您可以使用集中式介质管理数据库 (CMMDB) 代替本地介质管理数据库 (MMDB)。它支持您跨单元共享设备和介质。

IDB 架构

IDB 由以下几部分组成：

- MMDB (Media Management Database)
- CDB（目录数据库）
- DCBF（详细编目二进制文件）
- SMBF（会话消息二进制文件）
- 加密密钥库

IDB 的每个部分都存储了某些特定的 Data Protector 信息 (记录)，以不同方式影响 IDB 大小和增大，位于 Cell Manager 上一个单独的目录

中。请参阅 IDB 部分。

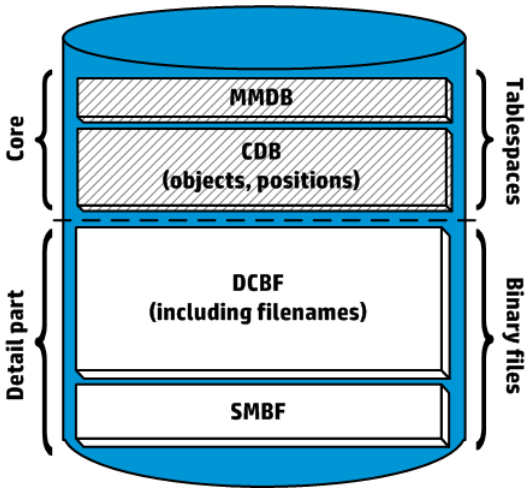
有关稳定性的注意事项，请参阅《Data Protector 帮助》索引: “IDB 的稳定性”。

基础技术

MMDB 和 CDB 部分使用由表空间构成的嵌入式数据库来实现。此数据库由 hpdp-idb、hpdp-idb-cp 和 hpdp-as 进程控制。CDB 和 MMDB 部分是 IDB 的核心部分。

IDB 的 DCBF 和 SMBF 部分由二进制文件构成。更新直接进行，无需使用事务。

IDB 的各个部分



介质管理数据库

介质管理数据库

MMDB 记录

介质管理数据库存储有关以下各项的信息：

- 配置的设备、库、库驱动器和插槽
- Data Protector介质
- 配置的介质池和介质盒

MMDB 大小和增大

MMDB 的大小不会变得非常大。MMDB 的最大部分通常被 Data Protector 介质的信息所占据。

编目数据库

编目数据库存储有关以下各项的信息：

- 备份、还原、对象复制、对象合并、对象验证和介质管理会话。这是发送给 Data Protector Monitor 窗口的信息的副本。
- 备份的对象、对象版本和对象副本。如果是加密的对象版本，则还会存储密钥标识符 (KeyID-StoreID)。
- 所备份的对象在介质上的位置。对于每个备份对象，Data Protector 都会存储有关其备份所用介质和数据段的信息。对于对象副本和对象镜像也是如此。

CDB 的大小与增长

CDB 记录在 IDB 中占较少空间。

详细编目二进制文件 (DCBF)

DCBF 信息

IDB 的详细信息编目二进制文件部分存储：

- 备份文件（文件名）的路径名以及客户机系统名称。在两次备份之间创建的文件名将添加到 DCBF。
- 文件元数据。此信息包含已备份文件的版本、其文件大小、修改时间、属性/保护和在备份介质上的备份副本位置。

将为每个 Data Protector 备份介质创建一个 DC (详细信息编目) 二进制文件。介质被覆盖时，将删除其 DC 二进制文件并创建一个新的。

文件名和文件属性部分的大小和增长

DCBF 中最大且增长最快的部分是文件名部分。文件名部分的增长与备份环境的增长和动态变化以及备份次数成正比。

在 IDB 中文件或目录大约占用 100 字节。

DCBF 剩余部分的大小和增长

在文件系统备份一般都使用“全部记录”选项的环境中，DCBF 占 IDB 的最大部分。

默认情况下，为 DC 二进制文件配置五个 DC 目录， dcbf0 至 dcbf4 。可以创建更多个 DC 目录，并将其存储在 Cell Manager 上的不同磁盘上，从而扩展 IDB 大小。

会话消息二进制文件

SMBF 记录

会话消息二进制文件存储任何 Data Protector 会话期间生成的会话消息。对于每个会话会创建一个二进制文件。文件按年份和月份进行分组。

SMBF 大小和增大

SMBF 大小取决于以下因素：

- 执行的会话数，因为对于每个会话将创建一个二进制文件。
- 会话中的消息数。一个会话消息大约占用 200 字节。可以通过指定 Report level 选项来更改在执行备份、还原和介质管理操作时显示的消息数。这也会影响存储在 IDB 中的消息数。

加密密钥库和编目文件

所有在加密备份期间创建的密钥，无论是手动还是自动创建，都存储在密钥库中。密钥也可用于对象复制、对象验证和还原会话。如果是硬件加密，密钥也可用于对象合并会话。

对于软件加密，密钥标识符（每个密钥标识符由 KeyID 和 StoreID 构成）会映射到加密的对象版本中。该映射存储在编目数据库中。介质中不同的对象可以有不同的（软件）加密密钥。

对于硬件加密，密钥标识符会映射到介质 ID，这些映射存储在编目文件中。该文件包含将加密介质导出到其他单元所需的信息。

IDB 操作

备份期间

备份会话启动时，将在 IDB 中创建会话记录。此外，还会为会话中的每个对象和每个对象镜像创建对象版本记录。所有这些记录均存储在 IDB 中，包含已备份数据的信息，备份时间以及备份目标位置。

如果为备份请求了软件加密，则会从密钥库中获取所涉及实用程序（主机）的活动加密密钥用于备份，密钥标识符（密钥 ID-库 ID）将链接到对

象版本并包含在 CDB 记录中。主机到密钥 ID-库 ID 的映射也存储在密钥库的编目中。

备份会话管理器在备份期间会更新介质。所有介质记录都存储在 MMDB 中，根据相关策略为备份分配介质。如果涉及的介质位于请求了硬件加密的驱动器中，则会从密钥库中首先获取实用程序（介质）的活动加密密钥。介质到密钥 ID-库 ID 的映射记录在密钥库的编目中并写入介质。

当数据段写入磁带再写入编目段时，都会为属于该数据段的每个对象版本，在 CDB 中存储一条介质位置记录。此外，在 DC (详细信息编目) 二进制文件中存储编目。每个 Data Protector 介质都将保留一个 DC 二进制文件。DC 二进制文件的名称为 MediumID_TimeStamp.dat 。如果介质在备份期间被覆盖，则将删除旧的 DC 二进制文件并创建新的二进制文件。

备份期间生成的所有会话消息都存储在会话消息二进制文件 (SMBF 部分) 中。

根据内部数据库备份规范的配置，IDB 备份过程可删除已备份的存档日志文件，并开始创建 IDB 还原所需的新文件。

> **注意**在 Incr 模式下的内部数据库备份 (PostgreSQL) 期间，配置文件进行完整备份。

恢复期间

配置恢复时，Data Protector 会在 CDB 和 DCBF 部分中执行一系列查询，以使用户能够浏览备份数据的层次结构（文件系统、应用程序对象）。这些浏览查询分为两步完成。第一步是选择特定对象（文件系统或逻辑驱动器）。如果此对象存储了多个备份版本和/或副本，则该操作可能需要一些时间，因为 Data Protector 要扫描 DCBF 来构建查找缓存以便以后浏览。第二步：浏览目录。

选择特定的文件版本后，Data Protector 会确定所需介质并定位所选文件使用的介质位置记录。这些介质则由介质代理读取，并将数据发送给还原所选文件的磁带客户机。如果涉及的介质进行了硬件加密，介质代理会先检测密钥标识符 (KeyID-StoreID) 再请求密钥，密钥由 Key Management Server (KMS) 从密钥库进行检索。

如果对有关备份使用了软件加密，磁带客户机接收加密数据时，会将检测到的密钥 ID-库 ID 提交给 KMS，并请求相关的解密密钥，解密密钥从密钥库进行检索。

对象复制或对象合并期间

对象复制或对象合并会话期间运行的操作与备份和还原会话期间相同。大体上是，像还原数据一样从源介质读取数据，然后像备份数据一样将数据写入目标介质。对象复制或对象合并会话对 IDB 操作的影响与备份和恢复相同。这并不适用于采用软件加密的对象合并，因为它不受支持。

对象验证期间

对象验证会话期间，运行与还原会话期间相同的数据库进程。大体上是，像还原数据一样从源介质读取数据，然后将数据发送到执行验证的主机的磁带客户机。对象验证会话对 IDB 操作的效果与还原会话相同。验证会话期间生成的所有会话消息都存储在会话消息二进制文件中。

导出介质

导出介质时，如果介质包含加密信息，则会将相关密钥从密钥库导出到 Cell Manager 上的 filename.csv 文件。该文件是将介质成功导入其他单元所必需的。

删除的项目

此外，还会删除多个项目：

- 从 CDB 中删除该介质上的所有介质位置记录。
- 从 CDB 部分中删除当前在任何其他介质上都没有位置的所有对象和对象副本。
- 删除超过 30 天的过时会话（其介质已被覆盖或导出）。同时还会删除这些会话的会话消息。
- 从 MMDB 部分中删除介质记录，并从 DCBF 部分中删除该介质的 DC 二进制文件。

删除详细信息编目

删除特定介质的详细编目时，同时还会删除其 DC 二进制文件。删除该介质上所有对象版本和对象副本的编目保护时，也会出现相同的结果（下一次有关 DC 二进制文件的日常维护是删除二进制文件）。所有其他记录均保留在 CDB 和 MMDB 内。因此，可以运行整个备份对象的还原，而不是单个文件的还原。

IDB 管理

IDB 配置

设置 Data Protector 备份环境时，最重要的步骤之一是配置 IDB。初始配置允许您设置有关 IDB 大小、IDB 目录位置和防止 IDB 损坏或灾难所需的 IDB 备份等的内部策略，以及设置 IDB 报告和通知的配置。

重要说明强烈建议安排每日执行 IDB 备份。为 IDB 备份创建备份规范是 IDB 配置的一部分。

警告始终应在对 IDB 配置进行任何修改后备份内部数据库，例如，在更改“内部数据库服务”和“应用程序服务器”用户帐户的密码后。未执行此操作可能会导致无法成功执行联机 IDB 恢复或脱机 IDB 恢复。

IDB 维护

配置 IDB 后，可最大限度地减少维护工作量，主要的维护工作就是针对通知和报告采取相应措施。

IDB 恢复

如果部分 IDB 文件有缺失或损坏，则需要执行 IDB 恢复。恢复过程取决于损坏程度。

IDB 增长和性能

正确的 IDB 配置和维护需要了解影响 IDB 增长和性能的关键因素，以及可按需调整的关键可调参数，从而尽可能有效地处理 IDB 增长和性能。

IDB 增长和性能的关键因素

IDB 增长和性能的关键因素包括：

- 日志记录级别设置

  日志记录级别定义备份期间数据写入 IDB 的详细程度。日志记录级别越详细，对 IDB 存储空间消耗影响越大。

- 编目保护设置

  编目保护确定备份数据信息在 IDB 中可以使用多久。设置的编目保护期限越长，对 IDB 的影响就越大。有关详细信息，请参阅IDB增长和性能: 关键可调参数。

- 已备份文件数

  Data Protector 会跟踪每个文件和文件的每个版本。不同的备份类型对 IDB 的影响也有所不同。

- 备份数

  执行备份的频率越高，IDB 中存储的信息就越多。

- 文件系统动态变化

  备份之间创建和删除的文件数对 IDB 文件名部分的增大有重要影响。可以使用“日志目录”日志记录级别避免文件系统动态变化导致的 IDB 增长。

- 备份环境的增长

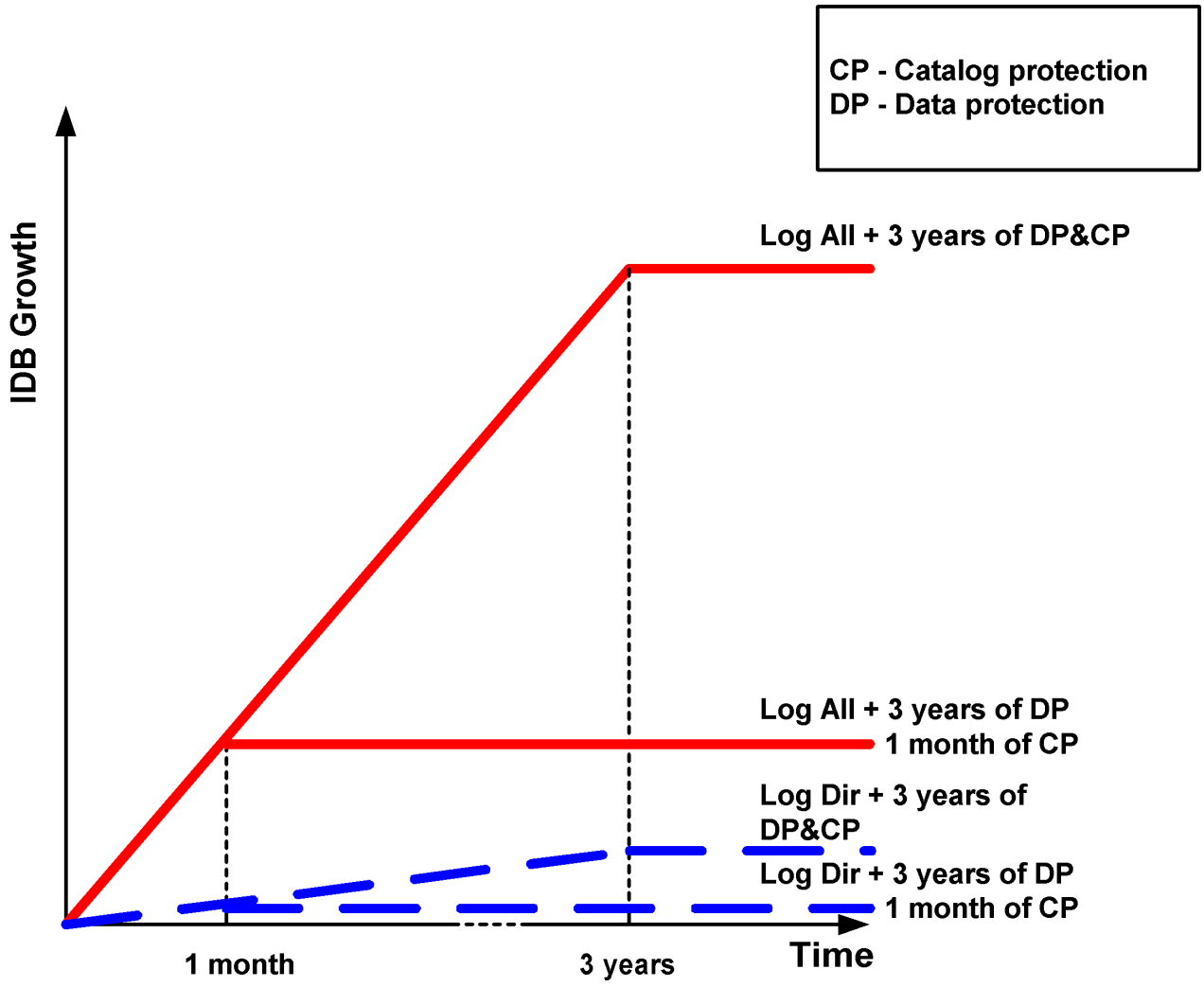
  在单元中备份的系统数目会影响 IDB 增长。请制定备份环境的增长计划。

- 对象副本数目和对象镜像数目

  创建的对象副本和对象镜像越多，IDB 中存储的信息就越多。IDB 中存储的对象副本和对象镜像的信息均与备份对象相同。

IDB 增长和性能：关键可调参数

日志记录级别和编目保护是影响 IDB 增长和性能的主要因素。它们对 IDB 的影响取决于所使用的设置。



作为 IDB 关键可调参数的日志记录级别

什么是日志记录级别？

Data Protector 日志记录级别定义了备份中写入 IDB 的备份文件和目录的详细信息总量。无论使用何种日志记录级别，您始终可以还原数据。

有如下四个日志记录级别：

日志记录级别

级别	描述
全部记录	记录有关备份文件和目录的所有详细信息（名称、版本和属性）。
记录文件	记录有关备份文件和目录的所有详细信息（名称和版本）。该日志记录级别的详细程度大约占备份文件和目录的所有详细信息的 30%。

日志目录	记录有关备份目录的所有详细信息（名称、版本和属性）。该日志记录级别的详细程度大约占备份文件和目录的所有详细信息的 10%。
不记录任何内容	IDB 中不记录有关备份文件和目录的信息。

不同的设置会影响 IDB 增长和浏览待恢复数据的方便程度。

日志记录级别和备份速度

无论所选的日志记录级别是什么，备份速度都大致一样。

日志记录级别和浏览还原

信息存储详细程度的变化会影响还原期间使用 Data ProtectorGUI 浏览文件的信息量。如果设置了“无日志”选项，则无法浏览；如果设置了“日志目录”选项，则可以浏览目录；如果设置了“日志文件”选项，则可以完整地浏览，但不显示文件属性 (大小、创建日期和修改日期等)。

无论日志记录级别有效性如何，始终都能还原数据:

- 与浏览数据不同，您始终可以手动选择要恢复的文件（如果知道文件名）。
- 可以从介质中检索备份数据的信息。

日志记录级别和还原速度

如果相应的备份会话使用“全部记录”、“日志目录”或“日志文件”日志记录级别运行，则还原速度大致相同。

如果以“无日志”日志记录级别运行备份会话，则还原速度可能在还原单一文件时降低。在这种情况下，Data Protector 必须从对象的开始处读取所有数据，再查找要恢复的文件。

在进行完整系统还原的情况下，无论如何都要读取整个备份对象，因此日志记录级别的影响不大。

作为 IDB 关键可调参数的编目保护

什么是编目保护？

编目保护确定备份数据信息在 IDB 中可以使用多久。编目保护与数据保护不同，后者确定备份数据在介质上可以使用多久。如果无编目保护，仍可还原数据，但不能在 Data Protector GUI 中浏览这些数据。

编目保护基于这样一个事实，即最近存储的数据非常重要，访问也很频繁。旧文件很少被搜索，因此搜索旧文件时允许花费更多时间。

到期的编目保护

目录保护到期后，并不会立即从 IDB 中删除信息。Data Protector 每天自动删除一次这些信息。由于 IDB 中的信息是按介质进行组织的，因此只有当介质上所有对象的编目保护都到期时，才会将其彻底删除。

性能影响

编目保护设置对浏览备份对象的性能有所影响。

编目保护和还原

编目保护到期时将还原数据，就像使用“无日志”选项备份了这些数据一样。请参见作为 IDB 关键可调参数的日志记录级别。

日志记录级别和编目保护的使用建议

始终使用编目保护

始终设置合理级别的编目保护。唯一的例外是设置了“不记录”选项的情况 (此时编目保护不适用)。

如果将编目保护设置为“永久”，则 IDB 中的信息只有在导出或删除介质时才会删除。在这种情况下，IDB 的大小线性增长，直到数据保护期限到期为止，即使单元中的文件数没有发生变化时也是如此。例如，如果数据保护期限为 1 年，介质循环使用，则 IDB 的显著增长将在 1 年后停止。添加的新编目数约等于删除的旧编目数。如果编目保护期限设为 4 周，则 IDB 的显著增长将在 4 周后停止。因此，保护期限设为 4 周时的 IDB 大小增速比设为 1 年时快 13 倍。

建议编目保护至少包含上次的完整备份。例如，可以将完整备份的编目保护设为 8 周，将增量备份的编目保护设为 1 周。

在同一单元中使用不同日志记录级别

一个单元通常由每日生成大量文件的邮件（或类似）服务器、将所有信息存储在少量文件中的数据库服务器和一些用户工作站组成。由于这些系统的动态变化截然不同，找到一种适合所有系统的设置非常困难。因此，建议使用以下日志记录级别设置创建多个备份规范：

邮件服务器： 使用“日志目录”选项。

数据库服务器: 由于其拥有自己的还原策略，因而无需进行日志记录。因此，使用“无日志”选项。

工作站和文件服务器： 使用“全部记录”或“记录文件”选项，允许搜索和还原文件的不同版本。对于使用“日志目录”或“无日志”选项进行的备份，可以从介质导入编目，从而能够在相当短的合理时间内浏览到选定对象。

对对象副本使用不同日志记录级别

备份对象和对象副本或对象镜像可以具有相同或不同的日志记录级别。根据备份策略，对象副本的所选日志记录级别可以比源对象更详细，或不如源对象详细。

例如，如果只是为了确保成功完成备份会话而创建对象镜像，可以为对象镜像指定“无日志”选项。或者，可以为备份对象指定“无日志”选项以提高备份性能，然后在后续对象复制会话中为该对象指定“全部记录”选项。

针对小单元

如果单元中的文件数相对很少，将来也不会明显增多，并且单元中的系统只是执行平常的业务活动，则可以始终使用“ 全部记录”选项，即 Data Protector 的默认设置。但是，您需要注意 IDB 增长，设置一个合理的编目保护级别。

针对大单元

如果文件数增长到非常大时，或每天生成大量文件，而您使用“全部记录”选项，则 IDB 增长会在相对较短的时间内成为困扰您的一大问题。在这种情况下，您有以下选择：

- 将日志记录级别降低到可接受的最低级别。

  设置“日志文件”选项可降低 IDB 大小，设置“日志目录”选项可更大程度降低其大小。当然，这种实际结果取决于单元中文件系统本身的性能。
- 将编目保护级别降到最低。
- 将单元一分为二。

  作为最后的解决办法，您总是可以引入其他的 IDB 并将部分系统重定向到该数据库。

服务管理

服务管理、报告和监视功能有助于管理员更加有效地管理备份环境。本节介绍服务管理功能背后的概念以及独立的 Data Protector 安装及其与服务管理产品集成后所具有的优点。

Data Protector 和服务管理

Data Protector 提供服务管理支持，可与服务管理应用程序集成。

Data Protector 功能

以下章节介绍 Data Protector 提供的“开箱即用型” 功能。

主要功能

- 内置的运行会话监视功能使您能够在备份环境下即时对事件作出响应。
- 使用 Data Protector 的内置通知和报告引擎，可以接收采用多种不同格式 (例如 ASCII、件、SNMP、广播 (仅在 Windows 系统中可用)、写HTML 和兼容电子表格的格式)，并通过各种方式 (例如电子邮件、SNMP、广播 (仅在 Windows 系统中可用)、写入文件和发送到外部命令) 交付的简洁报告以及即时警报。Data Protector 内置的通知引擎可以通过 SNMP 发送警报，因此几乎能够集成任何可接收 SNMP 陷阱的应用程序。
- Data Protector 备份会话审计可存储整个 Data Protector 单元延续期内执行的所有备份任务的信息，并在需要时以完整、可打印的方式提供这些信息，用于审计和管理目的。
- Data Protector 能够将重要事件和紧急事件发送到 Windows 事件日志，因此用户可以进行各种感兴趣的集成。

SNMP 陷阱

SNMP 陷阱允许服务管理应用程序在发生 Data Protector 事件时，或者在因 Data Protector 的检查和维护机制而发送 SNMP 陷阱时接收和处理 SNMP 陷阱消息。

Data Protector 监视器

Data Protector 监视器是 Data Protector 用户界面的一部分，通过它可以对当前正在运行的备份、还原和介质管理会话进行监管和执行纠正操作。使用监视可以查看某个单元中的所有会话，它会向您显示详细信息和这些会话的当前状态。在多单元环境中，您可以查看在其他单元的计算机系统中运行的会话。从监视器的用户界面可以中止备份、还原或介质管理会话或响应“装载”请求。

如果使用 Manager-of-Managers，则可以从一个用户界面同时监视多个单元的会话。

报告和通知

Data Protector 报告是一种功能强大、可自定义且灵活的工具，用于管理和规划备份环境。Data Protector 始终包含一组丰富的内置报告，系统管理员可依赖这些报告来管理 Cell Manager。IT 服务提供商现在可以使用这些相同的报告来展示数据保护符合 SLA。与服务级别管理尤为相关的内置报告包括：

- 库存/状态报告，如“未针对 Data Protector 配置的客户机”报告 (包含未受保护系统的信息)、“会话规范计划”报告 (列出所有计划的备份、对象复制和对象合并) 以及“池列表”报告 (介质库存报告)。
- 容量利用报告，如“许可报告”报告 (Data Protector 许可证利用情况报告) 和“Data Protector 未使用的已配置设备”报告 (列出当前未用于备份、对象复制或对象合并的可用设备)。
- 问题报告，如*会话统计信息报告*（包含关于失败的备份、复制和合并会话的信息）。管理员可以按小时、按日或按周接收有关失败作业及失败原因的电子邮件报告。

通知和报告功能是 Cell Manager 的固有功能 (但与早期版本相比，已进行了极大扩展)，利用这些功能您可以:

- 从大量预配置的报告中进行选择（包括但不限于，特定时间框架内的会话报告、IDB 报告和设备使用报告）
- 指定自己的报告参数（如时间框架、备份、复制和合并规范，以及备份组）
- 选择各种不同的输出格式（如 ASCII、HTML 和电子表格兼容的格式）
- 使用 Data Protector 内置的调度程序调度这些报告
- 根据事件触发报告发送（如设备故障、装载请求和会话结束）
- 从多种交付报告的交付方法中进行选择（如电子邮件、SNMP、广播（仅在 Windows 系统上可用）、写入文件以及发送至外部命令）

可以结合使用以上大多数不同的格式、交付方法、调度方式和触发方式。

例如：

报告和通知示例

- 每天早上 7:00 点创建一个有关最近 24 小时内所有备份、复制和合并会话的报告，采用 ASCII 格式发送到备份管理员的邮箱。而且，可以将同一报告以 HTML 格式写入 Web 服务器上的文件中，供其他人访问。
- 如果有设备故障或装载请求，系统会立即向备份管理员的 Windows 工作站发送广播消息，并触发外部命令来激活备份管理员的寻呼机。
- 在备份会话结束时，已备份系统的每位最终用户都会收到一封 ASCII 格式的电子邮件，邮件中包含备份状态报告。

事件日志记录和通知

Data Protector 事件日志是所有与 Data Protector 相关的通知的中央存储库。Data Protector 事件日志中记录的事件要么是进程触发的，要么是用户触发的。Data Protector 内置的通知引擎根据日志条目发送警报或激活 Data Protector 报告机制。事件日志是 Data Protector 或软件管理应用程序中 SLA 符合性报告的信息源。除了报告外，日志条目还通过 Data Protector SPI (智能插件) 向软件管理应用程序提供信息，这样软件管理应用程序就可以触发预防性操作或纠正操作。

由于 Data Protector 内置的通知引擎可以通过 SNMP 发送警报，因而几乎任何能接收 SNMP 陷阱的应用程序都可以与 Data Protector 集成。

只有“管理”组中的 Data Protector 用户和被授予“报告和通知”用户权限的 Data Protector 用户才可以访问事件日志。您可以使用事件日志查看器来查看或删除 Data Protector“事件日志”中的所有事件。

Data Protector 日志文件

某些服务管理应用程序允许您指定在哪些日志文件中监视特定日志条目以及监视时间。如果在文件中检测到指定条目，则可以指定操作。

您可以配置这样的服务管理应用程序以监视 Data Protector 日志文件中的特定日志条目 (Data Protector 事件)，同时可以定义检测到特定 Data Protector 事件时要执行的操作。

Windows 应用程序日志

某些服务管理应用程序监视 Windows 应用程序日志。

Data Protector 检查和维护机制

Data Protector 具有各种日常自动自检和维护机制，增强了检查和维护操作的可靠性和可预测性。Data Protector 的自检和维护任务包括：

- “介质可用空间不足”检查
- “Data Protector 许可证到期”检查

分布式环境下的集中管理

利用 Data Protector MoM，管理员可以集中管理包含多个 Data Protector Cell Manager 的企业环境。MoM 系统管理员可从单一控制台执行整个企业的配置、介质管理、监控和状态报告任务。借助 MoM，管理多个 Data Protector Cell Manager 就像管理一个单元那样方便。IT 服务提供商可以在不增加员工的情况下管理更大的客户机环境。

使用 Data Protector 提供的数据

如何使用数据？

下面是如何使用 Data Protector 提供的数据的示例：

- 向备份操作员、最终用户和管理层定期发送电子邮件报告（Data Protector 内置报告具有发送电子邮件的功能）。
- 将备份报告写入 Web 服务器以便按需使用（Data Protector 内置报告具有写入 HTML 的功能）。
- 将重要和紧急的 Data Protector 事件发送到网络管理解决方案 (例如，Data Protector 内置通知引擎能够发送 SNMP 陷阱)。

与应用程序集成

本主题简要介绍 Data Protector 与数据库应用程序的集成。

与数据库应用程序集成

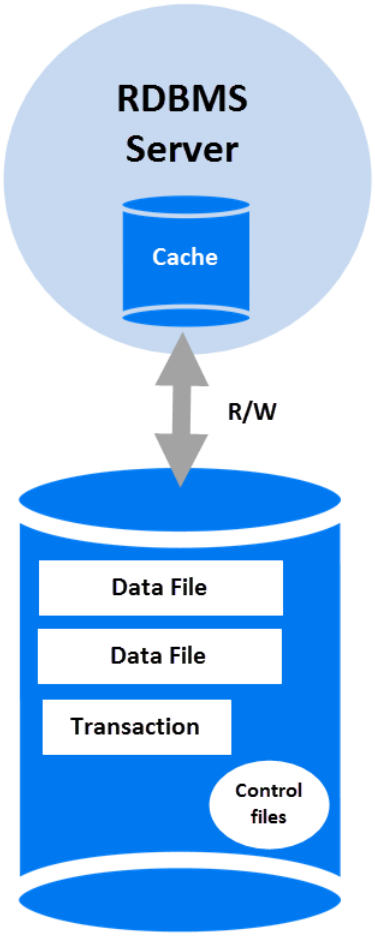
本节简要介绍 Data Protector 与数据库应用程序的集成。有关受支持的应用程序的详细列表，请参阅最新支持矩阵。

数据库操作概述

从用户的角度来看，“数据库”就是一个数据集。数据库中的数据存储在“表”中。关系表用列定义并命名。数据存储在表中的行内。表可以相互关联，数据库可用于加强这些联系。这样，数据就可以**关系格式**存储，或存储为**面向对象**的结构，如抽象数据类型和方法。对象可以关联其他对象，也可以包含其他对象。数据库通常由可保持数据完整性和一致性的服务器（管理器）进程管理。

无论使用关系结构还是面向对象的结构，数据库都会将数据存储在“文件”中。从内部来看，这些是提供数据到文件的逻辑映射的数据库结构，使不同类型的数据能分开存储。这些逻辑分类具有不同的名称，如**表空间**（例如，在 Oracle 中）、**数据库空间**（例如，在 Informix Server 中）和**段**（例如，在 Sybase 中）。

关系数据库



关系数据库显示了具有下述结构的典型关系数据库。

数据文件是包含所有数据库数据的物理文件。它们随机更改，并且可能很大。它们在内部分成多页。

在进一步处理之前，**事务日志**会先记录所有数据库事务。如果发生故障，不能将修改后的数据永久写入数据文件，就可以从日志文件获取这些更改。任何类型的恢复都由两部分组成：**前滚**，将事务更改应用于主数据库；**回滚**，删除未提交的事务。

“控制文件”保存数据库物理结构的信息，如数据库名称、数据库数据文件和日志文件的名称和位置，以及创建数据库的时间戳。这些控制数据保存在控制文件中。这些文件对于数据库操作至关重要。

数据库服务器进程的“缓存”包含数据文件最常用的页面。

事务处理的标准流程如下：

1. 首先将事务记录到事务日志中。
2. 事务中所需更改随即应用到缓存页面。
3. 不时地会有一组修改后的页面清空到磁盘上的数据文件中。

数据库和应用程序的文件系统备份

数据库会在联机时持续变化。数据库服务器由多个组件组成，它们能尽可能缩短连接用户的响应时间，提高性能。某些数据保留在内部缓存内存中，而某些数据则保留在临时日志文件中，这些文件在**检查点**刷新。

由于数据库中的数据可能在备份期间更改，如果不使数据库服务器进入特殊模式甚至脱机状态，数据库文件的文件系统备份就没有意义。保存的数据库文件必须处于一致的状态，否则数据也没用。

以下是配置数据库或应用程序的文件系统备份所必需的步骤：

- 识别所有数据文件。
- 选择两个命令或准备两个脚本或应用程序以分别用于关闭和启动数据库。
- 在包含所有数据文件的情况下配置文件系统“备份规范”，并将关机命令、脚本或应用程序指定为“pre-exec 命令”，将启动命令、脚本或应用程序指定为“post-exec 命令”。

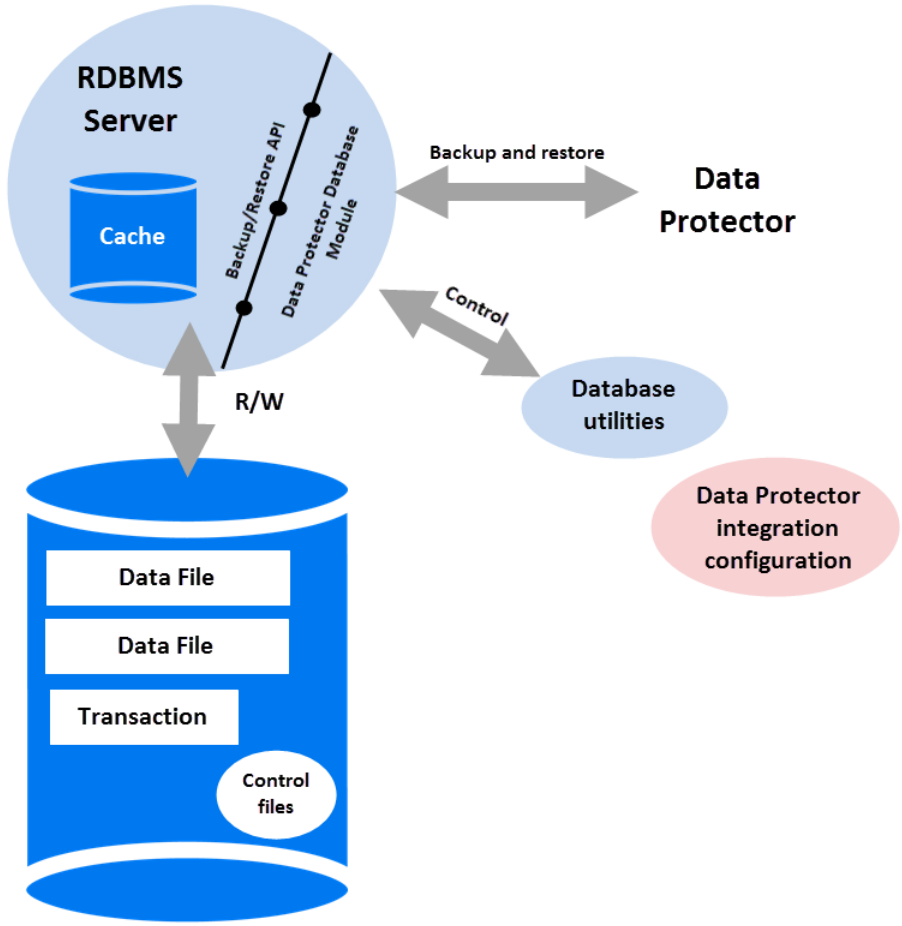
此方法相对简单易懂且容易配置，但有一个关键的缺点，即在备份期间将无法访问数据库，这对于大多数业务环境而言是无法接受的。

数据库和应用程序的联机备份

为避免在备份时关闭数据库，数据库供应商准备了可使数据库临时进入特殊模式以便将数据保存到磁带的界面。这样，备份或还原过程中，服务器应用程序就可以处于联机状态并供用户使用了。这些特定于应用程序的界面允许 Data Protector 之类的备份产品备份或还原数据库应用程序的逻辑单元。备份 API 的功能因数据库供应商而异。Data Protector 集成适用于主要的数据库和应用程序。有关受支持集成的详细列表，请参阅 Data Protector Product 产品公告、软件说明和参考。

备份界面的实质性作用是向备份应用程序提供一致的数据 (即使这些数据在磁盘上可能并不一致)，同时保持数据库处于运行状态。

与数据库集成的 Data Protector



与数据库集成的 Data Protector 显示了关系数据库如何与 Data Protector 集成。Data Protector 提供了链接到数据库服务器的“数据库库”。数据库服务器将数据发送到 Data Protector，并从中请求数据。数据库实用程序用于触发备份和还原操作。

通过 Data Protector 集成配置数据库备份的典型步骤如下：

1. 在数据库系统上安装特定于数据库/应用程序的代理
2. 为每个数据库配置 Data Protector 集成。使 Data Protector 与该数据库集成所需的数据存储在数据库系统上（在配置文件或注册表项

中）。通常，它包含路径名和用户名/密码。
3. 备份规范是通过 Data Protector 用户界面制定的。

除了数据库可始终处于“联机”状态这一关键优势外，使用 Data Protector 与数据库的集成还有其他优点:

- 无需指定数据文件的位置。这些文件可能位于不同的磁盘上。
- 可以浏览数据库的逻辑结构。可以只选择数据库的子集。
- 应用程序感知备份操作在进行，并且会跟踪备份的部分。
- 有几种备份模式。除了**完整**备份外，用户可以选择（块级别）**增量**备份或只备份事务日志。
- 存在多种还原模式，并且还原数据文件后，数据库可以自动还原事务日志并按配置应用它们。

与虚拟环境集成

本节简要介绍 Data Protector 与虚拟环境的集成。有关受支持环境的详细列表，请参阅最新支持矩阵。

虚拟机的联机备份

Data Protector 可在虚拟机正在运行时，使用虚拟环境所提供的特定接口来执行虚拟机的备份（联机备份）。启动备份之前，也可将虚拟机中的应用程序置于一致状态，具体取决于虚拟环境。

除了虚拟机可始终处于联机状态这一关键优势外，使用 Data Protector 与数据库的集成还有其他优点：

- 无需指定数据文件的位置。
- 虚拟环境感知备份操作在进行，并且会跟踪已备份的部分。
- 有几种备份模式。
- 有几种还原模式。

零宕机备份和即时恢复

本主题提供零宕机时间备份和即时恢复概念的基本概述。传统的备份数据方法不太适合于运行大量数据的应用程序，例如数据库应用程序。应用程序必须脱机，或者如果应用程序支持，则将进入“热备份”模式，同时数据将流式传送到磁带。脱机状态可导致应用程序操作出现重大中断。而热备份模式可生成多个大型事务日志文件，使应用程序系统增加额外的负载。

在当今的存储环境中，对数据可用性的要求不断增长。为了实现信息资源的高可用性，Data Protector 零宕机时间备份 (ZDB) 解决方案有助于满足业务需要、消除应用程序宕机时间并使任务关键型数据全天候可用。

零宕机时间备份是一种备份方式，在该备份方式中，使用数据复制技术来最大程度地降低备份操作对应用程序系统产生的影响。首先创建要备份数据的复本，并在复制的数据而非原始数据上执行所有后续备份操作。

由于备份在后台发生，同时应用程序保持联机并可供使用，因此在备份期间对环境的影响非常小。通过使用即时恢复功能也可以缩短恢复时间，这样恢复大量的数据只需在数分钟内即可完成，而不用花费数小时。这使 ZDB 和 IR 功能非常适合于高可用性系统和任务关键型应用程序。

Data Protector ZDB 和 IR 技术采用基于磁盘阵列的镜像和快照技术。以下是 ZDB 和 IR 背后的基本原则：

- 高速创建要备份数据的副本，然后对副本执行备份操作，而不是对原始数据。
- 将阵列上保存的数据的备份副本还原到阵列上的原始位置，以便高速恢复。

与传统备份和还原技术相比，零宕机备份 (ZDB) 和即时恢复 (IR) 具有以下两大优点：

- 在会话期间，宕机时间最小或对应用程序系统影响最小
- 更短的还原时间

比较表 - 磁带备份和还原与 ZDB 和 IR

功能	磁带备份和还原	ZDB 和 IR
数据可用性	在整个备份会话期间，应用程序操作必须脱机，直到完成数据流式传送到备份介质为止。	将应用程序宕机时间减小到最低限度，因此可以在备份期间减少对环境的影响。
备份速度	写入到磁带可能非常耗时。	写入到磁盘几乎可以即时完成。
恢复时间	还原可能要花费大量的时间，并且在还原期间应用程序不可用。	在数分钟内即可恢复大量的数据，而不是数小时或数天。
灾难的影响	由于恢复数据需要宕机时间，因此灾难可能导致重大问题。	由于可以高速还原，因此可使灾难的影响保持在最低限度。
数据存储容量	磁带存储容量通常有限制。	基于磁盘的阵列能够存储数 TB 的数据，因此有机会创建相同数据的多个副本。
灵活性	数据只能存储到磁带介质。一次只能创建一个数据副本；如果需要多个副本，则在每次创建副本时，都需要使应用程序脱机。	可以选择使用磁盘阵列作为主数据存储，也可以在阵列上创建副本之后将数据流式传送到磁带。容易创建数据的多个副本，因为可以在磁盘上完成单个备份，然后多次复制到磁带而不影响源。作为增强备份解决方案，能够组合磁盘和磁带备份技术。

磁盘阵列和存储虚拟化技术

使用 RAID 技术的大型磁盘阵列可容纳包含海量数据的大型应用程序数据库。利用存储虚拟化技术，通常可将磁盘阵列划分为多个虚拟磁盘。在磁盘阵列中可轻松对其进行复制，实际复制次数取决于磁盘阵列技术和可用的存储空间。这可实现对数据副本执行各种操作，而无需承担暴露原始数据的风险。特别是针对高可用性和任务关键型领域的应用程序的有效备份解决方案。

零宕机时间备份

备份到磁带的传统方法不适用于大型数据库应用程序；使用此方法将数据库中的数据流式传送到磁带的过程中，数据库必须处于脱机状态或者处于“热备份模式”(如果应用程序允许)。

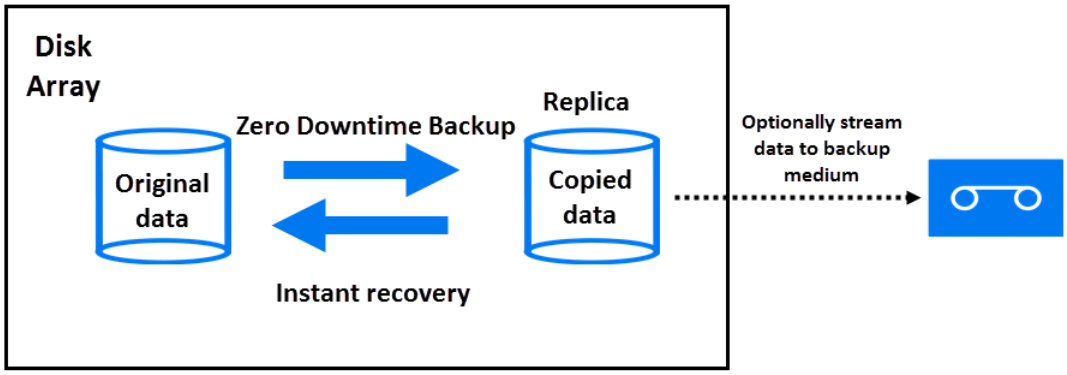
脱机状态可导致应用程序操作出现重大中断。而热备份模式可生成多个大型事务日志文件，使应用程序系统增加额外的负载。

零宕机时间备份 (ZDB) 利用磁盘阵列技术来尽可能减少中断。通俗地说，就是在磁盘阵列上创建或保留数据副本或“复本”。这样做不仅速度快，而且对应用程序的性能影响也很小。复本本身可用作备份，或者可以将其流式传送到磁带上，而不会造成应用程序对源数据库使用的中断。

根据创建复本时所使用的硬件和软件的不同，复本可能是准确复制（镜像、快照式克隆），也可能是要备份数据的虚拟副本（快照）。

在 ZDB 中，“替换”(创建或保留复本的过程) 是最小化应用程序中断的关键因素。

零宕机备份和即时恢复概念



联机和脱机创建复本

对于数据库应用程序，可以在数据库处于联机或脱机的状态下执行备份：

- **联机备份**

  创建要备份的分区的复本时，数据库处于热备份模式。在此模式下，对数据库的任何更改都将写入事务日志 (而不是数据库本身)。当数据库功能恢复正常后，将从事务日志对其进行更新。这使得用户能够在不停止应用程序的情况下执行数据库操作。

- **脱机备份**

  在创建复本时，数据库操作完全停止。在此期间，无法执行任何事务。

创建复本后，数据库将恢复正常。任何后续备份操作（如将数据流式传送到磁带）都将在复本上执行，数据库将始终处于联机状态并且不受影响。

在上述两种情况下，对应用程序的影响都受到复本创建时间的限制，但与标准磁带备份技术相比，这种影响要小得多。对于联机备份，数据库操作始终不会停止（零宕机）并且对性能的影响也微乎其微，主要影响是需要向事务日志写入更多信息。

创建复本

复制将在特定时刻创建应用程序或文件系统的复本。

包含要替换的源或原始数据对象的卷被称为“源卷”。它们被替换到等量“目标卷”中。当复制过程完成后，目标卷中的数据将构成复本。

目前有以下两种基本的复制技术 (有关详细信息，请参阅ZDB 和复制技术):

- **分割镜像**

  镜像是与源数据同步的、对源数据的动态复制。对源的任何更改都将应用到镜像中。

  此技术使文件系统或应用程序数据能够在正常使用应用程序的情况下得以创建和保留。

  要创建复本，镜像会暂时从源中分割出来。将从镜像中备份数据，然后将此镜像与源重新同步。

- **快照**

  快照复本是通过在特定时刻制作数据副本而创建的。快照可以是独立于源卷的完整副本，也可以是依赖于源卷的虚拟副本。

ZDB 类型

无论通过何种方法，创建复本后，均可对其进行备份。复本将装载到与创建复本所在的磁盘阵列连接的**备份系统**。要充分利用 ZDB，备份系统应该是一个独立的计算机系统。有三种形式的 ZDB：

- **ZDB 到磁带**

  1. 根据所选磁带备份类型，复本中的数据将流式传送到磁带上：

P9000 XP 磁盘阵列系列、3PAR StoreServ Storage (通过 3PAR SMI-S 代理) 和插入 SMI-S 代理的存储提供程序 (NetApp Storage):

Full、Incr 和 Incr1-9

P4000 SAN 解决方案、3PAR StoreServ Storage (通过 3PAR VSS 代理):

2. 然后将弃用此复本。

使用标准 Data Protector 技术可从磁带恢复数据。

- **ZDB 到磁盘**

  复本保留在磁盘阵列上，并且用作备份。

  使用即时恢复可还原数据 (请参阅即时恢复)，即恢复完整复本。

- **ZDB 到磁盘 + 磁带**

  1. 根据所选磁带备份类型，复本中的数据将流式传送到磁带上：

     P9000 XP 磁盘阵列系列、3PAR StoreServ 存储 (通过 3PAR SMI-S 代理):

     Full、Incr 和 Incr1-9

     P4000 SAN 解决方案、3PAR StoreServ Storage (通过 3PAR VSS 代理):

  2. 复本将保留在磁盘阵列上。

  这可提供更多灵活性，因为能以下述两种方式还原数据：

  - 使用标准 Data Protector从磁带还原（允许还原单个备份对象）
  - 使用完整复本的即时恢复（请参见）直接从复本恢复

支持的磁盘阵列

支持的复制技术与 ZDB 类型和磁盘阵列系列

ZDB 类型/ 磁盘阵列系列	ZDB 到磁带， 本地	ZDB 到磁带， 远程	ZDB 到磁带， 远程 + 本地	ZDB 到磁盘， 本地	ZDB 到磁盘 + 磁带， 本地
P4000 SAN 解决方案	快照	无	无	快照	快照
P9000 XP 磁盘阵列系列	分割镜像/ 快照	分割镜像	分割镜像/ 快照	分割镜像/ 快照	分割镜像/ 快照
3PAR StoreServ Storage	快照	无	无	快照	快照
NetApp Storage	快照	无	无	无	无

本地和**远程**是指复本所在的磁盘阵列，它既可以是源数据所在的阵列，也可以是远程站点上的独立磁盘阵列。有关这些术语及其含义的详细信息，请参见：

- 本地复制
- 远程复制
- 远程和本地复制

即时恢复和 ZDB 数据的还原

即时恢复

即时恢复要求复本与要还原的数据存在于同一磁盘阵列上。应用程序和备份系统均被禁用，且复本内容将直接还原到其原始位置或代替源卷的内容提供给系统。由于是在磁盘阵列内部执行还原，因此其运行速度非常快。

还原完成后，所涉及数据库或文件系统的分区将恢复到其创建复本时的状态，并且可重新启用应用程序系统。

根据所涉及的应用程序/数据库，只需完成上述操作即可。在某些情况下，对于完全恢复还需要执行其他操作，如应用单独备份的已存档事务日志文件。

其他 ZDB 数据还原方法

可以使用标准 Data Protector 还原过程还原备份到磁带的数据。

但是，对于特定的磁盘阵列系列，可以先从磁带恢复数据以更新复本，*然后*再将此复本内容恢复到其原始位置。这称为“拆分镜像还原”。将复本内容还原到其原始位置的过程与即时恢复的过程相似。只需在还原阶段暂挂应用程序操作，以尽可能减少对应用程序的影响。

有关更多详细信息，请参阅拆分镜像还原。

> **注意**复本还可用于除即时恢复外的其他用途，如数据挖掘。虽然 Data Protector 可以创建和管理此类用途的复本，但为即时恢复创建的复本应仅用于即时恢复。反之，可能会丢失已备份的数据。

ZDB 类型的恢复可能性

有关 ZDB 类型的还原可能性，请参阅下表:

	还原可能性		
ZDB 形式和技术	单个对象	灾难恢复	即时恢复
ZDB 到磁带（本地）	是	是	否
ZDB 到磁带（远程）	是	是	否
ZDB 到磁带（远程 + 本地）	是	是	否
ZDB 到磁盘（本地）	否	否	是
ZDB 到磁盘 + 磁带（本地）	是	是	是

ZDB 和复制技术

对于 Data Protector 支持的磁盘阵列集成，P4000 SAN 解决方案、3PAR StoreServ Storage 和 NetApp Storage 支持快照替换，而 P9000 XP 磁盘阵列系列集成支持拆分镜像和快照替换技术。对于这两种技术，都将生成包含指定源数据的卷副本。在同一磁盘阵列上的其他逻辑卷中创建这些副本，然后这些副本可呈现在主机系统中。在所有情况中，只能复制磁盘阵列上完整的逻辑卷，即使选择复制的数据仅占逻辑卷的一小部分。

包含要复制的源数据的卷被称为源卷。被复制到包含复制数据的等量目标卷中。当复制过程完成后，目标卷中的数据将构成复本。

复本可以在相同磁盘阵列上创建（称为本地复制），也可以在单独的远程磁盘阵列上创建（称为远程复制）。对于特定磁盘阵列系列，还可以组将这两种复制方法结合使用以获得最高级别的数据保护（称为远程加本地复制）。

从操作系统点角度看，特定源数据集的复本内容是相同的，不考虑用于产生副本的方法。但是，所使用的方法可能会对以下特点产生影响：

- 复制的速度。
- 使用的存储空间量。
- 对涉及的应用程序的影响。
- 数据安全。

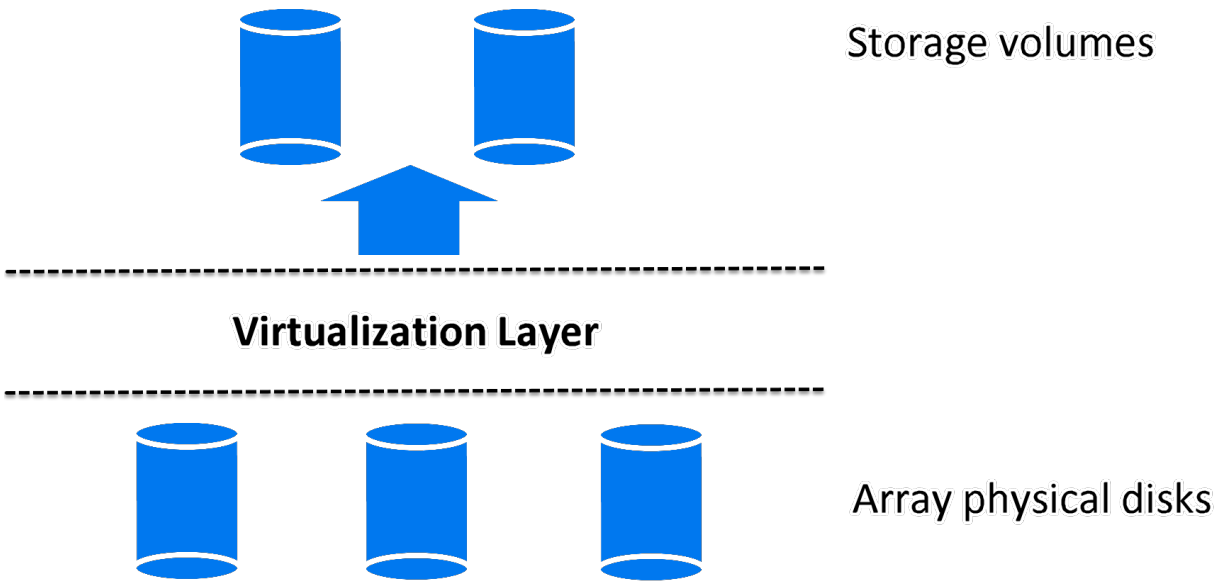
根据磁盘阵列类型还可能有某些硬件或软件限制。可用的复制技术取决于安装的磁盘阵列和复制软件的类型。

磁盘阵列基础

复制技术是否可用取决于磁盘阵列的类型和所安装的固件/软件。

磁盘阵列支持磁盘虚拟化技术，借助此技术可创建虚拟磁盘、逻辑卷等。

磁盘虚拟化



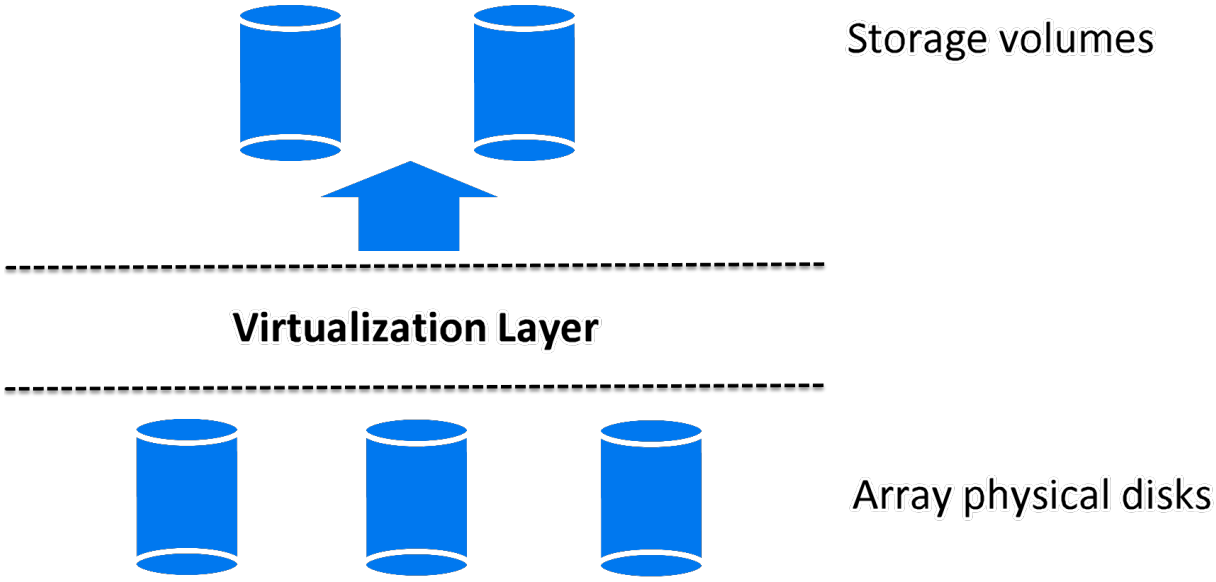
一组物理磁盘将配置为一个大型数据存储块。此存储块随后可划分为若干虚拟存储块，驻留在主机/操作系统中。

这些存储块的名称可以各不相同，但是其生成技术基本相似，为简便起见，将它们均视为“存储卷”。

RAID 技术

磁盘阵列使用 **RAID 技术**，此技术适用于对于 RAID 系统而言可用的存储，以提供数据冗余和增强数据保护。

通过 RAID 实现的磁盘虚拟化



各种 RAID 级别均可用，可提供不同级别的数据冗余、速度和访问时间。在某些情况下，可以根据可用存储量调整这些属性之间的平衡。

RAID 系统的运转方式是将数据分布在各物理磁盘上，并将其作为逻辑单元驻留在主机中，反之，可以将这些逻辑单元视为之前的磁盘虚拟化图中的物理磁盘。虚拟化完成后，最终驻留在主机操作系统上的是虚拟磁盘或存储卷。

复制技术

基本复制可在以下三种环境中执行：

- 本地（源和目标卷位于同一磁盘阵列上）
- 本地 – 与 HP-UX LVM 镜像的本地集成（源和目标卷位于同一磁盘阵列上，但至少需要两个磁盘阵列）
- 远程（源和目标卷位于不同磁盘阵列上）
- 远程和本地（远程磁盘阵列上的远程和本地复制）

对于操作系统而言，无论使用何种技术生成复本，特定源卷及其复本的内容都是相同的。但是，所使用的方法可能会影响到以下方面：

- 复制的速度
- 占用的存储空间量
- 对所涉及应用程序的影响
- 数据安全性

下文将讨论以下每种环境中的复制方法。

本地复制

在**本地复制**中，数据是在同一磁盘阵列内进行复制的，即源和目标卷位于同一磁盘阵列上。

有两种技术：

- 分割镜像
- 快照

本地复制的优点

- 可用于 Data Protector 支持的所有磁盘阵列类型。
- 可用于 Data Protector 支持的所有应用程序集成。
- 复制和同步过程都在本地磁盘阵列上执行。这意味着执行这些过程会非常快，且应用程序系统的中断时间会降至最低限度。
- 支持所有 ZDB 类型（包括即时恢复），从而增加了备份策略的选择灵活性。

缺点

- 源数据和复本均容易受到磁盘阵列或本地系统灾难性故障的影响。

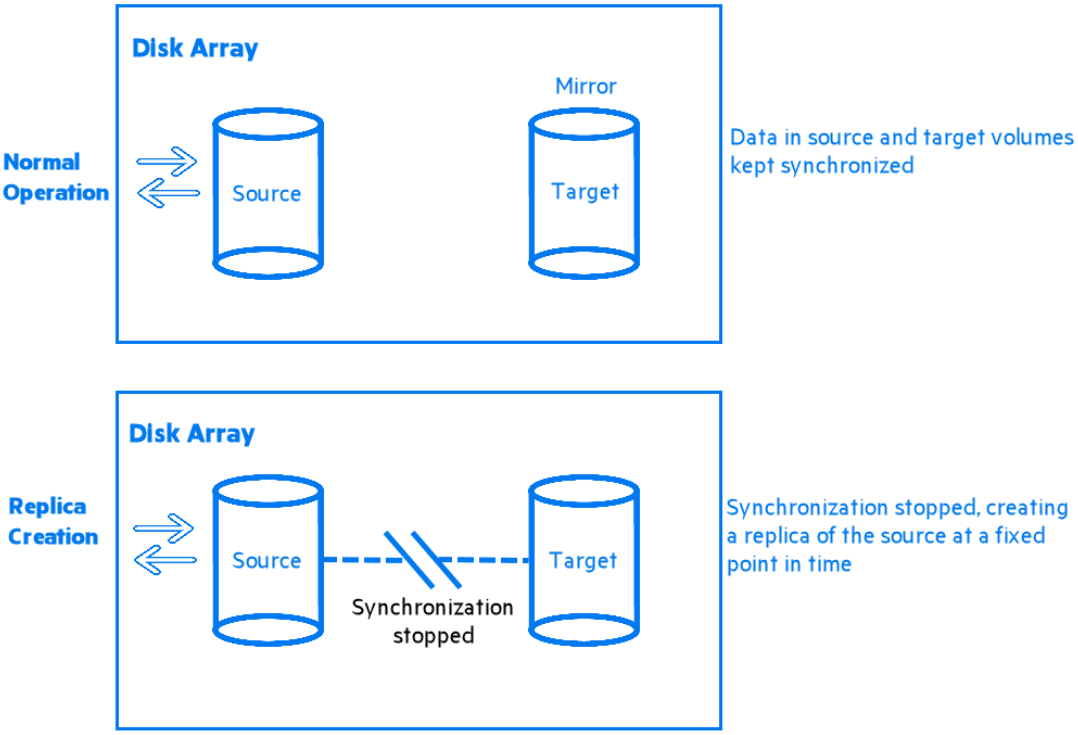
有两种形式的本地复制：

- 分割镜像复制
- 快照复制

分割镜像复制

在磁盘阵列术语中，“镜像”是源卷的动态副本。

分割镜像复制



首次创建镜像后，将同步其中的数据，直到它们与源卷中的数据完全一致为止。在正常使用应用程序期间，镜像将始终保持与源卷的同步。对源卷的任何更新都将应用到镜像中。

当管理任务（如备份）需要某个修复时间点的数据复本时：

1. 镜像卷之间的同步将停止（镜像被分割），并保留源卷的独立复本。
2. 复本将用于备份或其他任务，同时利用源数据使应用程序继续保持虚拟意义上的不受影响。
3. 如果需要，在对复本执行完操作后，会将两个数据集重新进行同步，直到其他管理任务再次需要镜像数据时为止。

分割速度非常快，并且对应用程序系统的影响也很小。

支持拆分镜像替换的 Data Protector 磁盘阵列集成有:

- 使用 Business Copy P9000 XP 配置的 P9000 XP 磁盘阵列系列集成，允许创建三个一级镜像供即时恢复使用。

分割镜像复本的特点

- 分割镜像复本是对源卷的完整复制（或克隆）,对于主机/操作系统而言，分割镜像复本与创建该复本时的源是完全相同的。

  在物理磁盘或逻辑单元级别，存在源存储块内容的完整物理副本。

- 它完全独立于原始数据。

  由于存在数据的独立物理副本，因此当磁盘阵列硬件遇到会影响源卷的局部故障时，这些目标卷将保持完好并且可用。

快照复制

快照复本是在特定瞬间创建的，并且立即可供使用。与分割镜像复本不同，快照复制最初不会复制任何数据，而是将通过虚拟化创建原始存储的复本。此时，复本是虚拟副本。实际数据由源和复本共享。

之后，当源卷中的数据首次发生更改时，原始数据将先复制到快照中，然后再更新源数据。随着时间的推移，快照将引用一部分其自身的独立数据和一部分共享数据（形式为指向未更改的源数据的指针）。但是，对于主机或操作系统而言，快照始终包含其创建时源卷的完整副本。

支持快照复制的 Data Protector 磁盘阵列集成有：

- 使用 Business Copy P9000 XP 配置的 P9000 XP 磁盘阵列系列集成。可以在磁盘阵列上创建大型复本集用于即时恢复，且成员数量受到磁盘阵列模型、所安装的磁盘阵列固件版本以及磁盘阵列上目标存储池的剩余存储容量的限制。
- 使用本地复制配置的 3PAR StoreServ Storage 集成和 NetApp Storage 集成。含标准快照和无容量快照的复本集中的最大复本数量受固件的限制。

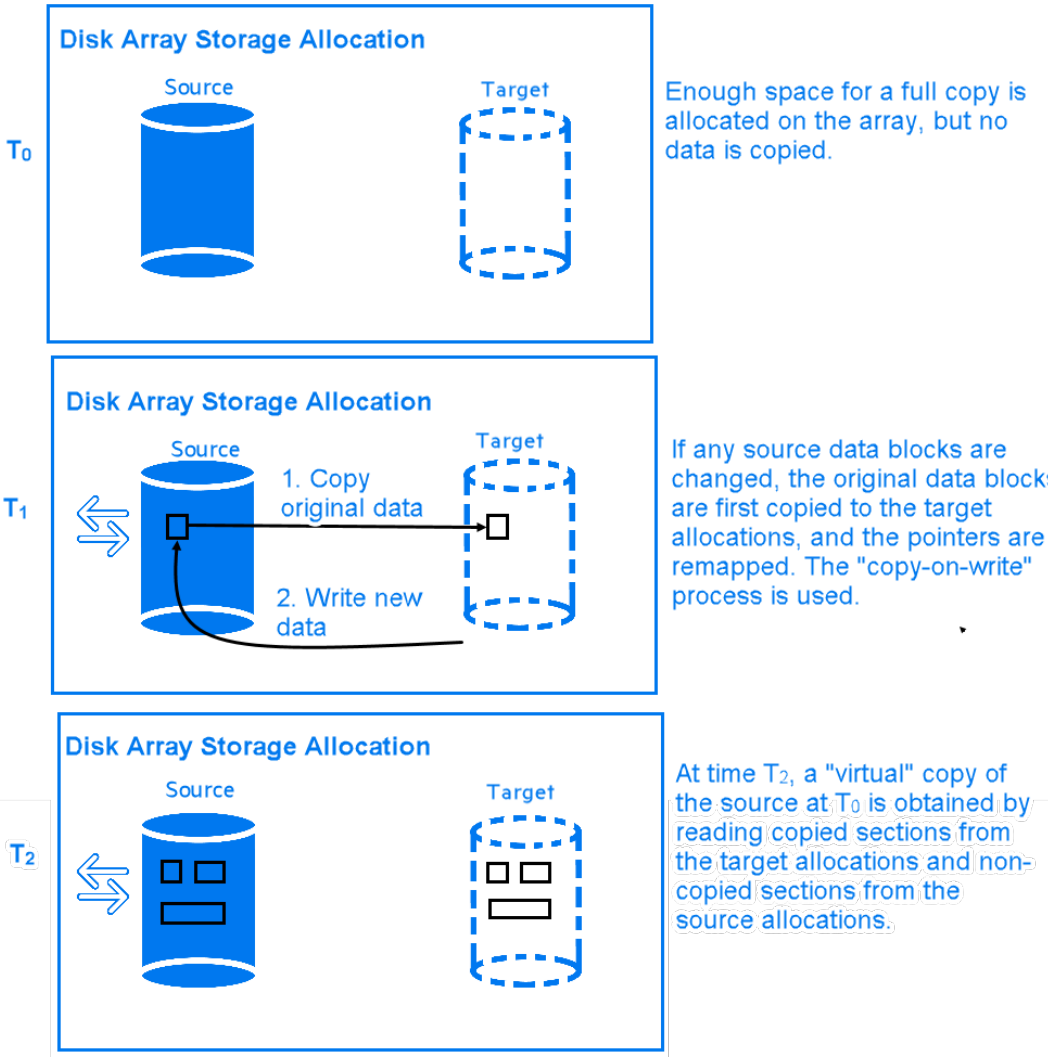
您可以通过阵列与 Data Protector 的受支持集成创建以下类型的快照：

- **标准快照**（也称为“预分配快照”、“完全分配快照”或简称“快照”），在创建快照时就会分配足够的空间以保存所有源数据的完整副本。
- “无容量快照”(也称为“实际无容量快照”或“按需求分配快照”)，不预分配任何空间。
- **快照式克隆**，最初与标准快照相同，但是其中的数据将作为后台任务进行复制，直到快照式克隆成为其创建时源卷的完整物理副本。

下文将进行详述。

标准快照

创建标准快照



1. 在 T_0 时，将在磁盘阵列上为目标卷分配与所涉及源卷占用的容量相等的存储容量。

   此时，不会从源存储块复制任何数据。而是将指针映射到保存原始数据的存储块，此时副本是完全虚拟的。但是对于主机而言，T_0 时源卷的完整复本存在于目标卷中且可供使用。

2. 创建快照后，T_0 源数据首次需要更新时，先将其复制到目标存储块中，然后再将快照中的指针重新映射到这些副本。之后才会更新源数据。

   这称为“写时复制”。

3. 此时，快照一部分是真实的（即其中已复制的源数据），一部分是虚拟的。当访问复本时，将从目标存储块读取任何之前已复制的数据，而从源存储块读取之前未复制的任何数据。因此对于主机而言，T_0 时源数据的完整复本仍然存在。

标准快照的特点

- 标准快照不是原始数据的独立复本（但是，它可以是更新后的源卷中已复制的单个存储块）。
- 即使源卷中的所有数据均有所更改，仍能保证为快照预留足够的空间。
- 空间利用率低。尽管通常只会占用部分预留空间，但是它仍将为所有数据均有所更改的情况而预留足够的空间。只要存在快照，未占用的预留空间就不得用作任何其他用途。

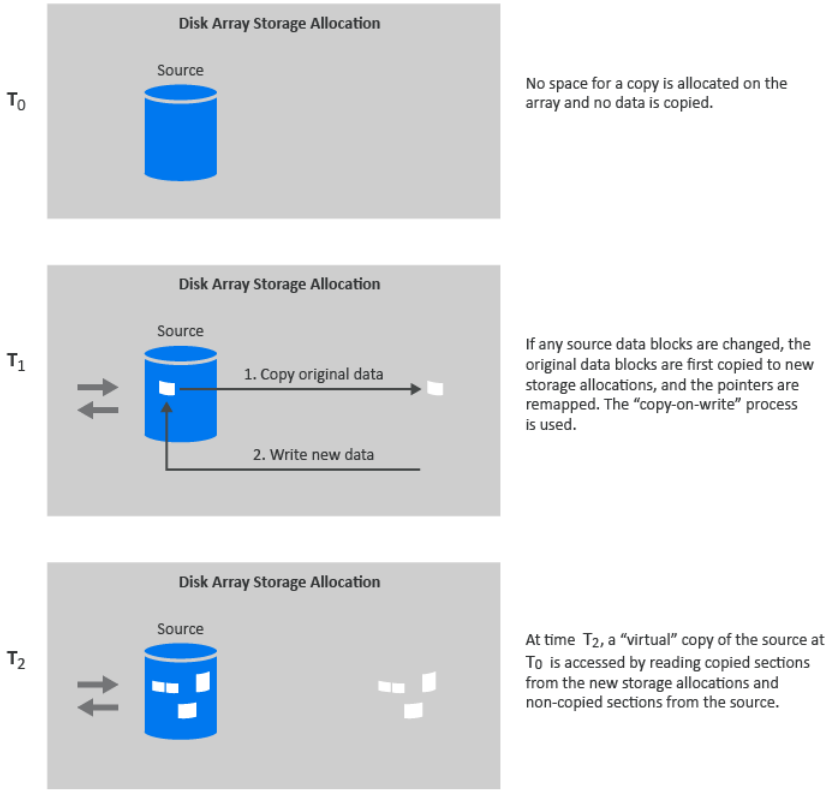
对应用程序性能的影响

当备份系统访问快照时，它将从源卷和复本中读取磁盘块。因此，将同时占用应用程序和备份系统磁盘的资源，这将导致磁盘阵列过载时应用程序的性能下降。

无容量快照

对于无容量快照，最初不会预留任何存储容量。否则，其处理过程将与标准快照雷同：

创建无容量快照



1. 在 T_0 时，仅将指针复制到目标，这与标准快照的过程相同，但是不会为目标卷预留任何空间。除指针所需空间外，无容量快照不会占用任何存储空间。
2. 快照创建后，T_0 源数据需要首次更新时，将使用“写时复制”，这与标准快照中的情况相同。只有更改的数据需要占用存储空间。
3. 与标准快照一样，此时的无容量快照一部分是真实的，一部分是虚拟的。

无容量快照的特点

- 与标准快照类似，无容量快照不是原始数据的独立复本。
- 无容量快照需要独立的磁盘容量管理，以保证为复本的增大预留足够空间。如果磁盘阵列空间用尽，无容量快照更新将失败，并且可能影响常规的磁盘阵列操作。
- 空间利用率高。无容量快照仅占用所需空间。
- 是暂时的。由于无容量快照的存储需求是动态的，因此如果在创建快照后对源卷进行多次更改，则磁盘阵列空间可能会用尽。对磁盘阵列的其他存储需求也可能导致磁盘阵列的存储空间用尽。

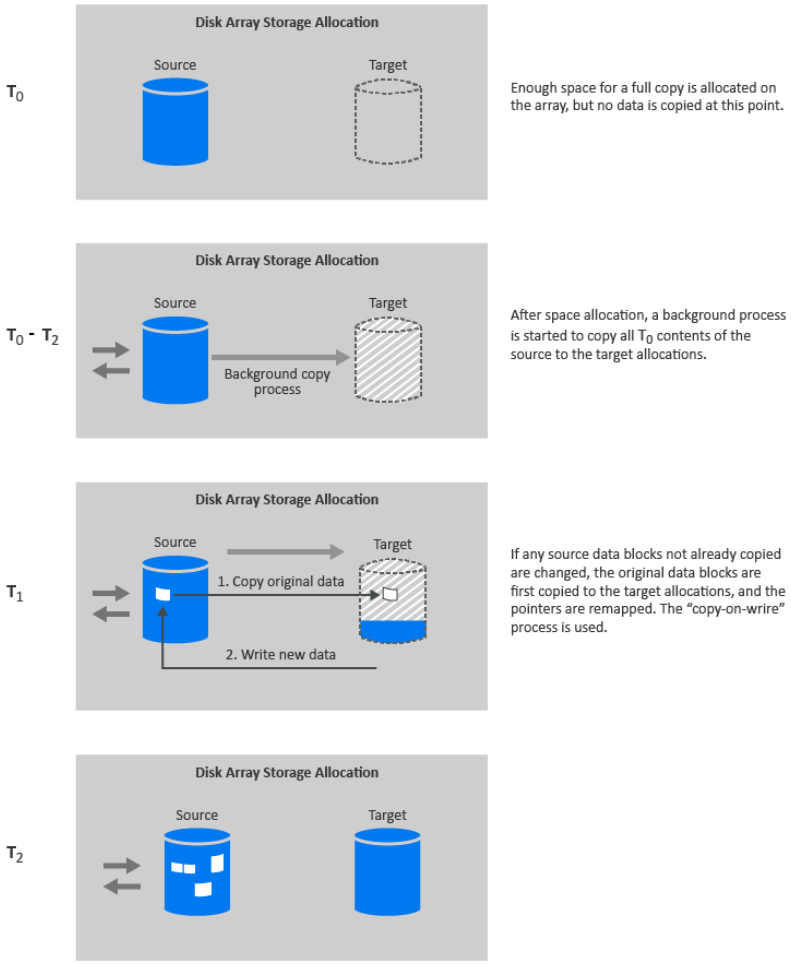
对应用程序性能的影响

与标准快照一样，当备份系统访问快照时，它将从源卷和复本中读取磁盘块。因此，将同时占用应用程序和备份系统磁盘的资源，这可能导致磁盘阵列过载时应用程序的性能下降。

快照式克隆

快照式克隆最初与标准快照的过程相同，而最终与分割镜像复本情况相似，即生成完整的复本（或克隆）。

创建快照式克隆



Data Protector 快照式克隆是与一种名为“容器”的存储对象一同创建的，以加速快照式克隆的创建过程并在数据复制期间减少对源卷的影响。容器是磁盘阵列上的空间，已为稍后用作标准快照、无容量快照或快照式克隆进行了预分配。可以从可用磁盘空间中创建容器，也可以将不再需要的存储卷转换成容器。

快照式克隆的创建过程如下：

1. 如果容器尚不存在，则将在磁盘阵列上创建大小和存储冗余级别都与源卷相同的容器。
2. 将源卷上的写入缓存策略设置为连续写入模式，因此缓存中的所有数据都将写入物理磁盘
3. 创建标准快照，包括为完整副本分配足够的空间。
4. 启动后台进程，将所有未更改数据从源存储块复制到目标存储块中。此时，写入缓存策略将自动恢复为写回模式。
5. 如果需要更新后台进程尚未复制的源数据，应先对其进行复制（写时复制），这与标准快照中相同。

   在后台复制进程执行期间，如果需要使用快照，其副本一部分是真实的，一部分是虚拟的，这与标准快照中相同。
6. 当将所有数据均复制到目标存储位置后，后台进程将停止，并保留 T_0 时源的独立复本或克隆。

快照式克隆的特点（复制完成后）

- 快照式克隆是源卷的完整复本，对于主机和操作系统而言，它与创建复本时的源完全相同。

  在物理磁盘或逻辑单元级别，存在源存储块内容的完整物理副本。
- 它完全独立于原始数据。

  由于物理副本是完整的，如果源卷的内容丢失或损坏，目标卷的内容将不受影响。
- 它是永久的。

对应用程序性能的影响

- 后台数据复制过程可通过资源竞争影响应用程序的性能。生成大型数据库的快照式克隆时，复制可能需要较长一段时间。

  通过使用容器，可以减小数据复制过程对应用程序性能的影响。此外，还可以显著缩短应用程序需停留在备份模式下的时间。
- 如果系统在克隆过程完成之前访问快照式克隆，则将从源卷读取尚未复制的磁盘块。在 ZDB 到磁带或 ZDB 到磁盘 + 磁带的情况中，读取数据时将同时占用应用程序和备份系统磁盘的资源；这可能降低应用程序的性能。为避免出现这种情况，如果克隆过程仍在进行中，则

Data Protector 将延迟将快照式克隆数据复制到磁带，最长可延迟 90 分钟。这是默认值；您可以在配置备份规范时在 Data Protector GUI 中对其进行更改。

与 HP-UX LVM 镜像集成的本地复制

与 HP-UX LVM 镜像集成的本地复制是一种特定集成，可减少为获取完整版本所需复制的存储量。同时，还可以配置 LVM 镜像，以提供类似于 Continuous Access (CA) 在远程加本地替换环境中有关拆分镜像和快照阵列的功能。

与 LVM 镜像集成的本地复制的优点

- 它可用于 Data Protector 支持的所有磁盘阵列类型。
- 通过制作部分已用磁盘的副本降低磁盘空间使用量。
- 与单纯的 CA 或 SRDF 环境相比，更易于设置和管理 LVM 镜像环境。
- 如果 I/O 通道失败，LVM 可以从复制源恢复数据。
- LVM 镜像环境的成本低于 CA 或 SRDF 环境的成本，因为不需要 CA/SRDF 许可证。只有在创建复本的系统上才需要 BC 许可证。

缺点

- LVM 镜像配置的设置可能更为复杂，并且与 BC 或 TimeFinder 环境相比，要求更为严格。
- LVM 镜像配置在执行即时恢复时更为复杂。在特定磁盘阵列中，不支持 LVM 镜像配置中已备份数据的即时恢复。

远程复制

在**远程复制**时，将数据从可以进一步备份到本地可用介质的位置复制到独立远程磁盘阵列。建立通信后，远程复制操作将继续保持无人看管状态，并且可提供连续的实时远程数据复制。

远程复制的优点

- 使数据免受灾难性故障（如存储系统缺失）的影响。如果远程磁盘阵列位于不同的（远程）计算中心，则远程复制也会消除由于火灾或任何其他灾难而同时损坏生产和备份环境的风险（甚至在整个计算中心损坏时也如此）。
- 适合进行灾难恢复。
- 确保重要数据的连续可用性。

缺点

- 网络和光纤通道连接性传送速度将增加复制对应用程序或数据库性能的影响。
- 需要同步传输，这可能会影响应用程序系统。
- 至少需要两个磁盘阵列以及相关联的许可证，这会增加成本。
- 保持远程同步的必要性可能会影响性能和应用程序。

分割镜像复制

与本地镜像相同，将创建源卷的复本并将其保留在目标卷上，只是在分割镜像复制中，目标卷位于远程磁盘阵列上。建立通信后，目标卷将与本地磁盘阵列上的源卷保持同步。

当需要特定时间点的源卷复本时，镜像卷之间的同步将停止。远程磁盘阵列随后将包含本地磁盘阵列上源卷的修复副本或独立复本。

但是，如果阵列是安装在独立站点上的，则可能会发生相距数千米的连续远程同步，而这可能会应用应用程序系统的性能。对于 Data Protector，到远程系统的链接通常必须保持同步。但是 CA 支持异步通信；Data Protector 在将数据复制到镜像时会切换为同步模式，然后再切换回异步模式。

可以选择此配置用作灾难恢复（通常在群集环境中），因为与保持 CA 链接相比，其利大于弊。为进行备份而断开链接将缩小灾难恢复的涵盖范围并导致无法进行故障转移。比较远程和本地复制。

Data Protector 支持在带有连续访问 P9000 XP 配置的 P9000 XP 磁盘阵列系列上使用镜像技术进行远程替换。

也不支持使用远程复制从 ZDB 会话创建的即时恢复，这意味着只能在 ZDB 到磁带会话中备份数据。

远程和本地复制

远程和本地复制采用远程和本地复制的方式；使用远程复制在远程磁盘阵列上创建复本，然后将其用作本地复制的源卷。

如果将远程站点用作灾难恢复站点，则通常使用此配置，但无法分割远程对。要自动化故障转移，可使用群集应用程序。

Data Protector 在以下磁盘阵列上支持远程加本地复制：

- 采用 Continuous Access P9000 XP 和 Business Copy P9000 XP 组合配置的 P9000 XP 磁盘阵列系列

远程和本地复制的优点

与远程复制相比，还具有以下优点：

- 允许创建磁带备份，而不会进一步影响应用程序系统或数据库。
- 可进行自动化故障转移。

缺点

与远程复制的缺点相同。

分割镜像复制

复制的远程部分

与远程复制相同，在独立的磁盘阵列上通过源卷和目标卷设置镜像卷。

建立通信后，远程磁盘阵列上的镜像卷将与源卷保持同步。对于 Data Protector，阵列之间的链接必须保持同步。

复制的本地部分

远程复制阶段的目标卷成为远程磁盘阵列上本地复制的源卷。

当需要复本时，本地镜像卷之间的同步将停止（镜像被分割），但是远程镜像卷之间将继续保持同步。远程磁盘阵列上的本地复本（复本的复本）随后将成为本地磁盘阵列上源卷的修复复本或独立复本。

快照复制

复制的远程部分

数据将从应用程序系统写入本地阵列上的源卷，并且将复制到远程磁盘阵列上的目标卷。在后台进行数据复制时，应用程序将不受影响地继续运行。

复制的本地部分

远程复制阶段的目标卷成为远程磁盘阵列上本地复制的源卷。

快照复本卷是在特定瞬间创建的，并且立即可供使用。

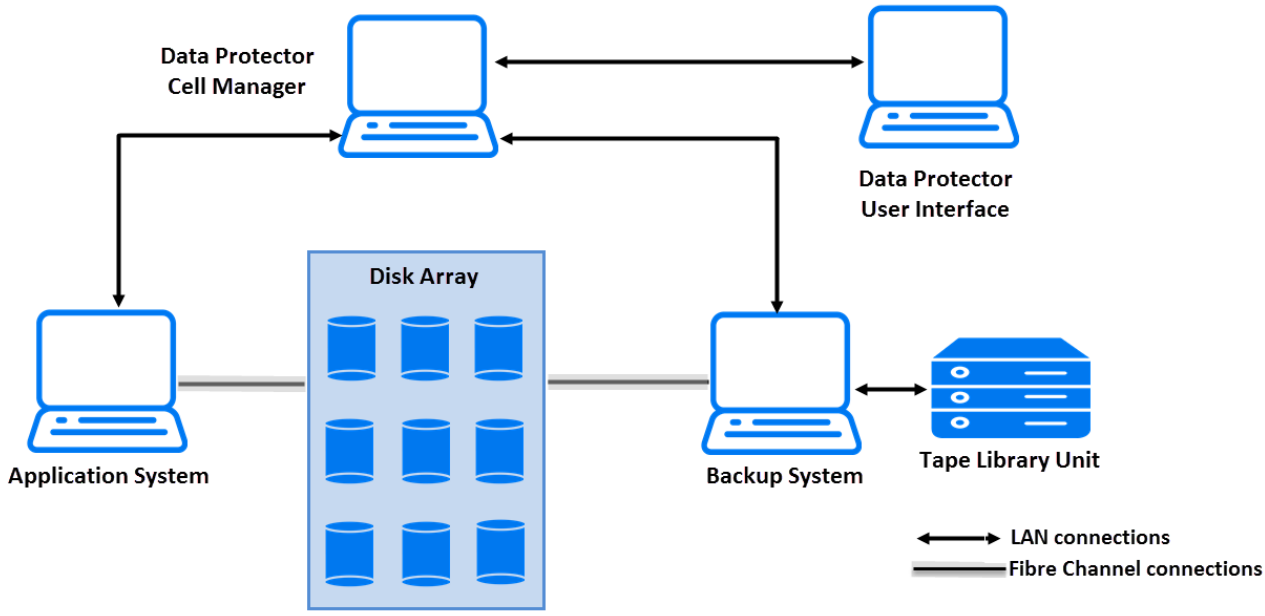
> **注意**远程和本地复制提供了在非故障转移和故障转移两种情况下理解和处理复本创建的方法，从而使您能够在源站点或目标站点执行 ZDB。

使用 Data Protector 进行 ZDB 和即时恢复

Data Protector 单元

Data Protector 使用“受管单元”的概念。下图显示如何为 ZDB 和 IR 设置单元：

Data Protector 为 ZDB 和 IR 设置单元

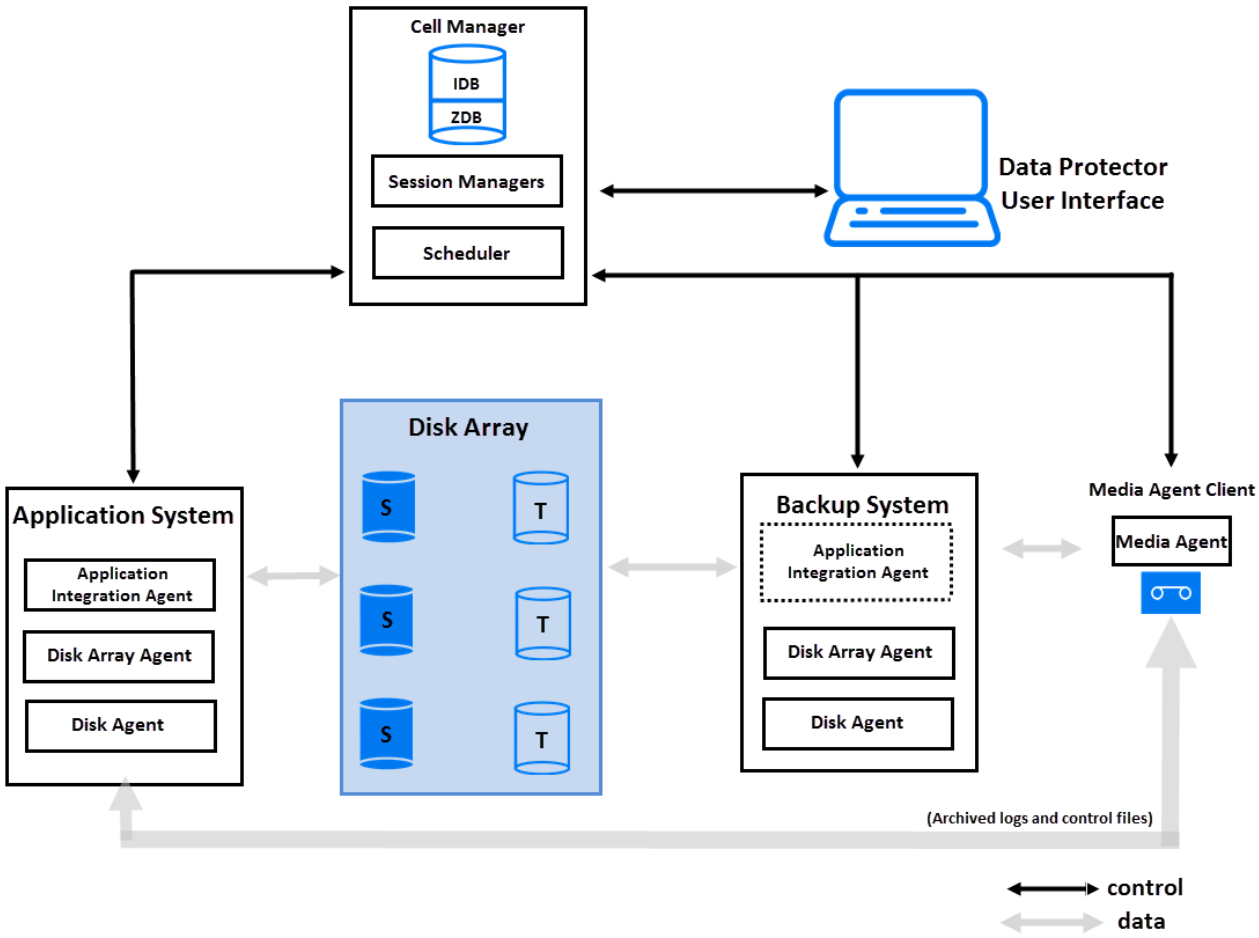


要能够使用 ZDB 和 IR 技术，要备份的应用程序数据库或文件系统数据必须位于该应用程序和备份系统均直接连接的磁盘阵列上。库或其他存储设备对于 ZDB 和 IR 应用程序是可选的。

单元组件

对于典型 Data Protector单元，应按下图所示在硬件中安装操作软件组件。

ZDB 和 IR 软件组件的位置



Cell Manager

Cell Manager 是单元的主系统。

应用程序系统

要创建复本的每个应用程序系统都必须安装有以下 Data Protector 组件：

- 磁盘阵列代理或 ZDB 代理，用于控制 Data Protector Cell Manager 与安装有应用程序数据库/文件系统的磁盘阵列之间的交互。每个受支持磁盘阵列类型都有其专用的代理。
- 应用程序集成代理，用于控制 Data Protector Cell Manager 与应用程序之间的交互。Data Protector 要求该代理执行若干功能，例如，在数据库应用程序的备份和还原会话期间控制数据库的状态。如果没有此代理，则只有文件系统备份可用。

备份系统

它是复本在创建后所驻留的系统，因此它也是可访问复本以供后续处理的系统，无论是否会将它所含数据备份到介质。备份系统和应用程序系统之间的联系仅限用于协调 ZDB 与 IR 会话中涉及的过程。备份系统可服务于运行不同应用程序的多个应用程序系统。它还会执行各种检查和管理功能。

备份系统必须：

- 能在合理的时间内执行备份。
- 安装有相关 Data Protector ZDB 代理。在某些情况下，它还需要应用程序集成代理。
- 将同一操作系统版本用作应用程序系统。

通常，备份系统与应用程序系统不是同一系统。

ZDB 数据库 (ZDB database)

ZDB 数据库是对 Cell Manager 上的 Data Protector 内部数据库 (IDB) 的扩展。其中包含有关复本的特定于阵列的信息，供即时恢复所用。

对于在 Data Protector 内本地支持 ZDB（和包括 IR 的大多数系列）的每个磁盘阵列系列，ZDB 数据库都有独立分区：

- 适用于 3PAR StoreServ Storage 和 NetApp Storage 的 SMISDB。

- 用于 P9000 XP 磁盘阵列系列的 XPDB

此外，独立分区还包含操作系统信息，如文件系统或卷管理配置：

- SYSDB

ZDB 中存储的准确信息取决于磁盘阵列。通常，每个分区都包含以下类型的信息：

- 有关磁盘阵列上所保留的复本的信息，包括：
  - 备份会话 ID
  - 备份会话的执行时间
  - 备份会话中所使用的备份规范的名称
  - 在会话中创建的目标卷的名称、ID 和 WWN
  - 有关主目录（CA+BC 配置）的信息
  - 备份会话中所使用的源卷的 ID
  - 目标卷是否可用于即时恢复（IR 标记）
  - 是否应删除目标卷（清除标记）
  - 会话涉及的应用程序和备份系统
- 从复本集循环和其他用途中排除的磁盘阵列卷。
- 其他配置信息：
  - *P9000 XP 磁盘阵列系列:*检测到 P9000 XP 阵列命令设备
- 一些磁盘阵列安全信息。
- ***仅 XP :*** 在 ZDB 到磁盘会话期间计算的 CRC。
- *仅 XP :* 有关 XP 命令设备的信息。

创建复本时，此信息会写入 ZDB 数据库，删除复本时，此信息随之删除。

ZDB 数据库仅存储备份规范中**在备份完成之后保留副本**选项处于选中状态的 ZDB 会话的信息。对于在 ZDB 到磁带会话中创建的复本，如果未选中此选项，则会在备份后从 ZDB 数据库中删除那些复本。

有关 ZDB 到磁带会话的信息以及有关 ZDB 到磁盘 + 磁带会话的某些信息存储在 IDB 的其他部分中。

用户界面

可以使用 Data Protector图形用户界面 (GUI) 或命令行界面 (CLI) 来执行 ZDB 和 IR 操作。

GUI

通过 GUI 可以从单个系统管理 ZDB 环境。可以：

- 为 ZDB 创建备份规范、调度它们并启动 ZDB 会话。
- 监视活动操作。
- 使用 Data Protector 报告和通知功能。
- 在**即时恢复**上下文中，浏览标记为要进行即时恢复的会话、定义必需的选项，以及启动即时恢复会话。
- 在“还原”上下文中，浏览存储在备份介质上的会话、定义必需的选项，以及从磁带启动标准 Data Protector 还原过程。

CLI

可以使用 CLI 执行 GUI 中可用的大多数 ZDB 和 IR 操作，但是某些管理任务只能通过 CLI 完成：

- 查询、同步和清除 ZDB 数据库
- 检查 ZDB 数据库的一致性
- 手动删除不再需要的复本或复本集及其存储在 ZDB 数据库中的相关信息
- 用 Data Protector 使复本排除或包含在使用中。

Data Protector 可实现的磁盘阵列集成

Data Protector 支持能够创建复本并且大多数情况下能够创建复本集的以下磁盘阵列：

与 Data Protector 集成的磁盘阵列

复本类型	支持的磁盘阵列	缩写
分割镜像	P9000 XP 磁盘阵列系列	P9000 XP 阵列
快照	P4000 SAN 解决方案	P4000 SAN 解决方案
	P9000 XP 磁盘阵列系列	P9000 XP 阵列
	3PAR StoreServ Storage	3PAR StoreServ
	NetApp Storage	NetApp

有关受 Data Protector 支持的当前配置列表，请参阅最新支持矩阵。

P4000 SAN 解决方案

P4000 SAN 解决方案支持创建使用按需分配的存储空间并基于“写时重定向”技术的快照。使用此磁盘阵列系列时，Data Protector 只支持本地复制。

P9000 XP 磁盘阵列系列

Data ProtectorP9000 XP 阵列集成支持以下配置:

- 本地复制
- 本地复制 – 与 LVM 镜像集成
- 远程复制
- 远程和本地复制（提供最高级别的数据保护）

在将源卷连接到应用程序系统的同时，将独立的备份系统连接到包含目标卷的磁盘阵列。分割镜像或创建快照后，将数据从复本流式传送到磁带上，因此在备份期间，应用程序系统仍处于联机状态并可供使用。

本地复制

对于本地替换，使用“Business Copy (BC) P9000 XP 配置”。这使您能够针对即时恢复创建“一级镜像”或“用于快照存储的卷”，换言之，就是一个复本集。

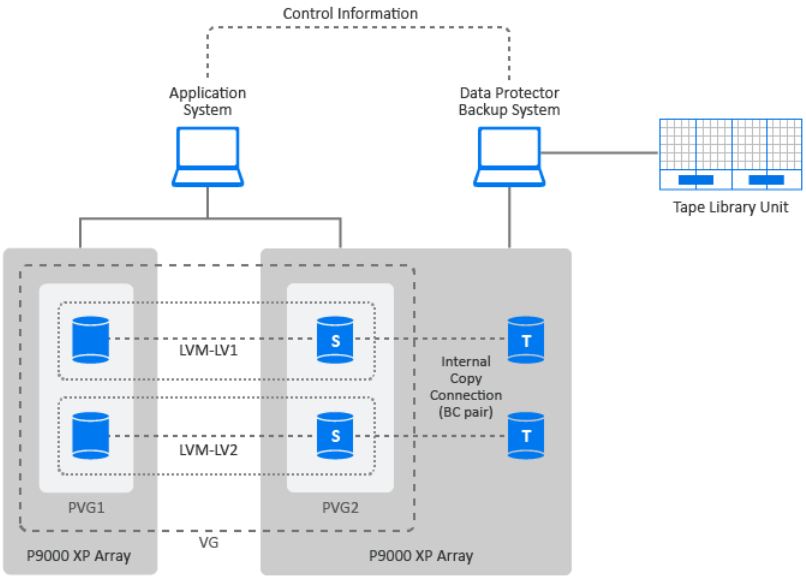
BC P9000 XP 配置的示例

File:DP202005 XP BCCA environment2 recreated.pngDP202005 XP BCCA environment2.png

与 LVM 镜像集成的本地复制

Data Protector P9000 XP 阵列集成在以下配置中支持 HP-UX Logical Volume Manager 镜像 (“LVM 镜像”): 配置中一个物理磁盘 (LDEV) 上的一个逻辑卷被镜像至另一个物理磁盘 (LDEV) 上的逻辑卷。

LVM 镜像配置 - P9000 XP 阵列的示例



远程复制

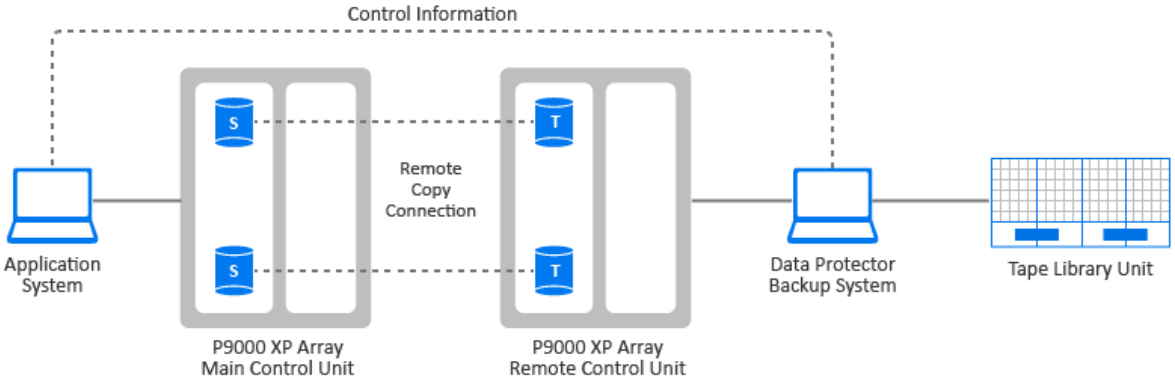
对于远程替换，使用“Continuous Access (CA) P9000 XP 配置”。这使您能够在相当长距离的远程系统上创建分割镜像复本。

CA P9000 XP 支持以下两种类型的接口:

- 适用于远距离的 Extended Serial Adapter (ESCON)
- 适用于最远 2 km 的 Fibre Channel (FC)

可以通过内置单模式光纤多路复用器使用 FC 交换机增加 Fibre Channel 距离。

CA P9000 XP 配置的示例



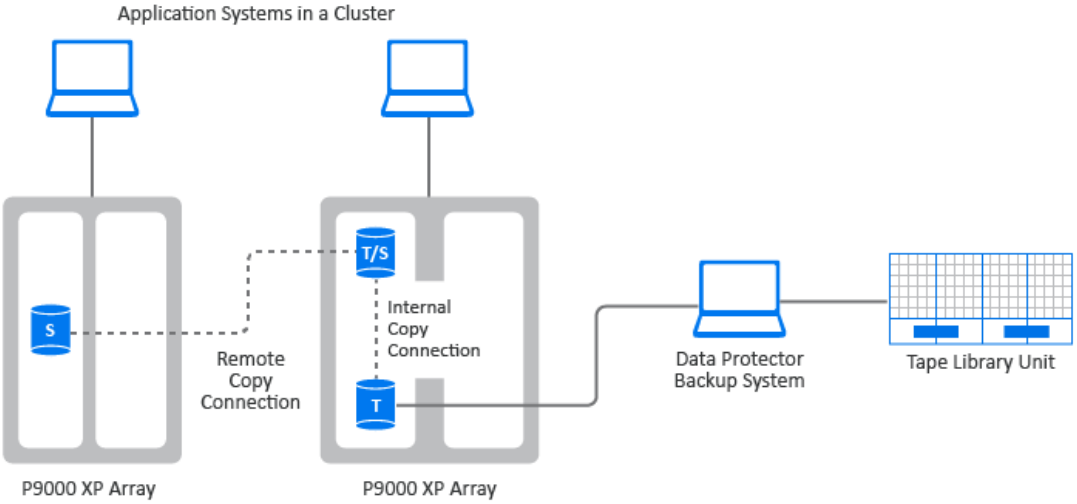
远程和本地复制

对于远程加本地替换，使用“CA P9000 XP 和 BC P9000 XP 配置的组合”。这使您能够在远程系统上创建分割镜像复本，然后在远程系统上为那些复本创建本地分割镜像或快照复本。

需要至少两个位于实际独立的站点中的磁盘阵列。

当需要复本时，集成会分割 BC 对。为确保数据一致性，会在执行 BC 对分割之前检查 CA 对的状态。这就确保了主控制单元中的所有数据均位于远程控制单元中。

群集中的 CA P9000 XP 配置



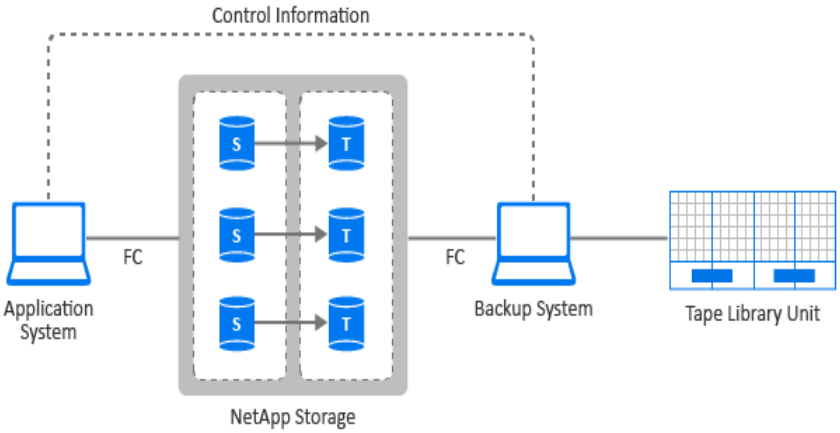
3PAR StoreServ Storage

3PAR StoreServ Storage 支持创建使用按需分配的存储空间并基于“写时重定向”技术的快照。使用此磁盘阵列系列时，Data Protector 只支持本地复制。

NetApp Storage

NetApp Storage 支持创建精简配置的复本（虚拟快照）和完全分配的复本配置类型。使用 NetApp Storage 时，Data Protector 仅支持本地复制。

NetApp Storage 配置的示例



应用程序集成

Data Protector 支持受支持磁盘阵列与以下数据库和虚拟环境应用程序及复制类型的集成（联机或脱机）：

- Oracle – 联机和脱机备份
- SAP R/3 – 联机和脱机备份
- Microsoft SQL Server – 联机备份
- Microsoft Exchange Server – 基于文件系统的脱机备份
- VMware Virtual Environment – 联机备份
  受 NetApp Storage 和 3PAR StoreServ Storage 支持。

Microsoft SQL Server 和 Microsoft Exchange Server 通过 Data Protector Microsoft 卷影复制服务集成同样受支持。

有关联机和脱机备份的信息，请参见冻结应用程序或数据库的操作。

所有复制技术（本地、远程、远程和本地）均适用于 Data Protector 支持的各种数据库和虚拟环境应用程序。但是，并非所有应用程序和虚拟环境集成都受到各种 ZDB 代理或其平台的支持。有关详细信息，请参阅最新支持矩阵。

应用程序数据一致性

逻辑卷或磁盘的简单 ZDB 只能保证文件系统的一致性，而无法确保应用程序数据的一致性。对此类备份进行即时恢复后，可能无法正确恢复数据库。对于支持的集成，Data Protector 可确保将应用程序设置为备份模式 (联机备份 - 可以减少应用程序可执行的一系列操作的持续时间) 或将其关闭 (脱机备份)，但是您必须单独备份事务日志。对于非集成应用程序，您必须确保备份可用于数据库恢复。您可以关闭应用程序或使用先执行脚本将其设置为适当的模式。

事务日志

当联机备份数据库应用程序时，需要单独备份任何已存档的数据库事务日志，以便能够执行完整的数据库恢复。事务日志不应与其余的数据库数据在同一零宕机时间备份会话中进行备份。

只有通过在 ZDB 会话之后运行单独的普通 Data Protector 备份会话，才能将已归档的数据库事务日志备份到磁盘或磁带。可在 Data Protector ZDB 备份规范中的“Post-exec”选项中指定启动备份会话的脚本。这样，在复本创建完成后，就会自动启动事务日志的备份。

还原

有关适用于受支持数据库应用程序的还原方法的详细信息，请参阅最新支持矩阵。

通过即时恢复，可以将数据库恢复到创建复本时的时间点。但在大多数情况下，要完全恢复数据库，还必须在之后应用事务日志。使用这些日志，还可以将数据库前滚至特定时间点。较短的 ZDB 备份时段会导致完整数据库恢复期间所需运用的存档日志文件数量减少。

应用程序集成和 Microsoft 卷影复制服务

在传统备份模型中，备份应用程序可与备份过程涉及的各种系统和组件协作：应用程序和备份系统及磁盘阵列。Data Protector P9000 XP 磁盘阵列系列集成就是这种情况，其中 P9000 XP 代理和 3PAR SMI-S 代理控制磁盘阵列，Data Protector 集成与数据库应用程序交互。

在 Windows 系统上，Microsoft 卷影复制服务 (**VSS**) 是一种统一备份和还原服务，可协调备份过程中涉及的各个组件。VSS 模型可提供应用程序（**写入程序**）和磁盘阵列（**提供程序**）的标准化界面。

写入程序与应用程序进行交互，以提供可备份项目的列表。写入程序可提供操作系统和应用程序级别上的数据完整性。

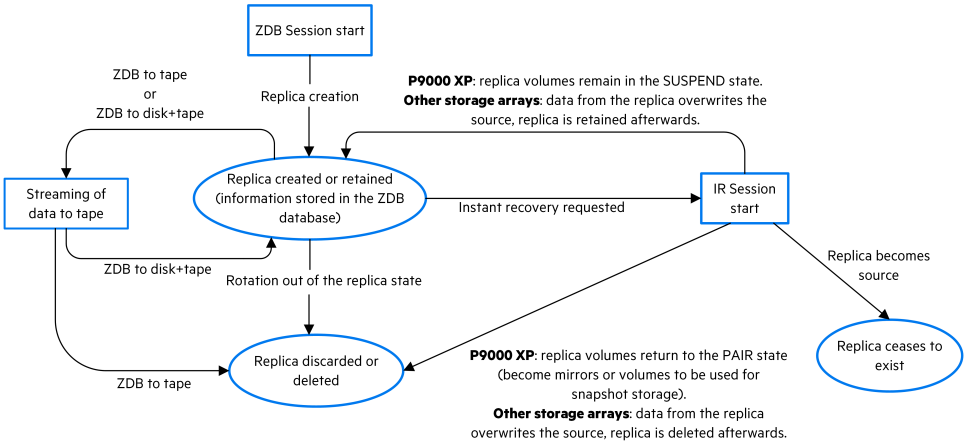
硬件提供程序会代替磁盘阵列代理的功能，并且它的行为从 Data Protector 的角度而言类似于磁盘阵列代理。

对在使用 Data Protector Microsoft 卷影复制服务集成的零宕机时间备份会话中已备份的数据执行即时恢复时，您可以选择使用 Microsoft 虚拟磁盘服务或磁盘阵列代理。该选择还取决于备份方式。

ZDB 复本生命周期

本节介绍复本的生命周期，如下图所示。

复本生命周期



复本生命周期取决于以下几点：

- 磁盘阵列模型
- 涉及 ZDB 和 IR 会话的 Data Protector 组件
- 针对零宕机时间备份会话选择的选项
- 从可用方法中选择的或由特定复本类型强制执行的即时恢复方法
- 针对即时恢复会话选择的其他选项

创建复本

使用分割镜像和快照复制技术时，基本原理是相同的，即：生成包含指定数据对象的存储卷（源卷）的副本或映像。在同一磁盘阵列上的其他存储卷（目标卷）中创建这些副本，稍后这些副本可驻留在主机系统中。

在任何情况下，只能复制磁盘阵列上的完整源卷。即使选定复制数据仅占源卷的一小部分，仍将复制完整的源卷。

创建复本的 ZDB 会话由“备份规范”定义，其中包含运行 ZDB 会话所需的全部信息:

- 要备份的应用程序或文件系统数据的类型
- 要备份的源数据
- 要创建的复本（或复本集，请参见复本集循环）
- 数据所驻留磁盘阵列的类型
- 要使用的应用程序和备份系统
- 复本管理和复本装载选项

对于不能与 Data Protector 完全集成的应用程序，也可以在复制之前设置选项以停止该应用程序，之后再重新启动它。

创建备份规范后，它将存储在 Cell Manager 上，可随时进行查看或更新。

操作员随后可使用 Data Protector 用户界面以交互的方式启动备份会话，或安排其在指定的时间自动启动。

> **注意**对于某些数据库应用程序，当联机备份会话正在运行时，还需要备份数据库当前所使用的日志文件。方法是将日志备份到文件，如果需要，之后可将该文件流式传送到磁带上。
>
> 通常*不*建议将日志文件包含在要复制的卷中。某些集成代理不允许这样做。而其他集成代理会减少或限制某些还原方案。

成功备份后，备份会话的详细信息会保存到 IDB 的 ZDB 部分中。

复本集

复本集是使用同一备份规范在不同时间创建的复本的集合。通常在创建以即时恢复为目的的复本时使用复本集。可为复本集定义的最大复本数量取决于以下一个或多个因素：复本类型、磁盘阵列型号、已安装的磁盘阵列固件版本、目标卷所用的快照类型（仅适用于快照复本）。

在 Data Protector 中，集合成员能以交互的方式或在调度程序指定的时间进行“复本集循环”。请注意，特定的磁盘阵列模型不支持复本集循环。

复本集循环

创建用于 ZDB 和即时恢复的备份规范时，需要指定复本集中的最大复本数量。每次运行备份时，均会创建新复本并添加到复本集中。当达到指定的复本集最大复本数时，新创建的复本将取代复本集中最早的复本。对于某些复本类型，将直接覆盖最早的复本；在其他情况下，则必须在创建新复本之前删除最早的复本。

计划复制

如果要自动运行复制会话，请在创建或修改备份规范时将所需次数的详细信息输入到 Data Protector“调度程序”中。既可以调度在特定时间运行的单个会话，也可以调度以一定的天数、周数或月数定期运行的定期会话。

使用复本

创建复本或复本集后，接下来要执行的操作取决于所使用的 ZDB 形式：

- ***ZDB 到磁带：***将复本中的数据流式传送到磁带上。然后，弃用该复本。
- ***ZDB 到磁盘：***将数据保留在磁盘阵列上以供即时恢复。
- ***ZDB 到磁盘 + 磁带：***将复本中的数据流式传送到磁带上，并将其保留在磁盘阵列上以供即时恢复。

在“ZDB 到磁盘”和“ZDB 到磁盘 + 磁带”会话之后，可在一个磁盘阵列上保留一个或多个复本。可以使用复本集循环来保留使用同一备份规范在不同时间创建的复本集，其中每个新复本会替换集合中最早的复本。每个副本将一直存在，直到从副本集循环出来为止，您可以使用 Data Protector CLI 将其删除，也可以使用特定的即时恢复方法在会话中“使用”它。

ZDB 到磁带

对于 ZDB 到磁带备份类型，复本通常只是暂时保留在磁盘阵列上。它实际上是一种分阶段备份到磁带的过程。

创建复本后，复本将装载到备份系统上，而在备份规范中指定的备份对象则会流式传送到磁带（或其他备份介质）上。

备份完成后，就不再需要备份复本，因此默认情况下会自动从磁盘阵列中将其删除。但是，您可以选择将该复本保留在磁盘阵列上，从而为使用同一备份规范的更多 ZDB 到磁带的会话预留磁盘阵列空间。这样，就保证了磁盘阵列上有足够的空间可用于备份。

> **重要说明**副本*不*可用于即时恢复。

优点	缺点
适合进行备份和灾难恢复。	对于灾难恢复，高可用性系统中大型数据库完整会话的还原需要花费很长的时间。
可从磁带备份还原单个数据对象。	
默认情况下，会从磁盘阵列中删除复本，以释放空间。	不能进行即时恢复。
支持扩展磁带库。	

ZDB 到磁盘

对于 ZDB 到磁盘备份类型，复本将保留在磁盘阵列上以作为备份映像用于即时恢复。

在磁盘阵列上可保留一个或多个复本。可以使用复本集循环来保留在不同时间创建的复本集，其中每个新复本会替换集合中最旧的复本。

优点	缺点
适合进行备份和即时恢复。	复本将永久占用磁盘空间。
	相比 ZDB 到磁带备份类型，提供有限的磁盘阵列支持。

ZDB 到磁盘 + 磁带

ZDB 到磁盘 + 磁带备份类型基本上是 ZDB 到磁盘和 ZDB 到磁带备份的组合。

与 ZDB 到磁盘备份类型相同，复本创建于磁盘上，随后会将复本流式传送到磁带或其他备份介质上。与 ZDB 到磁带备份不同，将保留磁盘副本

并*可*将其用于即时恢复。

复制方法/磁盘阵列支持与 ZDB 到磁盘备份相同。

可以使用同一备份规范如同 ZDB 到磁盘会话那样在同一调度中指定 ZDB 到磁盘 + 磁带会话。这意味着您可以设置更复杂的备份安排，如使用同一备份规范每周六天执行 ZDB 到磁盘备份，并且第七天执行 ZDB 到磁盘 + 磁带备份。这增强了还原的灵活性。请注意，对于上述两种会话类型将使用同一复本集。

优点	缺点
适合进行备份和即时恢复。	复本将永久占用磁盘空间。
可从磁带备份还原单个数据对象。	相比 ZDB 到磁带备份类型，提供有限的磁盘阵列支持。
可以使用 ZDB 到磁盘和 ZDB 到磁盘 + 磁带备份进行复杂的备份组合。	
甚至对于磁带，也支持复本集循环。	

即时恢复

您可以通过即时恢复，使用在 ZDB 到磁盘或 ZDB 到磁盘 + 磁带会话中创建的复本，将数据对象还原到特定时间点的状态。

在即时恢复会话之后对复本执行的操作取决于磁盘阵列模型、选择的可用即时恢复方法以及为即时恢复会话选择 (GUI) 或指定 (CLI) 的其他选项：

- 使用 P9000 XP 磁盘阵列系列时:
  - 通过切换磁盘（在分割镜像复本情况下），复本将不再作为复本存在。
  - 通过重新同步源卷（在分割镜像复本情况下）或将数据从复本还原至源卷（在快照复本情况下）：

    – 如果只使用 Data ProtectorP9000 XP 代理，则能否在磁盘阵列上保留复本取决于为即时恢复会话选定的 (GUI) 或指定的 (CLI) 选项。

    – 如果使用 Data Protector MS 卷影复制集成和 Data ProtectorP9000 XP 代理，则复本将保留在磁盘阵列上。
- 对于其他存储阵列，将复本数据复制回源卷，并在磁盘阵列上保留复本。

删除复本

可自动或手动删除复本：

- *自动：*
  - 当复本成为复本集中最旧的成员时，它将自动由集合中创建的新复本所覆盖（或删除）。

    但是，您可以排除复本的使用以保护复本。
  - 如果复本用于 ZDB 到磁带会话，则在会话后将自动删除复本，除非您明确指定保留复本。
  - 如果这样配置即时恢复选项，则将在即时恢复后删除复本。
  - 在使用特定即时恢复方法的会话后，复本不能再用作复本: 使用 P9000 XP 磁盘阵列系列时，以及使用切换磁盘的即时恢复方法时，复本在成为恢复的源之后不再作为复本存在。
- *手动：*

  当 Data Protector 不再需要使用复本时，您可以使用 Data Protector CLI 将复本从磁盘阵列中删除。

ZDB 会话过程

对于传统的 Data Protector备份，在将数据流式传送到备份介质这一过程完成之前的整个备份会话期间，应用程序操作都会受到影响。对于 Data Protector 零宕机时间备份，应用程序操作仅在创建复本时才受影响。

ZDB 过程的主要步骤如下：

1. 查找要备份的数据对象。请参见查找数据对象。
2. 冻结应用程序数据库的操作。请参见冻结应用程序或数据库的操作
3. 创建包含指定数据对象的复本。请参见创建复本。
4. 如果需要备份到磁带，请将复本流式传送到磁带。请参见将复本流式传送到磁带。
5. 如果需要执行即时恢复的功能，请记录有关会话的信息。请参见记录会话信息。

查找数据对象

可按如下所述查找并准备要备份的数据：

1. Data Protector 在应用程序和备份系统上启动相关进程。
2. 备份会话管理器会读取 ZDB 备份规范并将向应用程序系统上的 Application Integration Agent 和 Disk Array Agent 以及备份系统上的 Disk Array Agent 传递必要的指令。

   应用程序系统上的 ZDB 代理会将数据对象解析到文件系统（如果有）、卷组（如果有）以及基础存储卷。这些数据对象可能直接来自备份规范，也可能由某个受支持的应用程序集成提供。
3. 准备好应用程序系统，使数据保持一致的状态。对于联机备份，数据库处于静态状态。对于脱机备份，数据库处于脱机状态。如果选择 ZDB 选项“在复本生成之前卸除应用程序系统上的文件系统”(3PAR StoreServ Storage、NetApp Storage) 或“卸除应用程序系统上的文件系统”(P9000 XP 磁盘阵列系列)，则将卸除所涉及的文件系统。

冻结应用程序或数据库的操作

在创建复本时，必须冻结所涉及的应用程序操作或数据库分区。

Application Integration Agent 将使应用程序数据库或文件系统处于所需状态。对于脱机复制，这可能会使所有数据库更新都停止，而对于联机复制，则可能使所有数据库更新重新路由至日志文件：

- “脱机”替换中，数据库处于脱机状态，因此在创建复本期间，所有文件 I/O 均已停止。数据库通常处于一致的状态，例如通过应用任何之前未应用的重做日志。

  尽管创建复本的速度非常快，但是应用程序也将短暂地处于脱机状态，因此该方法对于高可用性应用程序而言仍有待完善。
- 在“联机”替换中，创建复本时，数据库处于于“热备份模式”。在此模式下，数据库将保持联机状态，但是所有数据库 I/O 将转移到事务日志文件而不更新数据库。复本制作完成后，会将事务日志文件应用到数据库以进行更新。

  此复制方法可最大限度地减小对应用程序的影响，因而更适用于不间断操作。

当备份 Data Protector 支持的数据库应用程序时，上述操作中的步骤可实现自动控制。但是，也可以在备份其他应用程序或文件系统时设置类似行为；可以通过先执行和后执行选项指定在复制前和复制后要运行的脚本。

在这两种情况下，备份过程都仅在创建复本时才会对应用程序造成影响。在“联机”情况下，数据库操作不会停止（零宕机时间）且对性能的影响最小，最主要的影响是在此期间需要将增加的信息写入事务日志中。

无需使用 ZDB 复制技术，也可在 Data Protector 中使用联机和脱机备份。但是，会对应用程序/数据库操作造成更大影响，因为对于传统的备份到磁带的方法，数据库在整个备份会话期间都必须处于热备份模式或脱机状态。

创建复本

1. 复本已创建。
2. 应用程序系统恢复正常。将重新装载任何已卸除的文件系统。

   对于脱机备份，此时可使数据库恢复联机状态并再次启动正常操作。

   对于联机备份，此时会将事务日志文件以及在复本创建期间缓存的信息应用到数据库。
3. 为复本磁盘和数据准备好备份系统环境。通过扫描发现新设备。将导入并激活任何卷组。将装载文件系统。

复制数据对象

在数据库/文件系统处于所需状态的情况下，将触发应用程序系统和备份系统上的磁盘阵列代理以执行复制。

两个磁盘阵列代理将成对运行：

- 在应用程序系统上，代理会将指定数据解析到包含此数据的卷。

- 在备份系统上，代理会分配复本所需的卷。

然后，磁盘阵列会在其磁盘上创建复本。

复制方法取决于所使用的磁盘阵列的类型、该磁盘阵列配置用于本地还是远程复制、是否需要 LVM 镜像等。有关如何执行分割镜像和快照复制的信息，请参见复制技术。

将复本流式传送到磁带

1. 在 ZDB 到磁带和 ZDB 到磁盘 + 磁带的备份中，复本将流式传送到磁带。
2. 清理备份系统。卸除文件系统。停用并移除新的卷管理系统。

将复本备份到磁带

创建装载点

在可将数据从复本移动到磁带或其他备份介质之前，必须先将复本装载到备份系统上。

Data Protector 将在备份系统上创建装载点并将复本中的文件系统装载到其中。此过程取决于是否正在执行应用程序、磁盘映像或文件系统备份。

到磁带的标准数据移动

根据备份规范中的规定，使用 Data Protector 介质代理将数据对象流式传送到磁带。

Data Protector 会认为数据对象来自其原始位置而非来自复本，并基于这种认知将信息写入磁带，因此磁带上和 IDB 中的会话信息与执行到磁带的传统备份的会话信息是相同的。这意味着可使用标准恢复过程将 ZDB 到磁带和 ZDB 到磁盘 + 磁带会话中的数据对象直接还原到应用程序系统。

增量 ZDB

增量 ZDB 是“文件系统”ZDB 到磁带或 ZDB 到磁盘 + 磁带会话，其中 Data Protector 仅将符合增量备份标准 (即用于增量非 ZDB 会话的标准) 的文件流式传送到磁带上。请注意，完整和增量 ZDB 会话的复本创建方式是相同的。

在 Windows 系统上，**不使用归档属性**文件系统选项将影响增量 ZDB 行为。如果不选择此选项，则尽管已经指定增量备份类型，也可能最终执行完整备份。因此，要避免备份可能没有更改的文件，请在创建 ZDB 备份规范时选择此选项。

创建后的复本

创建复本后：

- 对于 *ZDB 到磁盘*和 *ZDB 到磁盘 + 磁带*，复本保留在磁盘阵列上以用于即时恢复。如果它是复本集的一部分，则在其成为集合中最旧的复本之前将一直会保留在磁盘阵列中。随后，它将替换为使用同一备份规范（除非从使用中将其排除）执行的下一 ZDB 到磁盘或 ZDB 到磁盘 + 磁带会话中创建的复本。
- 执行完 *ZDB 到磁带* 会话后，如果将数据备份到磁带，默认情况下会自动删除该复本。可以选择将此复本保留在磁盘阵列上，但是无法将其用于即时恢复。

在备份系统上装载复本

Data Protector 将在备份系统上创建装载点并将复本的文件系统装载其中。装载点路径取决于要执行的是应用程序备份还是文件系统备份以及您在 GUI 中所选的备份规范选项。还可以选择在 ZDB 会话完成之后，仍将文件系统保留装载于装载点路径上。

使用 VSS 集成时，在 GUI 中选择的备份规范选项将决定是否在备份系统中创建装载点，以及复本文件系统是以读写模式还是只读模式装载到装载点。

记录会话信息

在此阶段，可以回收创建的复本以用于下一会话。如果已启用即时恢复，则其他 IR 会话信息将存储在 IDB 中，并且将保留复本以备 IR 之需。

将会话信息写入 IDB

与传统的 Data Protector 备份一样，整个会话期间的 ZDB 会话信息都将写入 IDB，包括有关备份介质和可还原的数据对象的信息。

- 对于 *ZDB 到磁盘*和 *ZDB 到磁盘 + 磁带*的备份，特定于磁盘阵列的有关复本的信息也将写入 ZDB 数据库，以用于即时恢复。
- 对于 *ZDB 到磁带* 的备份，即使在备份后将复本保留在磁盘阵列上，也不会将任何即时恢复信息记录到 ZDB 数据库中。

“ZDB 数据库”是在 Cell Manager 上对 IDB 的扩展。对于在 Data Protector 内本地支持 ZDB 和 IR 的每个磁盘阵列，它都有一个独立分区：

- 适用于 3PAR StoreServ Storage 系列和 NetApp Storage 的磁盘阵列的 SMISDB。
- 用于P9000 XP 磁盘阵列系列的磁盘阵列的 XPDB

创建复本时，就会将信息写入 ZDB 数据库；删除复本时，就会删除信息。

从 ZDB 进行即时恢复和应用其他还原的技术

通过即时恢复，可以高速还原完整复本，且基本不影响应用程序系统。包含备份规范中指定数据对象的所有卷都将还原为其特定时间点的状态。

执行完 ZDB 会话后，您可以在以下 GUI 上下文中查看相关联的还原对象和还原会话：

- 在完成“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”的备份后，在**还原**上下文中，启用从磁带还原数据对象。
- 在完成“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”的备份后，在**即时恢复**上下文中，启用从复本还原。

或者，您可以使用 Data Protector CLI。

还原方法取决于所执行的 ZDB 会话的类型以及所使用的磁盘阵列的类型。以下章节将详细介绍可用的方法。

即时恢复

可用性

在本地复制中：

- 从 ZDB 到磁盘
- 从 ZDB 到磁盘 + 磁带

> **注意**EMC 阵列不支持即时恢复；仅支持 ZDB 到磁带的备份。

功能

可以高速还原完整复本，且基本不影响应用程序系统。包含备份规范中指定数据对象的所有卷都将还原为其特定时间点的状态。

详细信息

请参见“即时恢复”。

由于涉及不同类型的复本以及各种磁盘阵列限制，每种磁盘阵列类型的具体还原过程各不相同。

标准 Data Protector 还原

可用性

在本地和远程复制中：

- 从 ZDB 到磁带
- 从 ZDB 到磁盘 + 磁带

功能

可以将单个备份对象从磁带直接还原到应用程序系统。

标准还原的可用性取决于实际流式传送到磁带的数据。这反过来取决于 ZDB 到磁带或 ZDB 到磁盘 + 磁带备份规范的创建方式。如果在备份规范中选择了源卷的完整内容，则所有对象均将流式传送到磁带。否则，即使复制了整个源卷，也只会将所选备份对象流式传送到磁带。

分割镜像还原

可用性

具体磁盘阵列模型上的本地复制中：

- 从 ZDB 到磁带
- 从 ZDB 到磁盘 + 磁带

可用于磁盘映像、文件系统和基于文件系统的应用程序备份。

> 注意: 由于当今 SAN 附接的磁带驱动器速度很快，直接恢复到应用程序系统通常比使用分割镜像还原更快。

功能

可以将单个备份对象的任何内容还原为复本的完整内容，且基本不影响应用程序系统。分割镜像还原可用于执行对部分损坏但仍能运转的系统的低影响恢复。

与上述标准还原一样，分割镜像还原的可用性取决于实际流式传送到磁带的数据。

详细信息

请参见分割镜像还原。

即时恢复

通过即时恢复，可以用已知的完好数据替换丢失或损坏的数据，这些完好数据之前已复制到磁盘阵列上的其他卷。将在完整的存储卷级别对这些之前已复制的数据进行处理。此过程的其他步骤取决于所涉及的应用程序：

- 如果已复制*文件系统*，则此步骤只需将数据恢复到其在创建复本时的状态。
- 对于*数据库应用程序*，可能需要执行其他操作（如还原和应用事务日志文件），以在执行即时恢复后完全恢复数据库。这样，如果存在复本创建后某个稍晚时间点的日志文件，您就能够将数据库恢复到此时间点 (通常称为“前滚”)。这通常涉及另一个备份介质或设备的使用。

即时恢复期间，或是目标卷代替源卷驻留在系统中（此即时恢复方法只适用于快照式克隆），亦或是在目标卷上的数据替换源卷上的数据时执行数据复制操作。这些操作在磁盘阵列内部执行，不涉及其他备份介质或设备。因此会使即时恢复非常迅速。

在仅使用 Data Protector 磁盘阵列代理的即时恢复会话中，无法定义应该还原备份规范中指定的哪些备份对象；只能为即时恢复选择完整的备份对象集，因此，只能还原完整复本。此外，在配置了 LVM 的 UNIX 系统上，不仅会恢复构成复本的卷，而且会将这些卷所在的整个卷组还原到复本创建时的状态。

在使用 Data Protector Microsoft 卷影复制服务集成的即时恢复会话中，可以分别选择在即时恢复的备份规范中指定的备份对象，只要选择要在即时恢复会话中涉及的每个单个卷上存储的所有备份对象即可。仅还原为即时恢复选择的对象所在的卷，同一卷组的其他卷将保持不变。

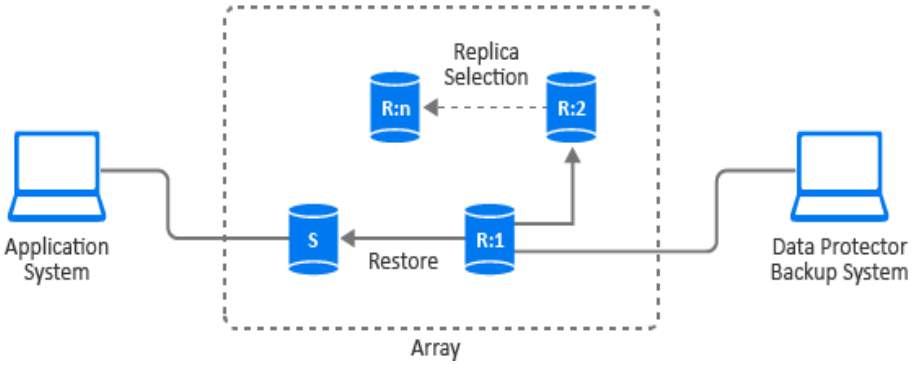
在 Data Protector GUI 中无法直接显示或选择复本，但是可以显示或选择用于创建可供即时恢复的复本的会话。

由于涉及不同类型的复本以及各种磁盘阵列限制，每种磁盘阵列类型的具体还原过程各不相同，同时还取决于是否涉及 Data Protector Microsoft 卷影复制服务集成。

即时恢复过程

以下是即时恢复的示例：

即时恢复的示例



1. 确定要还原的复本并选择创建此复本的 ZDB 会话。
2. 选择即时恢复选项，主要用于选择即时恢复方法和数据安全等级。

   根据操作系统、选择的即时恢复方法和磁盘阵列模型，可借助这些选项执行以下操作：

   - ***已配置 LVM 的 UNIX 系统：***检查即时恢复中所涉及卷组的配置在要还原的复本创建后是否发生过更改。

此检查还将验证对要还原复本中的数据执行的 CRC 是否与创建复本时所生成的 CRC 相匹配。

- 使用特定的即时恢复方法，在即时恢复会话后将复本保留在磁盘阵列上，以应对数据还原后任何步骤的潜在问题。

3. （可选）执行即时恢复会话的预览，以提供其他级别的安全性。

> **注意**即时恢复预览在使用 Data Protector Microsoft 卷影复制服务集成的即时恢复会话中不可用。

4. 启动即时恢复。

Data Protector 随后将：

1. 启动应用程序和备份系统上的过程。
2. 从 IDB 提取会话信息，并从 ZDB 数据库提取与会话相关联的特定于阵列的信息。
3. 执行必要的检查以验证是否满足成功恢复的所有必需条件（包括指定的任何即时恢复选项）。
4. 通过停用任何卷组（在已配置 LVM 的 UNIX 系统上）并卸除与复本相关联的任何文件系统，准备好应用程序系统。
5. 还原原始数据。

   根据磁盘阵列模型、即时恢复方法，可以是从可用方法中选择的或是由特定复本类型强制执行的方法，以及为即时恢复会话选择的其他选项，以下即时恢复方法可用：

   - 使用 P4000 SAN 解决方案时，只有一种即时恢复方法可用:
     - 将复本数据复制回源卷

       复本上的数据被复制回原始存储，并且未保留源卷。已保留复本，但是复本集中若存在比选定的即时恢复复本更新的复本，则将从磁盘陈列上移除较新的复本。

       对于此方法，将同时使用 Data Protector Microsoft 卷影复制服务集成和 Data Protector P4000 代理。
   - 使用 P9000 XP 磁盘阵列系列时，可以使用两种即时恢复方法:
     - 切换磁盘：

       将用原始源卷代替选定的分隔镜像复本。然后，将根据之前为原始源卷创建的任何主机演示，为还原的复本卷创建主机演示，实际上，恢复的复本卷将成为新的源卷。对于 Data Protector 而言，复本将从相关联的复本集中删除。无法再次进行即时恢复。可以选择保留或删除旧的源卷。

       对于此方法，将同时使用 Data Protector Microsoft 卷影复制服务集成和 Microsoft 虚拟磁盘服务。
     - 重新同步源卷（使用分割镜像复本）或把数据从快照还原至源卷（使用快照复本）：

       如果使用分割镜像复本，源卷将和已选择的复本的源卷重新同步。如果使用快照复本，已选复本上的数据将会复制到源卷。

       对于这种方法，根据零宕机时间备份会话涉及的 Data Protector 组件，只可使用 Data ProtectorP9000 XP 代理，或使用 Data Protector Microsoft 卷影复制服务集成与 P9000 XP 代理。
   - 使用 3PAR StoreServ Storage 时，只有一种即时恢复方法可用:
     - 将复本数据复制回源卷

       复本上的数据被复制回原始存储，并且未保留源卷。复本被保留在与其相关联的复本集中。

       对于此方法，可以使用 6000/3PAR SMI-S 代理，也可以同时使用 Data Protector Microsoft 卷影复制服务集成和 Data Protector 3PAR VSS 代理。

6. 重新启用已禁用的任何卷组，并重新装载已卸除的任何文件系统。

在即时恢复后，源卷的内容将恢复到其在创建复本时的状态。

即时恢复和 LVM 镜像

在 HP-UX 系统 (带 LVM 镜像和 BC 或 BC P9000 XP 配置) 上生成的 ZDB 会话支持即时恢复。但是，还需要执行其他手动步骤。

群集中的即时恢复

在应用程序系统上的群集环境中运行的应用程序和文件系统支持即时恢复。但是，还需要执行其他步骤。

分割镜像还原

> **注意**由于当今 SAN 附接的磁带驱动器速度很快，直接恢复到应用程序系统通常比使用分割镜像还原更快。

在分割镜像还原中，备份对象将首先从磁带移动到备份系统上的复本（已存在或新创建）中。然后，复本上的数据将会还原至应用程序系统可用的源卷中，并有效替换源卷的现有内容。它可用于还原完整会话或单个备份对象。

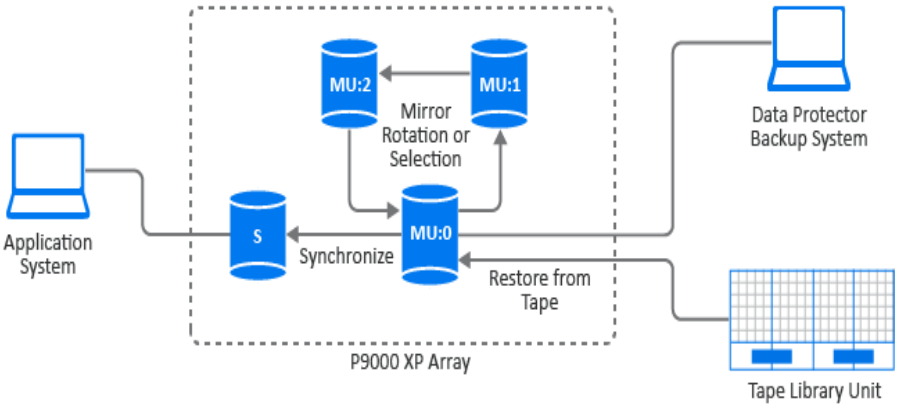
此方法可用于从文件系统中还原数据，或者从在以下条件下生成的 ZDB 到磁带或 ZDB 到磁盘 + 磁带的会话中还原磁盘映像：

- 在 P9000 XP 阵列上，使用 Business Copy (BC) P9000 XP 配置。
- 在 EMC 上，使用 SRDF 配置。

分割镜像还原过程

以下是在 P9000 XP 阵列上拆分镜像还原过程的示例:

分割镜像还原的示例



1. 选择用于还原的复本或创建新复本以生成最新的源卷复制。
2. 通过备份系统将所需对象从磁带还原到复本。
3. 从复本上还原数据，并使用存储在复本上的数据有效替换位于源卷上的数据。

过程完成后，所选复本的内容将替换源卷内容：

- 从磁带还原到复本中的备份对象将还原到其在执行 ZDB 会话时的状态。
- 其他内容将恢复到在创建其复本时的状态。

ZDB 计划

要规划 ZDB 策略，需要考虑以下步骤：

1. 定义备份需求和限制，如：
   - 您的数据需要多久备份一次？
   - 是否需要在其他介质集上存储已备份数据的更多副本？
2. 了解影响磁盘阵列性能的因素。
3. 制定支持您的备份概念的备份策略及其实现方式。

本节提供一些重要信息和注意事项，可帮助您规划备份解决方案和改善 ZDB 性能。

恢复的灵活性

为了在恢复到某个时间点时实现最大的灵活性，可以：

- 定期创建复本并将其保留在磁盘阵列上。
- 定期备份日志文件。

要通过定义基于计划的 ZDB 备份会话的备份策略来控制磁盘阵列空间使用量，需要设置一系列基于时间的复本，每一个复本对应一个特定的时间点。此复本集中的复本数取决于可用磁盘阵列空间以及所要的时间范围。

请注意，由于快照复本的特定类型，集合中的复本数量上限可能受限于磁盘阵列模型和/或者已安装的磁盘阵列固件版本。

分割镜像磁盘阵列

P9000 XP 磁盘阵列系列集成可提供使您能够定义备份策略的选项，如:

- 将原始数据的镜像副本移动到磁带中。
- 保留镜像分割或对其进行重新同步。
- 准备用于备份的下一磁盘。

您能够在本节中找到有关拆分镜像磁盘阵列性能的一般建议和限制。

ZDB 计划

如果使用 Data ProtectorP4000 SAN 解决方案集成，请在计划备份策略时考虑以下事项:

- 即时恢复 – 请参见特定于磁盘阵列的注意事项。

如果使用 Data ProtectorP9000 XP 磁盘阵列系列集成，请在计划备份策略时考虑以下事项:

- 复本类型（分割镜像或快照）– 请参见特定于磁盘阵列的注意事项
- 即时恢复 - 请参阅特定于磁盘阵列的注意事项和《Data Protector 零宕机时间备份管理员部分》

如果使用 Data Protector 3PAR StoreServ Storage 集成，请在规划备份策略时考虑以下事项:

- 复本创建 – 请参见特定于磁盘阵列的注意事项。

如果使用 Data Protector NetApp Storage 集成，请在计划备份策略时考虑以下事项：

- 复本创建 – 请参见特定于磁盘阵列的注意事项。
- 快照类型（精简配置或完全分配）
- 传输模式（对于适用于 VMware 的虚拟 ZDB 集成）

特定于磁盘阵列的注意事项

P4000 SAN 解决方案上的复本集

虽然您能够创建复本集，但是此磁盘阵列系列不支持复本集循环。

P4000 SAN 解决方案上的即时恢复

在选择了用于即时恢复的目标卷后，如果对于同一源卷存在版本比选定的现有目标卷高的目标卷，则会自动将高版本的目标卷从磁盘阵列中删除，而不考虑高版本的目标卷所属的复本集。如果无法移除某个特定的较新目标卷，例如，由于磁盘阵列上存在其智能克隆，则即时恢复会话会失败。如果存在针对即时恢复而选择的源卷的较新快照，但是该快照并非是由 Data Protector 所创建，则即时恢复会话同样会失败。

当多个 ZDB 备份规范中包含同一源卷时，运行基于某一特定 ZDB 备份规范的即时恢复会话可能会导致无法执行基于其他 ZDB 备份规范的即时恢复会话。如果按照下列顺序进行操作，将发生问题：

1. 运行基于某一特定 ZDB 备份规范（规范 A）的即时恢复会话时，将会从磁盘阵列中移除选定的用于即时恢复的较新目标卷。基于另一个

ZDB 备份规范（规范 B），在 ZDB 会话（会话B）中创建已移除的目标卷。
2. 与该 ZDB 会话（会话 B）对应的即时恢复会话随即启动。

P9000 XP 阵列上的复本类型选择

当创建 ZDB 备份规范时，您无法在 Data Protector GUI 中直接选择所需副本类型。通过指定相应的镜像单元 (MU) 数量或数量范围，您可以确保 Data Protector 使用特定副本类型。当在零宕机时间备份会话中使用属于某一特定 MU 数量的源卷时，Data ProtectorP9000 XP 代理会根据配对的虚拟磁盘类型选择复本类型，并且必须使用 P9000 XP Remote Web Console 对该虚拟磁盘进行预先配置。

P9000 XP 阵列上的即时恢复

选择即时恢复的副本时，如果副本集中存在比已选副本更新的副本，则将在会话后保留这些较新的副本，不论其类型为何：分割镜像或快照。

选择在备份策略的范围内运行的 ZDB 会话中要使用的复本类型之前，请考虑以下事项: 选择拆分镜像复本以用于即时恢复时，此即时恢复过程运行速度最快，且会在预先配置磁盘阵列上的复本卷期间启用 P9000 XP 阵列功能快速还原模式。

3PAR StoreServ 系统上的复本创建

每次在 3PAR StoreServ 系统上调用副本创建时，实际上会为每个源卷创建两个快照：一个只读快照和一个读写快照。读写快照仅供给外部应用程序使用，而只读快照仅供存储系统内部使用。有关存储空间消耗的更多信息，请参阅 3PAR StoreServ Storage 文档。

NetApp 存储系统上的副本创建

每次在 NetApp 存储系统上调用副本创建时，实际上会为每个源卷创建两个快照：一个只读快照和一个读写快照（LUN 克隆）。读写快照仅供给外部应用程序使用，而只读快照仅供存储系统内部使用。有关存储空间消耗的详细信息，请参见 NetApp 文档。

并发处理

锁定

备份设备锁定

常规（非 ZDB）Data Protector 备份和恢复会话在备份或恢复会话开始时会锁定会话中使用的磁带设备，并在会话结束时解除该设备的锁定。对于 ZDB 集成，磁带设备锁定有所不同，以便设备仅在需要与磁带设备相互传送数据时才会锁定：

- 在 ZDB 到磁带的会话或 ZDB 到磁盘 + 磁带的会话期间，锁定发生在复本创建之后，但在将已复制数据流式传送到磁带之前。
- 在分割镜像还原会话（在特定磁盘阵列系列上受支持）期间，锁定发生在复本创建之后，但却在备份数据从磁带设备移动到复本之前。

当与磁带设备之间的数据流式传送完成时，即会释放设备。

在 ZDB 到磁盘或即时恢复会话期间，不会使用磁带设备，因此对于这两种操作，不锁定任何磁带设备。

磁盘锁定

为防止 ZDB 或即时恢复会话访问其他会话仍在使用的存储卷，Data Protector 引入了内部磁盘锁定机制。通过此机制，在其他操作正在使用存储卷期间，将锁定存储卷。

如果 Data Protector 无法锁定所需操作要使用的存储卷（因为它们已由另一进程锁定），则会发出警告并中止会话。

备份方案

备份策略可由完整备份和增量备份构成。这些会话并不一定都是 ZDB 或都是非 ZDB。您可以通过各种方式将它们组合起来。支持的组合如下：

备份方案

完整备份	增量备份
ZDB	ZDB
ZDB	非 ZDB
ZDB	非 ZDB 和 ZDB
非 ZDB	ZDB
非 ZDB	ZDB 和非 ZDB

> **注意**如果要在 ZDB 和非 ZDB 会话中备份相同的对象，则为每个备份类型创建单独的备份规范。例如，为“ZDB 到磁盘 + 磁带”备份类型、“ZDB 到磁带”备份类型和非 ZDB 会话分别创建一个备份规范。
>
> 确保备份规范中的所选备份对象相互匹配（相同的客户端、装载点和描述）。否则，在恢复期间，从磁带进行的增量备份和完整备份将无法包含在同一恢复链中，因为 Data Protector 会将这些备份视为独立对象。

以下是增量 ZDB 会话的一些优点：

- 良好的即时恢复粒度 (前提是在备份规范中选中“跟踪复本以用于即时恢复”选项)
- 在备份期间，对应用程序系统性能的影响较小
- 流式传送到磁带的数据量较少

示例

为提供良好的即时恢复粒度，可通过每 2 或 3 天创建复本并将其保留用作即时恢复来实现；为减少流式传送到磁带的数据量，可考虑以下备份策略：

- 在星期日执行 ZDB 到磁盘 + 磁带会话的完整备份
- 在星期二和星期四执行 ZDB 到磁盘 + 磁带会话的增量备份
- 在其他日期执行 ZDB 到磁带会话的增量备份

在这种情况下，按如下方式配置备份：

- 创建 ZDB 到磁盘 + 磁带的备份规范，并在星期日调度执行完整备份，在星期二和星期四执行增量备份。
- 创建 ZDB 到磁带的备份规范，并安排在星期一、星期三、星期五和星期六执行增量备份。

要恢复数据，可以随后使用复本（快速还原）或来自磁带的备份。也可以通过先还原复本，然后再从磁带中的特定备份映像恢复单独文件，将上述两种还原类型组合使用。

支持的配置

本主题提供有关不同磁盘阵列所支持的配置的信息。有关受支持配置的最新列表，请参阅最新支持矩阵。如果要在未列出的配置中备份数据，这并不意味着该配置不受支持。请联系当地代表或顾问以了解是否支持其他配置。

由于性能问题，不推荐单主机 (BC1) 配置；在单主机配置中，单个系统充当应用程序系统和备份系统。只有文件系统和磁盘映像备份才有可能采用 BC1 配置。

不支持基于 Linux 平台的 3PAR StoreServ Storage 单主机 (BC1) 配置。在此类配置中，单个 Linux 系统充当应用程序系统和备份系统。

下表列出了受 Data Protector 支持并且能够创建副本（且在大多数情况下，能够创建副本集）的磁盘阵列。

与 Data Protector 集成的磁盘阵列

磁盘阵列系列	缩写	支持的复制技术可用
P4000 SAN 解决方案	P4000 SAN 解决方案	快照
P9000 XP 磁盘阵列系列	P9000 XP 阵列	分割镜像，快照
3PAR StoreServ Storage	3PAR StoreServ	快照
NetApp Storage	NetApp	快照

对于所有受支持的配置，ZDB 备份规范只能包括一个应用程序系统和一个备份系统。但是，每个应用程序系统可具有多个 ZDB 备份规范，您可以使用这些规范将同一应用程序系统同时备份到不同的文件系统。对于所有配置，原始数据和备份数据可分布于同一类型的多个磁盘阵列。

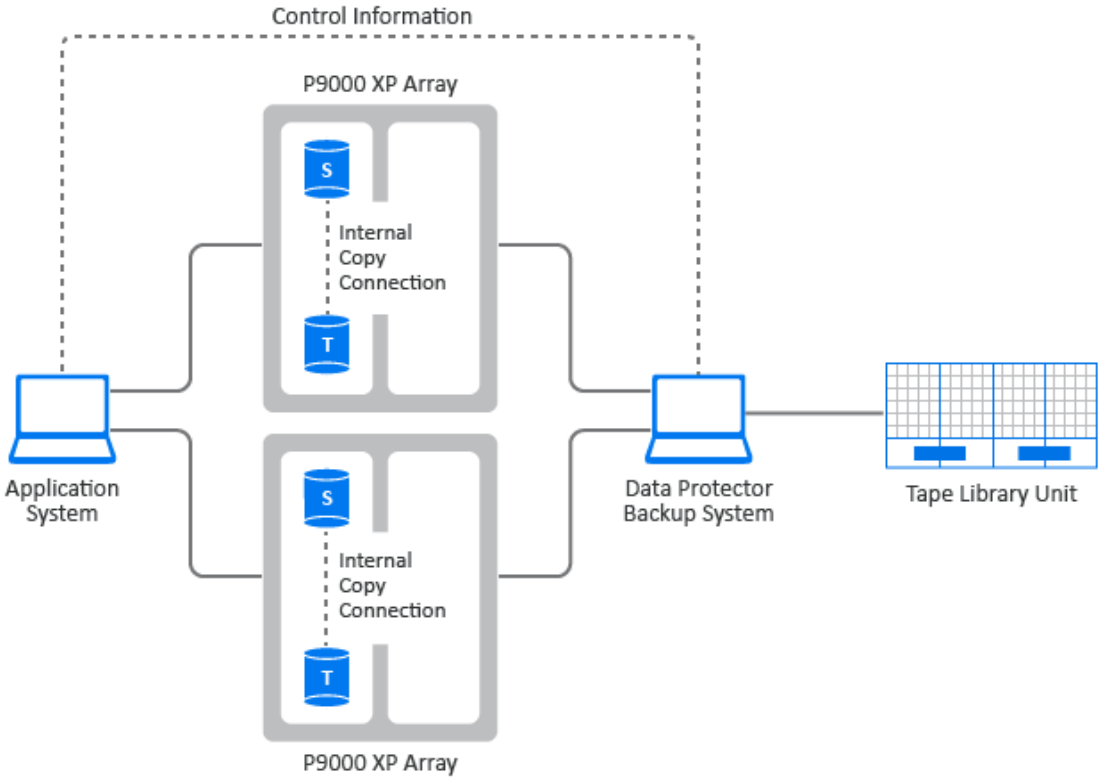
请注意，每个配置都具有特定的行为模式，对控制功能有特定要求，以保证备份和恢复功能。

支持的 P9000 XP 磁盘阵列系列配置

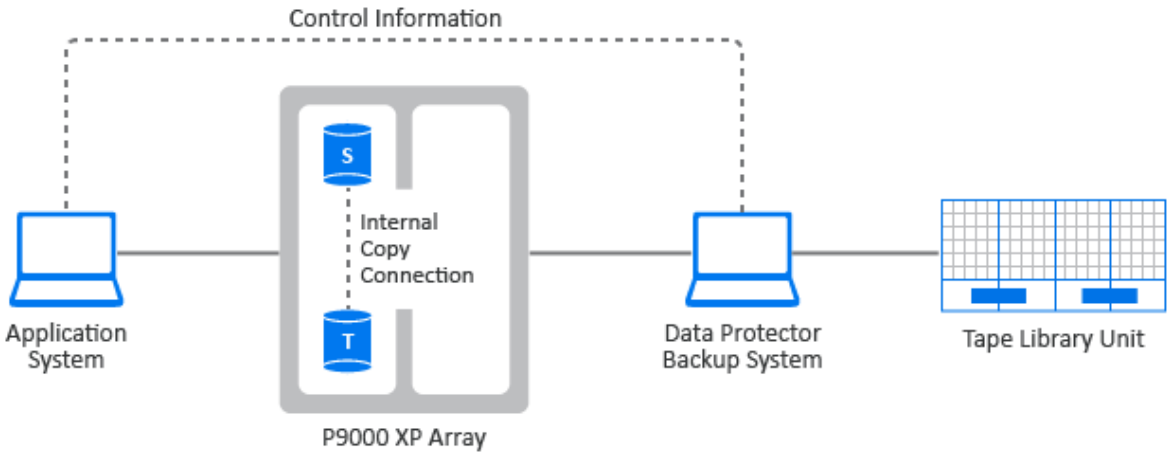
本地复制配置

BC P9000 XP 配置 1 至 BC P9000 XP 配置 3 是 P9000 XP 阵列上受支持的本地复制配置的示例。

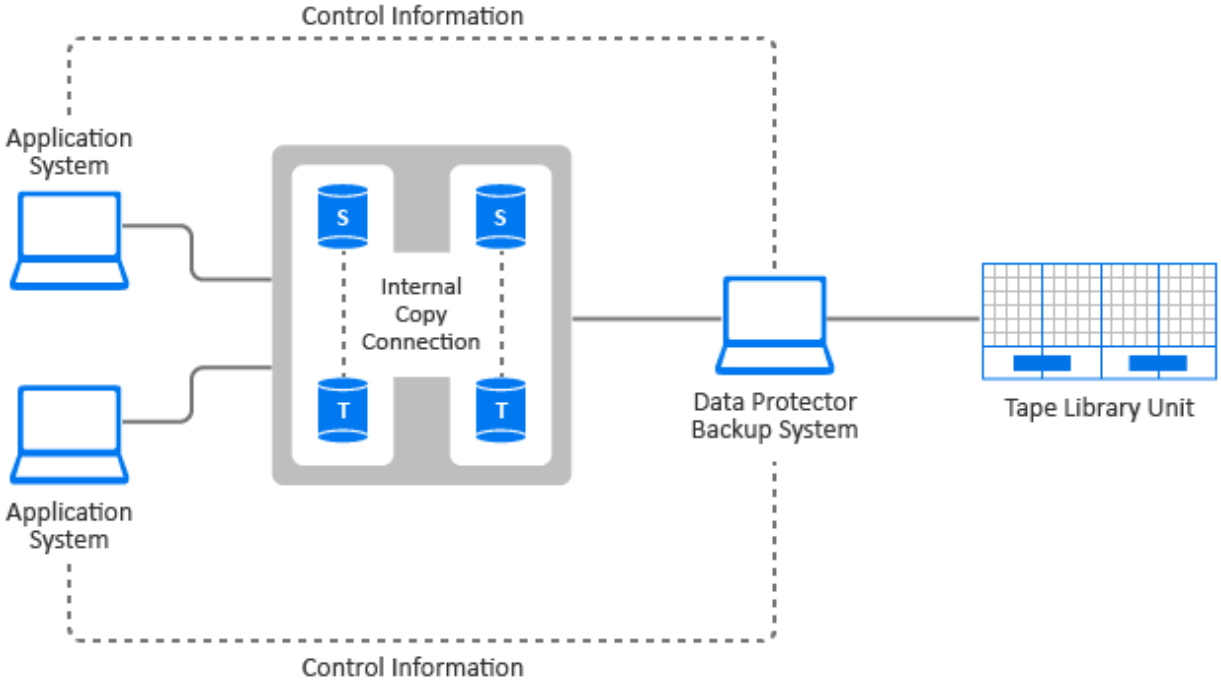
BC P9000 XP 配置 1



BC P9000 XP 配置 2



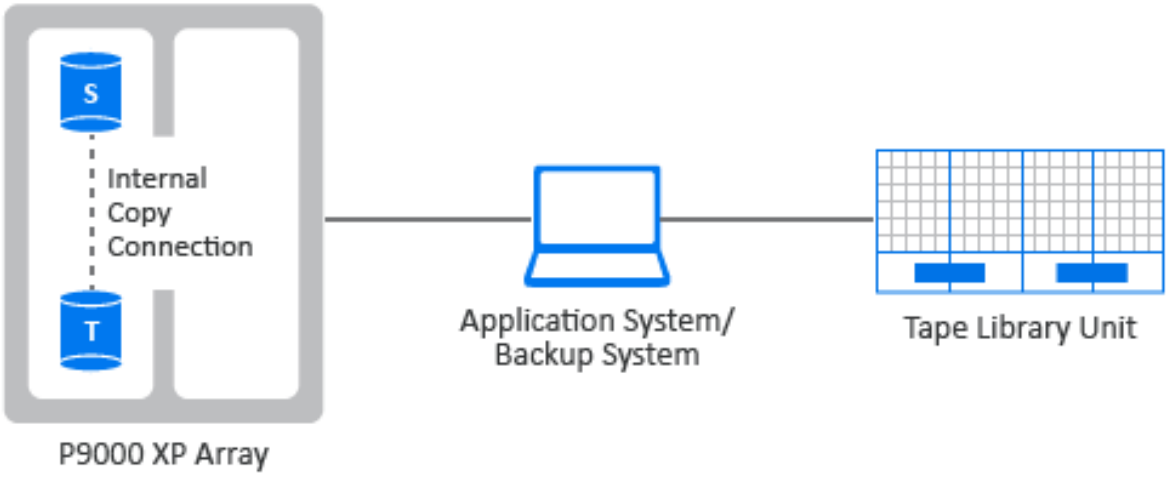
BC P9000 XP 配置 3



单主机 (BC1) 配置

下图是单主机配置，也称为 **BC1** 配置。

BC1 P9000 XP 配置

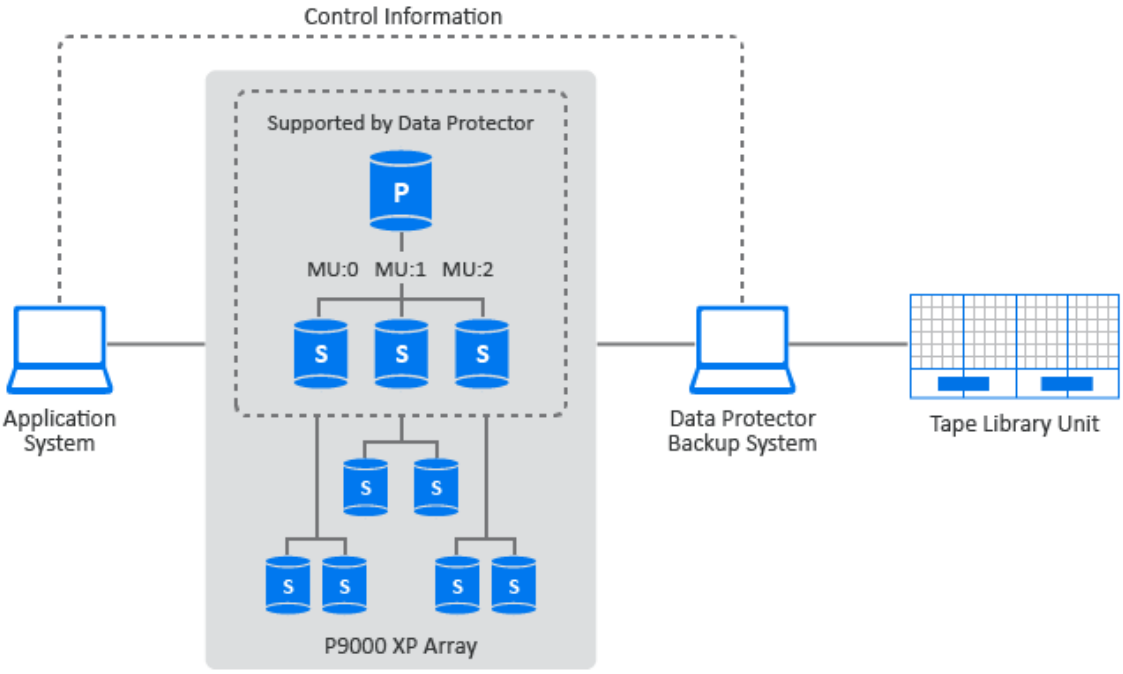


级联配置

通过 P9000 XP 磁盘阵列系列可为每个一级镜像或快照卷配置其他二级镜像或快照卷。这称为**级联配置**。但是，Data Protector 只能在零宕机时间备份、即时恢复和分割镜像还原会话中使用一级镜像或快照卷。

下图是级联配置的示例，其中 MU:0、MU:1 和 MU:2 是 Data Protector 支持的一级镜像，下方的六个镜像是二级镜像。

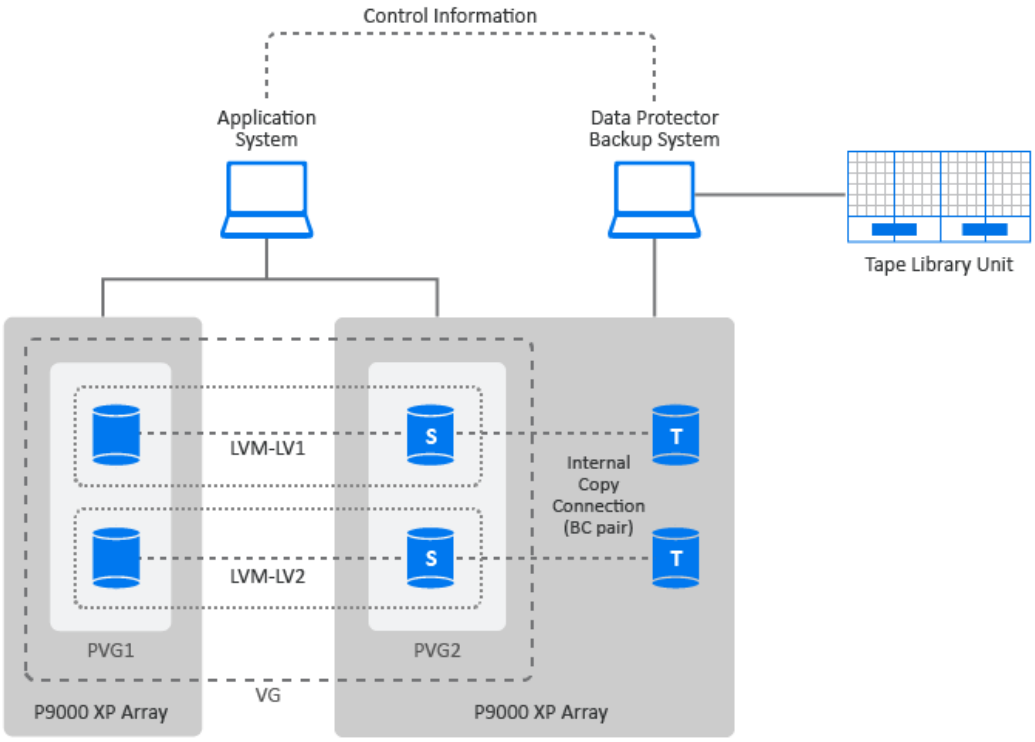
级联配置



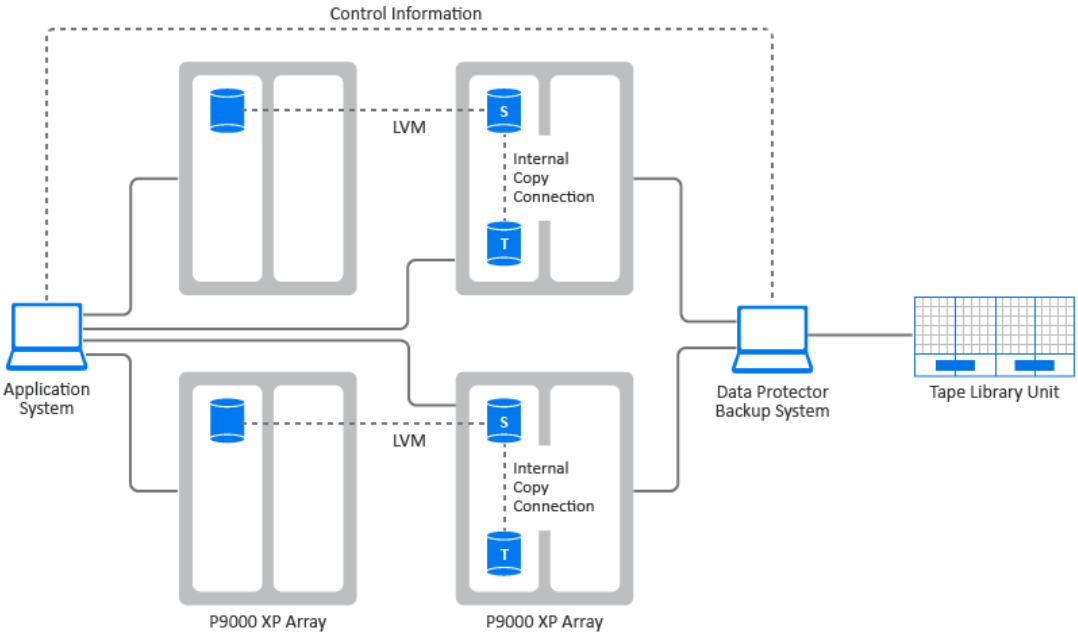
使用 HP-UX LVM 镜像的本地复制配置

LVM 镜像配置 1 至群集中的 LVM 镜像配置是 P9000 XP 阵列上受支持的 LVM 镜像配置的示例。

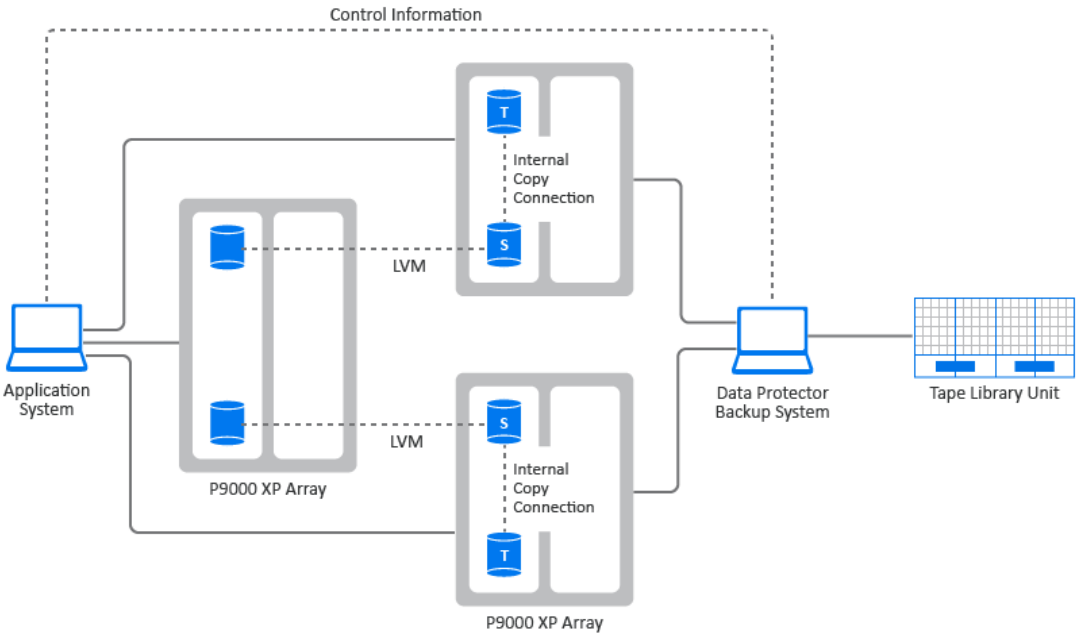
LVM 镜像配置 1



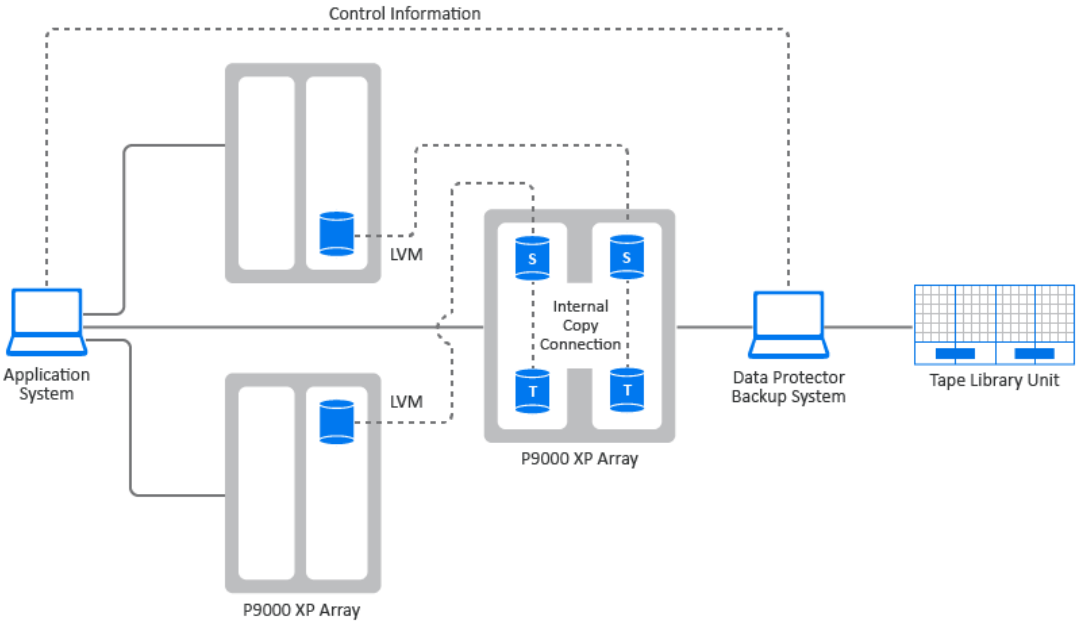
LVM 镜像配置 2



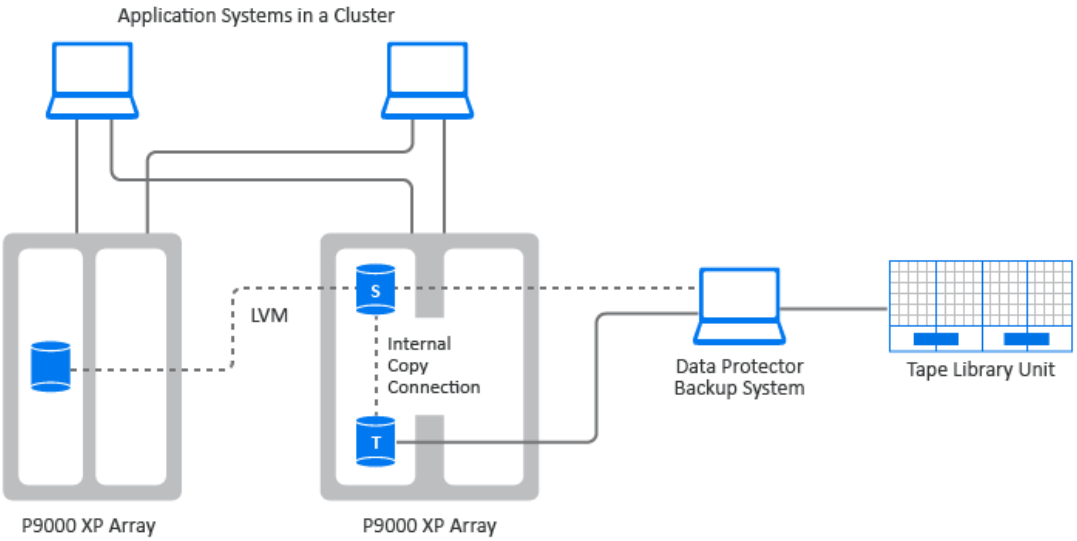
LVM 镜像配置 3



LVM 镜像配置 4



群集中的 LVM 镜像配置



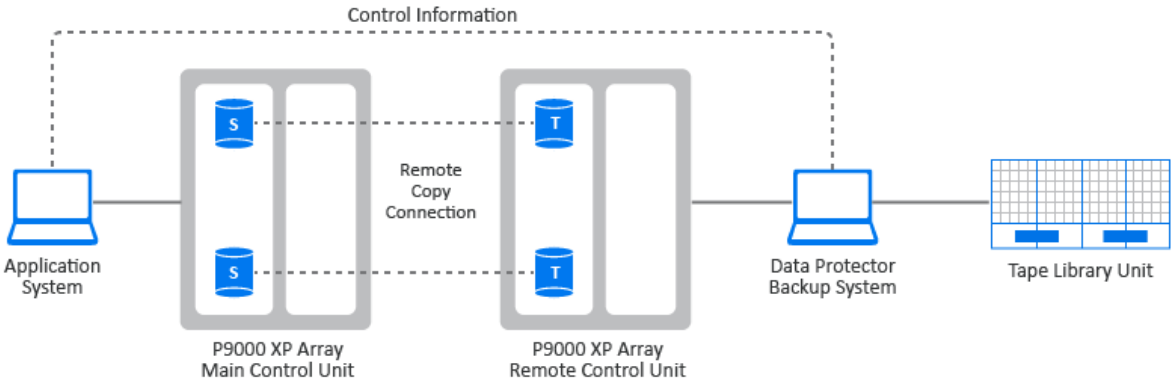
远程复制配置

单个备份系统和单个 P9000 XP 阵列可用于备份多个主磁盘阵列。请参阅 CA P9000 XP 配置 4。通过这种方法，可以构建中央备份站点。此类配置需要至少两个位于实际独立的站点中的磁盘阵列。

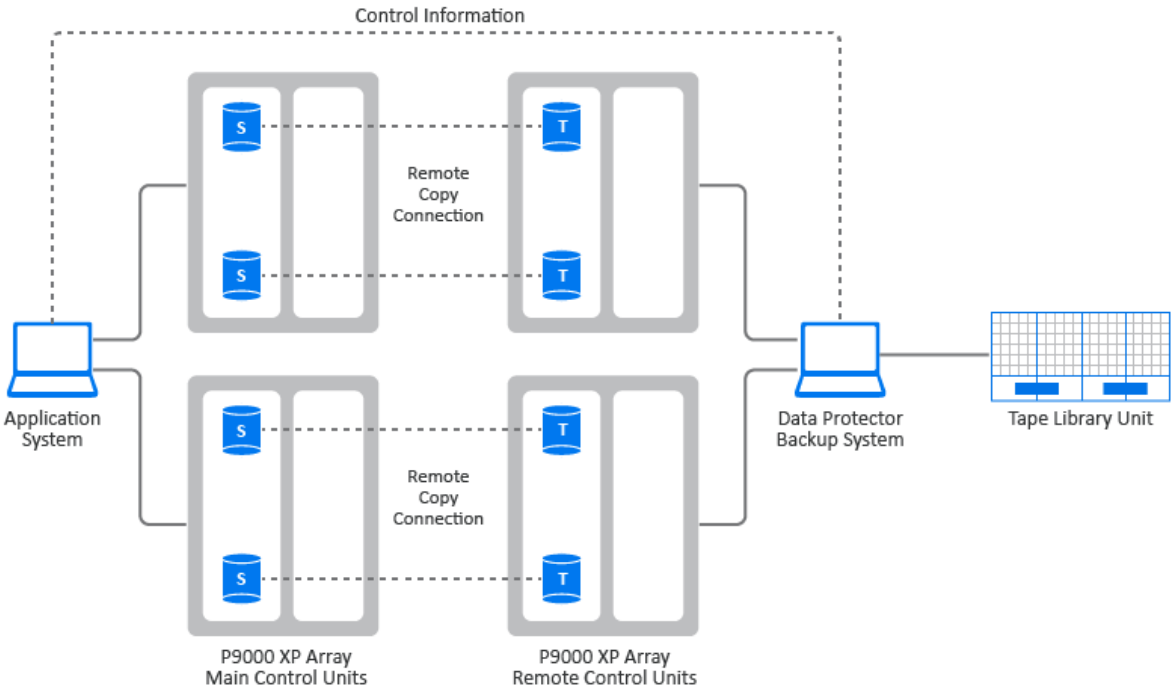
在 Data Protector 会话期间，为了实现零宕机时间备份，将在磁盘阵列之间使用镜像 (CA) 链接。为了同时保持数据的完整高可用性，还需要其他镜像 (CA) 链接。

CA P9000 XP 配置 1 至 CA P9000 XP 配置 4 是 P9000 XP 阵列上受支持的远程复制配置的示例。

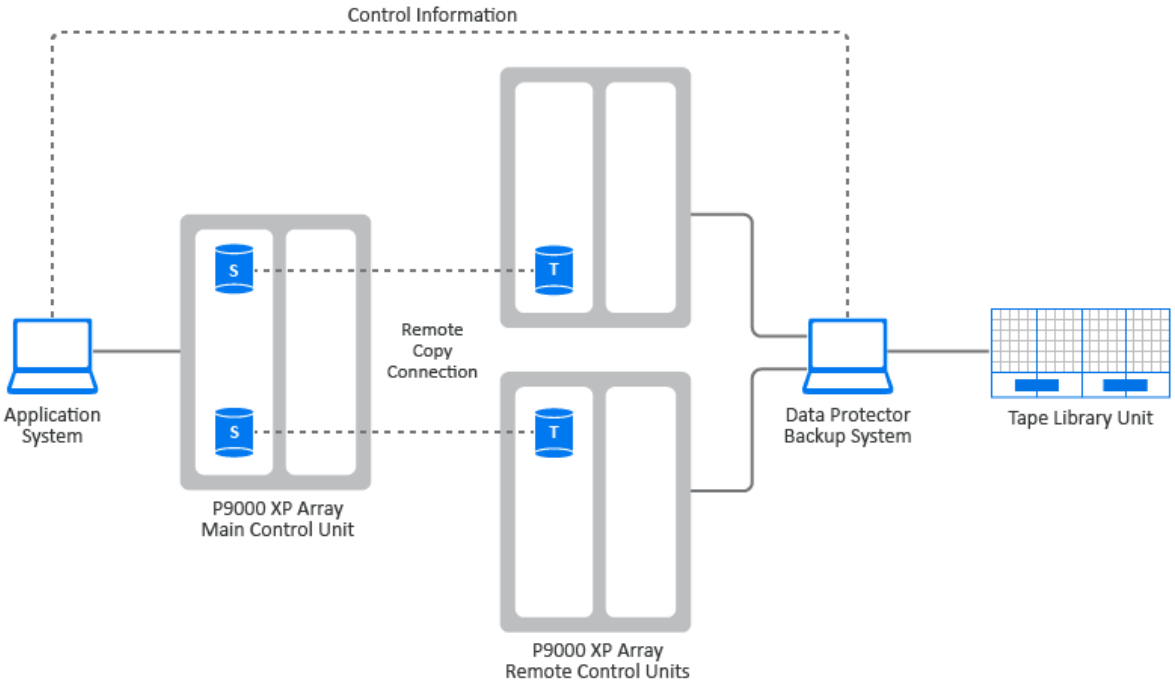
CA P9000 XP 配置 1



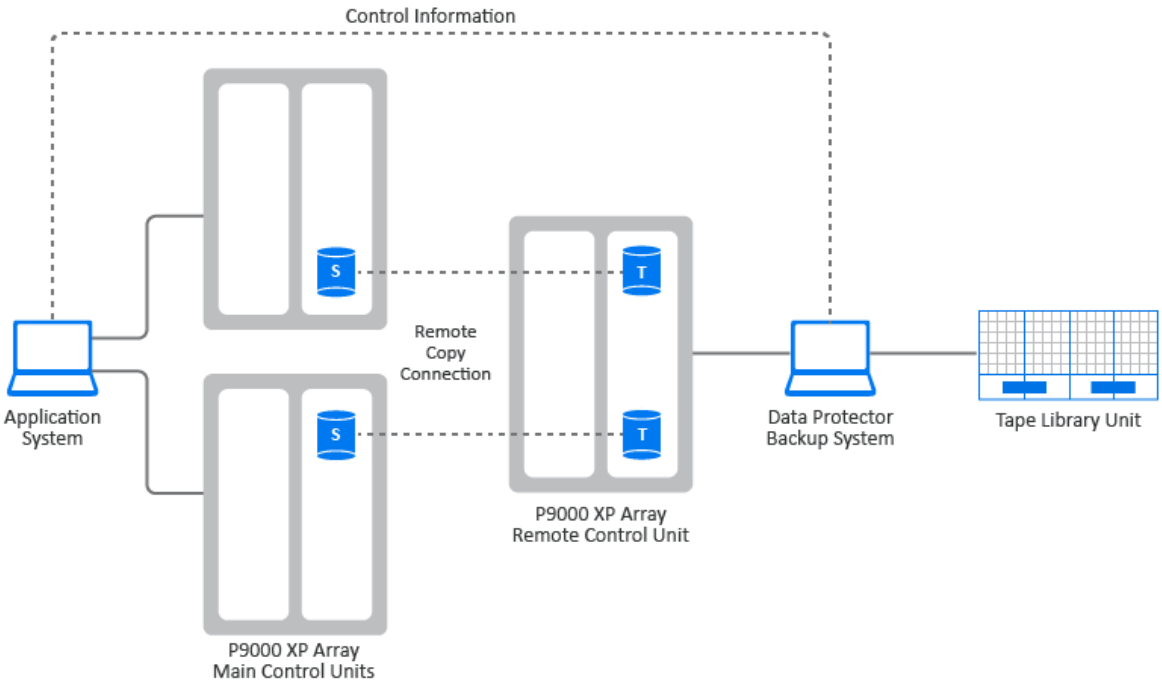
CA P9000 XP 配置 2



CA P9000 XP 配置 3



CA P9000 XP 配置 4



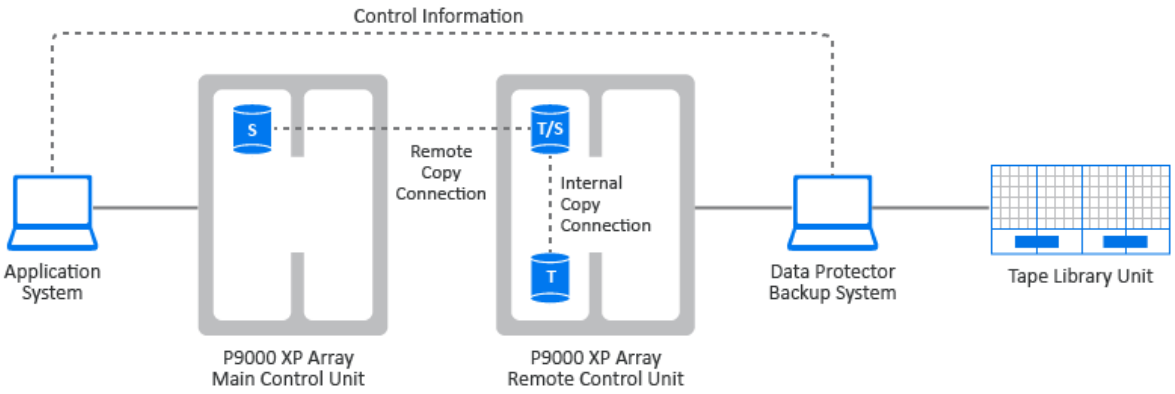
远程和本地复制配置

限制

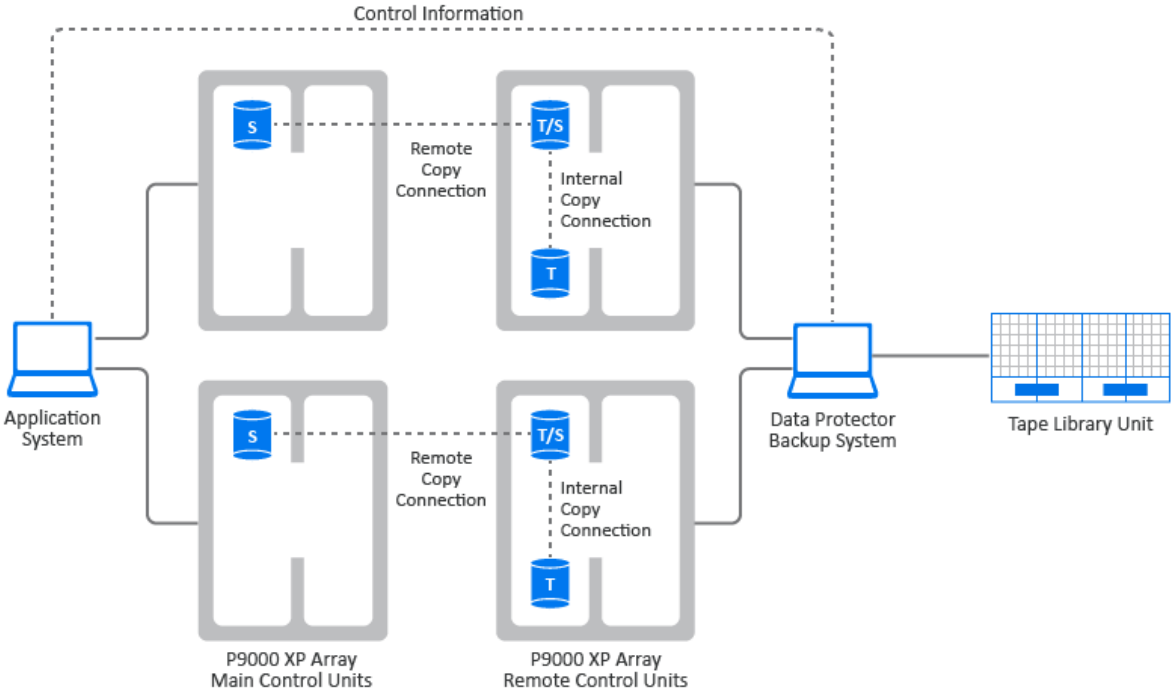
- 在 HP-UX 上，建议仅将 BC 目标卷连接到备份系统。如果出于任何原因还连接了 CA 目标卷，则必须给予特别注意。
- 不支持作为 CA+BC 组合配置一部分的异步 CA 配置。

CA+BC P9000 XP 配置 1 至 CA+BC P9000 XP 配置 4 是 P9000 XP 阵列上受支持的远程和本地复制配置的示例。

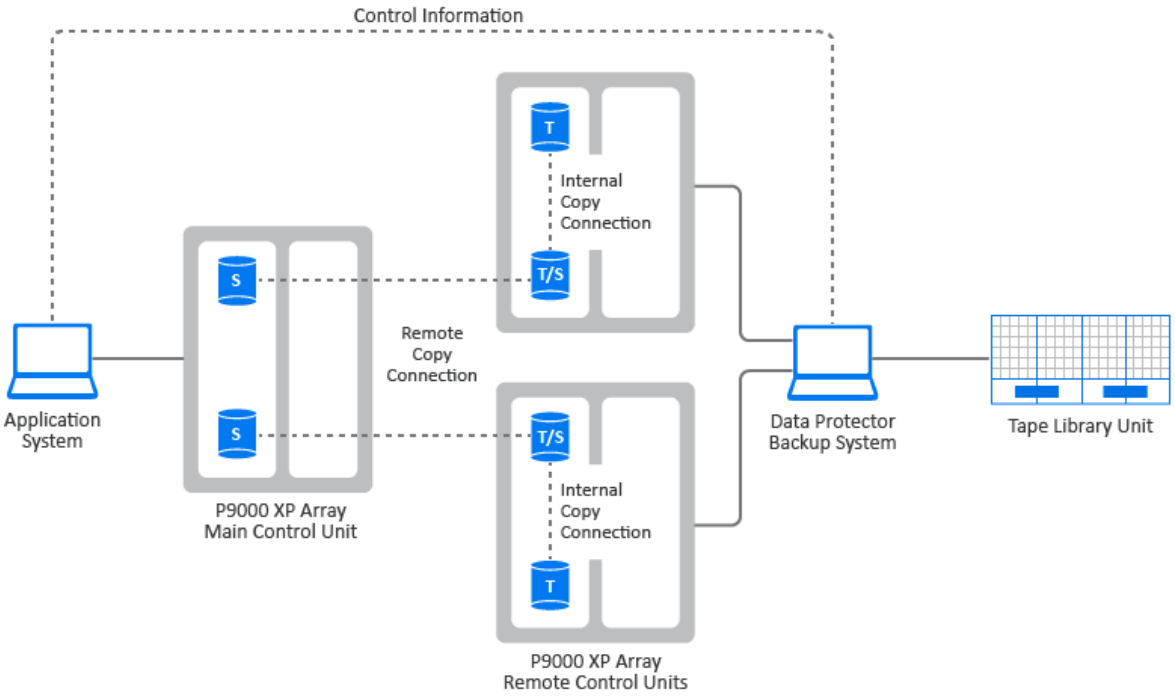
CA+BC P9000 XP 配置 1



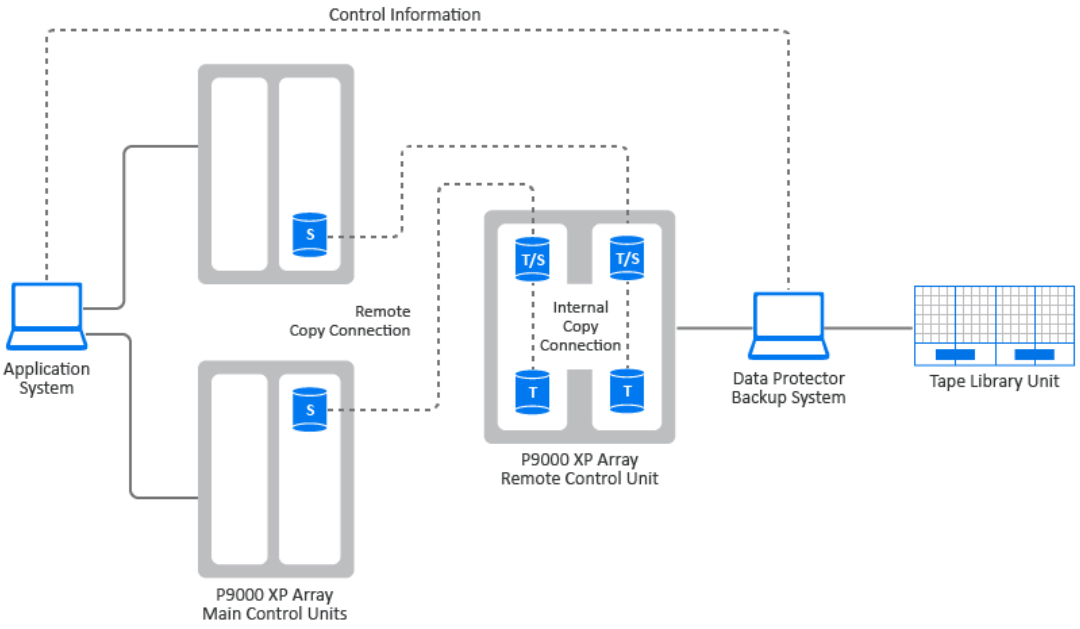
CA+BC P9000 XP 配置 2



CA+BC P9000 XP 配置 3



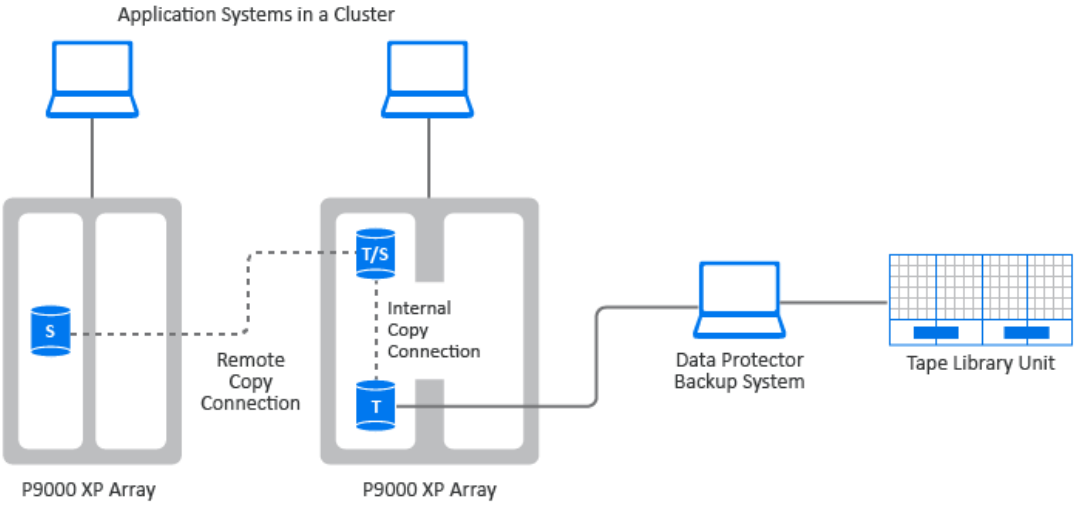
CA+BC P9000 XP 配置 4



群集配置

下图是群集中的 CA+BC P9000 XP 阵列配置的示例。

群集中的 CA+BC P9000 XP 配置



支持的 HACMP 群集配置

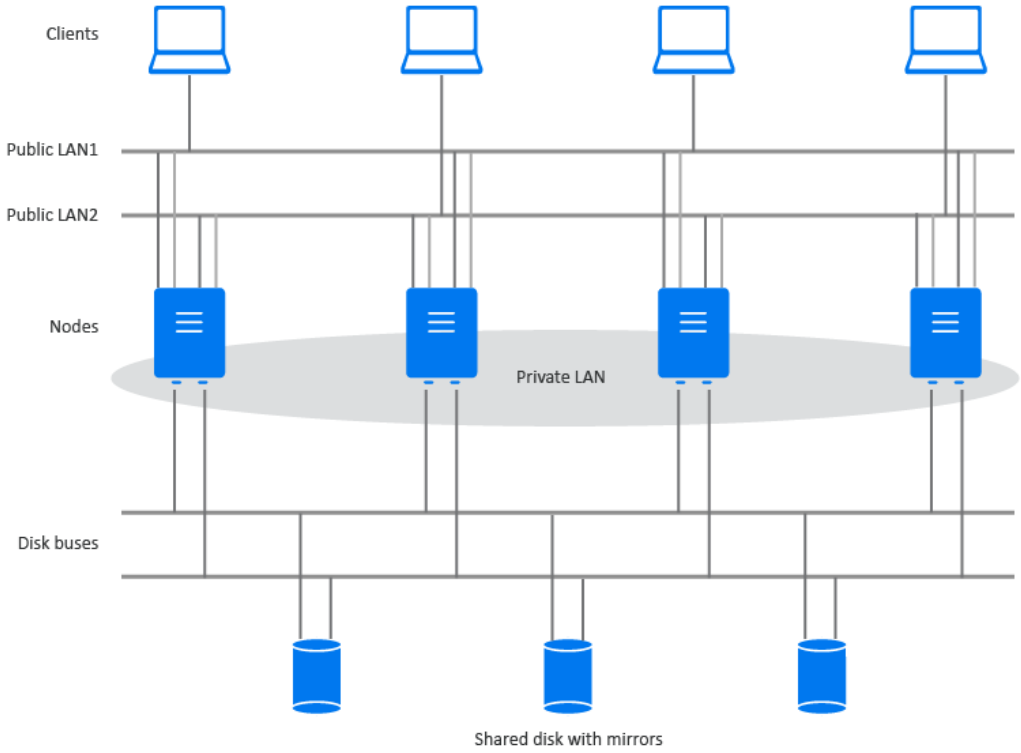
HACMP 软件是 IBM 关于建立基于 UNIX 的任务关键计算环境的解决方案，它基于高可用性 (HA) 和群集多处理 (CMP) 技术。它确保具备应用程序等关键资源可供处理。

创建 HACMP 群集的主要原因是为任务关键应用程序提供一个高度可用的环境。例如，HACMP 群集可以运行一个数据库服务器程序，为客户机应用程序提供服务。客户机向服务器程序发送查询，后者通过访问存储在共享外部磁盘上的数据库响应其请求。

要确保 HACMP 群集中这些应用程序的可用性，请由 HACMP 控制这些应用程序。HACMP 确保即使群集中有组件发生故障，应用程序对客户机进程也保持可用。如果有组件发生故障，则 HACMP 将应用程序（连同确保可访问应用程序的资源一起）移至群集中的另一个节点。

通过虚拟服务器名称（虚拟环境域名）访问整个群集，该名称代表网络上的整个 HACMP 群集。

典型的 HACMP 群集设置



如图所示，HACMP 群集由以下物理组件组成：

- 节点
- 共享外部磁盘接口
- 网络
- 网络接口
- 客户机

节点

节点组成了 HACMP 群集的核心。每个节点都由一个唯一名称标识，并包含一个用于运行 AIX 操作系统、HACMP 软件和应用程序软件的处理器。节点可能拥有一组资源磁盘、卷组、文件系统、网络、网络地址和应用程序。

共享外部磁盘接口

每个节点都可以访问一个或多个共享外部磁盘设备（以物理方式连接到多个节点的磁盘）。共享磁盘存储任务关键数据，通常进行镜像或配置 RAID 以形成数据冗余。注意，HACMP 群集中的节点使用内部磁盘存储操作系统和应用程序二进制文件，但不共享这些磁盘。

网络

HACMP 软件作为 AIX 操作系统的一个独立分层组件，旨在配合任何基于 TCP/IP 的网络一起工作。节点使用网络可：

- 允许客户机访问群集节点、
- 使群集节点可以交换波动信号消息、
- 序列化对数据的访问（在并发访问环境中）。

HACMP 软件定义两种类型的通信网络，具体取决于这些网络所使用的通信接口基于 TCP/IP 子系统（基于 TCP/IP）还是基于非 TCP/IP 子系统（基于设备）。

客户机

客户机是可以通过 LAN 访问群集中节点的处理机。每个客户机都运行一个“前端”，即客户机应用程序，

以查询群集节点上运行的服务器应用程序。

备份系统

以下步骤显示如何创建备份规范和执行简单备份：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份 (Backup)**，然后单击**备份规范 (Backup Specifications)**。
3. 右键单击要备份的项目类型 (例如“文件系统”)，然后单击“添加备份”
4. 在“创建新备份”对话框中，选择一个可用的模板以及备份类型，然后根据需要选择其他选项。单击“确定”打开向导。
5. 在“结果”区域中出现的“源”页面中，选择所需的备份类型选项。
6. 浏览并选中要备份的目录和文件旁边的复选框，然后单击“下一步”。

> 注意:
> - 允许的最大文件或文件夹绝对路径名为 1024 个字符。因此，不能浏览绝对路径名大于 1024 个字符的文件或文件夹。
> - 如果没有连接磁带设备，则仅选择一些小目录。

7. 使用默认备份规范选项或选择所需的备份选项，然后单击**下一步 (Next)**。
8. “结果区域 (Results Area)”中将显示备份规范摘要。单击“下一步”。
9. 单击**另存为**保存备份规范以供将来使用。或者，您也可以单击**保存并调度**选项进行保存，然后使用调度程序对备份规范进行调度。
10. 单击**开始备份 (Start Backup)** 以运行备份。
11. “开始备份 (Start Backup)”窗口打开后，单击**确定 (OK)** 以使用默认规范开始备份。
12. “备份 (Backup)”窗口将显示备份会话的进度。“会话信息 (Session Information)”窗口将显示备份何时才能完成。

从备份还原

默认情况下，将备份对象还原到从中备份它的同一路径下。以下步骤显示如何执行简单还原:

1. 在“上下文列表”中，单击**恢复**。
2. 浏览**文件系统 (Filesystem)** 项并选择要还原的客户机对象。此时将在“结果区域 (Results Area)”中显示“还原 (Restore)”视图。
3. 浏览并选中要还原的目录/文件旁边的复选框。
4. 选择**目标 (Destination)** 选项卡以选择还原的目标位置。如果未选择任何位置，则选定的目录/文件将还原到原始路径下。
5. 单击**开始还原 (Start Restore)** 按钮。此时将显示还原向导。
6. 使用向导中的建议默认设置（单击**下一步 (Next)** 和**完成 (Finish)**）。
7. 此时将打开“开始还原会话 (Start Restore Session)”窗口，此窗口显示要还原到系统的选定对象的进度。

使用案例: 设置 Data Protector

尽管配置 Data Protector 很容易，但某些高级计划将帮助您配置环境和优化备份。本节概述了设置备份环境的各种全局任务。

根据环境的大小和复杂程度，可能不必完成以下所有步骤。

1. 分析网络和组织结构。确定需要备份的系统。
2. 检查是否有任何特殊的应用程序和数据库要备份，如 Microsoft Exchange Server、Microsoft SQL Server、Oracle Server、SAP R/3 等等。Data Protector 提供与这些产品的特定集成功能。

   有关如何配置集成的信息，请参阅集成。
3. 确定 Data Protector 单元的配置，如：
   - 要作为 Cell Manager 的系统
   - 要从中安装用户界面的系统
   - 本地备份与网络备份
   - 控制备份设备和库的系统
   - 连接、LAN 和/或 SAN 的类型
4. 根据设置购买所需的 Data Protector 许可证。这样即可获得安装所需的密码。

   或者，您也可以使用即开即用密码运行 Data Protector。但是，这种密码仅在安装之日起 60 天内有效。
5. 考虑安全方面：
   - 分析安全注意事项。
   - 考虑需要配置的用户组。
   - 通过将数据以加密格式写入介质增强安全性。
6. 确定如何构建备份：
   - 希望有哪些介质池以及如何使用它们？
   - 将使用哪些设备，以及如何使用？
   - 每个备份需要多少个副本？
   - 需要多少个备份规范以及应如何将其分组？
   - 如果计划备份到磁盘，请考虑高级备份策略，如合成备份和磁盘分段。
7. 安装 Data Protector Cell Manager 和安装服务器。然后，使用 Data Protector GUI 将 Data Protector 代理分发到其他系统。
8. 配置备份设备。
9. 配置介质池并准备介质。
10. 配置备份规范，包括 IDB 备份。
11. 配置报告（如果需要）。
12. 为灾难恢复做准备。
13. 熟悉以下任务：
    - 处理失败的备份
    - 执行还原
    - 复制已备份数据和保管介质
    - 测试灾难恢复
    - 维护 IDB

相关主题

- 关于备份设备
- 关于介质管理
- 关于备份
- 关于复制备份数据
- 关于报告

词汇表

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

应用程序代理

应用程序代理是 Data Protector 的组件，该组件安装在客户机系统上，用于备份联机数据库和应用程序，例如 SAP HANA、PostgreSQL 和 Microsoft SharePoint。它读取或写入从数据库和应用程序实用程序接收的数据，并向介质代理发送数据或从介质代理接收数据。

备份

备份是在目标设备上创建数据副本的过程。该副本的存储和保留是供将来万一发生原始数据损坏时使用。

备份代理/磁盘代理 (DA)

备份代理/磁盘代理会从系统上的磁盘中读取数据或将数据写入磁盘，并将数据发送到介质代理或从介质代理接收数据。备份代理/磁盘代理安装在备份的客户机系统上。备份客户机还安装在 Cell Manager 上，从而可以备份 Cell Manager 上的数据、Data Protector 配置和内部数据库 (IDB)。

备份设备/目标设备/目标介质

配置有 Data Protector 的物理或虚拟设备/介质，可以从存储设备/介质读取数据并将数据写入存储设备/介质。

备份会话

执行备份规范以在目标设备上创建数据副本的过程实例。它可以使用 Data Protector 用户界面由操作员交互启动，也可以使用 Data Protector 调度程序以自动方式启动。

备份规范

备份规范定义了要备份的数据源、要使用的目标设备以及执行备份的时间表。

基于块的备份

通过基于块的备份，您可以在块级别执行文件系统备份。

基于块的还原

通过基于块的还原，您可以还原在块级别备份的数据。

单元

Data Protector 单元是由 Cell Manager 系统、客户机系统和目标设备组成的网络环境。(可选) 可能有一个报告服务器以及一个或多个安装服务器。

Cell Manager (CM)

Cell Manager 是从中心点控制 Data Protector 单元的主要系统，其中安装了 Data Protector 核心软件和内部数据库。Cell Manager 是控制备份和还原工作流并存储元数据以供将来参考的单元的一部分。

客户机系统

客户机系统是由 Data Protector 备份的系统以及在其上配置备份设备的系统。

Data Protector Express

Data Protector Express 是基于套接字许可模式的虚拟专用产品。Express 版是专门为虚拟环境设计的。它包括针对 VMware 和Hyper-V 工作负载的无代理保护以及高级 VM 恢复功能，例如粒度恢复、开机、实时迁移和零宕机时间备份 (ZDB) 集成。报告和分析也包含在 Express 版中。

Data Protector 集成

Data Protector 集成是一些软件组件，可让您使用 Data Protector 运行应用程序或存储阵列的备份。

Data Protector Premium

Data Protector Premium 是基于容量许可模式的产品。Premium 版适用于需要针对物理、虚拟和混合环境的统一备份和灾难恢复解决方案的企业。Data Protector Premium 包含 Data Protector 的全部功能。其中包括软件加密、高级报告和分析、与关键任务应用程序、云和存储平台的集成，以及诸如 Micro Focus Business Value Dashboard 和 Operations Orchestration 之类的 IT 运营工具。

Data Protector ZDB 集成

Data Protector ZDB 集成是一些软件组件，通过它们可以运行使用磁盘阵列 (例如 3PAR、Unity 和 NetApp) 的零宕机时间备份和即时恢复。

差异备份

差异备份对从上次完整备份以来的所有更改数据进行备份。

灾难恢复

灾难恢复是将目标 Data Protector 系统恢复到原始系统配置的系统过程。

完整备份

完整备份是数据的完整备份。完整备份可实现简单快速的还原，但需要更多时间和介质空间来进行备份。

粒度恢复

粒度恢复是一种使您可以在粒度或单个级别恢复数据 (例如文件、电子邮件和 SharePoint 项目) 的方法。

Granular Recovery Extension (GRE)

需要在 VMware vCenter 服务器、Microsoft Exchange 服务器或 Microsoft SharePoint 服务器上安装此插件才能使用粒度恢复功能。

增量备份

增量备份是自上次完整、增量或差异备份以来所有已更改块的备份。

安装服务器 (IS)

安装服务器是存储 Data Protector 软件存储库的计算机。

即时恢复 (IR)

通过即时恢复，您可以从磁盘阵列快照或以前由零宕机时间备份 (ZDB) 创建的克隆中还原数据。

集成客户机

集成客户机是一些软件组件，通过这些组件，您可以使用 Data Protector 运行应用程序联机备份。

内部数据库 (IDB)

内部数据库 (IDB) 是位于 Cell Manager 上的嵌入式数据库，存储的信息包括备份数据，数据所处备份介质，备份、还原、对象复制、对象合并、对象验证和介质管理会话的结果，以及配置的备份设备和库。

传统调度程序

通过传统调度程序，可以定期自动执行各种操作，例如备份、复制、合并、验证、报告和介质复制。

Manager-of-managers (MoM) 环境

Data Protector Manager-of-Managers (MoM) 是一种软件体系结构，可使管理员管理由多个 Data Protector Cell Manager 作为一个单元组成的企业环境。

介质代理 (MA)

介质代理与磁盘或集成代理进行通信，以从目标设备读取数据或向目标设备写入数据。

介质管理会话

介质管理会话用于对介质执行一些操作，比如对介质进行初始化、扫描内容、验证介质上的数据和复制介质等。

介质池

介质池是作为单元管理的相同类型的备份介质集合。

对象合并会话

对象合并会话是将包含一个完整备份和至少一个增量备份的备份对象还原链合并为该对象的新合并版本的过程。在对象合并会话期间，Data Protector 会从源介质读取备份的数据，合并数据，并将合并后的数据版本写入目标介质。

对象复制会话

对象复制会话是在其他介质集上创建已备份、已复制或已合并数据的副本的过程。

开箱即用

默认情况下，产品提供开箱即用功能。无需其他配置即可使用该功能。

对等

对等是一个系统，其中所有计算机都相互连接，不需要中央服务器。

推送安装

推送安装是一种使用 Data Protector 图形用户界面 (GUI) 或命令行界面 (CLI) 在客户机上远程安装 Data Protector 软件组件的方法。

恢复点目标 (RPO)

恢复点目标是按时间衡量的最大可接受数据丢失量。该指标有助于衡量上次备份与灾难之间的时间差，而不会对您的业务造成严重损害。它还用于确定备份频率。

恢复时间目标 (RTO)

恢复时间目标是灾难发生之后、还原到正常操作之前的最大可接受宕机时间。该指标确定灾难发生之后您需要多长时间恢复 IT 基础架构和服务以保持业务连续性。

复制

替换是一个过程，其中数据从一台设备复制到另一台而不通过介质代理客户机。

替换会话

复制会话是在其他能够执行复制的备份到磁盘 (B2D) 设备上创建已备份、已复制或已合并数据的其他复本的过程。

报告服务器 (RS)

报告服务器是 Data Protector 的组件，您可以使用它查看用于管理和计划备份环境的集成报告。报告服务器必须安装在非 Data Protector Cell Manager 的服务器上。

还原

还原是从备份副本重新创建原始数据的过程。该过程由数据准备及实际还原和一些还原后的操作组成，执行还原后操作是为了使还原的数据可用。

还原会话

还原会话是将备份中的数据还原到磁盘的过程。还原会话可以由操作员通过 Data Protector 用户界面交互启动。

保管

保管就是将介质放在安全位置保存一段时间的过程，这个安全位置通常称为保管库。

基于 Web 的调度程序

基于 Web 的调度程序提供了简化的 Web 界面，可定期计划诸如备份、对象合并、验证和复制、介质复制之类的操作。

ZDB 集成客户机

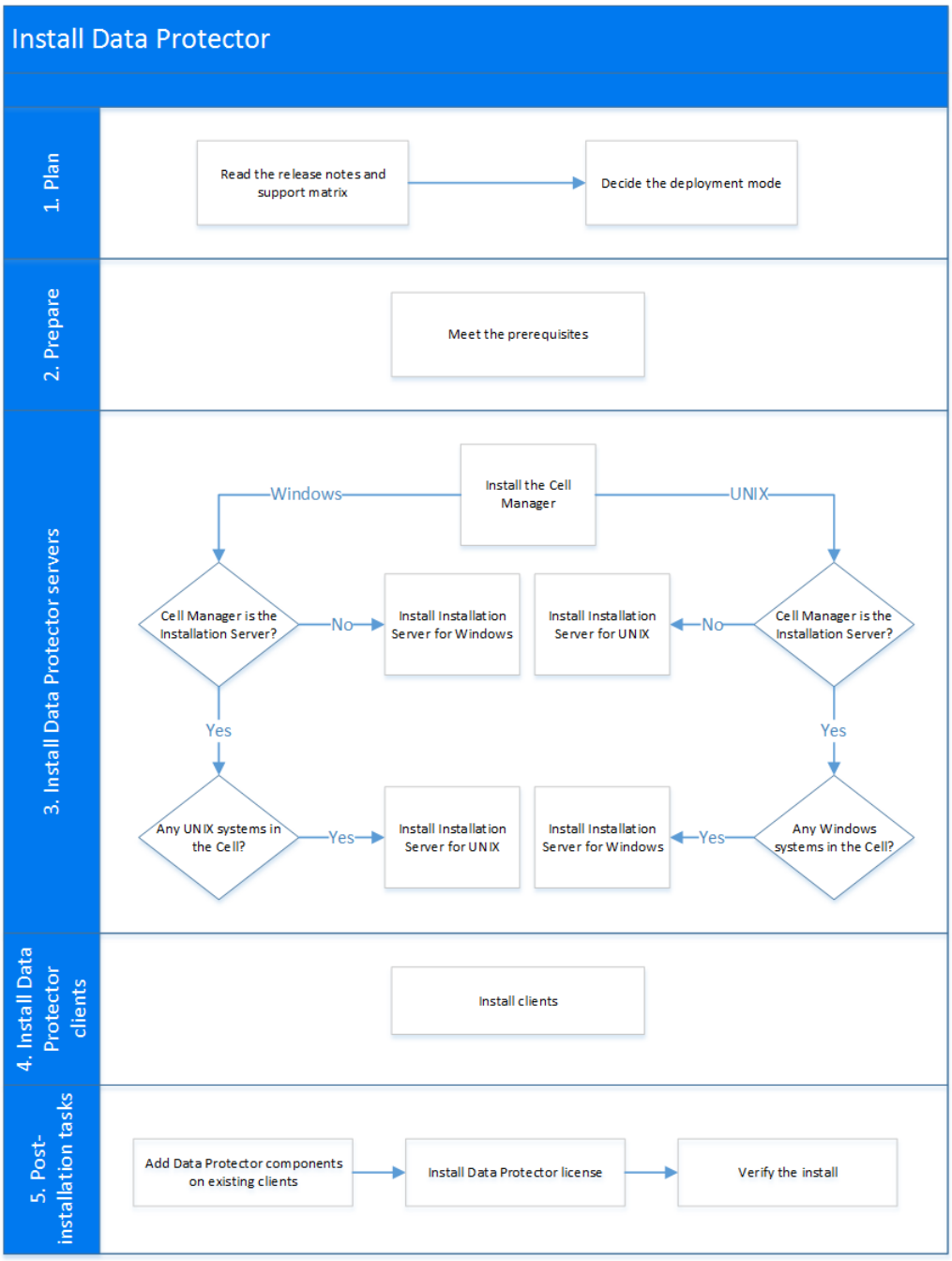
使用 ZDB 磁盘阵列备份和存储数据的系统称为 ZDB 集成客户机。这些系统是单元的一部分，该单元的数据存储在从存储阵列 (如 3PAR 和 Netapp) 提供的逻辑单元号 (LUN) 上。

零宕机时间备份 (ZDB)

零宕机时间备份是一种从存储阵列备份数据的备份方法，可最大程度地减少应用程序系统的开销。在零宕机时间备份中，创建要备份数据的复本，并在替换的数据而非原始数据上执行所有后续备份操作。

安装

以下流程图描述了典型的 Data Protector 安装工作流:



在安装 Data Protector 之前，请查看以下主题以获取有关安装 Data Protector 的先决条件、支持矩阵和过程的信息。

- 计划 Data Protector 安装
- 准备安装
- 安装 Cell Manager 和安装服务器
- 安装报告服务器
- 安装 Data Protector 客户机
- 安装 Data Protector 集成客户机
- 安装更改后的块驱动程序
- 安装后任务
- 卸载 Data Protector 软件
- 许可证
- 使用 Unix 系统本机工具安装和升级
- 系统准备和维护任务
- 安装问题的故障诊断

计划安装

典型的 Data Protector 安装包括安装 Data Protector Cell Manager、一个或多个安装服务器、报告服务器和客户机。查看以下主题以计划 Data Protector 安装:

- 支持矩阵
- 可扩展性

支持矩阵

本节提供 Data Protector 支持矩阵的链接，其中包括有关受支持平台、设备和集成的详细信息。

Data Protector Express

可以使用以下支持矩阵:

- Data Protector 精简版支持矩阵

Data Protector Premium

可以使用以下支持矩阵:

- Data Protector 支持矩阵版本 – 新增功能
- Data Protector 设备支持矩阵
- Data Protector 灾难恢复支持矩阵
- Data Protector 网络连接存储 (NAS) 支持矩阵
- Data Protector 平台和集成支持矩阵
- Data Protector 虚拟化支持矩阵
- Data Protector VSS 集成支持矩阵
- 针对 Dell EMC Storage 的 Data Protector 零宕机时间备份支持矩阵
- 针对 NetApp Storage 的 Data Protector 零宕机时间备份支持矩阵
- 针对 HPE Storage 的 Data Protector 零宕机时间备份支持矩阵
- Data Protector Management Pack 支持矩阵
- Data Protector 过时文档

可扩展性

Data Protector 可扩展性

以下主题介绍 Data Protector 软件的可扩展性。

备份基础结构可扩展性

备份基础结构指标	限制
Data Protector 单元中的客户机	5000
Data Protector Manager-of-Manager (MoM) 单元中的 Cell Manager (单元)	50
MoM 环境中的客户机总数	50000

内部数据库可扩展性

下表显示了特定限制。要重新配置限制，请调整 Data Protector 全局选项:

基础内部数据库容量	限制
存储在内部数据库 (IDB) 中的 Data Protector 会话数	1 亿 (100,000,000)
具有 IDB 中引用的元数据的文件名数	1 万亿 (1012)
IDB 中引用的备份对象数	1 百万 (1,000,000)
IDB 中引用的备份对象版本数	5 千万 (50,000,000)

详细信息编目二进制文件容量	最大可配置限值 (预定义的默认限值)
详细信息编目 (DC) 目录数	100 (50)
每个 DC 目录的大小	2047 TB (200 GB)
每个 DC 目录的文件数	500 000 (100 000)
DC 二进制文件大小	不适用
DC 目录最小空间（目录大小的有效限值的最小差值）	不适用 (2 GB)

Media Management Database 容量	限制
Media Management Database 中的备份介质数 (MMDB)	5 千万 (50,000,000)
MoM 环境中所有 MMDB (或 CMMDB) 中的备份介质的总数	25 亿 (2 500 000 000)
介质池中的备份介质数	200 000

Data Protector GUI 限制

GUI 限制	限制
展开文件夹时，树展开视图中显示的文件和文件夹的数量。	64000

并发限制

备份会话并发指标	最大可配置限值 (预定义的默认限值)
并发备份会话	1000 (100)
MoM 环境中的并发备份会话总数	50 000
一天的备份会话数	99 999

备份设备并发指标	限制
磁盘代理并发（设备并发）	32
在备份、对象复制、对象合并或还原会话中使用的备份设备数（驱动器数）	128
并发物理驱动器数 (DLT7000 和性能较低的型号)	1000
并发物理驱动器数（DLT8000、SDLT、LTO）	500
并发虚拟驱动器数 (LTO - 其中驱动器并发被设置为 1)	1000

会话内并发指标	限制
在会话中同时处理的备份对象数	4096
同时导入的备份介质数	100

增加并发备份会话

如果将 MaxBSessions 全局选项的值增大到特定值 (例如，近 1000)，则可能需要修改 Cell Manager 上限制并发会话总数的特定系统参数。所做的修改取决于 Cell Manager 的操作系统。

Windows 系统

这适用于 Windows 上运行的 Cell Manager。

非交互式桌面堆大小

默认的非交互式桌面堆的大小用于大约 100 次并行会话足够了。因此，如果要超出此操作系统限制，则需要增加非交互式桌面堆的大小。以下注册表值控制每个桌面堆分配的大小:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows
```

该注册表值的默认数据看起来与以下内容相似：

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480, 768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
```

SharedSection 后面的数值 (以千字节为单位指定) 控制桌面堆的分配。

- 1024 - 所有桌面常用的共享堆大小
- 20480 - 与交互式窗口站关联的每个桌面的桌面堆大小
- 768 - 与非交互式窗口站关联的每个桌面的桌面堆大小

您必须将与非交互式窗口站关联的桌面堆值从 768 更改为 20480 。此更改需要重新启动才能生效。

Data Protector INET 使用的线程数

Windows 上的 Data Protector INET 服务负责客户机 (包括 Cell Manager) 的所有连接。Data Protector INET 在系统中检测到的每个 CPU 最多具有 8 个线程。特别是在具有少量 CPU 或大量连接的系统上，这可能成为瓶颈。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\omniInet\ImagePath
```

该注册表值的默认数据看起来与以下内容相似：

```
"C:\Program Files\OmniBack\bin\omniinet.exe"
```

要调整最大 INET 线程数，请附加 -threadCount n 参数并重新启动 Data Protector INET 服务和 Cell Manager 服务。

例如，如果具有 4 个 CPU 的系统上的 32 个线程不够，则将其增加到 64 个:

```
"C:\Program Files\OmniBack\bin\omniinet.exe" -threadCount 64
```

带有 xinetd 的 Linux 系统

这适用于 Data Protector Cell Manager 和在带有 xinetd 的 Linux 上运行的客户机。

Data Protector INET 使用的进程数

Linux 上的 Data Protector INET 服务负责客户机 (包括 Cell Manager) 的所有连接。如果 Data Protector INET 由 xinetd 启动，则可能需要调整 /etc/xinetd.d/omni 文件中的 cps 参数，然后重新启动 xinetd。

```
service omni { socket_type = stream protocol = tcp wait = no user = root server = /opt/omni/lbin/inet server_args = inet -log /var/opt/omni/log/inet.log disable = no cps = 2200 10 instances = UNLIMITED per_source = UNLIMITED }
```

带有 systemd 的 Linux 系统

这适用于 Data Protector Cell Manager 和在带有 systemd 的 Linux 上运行的客户机。

Data Protector INET 使用的进程数

Linux 上的 Data Protector INET 服务负责客户机 (包括 Cell Manager) 的所有连接。对于由 systemd 启动的 Data Protector INET，则可能需要将 TriggerLimitBurst 和 TriggerLimitIntervalSec 参数添加到 /usr/lib/systemd/system/omni.socket 文件并使用 systemctl daemon-reload 和 systemctl restart omni.socket 重新启动 omni.socket 。

```
[Unit] Description=DATA-PROTECTOR-INET PartOf=omni.service [Socket] ListenStream=5565 Accept=yes MaxConnections=1000000 MaxConnectionsPerSource=100000 TriggerLimitBurst=2200 TriggerLimitIntervalSec=10 [Install] WantedBy=sockets.target
```

> 注意**:** 对于与连接有关的问题，例如“触发限制命中，拒绝进一步激活”，则可以改为使用 TriggerLimitBurst=0 。

文件库仓库大小

允许的最大文件仓库大小为 2 TB，默认大小为 5 GB。创建较大的文件需要更多的 CPU 和内存资源，但是可以大大减少大量 5 GB 文件仓库所需的处理开销。您可以评估更改默认设置对于介质代理服务器的影响后再进行更改。在具有分布式文件介质格式 (DFMF) 的文件库使用的磁盘上，

预期性能较低且碎片化程度较高。如果文件库没有 DFMF 且每个写入程序设备的并发性较低，则性能较高且磁盘碎片化程度较低。

增强型增量备份

- 每个新增强型增量数据库最多可以支持每个装载点 400 亿个文件和每个目录 4000 万个文件。
- 一个目录中的最大文件数量决定了最大内存消耗。最大内存消耗大约为一个目录中每 1 百万个文件 130 MB。
- Data Protector 支持每个目录以下数量的文件增强型增量备份：
  - Windows 系统上为 1000 万个文件
  - Linux 和 HP-UX 系统上为 500 万个文件

准备安装

在安装 Data Protector 之前，查看以下主题以帮助您准备安装:

一般先决条件

确定要安装的系统

在网络上安装 Data Protector 之前，定义以下系统:

- 将要安装 Cell Manager 的系统。如需了解受支持的操作系统和版本，请参阅最新支持矩阵。

  每个单元仅可拥有一个 Cell Manager。如果不安装 Cell Manager，则无法运行 Data Protector。

- 用于通过用户界面访问 Data Protector 功能的系统。这些系统必须安装了用户界面组件。
- 将要备份的系统。这些系统必须已安装磁盘代理组件 (用于文件系统备份) 以及相关的应用程序代理组件 (用于联机数据库集成)。
- 连接备份设备的系统。这些系统必须安装介质代理组件。
- 要在其上安装 Data Protector 安装服务器的一个或多个系统。有两种安装服务器可用于远程软件安装: 一种用于 UNIX 客户机，另一种用于 Windows 客户机。针对安装服务器选择系统独立于 Cell Manager 和要在其上安装“用户界面”的系统。Cell Manager 和安装服务器可以安装在同一系统上，也可以安装在不同系统上。安装服务器可在多个 Data Protector 单元之间共享。

注意: 如果 Windows 系统上已经安装了安装服务器，那么不可在该系统上远程安装 Data Protector 客户机。若要在同一系统上安装安装服务器和客户机组件，必须从 Data Protector Windows 安装包 (zip) 执行本地客户机安装。在“自定义安装”窗口中，选中所有需要的客户机组件和安装服务器组件。OpenVMS 客户机也无法进行远程安装。在这些客户机上必须进行本地安装。

选择 Cell Manager 系统

Cell Manager 是 Data Protector 单元中的主系统。它从中心点管理单元。Cell Manager 将执行以下操作:

- 运行核心 Data Protector 软件。
- 主机 Data Protector 内部数据库 (IDB) 服务器。
- 收集和维护包含有关 Data Protector 会话信息的数据。
- 运行启动的会话管理器，停止不同类型的 Data Protector 会话，并将相关信息存储到 IDB 中。

在决定要在环境中的哪个系统上安装 Cell Manager 之前，请注意以下几点:

- 支持的平台

Cell Manager 可以安装在 Windows 和 Linux 平台上。有关这些平台受支持的版本或发布的详细信息，请参阅最新支持矩阵。

- Cell Manager 系统的可靠性

由于 Cell Manager 包含 IDB，并且一旦 Cell Manager 不正常工作，备份和还原将无法执行，因此选择环境中极其可靠的系统进行安装就显得非常重要。

- 数据库增长和和所需磁盘空间

Cell Manager 包含 Data Protector 内部数据库 (IDB)。IDB 包含有关已备份数据及其介质、会话消息和设备的信息。IDB 的规模可能会增长到非常大，具体取决于您的环境。例如，如果大部分备份始于文件系统备份，那么通常 IDB 大小为备份数据所使用的磁盘空间的 2%。

不必将 Cell Manager 用作用户界面系统。例如，可以将 Linux Cell Manager 系统和 Data Protector 用户界面组件安装在带 Windows 平台的其他系统上。

系统密码建议

以下是建议在安装 Data Protector 的系统上创建安全管理员密码的一组准则：

- 密码的最小长度必须为八个字符。
- 密码必须是以下各项的组合：数字、大写字母、小写字母和特殊字符。
- 密码不能与用户名相同。
- 密码不能是用户名的组合。
- 密码必须每 90 天更新一次。避免使用过去使用过的密码。

安装介质

Data Protector 支持各种操作系统和多种处理器体系结构。该软件以 zip/tar 形式提供。

下表列出了可从 https://entitlement.microfocus.com/mysoftware/index 下载的不同包。

包名称	内容
Data Protector 软件，Windows Micro_Focus_DP_*xx.xx*_Windows_DP_A*xxxx*_Windows_OVMS.zip	• 适用于 64 位 Windows 系统的 Cell Manager 和安装服务器 • Windows 32/64 位客户机 • OpenVMS 客户机（Alpha 和 Itanium 系统） • 产品信息

Data Protector 软件，Linux Micro_Focus_DP_*xx.xx*_Linux_DP_A*xxxx*_GPLx86_64.tar.gz	• 适用于 64 位 Linux 系统的 Cell Manager、安装服务器和客户机 • 适用于其他 UNIX 系统 (HP-UX、Solaris、macOS 和 IBM AIX) 的客户机 • 产品信息
Data Protector 软件，UNIX Micro_Focus_DP_*xx.xx*_Unix_Local_Installation_DP_A*xxxx*_Unix_Local_Install.tar.gz	• 适用于 UNIX 系统 (HP-UX、Solaris、macOS 和 IBM AIX) 的客户机仅用于客户机的本地安装 • 产品信息

许可证

有关许可证的信息，请参阅许可证。

系统要求

先决条件

Data Protector 安装程序检查 Cell Manager 安装的以下先决条件:

- 可用磁盘空间不足
- 至少 16 GB 内存 (RAM)
  注意**:** Linux 系统上报告的内存少于安装的物理内存，因为内核将使用一些内存且会预留少量内存。同样，对于在 Linux 中安装 Cell Manager，内存达到 15 GB 即可。
- INET、IDB 和 AS 端口。
- 对于 Linux 上的安装:
  - 用户 hpdp (或等效用户) 本地存在于 /etc/passwd 中，位于专用组 hpdp (或等效组) 中
  - 存在用户 hpdp 的主目录 (例如 /home/hpdp)
    重要说明**:** hpdp 用户对于 Linux Cell Manager 上安装的 Data Protector 的正常运行至关重要。确保在安装期间或安装之后不会删除 hpdp 用户。如果在安装过程中不存在 hpdp 用户，则安装将失败。如果 hpdp 用户在安装后被删除，则您可能会遇到诸如添加用户、IDB 更新问题等任务的问题。
  - 是否支持长文件名。
  - 默认用户 umask 是否设置为 022。
  - 是否已安装基本的命令行计算器 (bc)。
  - 文件处理能力为至少能打开 8192 个文件。请参阅打开文件限制。
- 主机名检查:
  - 主机名或域中的名称不得为单个字符。有关主机名规范，请参阅 RFC 1123。
  - 主机名或域中的名称不得包含下划线 (_)。
  - 主机名全长必须小于或等于 60 个字符。
  - 对于 Windows，NetBIOS 名称的长度必须多于两 (2) 个字符且不超过 15 个字符。
- Windows 操作系统和补丁级别。请参阅 Windows OS 和补丁级别。

必须手动执行以下任务:

- 安装服务器和客户机的主机名的反向查询。
- 在客户机的 sudo 用户文件中，为将用于推送安装的非 root 用户配置无密码访问。
- 检查 C:\ProgramData 文件夹是否添加为 Windows Defender 中的排除项。

以下限制适用：

- 如果安装路径出现以下情况，则无法安装 Data Protector：
  - 包含非 ASCII 字符
  - 包含 "@" 或 "#" 或 "&" 字符
  - 包含以“!”字符结尾的目录
  - 长于 80 个字符
- 如果从具有以上任意字符的路径中升级，则必须将安装迁移到其他目录。

硬件要求

下表描述了安装各种 Data Protector 组件的硬件要求。这些仅为组件的要求。不包括用于操作系统、其分页文件及其他应用程序的空间分配。

Data Protector 组件	处理器	内存	磁盘空间
Cell Manager	4 个 CPU 内核	16 GB 要恢复内部数据库，需要两倍的总 RAM。	1.5 GB + 每个备份文件大约 100 字节 (供 IDB 使用) 如果所选磁盘卷上的可用存储空间不足，可以将其他卷装载到此磁盘卷中的目录，但应在安装之前执行此操作。
磁盘代理		最少：64 MB 推荐: 128 MB	1 GB
介质代理		最少：64 MB 推荐: 128 MB	1 GB
用户界面		512 MB	1 GB
报告服务器	4 个 CPU 内核	16 GB	
文档 (集成帮助)			100 MB

软件要求

- Windows OS 和补丁级别
- 非 root 用户的 sudo 访问权限
- 打开文件限制

Windows OS 和补丁级别

Data Protector 安装程序 (Windows) 在受支持的 OS 版本上检查最低补丁级别。 在安装 Data Protector 之前，确保满足 Windows OS 要求。有关详细信息，请参阅支持矩阵。

Microsoft Visual Studio 2019 可再发行组件要求

Microsoft Visual Studio 2019 Redistributable 与 Data Protector 安装介质捆绑在一起。在 Data Protector 安装期间，安装程序会检查 Microsoft Visual Studio 2019 可再发行组件版本 14.25.28508 或更高版本是否在 Windows 服务器或客户机系统中可用。如果不可用，则 Data Protector 安装程序将安装它。如果早于 14.25.28508 的现有 Microsoft Visual Studio 2019 可再发行版本可用，则 Data Protector 会尝试升级现有的 Microsoft Visual Studio 2019 可再发行组件包。如果其他应用程序正在使用它，升级将失败，从而导致安装程序退出。

在这种情况下，请使用 Microsoft 的 Visual Studio 2019 (x64) 可再发行组件的最新版本。如果以前安装了 Microsoft Visual Studio 2015 或 2017 (x86) 可再发行版本，则建议也应用最新版本的 Visual Studio 2019 (x86) 可再发行版本。完成此操作后，您可以重试安装。

有关安装 Microsoft Visual Studio 2019 可再发行组件的系统要求的详细信息，请参阅 Visual Studio 2019 产品系列系统要求。

非 root 用户的 sudo 访问权限

Data Protector 允许非 root 用户安装 Data Protector 客户机。非 root 用户必须是 SUDO 用户组的成员才能安装 Data Protector 客户机。

要使非 root 用户能够安装 Data Protector 客户机，请配置 SUDO 访问权限。执行以下任务:

- 为 Linux 用户配置 sudo 访问权限
- 为 AIX 用户配置 sudo 访问权限
- 为 HP-UX 用户配置 sudo 访问权限

为 Linux 用户配置 sudo 访问权限

按照以下链接中的步骤为 Linux 用户配置 sudo 访问权限: https://wiki.centos.org/TipsAndTricks/BecomingRoot
请注意，以上链接仅供一般参考。有关配置 sudo 访问权限的更具体信息，请参阅 Linux 供应商文档。

为 AIX 用户配置 sudo 访问权限

按照以下链接中的步骤为 AIX 用户配置 sudo 访问权限: https://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/igi/unixandlinux/install_config/t_suaix.htm

AIX 7.1 不支持非 root 用户推送安装。

为 HP-UX 用户配置 sudo 访问权限

按照以下步骤为 HP-UX 用户配置 sudo 访问权限:

1. 从 HP-UX 移植和存档中心下载与 HP-UX 版本相关的以下包的最新版本，网址为: http://hpux.connect.org.uk。将下载的文件提取到临时位置。
   - gettext
   - libiconv
   - sudo
   - zlib
2. 检查服务器中是否已安装这些包。运行以下命令：
   swlist -l product | grep -i *<packagename>*
   如果已安装这些包，则无需再次安装。
3. 安装下载的包。
4. 创建新用户。运行以下命令：
   useradd –d /home/<userfolder> –s /sbin/sh –m <username>
   例如， useradd –d /home/dpuser –s /sbin/sh –m dpuser
   确保 **.profile** 文件创建于 /home/*<usernfolder>* 路径下。如果不是，请在该路径下创建 .profile 文件。
5. 在 .profile 文件的 PATH 环境变量中设置以下内容:
   PATH=/usr/bin:/usr/sbin:/etc:/usr/local/bin:/usr/sam/lbin:/usr/sbin/acct:
6. 确保用户路径中提供 **sudo** 二进制文件。
7. 配置 sudo 访问权限。
   所有包均安装完毕后，安装路径下会添加以下文件:
   - <install_path>/bin/sudo
   - <install_path>/sbin/visudo
   - <install_path>/etc/sudoers
     使用 **visudo** 编辑器编辑 <install_path>/etc/sudoers 文件，以列出具有 sudo 访问权限的新用户/用户组。
     默认情况下，**sudo** 文件位于 **/usr/local** 文件夹下。将 **PATH** 变量设置为指向此文件夹**: PATH=$PATH:/usr/local/bin:/usr/local/sbin**
8. 将 NOPASSWD 标记添加到 sudoers 文件条目。
   默认情况下，sudo 命令需要对用户进行身份验证。要更改此行为，请按如下所述为二进制文件设置 NOPASSWD 标记:

   ```
   <username>=NOPASSWD:/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,/usr/bin/ls,/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/
   ```

   例如：

   ```
   dpuser=NOPASSWD:/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,/usr/bin/ls,/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,/usr/sbin/userde
   ```

9. 验证 **/etc/sudoers** 文件的语法。运行以下命令：
   visudo -c
   如果语法错误，该命令将返回错误消息。例如 >>> sudoers file: syntax error, line 30 <<< 。调试并解决错误。
10. 为新创建的用户设置密码。运行以下命令：
    passwd dpuser
    在提示符下输入密码。

打开文件限制

在 Cell Manager 主机上，Data Protector 进程可能需要同时打开多个文件。因此，Data Protector 希望将操作系统的打开文件句柄限制至少设置为 8192。为此，请编辑 /etc/security/limits.conf 文件 (Linux) 中的 nofile 参数以添加建议值:

- 对于 **root** 用户: 软限制为 8192 个文件，硬限制为 16384 个文件或更多

- 对于 **hpdp** 用户: 软限制为 8192 个文件，硬限制为 16384 个文件或更多

编辑文件后，建议注销当前会话，然后再次登录以确保安装程序检测到修改后的打开文件限制。

非群集安装的先决条件

非群集模式下的 Windows Cell Manager

- Data Protector 10.00 GUI 的早期版本与最新的 Data Protector Cell Manager 不兼容。
- Data Protector 单元中的所有配置和会话信息文件都存储在 Cell Manager 上。要将该信息传输到另一个系统是很困难的。因此，请确保 Cell Manager 是处于稳定受控环境中的可靠系统。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 如果内存小于 16 Gb，则 Cell Manager 的安装将失败。
- Data Protector Cell Manager 系统不支持主机名中使用下划线 "_"。
- 用于安装的用户帐户必须：
  - 拥有选定目标系统的管理（管理员）特权。
  - 在 Windows 本地安全策略中设置了网络访问用户权限。
- 可以使用本地组策略编辑器 (gpedit.msc) 设置用户帐户特权，方法是导航到 **Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment** 文件夹或咨询您所在组织的网络管理员。
- 默认情况下，Data Protector Inet 服务使用 Windows 本地用户帐户 SYSTEM 运行。然而，如果因各种原因导致 Inet 服务使用 Windows 域用户帐户运行，则必须额外地对其授予以下 Windows 操作系统安全策略权限：
  - 身份验证后模拟客户机

    为此，请执行以下步骤:
    1。转到“开始” >“程序” >“管理工具” 或“开始” >“控制面板” >“管理工具” 。
    2。打开“本地安全策略” >“本地策略” >“用户权限分配” >“身份验证后模拟客户端” 。
    3。在“本地安全设置”选项卡中选择用户帐户，然后单击“确定” 。

    4。关闭“本地策略”和“管理工具”窗口。
  - 替换进程级别令牌

    为此，请执行以下步骤:

    1。转到“开始” >“程序” >“管理工具” 或“开始” >“控制面板” >“管理工具” 。
    2。打开“本地安全策略” >“本地策略” >“用户权限分配” >“替换一个进程级令牌” 。
    3。在“本地安全设置”选项卡中选择用户帐户，然后单击“确定” 。

    4。关闭“本地策略”和“管理工具”窗口。

  有关详细信息，请参阅《Data Protector 帮助》索引: “Inet 用户模拟”。
- 将成为 Cell Manager 的系统必须满足“硬件要求”部分中描述的硬件要求。如果所选磁盘卷上的可用存储空间不足，可以将其他卷装载到此磁盘卷中的目录，但应在安装之前执行此操作。此外:
  - 对于每个并发备份会话，需要 40 MB RAM。例如，如果要运行 1000 个并行备份会话，Cell Manager 上就需要额外的 40 GB RAM。如果 Cell Manager 也用作介质代理，则需要额外系统资源。
  - 系统驱动器具有 2 × size_of_the_biggest_package_to_be_installed + 10 MB 的磁盘空间。
  - 已配置防火墙，以额外接受“远程服务管理”(NP) 连接（端口 445）。
  - 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。协议必须能够解析主机名。计算机名和主机名必须相同。
  - 分配有静态 IP 地址。如果系统配置为 DHCP 客户机，则它的 IP 地址会改变；因此，需要或者为该系统分配一个永久的 DNS 条目（并重新配置它），或者配置 DHCP 服务器，使之为该系统保留一个静态 IP 地址（IP 地址与系统的 MAC 地址绑定）。
  - 确保以下端口可用:
    - 5565 - 在 Data Protector 中执行新安装所需的端口。
    - 5555 - Data Protector 安装升级期间所需的端口。
    - 7112 - 内部数据库服务端口
    - 7113 - 内部数据库连接池程序 (IDB CP) 端口
    - 7116 - 应用程序服务器 (HTTPS AS) 端口
    - 9999 - 应用程序服务器管理端口

    在安装期间可以更改上述服务端口。
  - 如果预计 DC 二进制文件会增长到大于 2 GB (其大小仅受文件系统设置限制)，建议使用 NTFS 文件系统进行存储。
- 要在 Windows Cell Manager 上运行大量会话 (最多 1000 个)，您必须调整某些参数。请参考增加并发备份会话以获取详细说明。
- 要通过 Microsoft 终端服务客户机在 Windows 上安装 Data Protector，请确保要在其上安装 Data Protector 的系统已针对“终端服务器模式” 选择“远程管理”：

1. 在 Windows 控制面板中，单击“管理工具”，然后单击“终端服务配置”。
2. 在“终端服务配置”对话框中，单击“服务器设置”。确保“终端服务”服务器以“远程管理”模式运行。

非群集模式下的 Linux Cell Manager

- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 已启动并正在运行 xinetd 或 systemd 后台程序。如果必须调整由 Data Protector INET 处理的连接数，请参阅增加并发备份会话以获取详细说明。
- 默认情况下 RHEL 8.x 没有 /usr/lib64/libnsl.so.1。必须安装 libnsl-2.28-18.el8.x86_64.rpm，Data Protector 才能正常工作。
- 已在 64 位 Linux 系统 (x86_64) 上安装 32 位 GNU C 库 (glibc)。
- 已安装 net 工具（安装期间需要一些 net 工具实用程序）。
- 默认用户 unmask 必须设置为 022，否则一些 Data Protector 服务可能无法启动。
- 用于安装的用户帐户必须对选定的目标系统具有管理 (root) 特权。
- 将成为 Cell Manager 的系统必须：
  - 安装了受支持的 Linux 操作系统。有关 Cell Manager 所支持的操作系统的列表，请参阅最新支持矩阵。
  - 满足“硬件要求”部分中列出的硬件要求。

    对于每个并行备份会话，需要 40 MB RAM，每个数据段大小 5–8 MB。例如，如果您要运行 60 个并行备份会话，就需要 3 GB RAM + 512 MB 的数据段。

    您可以通过安装 Data Protector 到链接目录中来克服可用磁盘空间不足。
  - Cell Manager 上每个进程的软文件限制至少应为 8192。
  - 有足够的磁盘空间可用于 Data Protector 内部数据库 (IDB)。要恢复内部数据库，需要两倍的总 RAM。1.5 GB 可用磁盘空间 + /var 目录 (其中已存储 IDB) 中每个备份文件大约 100 字节 (供 IDB 使用)。请注意，当前的 IDB 设计允许重新放置数据库二进制文件（如果由于数据库规模增长而需要这么做）。

    如果磁盘卷的可用存储空间不足，则可以使用链接目录，但必须在安装之前先创建这些链接，并确保目标目录存在。
  - TCP/IP 协议已安装，并且正在运行。协议必须能够解析主机名。
  - 可识别 Cell Manager 系统 (如果使用 NIS 服务器)。

    将 Data Protector 信息添加到 NIS 服务器

    注意: 在 NIS 环境中，nsswitch.conf 文件定义了各个配置文件的使用顺序。例如，可以定义是在本地计算机上还是从 NIS 服务器上使用 /etc/inetd.conf 文件。还可以在该文件中插入语句，声明由 nsswitch.conf 文件来控制保留名称的位置。请参见手册页获得详细信息。

    如果已经安装了 Data Protector，则您必须准备 NIS 服务器，然后在同时作为 Data Protector 客户机的每台 NIS 客户机上使用 kill -HUP pid 命令终止相关进程，以重新启动 inet 服务。

    1. 以 root 身份登录到 NIS 服务器。
    2. 如果通过 NIS 管理 /etc/services 文件，将下面的行附加到 /etc/services 文件:

       omni 5565/tcp # Data Protector for Data Protector inet server

       如果端口 5565 不可用，将其替换成其他端口。

       如果通过 NIS 管理 /etc/inetd.conf 文件，将下面的行附加到 /etc/inetd.conf 文件:

       #Data Protector

       omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log
    3. 运行下面的命令，使 NIS 服务器读取文件并更新配置。

       cd /var/yp; make
  - 有以下空闲端口：
    - 5565 - 在 Data Protector 中执行新安装所需的端口。
    - 5555 - Data Protector 安装升级期间所需的端口。
    - 7112 - 内部数据库服务端口
    - 7113 - 内部数据库连接池程序 (IDB CP) 端口
    - 7116 - 应用程序服务器 (HTTPS AS) 端口
    - 9999 - 应用程序服务器管理端口
  - 支持长文件名。要检查文件系统是否支持长文件名，请执行 getconf NAME_MAX DirectoryPath 命令。
  - 已安装基本的命令行计算器 (bc)。

- 已将用户组 hpdp 和该用户组中的专用用户帐户 hpdp 配置为由 Data Protector 使用。
- 已经为 hpdp 用户配置现有主文件夹，否则部分 Data Protector 服务将无法启动。
- hpdp 用户必须能够从系统中已经存在的以下路径访问任何目录:
  - /opt/omni/*
  - /etc/opt/omni/*
  - /var/opt/omni/*
- 建议在存储 Data Protector 内部数据库和预计可增长到大于 2GB 的 DC 二进制文件的文件系统上使用大文件支持 (LFS)。

设置 Linux 内核参数

- 将内核参数 shmmax（最大共享内存段大小) 至少设置为 2.5 GB。要检查此配置，请执行以下命令：

  cat /proc/sys/kernel/shmmax

  要恢复内部数据库，内核参数值应设为以上值的两倍。
- 建议将数据段大小至少设置为 3221225472 字节或 unlimited 。

非群集模式下的 Windows 安装服务器

- 安装了一种受支持的 Windows 操作系统。有关安装服务器所支持的操作系统的详细信息，请参阅最新支持矩阵。
- 有足够的磁盘空间可用于完整的 Data Protector 软件仓库。以下是最低要求：
  - 512 MB 的总 RAM
  - 2 GB 可用磁盘空间
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- TCP/UDP 445。对于新的 Data Protector 客户机推送安装（客户机上没有任何 Data Protector 组件），需要可访问的安装服务器共享。或者，如果无法访问安装服务器库共享，则必须在本地执行初始 Data Protector 客户机安装。
- 5565 - 在 Data Protector 中执行新安装所需的端口。
- 5555 - Data Protector 安装升级期间所需的端口。
- 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。协议必须能够解析主机名。计算机名和主机名必须相同。
- 由于 Windows 操作系统所施加的安全限制，下列条件之一必须属实：
  - 安装服务器和客户机不在同一域中。
  - 安装服务器和客户机在同一域中。
- 如果不在网络上安装适用于 Windows 的安装服务器，则必须通过安装包 (zip) 在本地安装每个 Windows 客户机。
- 如果 Windows 系统上已经安装了安装服务器，那么不可在该系统上远程安装 Data Protector 客户机。要在同一系统上安装“安装服务器”和客户机组件，必须执行本地客户机安装。在安装过程中，选择所有需要的客户机组件和安装服务器组件。

非群集模式下的 Linux 安装服务器

要成为安装服务器，系统必须满足以下要求:

- 已安装 HP-UX 或 Linux 操作系统。有关安装服务器所支持的操作系统的详细信息，请参阅支持矩阵。
- 已启动并正在运行 inetd 、 xinetd 或 systemd 后台程序。
- 默认情况下 RHEL 8.x 没有 /usr/lib64/libnsl.so.1 。必须安装 libnsl-2.28-18.el8.x86_64.rpm ，Data Protector 才能正常工作。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 端口号 5555/5565（默认）可用。
- TCP/IP 协议已安装，并且正在运行。协议必须能够解析主机名。
- 有足够的磁盘空间可用于完整的 Data Protector 软件仓库。以下是最低要求：
  - 1 GB 的总 RAM
  - 安装或升级时，有 5 GB 的可用磁盘空间
- 您需要 root 访问权限或具有 root 特权的帐户。
- Data Protector 单元中的 Cell Manager 必须为最新版本。
- 要将 Data Protector 安装到链接目录中，例如：
  - /opt/omni/ -> /prefix/opt/omni/
  - /etc/opt/omni/ -> /prefix/etc/opt/omni/
  - /var/opt/omni/ -> /prefix/var/opt/omni/

  请在安装之前创建这些链接，并确保目标目录存在。
- 要通过网络从某个设备安装软件，需要先在计算机上装载源目录。

群集感知安装的先决条件

群集模式下的 Cell Manager

安装前确保所有节点都满足先决条件。如果任何节点的内存小于 16 GB，则该节点上的安装将失败。

Serviceguard 群集

在 Serviceguard 上安装 Data Protector Cell Manager 之前，请检查以下各项:

- 决定哪些系统将作为主 Cell Manager 和辅助 Cell Manager。它们全部都必须安装 Serviceguard，并且必须配置为群集成员。建议至少为每个 Data Protector Cell Manager 包设置一个专用的辅助节点。
- 在主节点和每个辅助节点上，都必须安装 Data Protector Cell Manager (带有建议的补丁)，以及要在群集中部署的集成的所有其他 Data Protector 软件组件。
- 如果 Cell Manager 需要以群集感知模式运行，请注意应对许可证使用虚拟服务器 IP 地址。
- 用户组 hpdp 和专用用户帐户 hpdp 在两个节点上必须具有相同 ID。
- 在此群集环境中，Data Protector Cell Manager 应有自己的包。在 Serviceguard 中安装 Data Protector Cell Manager 之前，需要从网络管理员处获得以下信息:
  - 虚拟服务器名称（群集包中指定的主机名）
  - 包 IP 或虚拟 IP 地址
- 确保群集节点和包 IP（虚拟 IP）位于相同的子网上。
- 如果环境中有 DNS，则确保将群集中的所有节点和包 IP 都注册到 DNS 服务器。
- 在多单元环境 (MoM) 中，所有 Cell Manager 必须安装相同的 Data Protector 版本。

此外，配置 Cell Manager 包必须满足以下先决条件:

- 在两个群集节点上都应安装并配置了 Data Protector Cell Manager。
- 配置 Data Protector 群集包之前，应创建并编辑一个群集配置文件。

旧包配置始终包括 2 个文件，包配置文件和包控制脚本。旧包配置文件作为 ASCII 文件创建，然后使用 cmapplyconf 命令存储在二进制 Serviceguard 配置中。模块化包配置文件将所有包文件系统、装载点和服务定义包含在单个文件中，该文件使用 cmapplyconf 命令存储在二进制 Serviceguard 配置中。在运行此命令之前，确保 Data Protector 后台程序不再在任一群集节点上运行。

Veritas Cluster

在 Veritas 群集上安装 Data Protector Cell Manager 之前，必须符合以下先决条件:

- 确定主和辅助 Cell Manager 系统。它们全部都必须安装 Veritas Cluster Server，并且必须配置为群集成员。
- 在主节点和每个辅助节点上，都必须安装 Data Protector Cell Manager (带有建议的补丁)，以及要在群集中部署的集成的所有其他 Data Protector 软件组件。
- 用户组 hpdp 和专用用户帐户 hpdp 在两个节点上必须具有相同 ID。
- 在群集环境中，Data Protector Cell Manager 必须具备其自己的群集服务组，该服务组必须在群集感知 Cell Manager 配置之前创建和准备。在 VCS 中安装 Data Protector Cell Manager 之前，您需要获取虚拟服务器名称及相应的 IP。之后，该服务器名称或 IP 用作 Data Protector Cell Manager 虚拟服务器名称或 Data Protector 服务组 IP。
- 确保群集节点和 Data Protector 服务组 IP（虚拟 IP）位于相同的子网上。

  注意: 确保 Data Protector 服务组 IP 和 Veritas Cluster IP 不同。
- 如果环境中有 DNS，则确保将群集中的所有节点和 Data Protector 服务组 IP 都注册到 DNS 服务器。
- 完成安装之后，必须对已安装的主 Cell Manager 和辅助 Cell Manager 以及 Cell Manager 包进行配置。
- 要为 Data Protector Cell Manager 准备群集服务组，必须使用以下资源创建群集 (Data Protector) 服务组:
  - IP 群集资源 - 是指用于 IP 资源配置的虚拟 IP。
  - 装载群集资源 — 是指带有相应从属资源的装载资源，用于控制共享卷，在共享磁盘上创建，可通过所有节点访问，其中可能运行 Data Protector。该共享卷用于节点之间共享的 Data Protector 配置和数据文件。

Microsoft 群集服务器

安装群集感知 Data Protector Cell Manager 之前，必须符合以下先决条件：

- 必须在所有群集节点上都正确安装了群集功能。例如，必须能够根据需要多次将组从一个节点移动到另一个节点，而不会产生有关共享磁盘的问题。
- 确保群集上不存在具有以下名称的资源：

  OBVS_MCRS 、 OBVS_HPDP_AS 、 OBVS_HPDP_IDB 、 OBVS_HPDP_IDB_CP 和 OmniBack_Share 。

  Data Protector 将这些名称用于 Data Protector 虚拟服务器。如果存在此类资源，请删除或重命名它们。

  可以通过以下步骤完成该操作：

  1. 单击“开始” >“程序” >“管理工具” >“群集管理员” 。
  2. 检查资源列表，并根据需要删除或重命名这些资源。
- 至少应为群集中的一个组定义文件群集资源。Data Protector 会将其某些数据文件安装在此文件群集资源中的某个特定文件夹下。数据文件安装在用户安装时选择的共享文件夹下的“文件服务器”资源中。

有关如何定义文件群集资源的说明，请参见特定于群集的文档。请注意，文件群集资源的文件共享名称不能为 OmniBack 。

- 如果与文件群集资源相同的组中不存在虚拟服务器，则使用免费注册的 IP 地址和与之关联的网络名称来创建新的虚拟服务器。
- Data Protector 要安装到的文件群集资源必须在文件群集资源依赖关系中设置 IP 地址 、网络名称 和物理磁盘 。这可确保 Data Protector 群集组能够在独立于任何其他组的任意节点上运行。
- 应当只有群集管理员有权访问文件群集资源的共享文件夹，并且它们应具有对于共享文件夹的完全访问权。
- 在所有群集节点上，Data Protector 将安装在相同的位置（驱动器和路径名）。请确保这些位置可供使用。
- 如果从网络共享启动群集感知 Cell Manager 安装，则必须从所有群集节点都能访问此共享。
- 请确保在任何群集节点上，不运行任何其他基于 Microsoft Installer 的安装。
- 群集的每个系统（节点）应正在运行，并且正常工作。
- 安装程序必须使用文件群集资源处于活动状态的系统（节点）上的群集服务帐户启动，以便可以直接访问文件群集资源的共享文件夹。可以使用群集管理器确定资源所有者（其中资源处于活动状态的系统）。
- 要正确安装和配置群集感知 Data Protector Cell Manager，必须在安装期间提供具有以下用户权限的域帐户：
  - Cell Manager 系统上的管理员权限
  - 群集中的 Cluster Administrator 权限
  - 密码永不过期
  - 作为服务登录
  - 用户无法更改密码
  - 允许所有登录时间

  重要说明: 对于 Microsoft 群集服务器安装，需要在所有群集系统（节点）上都具有管理员权限的帐户。您还应使用此帐户来安装 Data Protector。否则会导致 Data Protector 服务以普通模式而非群集感知模式运行。
- 在所有群集节点上必须赋予用于 Inet 服务的 Windows 域用户帐户以下 Windows 操作系统安全策略特权：
  - 身份验证后模拟客户机
  - 替换进程级别令牌

除了上述先决条件外，还必须准备在 Windows Server 2008、Windows Server 2012 和 Windows Server 2016 上运行的 Microsoft 群集服务器，这样才能安装 Data Protector。如果未准备，可能会导致备份本地的 CONFIGURATION 对象 (该对象必须在准备期间予以备份，以便进行灾难恢复) 会话失败，甚至有可能导致数据丢失。有关支持的 Data Protector 单元角色与群集 Windows 操作系统版本的组合的信息，请参阅最新支持矩阵。请确保您已使用域用户帐户登录到系统。域用户帐户必须是本地 Administrators 组的成员。

执行以下步骤来准备群集节点:

1. 在两个群集节点上，启动 Windows 防火墙，并为“文件和打印机共享” 程序启用例外。
2. 在活动的群集节点中，启动“故障转移群集管理 (Failover Cluster Management)”，并验证 quorum 资源中的见证磁盘是否已联机。如果该资源已脱机，请将它联机。

   仅在活动的群集节点中执行以下步骤。
3. 如果正在准备尚未配置多数节点集 (MNS) 的群集，请启动 Windows 资源管理器，并将 WitnessDiskLetter:\Cluster 文件夹的所有权更改为本地 Administrators 组。在“群集的高级安全性设置”窗口中更改所有权时，请确保已选中“替换子容器及对象的所有者” 选项。在“Windows 安全性”对话框中，通过单击“是” 确认建议操作，然后再通过单击“是” 来确认通知。
4. 如果正在准备尚未配置 MNS 的群集，请在 Windows 资源管理器中将 SYSTEM 和本地 Administrators 组对 WitnessDiskLetter:\Cluster 文件夹的权限更改为允许完全控制。
5. 如果要准备将承担 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理”中添加“群集访问点” 资源。选择“添加资源” ，然后单击“1- 客户端访问点” 以启动“新建资源”向导:
   1. 在“客户机访问点 (Client Access Point)”窗格中，在“名称 (Name)”文本框中输入虚拟服务器的网络名称。
   2. 在“地址 (Address)”文本框中，输入虚拟服务器的 IP 地址。
6. 如果在准备一个将执行 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理 (Failover Cluster Management)”中，将一个共享文件夹添加到群集。单击“添加共享文件夹” 以启动“设置共享文件夹”向导:
   a. 在“共享文件夹位置 (Shared Folder Location)”窗格上的“位置 (Location)”文本框中，输入目录路径。请确保所选目录具有足够的可用空间，可以存储在 Data Protector 安装过程中创建的数据。单击“下一步” 。
   b. 在“NTFS 权限 (NTFS Permissions)”、“共享协议 (Share Protocols)”和“SMB 设置 (SMB Settings)”窗格中，保留默认选项值不变。单击“下一步” ，移到下一个窗格。
   c. 在“SMB 权限”窗格上，选中“管理员拥有完全控制权限，所有其他用户和组只有读取访问权限” 选项。单击“下一步” 。
   d. 在“DFS 名称空间发布 (DFS Namespace Publishing)”中，保留默认选项值。单击“下一步” 。
   e. 在“查看设置”和“创建共享”窗格中，单击“创建” 。

客户机安装的先决条件

RAM 和磁盘空间要求

客户机系统组件	RAM (MB)	磁盘空间 (MB)
磁盘代理	64（推荐 128）	1 GB
介质代理	64（推荐 128）	1 GB
集成组件	64（推荐 128）	20 MB
英语文档 (脱机帮助)	不适用	95 MB

Windows 客户机

要安装 Windows 客户机，必须具有管理员权限。要成为未来的 Data Protector 客户机系统，Windows 系统必须满足以下要求：

- 有足够的磁盘空间可用于 Data Protector 客户机软件。
- 端口号 5555/5565（默认）可用。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。协议必须能够解析主机名。计算机名和主机名必须相同。
- 确保在 Windows 本地安全策略下，为执行安装的帐户设置网络访问用户权限。
- 在安装 Data Protector 之前，检查系统上是否已安装 Microsoft Installer (MSI) 2.0。如果已安装了早期版本，建议先升级到 2.0 版本，再开始 Data Protector 安装。如果事先不升级 MSI，Data Protector 安装向导会自动升级到所需的版本。在这种情况下，Data Protector 会相应地通知您有关 MSI 升级的情况。
- 如果 MSI 已升级，强烈建议重新启动系统。

HP-UX 客户机

- 此时，您应当已在网络上安装了适用于 Linux 的 Cell Manager 和安装服务器。
- 您将需要 *root* 访问权或具有 *root* 权限的帐户。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 对于 HP-UX 11.11，需要 IPv6NCF11i 软件包或者 TOUR/IPv6 支持来启用 Internet 协议版本 6 (IPv6)。
- UNIX 系统上 Data Protector 客户机组件的 RAM 和磁盘空间要求。

  下表列出了 Data Protector UNIX 系统上不同客户机组件的最低 RAM 和磁盘空间要求。这些数字只表示组件的要求。数字不包括操作系统、分页文件或其他应用程序的空间分配。

客户机系统组件	RAM (MB)	可用磁盘空间 (MB)
磁盘代理	每个 64（建议 128）	每个 20
介质代理		
集成组件		
英语文档（指南、帮助）	不适用	100

Solaris 客户机

- 安装介质代理时，确保以下条目位于文件 /etc/system 中:

  ```
  set semsys:seminfo semmni=100
  ```

- 此时，您应当已在网络上安装了适用于 Linux 的 Cell Manager 和安装服务器。
- 要安装 Solaris 客户机，您需要 *root* 访问权或具有 *root* 权限的帐户。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。

Linux 客户机

- 必须在 64 位 Linux 系统 (x86_64) 上安装 32 位 GNU C 库 (glibc) 包。
- 此时，您应当已在网络上安装了适用于 Linux 的 Cell Manager 和安装服务器。
- 必须安装并设置 rpm 实用程序。其他打包系统 (例如 deb) 不受支持。
- 要在远程系统上安装 Data Protector 组件，远程系统必须满足以下先决条件:

- inetd 、 xinetd 或 systemd 服务必须正在运行或已安装，这样 Data Protector 才能够启动它。
- 默认情况下 RHEL 8.0 没有 /usr/lib64/libnsl.so.1 。必须安装 libnsl-2.28-18.el8.x86_64.rpm ，Data Protector 才能正常工作。
- 应为客户机配置了无密码身份验证或 ssh 。

- 确保内核支持 SCSI 设备 (模块 SCSI support 、 SCSI tape support 、 SCSI generic support)。 Probe all LUNa on each SCSI device 参数为可选。

  关于 Linux 内核中 SCSI 支持的详细信息，请参见 Linux 分发文档或者 Linux 内核文档。

- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。

注意: Data Protector 使用默认端口号 5555/5565。因此，其他程序不应使用该特定端口号。一些 Linux 操作系统分发版本将该端口号用于其他用途。如果端口号 5555/5565 已在使用，则应使之可供 Data Protector 使用，或者也可以将默认端口号更改为某个未用端口号。

IBM AIX 客户机

- 有关系统要求、磁盘空间要求、受支持的平台和 Data Protector 组件，请参阅支持矩阵。
- 此时，您应当已在网络上安装了适用于 Linux 的 Cell Manager 和安装服务器。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。
- 在安装磁盘代理 组件之前，请检查端口映射器是否已在选定系统上启动并正在运行。 /etc/rc.tcpip 文件中必须存在用于启动端口映射器的行:

  ```
  start /usr/sbin/portmap “$src_running”
  ```

  如果 srcmstr 后台程序正在运行，则 src_running 标志会设置为 1。 srcmstr 后台程序是系统资源控制器 (System Resource Controller, SRC)。 srcmstr 后台程序可以派生并控制子系统、处理子系统短状态请求、向子系统传递请求，以及处理错误通知。

HPE OpenVMS 客户机

在 OpenVMS 平台上安装 Data Protector 客户机之前，请检查以下方面：

- 确保装有 TCP/IP 传输协议并正在运行。
- 通过执行命令 SYS$MANAGER:UTC$TIME_SETUP.COM 设置系统的 TIMEZONE 功能。
- 登录到 OpenVMS 系统的 SYSTEM 帐户。请注意，您必须具有相应的权限。
- 确保您有权访问含有 HP OpenVMS 客户机安装程序包的 Data Protector 安装程序包 (zip/tar)。
- 对于 Data Protector 单元中所有 Data Protector 组件，建议在主机名解析过程中执行反向 DNS 查询。

ADIC/GRAU 库介质代理

在系统上安装介质代理之前，必须满足以下安装先决条件：

- ADIC/GRAU 库必须已配置，并且正在运行。请参见 ADIC/GRAU 库随附的文档。
- DAS 服务器必须已启动并正在运行。

  要控制 ADIC/GRAU 库，DAS 软件是必需的。每个 DAS 客户机上必须安装 DAS 客户机软件。由 Data Protector 启动的每个介质和设备相关操作首先从 DAS 客户机传送到 DAS 服务器。然后，它被传递给 ADIC/GRAU 库的内部部分 (AMU - AML Management Unit)，该部分控制机械手和移动或加载介质。操作完成之后，DAS 服务器会答复 DAS 客户机。请参见 ADIC/GRAU 库随附的文档。

- 安装介质代理之前，必须先获取以下信息：
  - DAS 服务器（在 OS/2 主机上运行的应用程序）的主机名。
  - 可用驱动器的列表，以及驱动器相应的 DAS 名称。获取的驱动器名称将在 Data Protector 中配置 ADIC/GRAU 驱动器时使用。

    如果已经为 ADIC/GRAU 系统定义了 DAS 客户机，则可以使用以下 dasadmin 命令之一获取该列表:

    ```
    dasadmin listd2 client
    ```

    ```
    dasadmin listd client
    ```

    其中， client 是要显示为其保留的驱动器的 DAS 客户机。

    dasadmin 命令可以从 OS/2 主机上的 C:\DAS\BIN 目录中调用；或者，如果安装在其他系统上，则可以从安装了 DAS 客户机软件的目录中调用。在 UNIX 客户机系统上，该目录通常为 /usr/local/aci/bin 系统目录。

  - 可用“插入/弹出区域”的列表，以及相应的格式规范。

    在 OS/2 主机上，可以在 AMS (AML Management Software) 的“图形配置”中获得可用“插入/弹出区域”的列表：

    1. 从“管理”>“配置” 菜单启动该配置。
    2. 通过双击“I/O 单元” 图标，打开“EIF 配置” 窗口，然后单击“逻辑范围” 字段。在文本框中，将会列出可用的“插入/弹出区域”。

       注意: 一个 Data Protector 库设备只能处理一种介质类型。记住哪种介质类型属于每个指定的“插入/弹出区域”非常重要，因为稍后将需要该数据来为 Data Protector 库配置“插入/弹出区域”。

  - 驱动器的 UNIX 设备文件列表（如果要在 UNIX 系统上安装介质代理）。

    在系统上运行 ioscan -fn 系统命令以显示所需的信息。

  - 驱动器的 SCSI 地址的列表（如果要在 Windows 系统上安装介质代理）。例如 scsi4:0:1:0 。

StorageTek 库介质代理

安装介质代理之前，必须满足以下安装先决条件：

- StorageTek 库必须已配置，并且正在运行。请参见 StorageTek 库随附的文档。
- 必须安装并配置 Data Protector。
- 开始安装介质代理软件之前，必须先获取以下信息：
  - 运行 ACSLS 的主机的主机名。
  - 要用于 Data Protector 的 ACS 驱动器 ID 的列表。获取的驱动器 ID 在 Data Protector 中配置 StorageTek 驱动器时使用。要显示列表，请登录运行 ACSLS 的主机，并执行以下命令：

    rlogin “ACSLS hostname” -l acssa

    您需要输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：

    ACSSA> query drive all

    ACS 驱动器的格式规范必须为以下形式：

    ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
  - 可用 ACS CAP ID 的列表和 ACS CAP 格式规范。要显示列表，请登录运行 ACSLS 的主机，并执行以下命令：

    rlogin “ACSLS hostname” -l acssa

    输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：

    ACSSA> query cap all

    ACS CAP 的格式规范必须为以下形式：

    ACS CAP: ID:#,#,# - (ACS num, LSM num, CAP num)
  - 驱动器的 UNIX 设备文件列表（如果要在 UNIX 系统上安装介质代理）。

    在系统上运行 ioscan -fn 系统命令以显示所需的信息。
  - 驱动器的 SCSI 地址的列表（如果要在 Windows 系统上安装介质代理）。例如 scsi4:0:1:0 。
- 确保将用于 Data Protector 的驱动器处于 online 状态。如果某个驱动器不处于 online 状态，则在 ACSLS 主机上使用以下命令更改状态: vary drive drive_id online
- 确保将用于 Data Protector 的 CAP 处于 online 状态，并处于 manual 工作模式。

  如果某个 CAP 未处于 online 状态，则使用以下命令更改状态:

  vary cap cap_id online

  如果某个 CAP 未处于 manual 工作模式，则使用以下命令更改模式:

  set cap manual cap_id

群集感知客户机 - Microsoft 群集服务器

安装群集感知 Data Protector 客户机之前，必须满足以下先决条件：

- 必须在所有群集节点上都正确安装了群集功能。例如，必须能够根据需要多次将组从一个节点移动到另一个节点，而不会产生有关共享磁盘的问题。
- 群集的每个系统应正在运行，并且正常工作。
- 要支持在服务器群集 (在 Windows Server 2008 或 Windows Server 2012 中运行 Microsoft Cluster Service (MSCS)) 中安装群集感知 Data Protector 客户机，请执行准备在 Windows Server 2008 或 Windows Server 2012 中运行的 Microsoft 服务器群集上安装 Data Protector 中所述的过程。

集成客户机

- 有关系统要求、磁盘空间要求、受支持的平台、处理器和 Data Protector 组件，请参阅支持矩阵。
- 您需要具有许可证才能使用 Data Protector 与数据库应用程序的集成 (VSS 集成除外)。
- 此时，您应当已在网络上安装了 Cell Manager 和安装服务器 (可选，用于进行远程安装)。

在开始安装过程之前，请确定要与集成组件一起在客户机上安装哪些其他 Data Protector 软件组件。

请注意，对于下面说明的情形，需要安装以下 Data Protector 组件：

- 磁盘代理 组件，以便能够通过 Data Protector 备份文件系统数据。您可以将磁盘代理用于以下用途：
  - 对无法使用数据库应用程序备份进行备份的重要数据运行文件系统备份。
  - 对数据库应用程序服务器（例如，Oracle Server 或 Microsoft SQL Server）运行文件系统测试备份。在配置 Data Protector 与数据库应用程序的集成之前，您需要对文件系统备份进行测试，并解决通信和与应用程序及 Data Protector 有关的其他问题。
  - 运行文件系统或磁盘映像的零宕机时间备份。
  - 对于 SAP R/3 ZDB 集成，从备份介质将数据还原到 LAN 上的应用程序系统中。
- 用户界面组件，用于访问 Data Protector 集成客户机上的 Data Protector GUI 和 Data Protector CLI。

- 常规介质代理组件 (如果有与 Data Protector 集成客户机连接的备份设备)。在用于通过 NDMP 服务器访问 NDMP 专用驱动器的 Data Protector 客户机上，需要 NDMP 介质代理 。

适用于 Microsoft Exchange Server 的 Granular Recovery Extension

- 将以下对象安装到所选的 Microsoft Exchange Server 系统：
  - Data Protector MS Exchange Server 2010+ 集成 组件
  - Data Protector MS Exchange Server 2010+ 集成 组件
  - 所有必需的非 Data Protector 组件
- 将 TCP/IP 端口 60000（默认）在所选 Microsoft Exchange Server 系统上保持空闲。

Microsoft Exchange Server 软件
安装以下各项:

- Microsoft Exchange Server

  确保已正确安装和配置 Microsoft Exchange Server 环境。

  有关受支持版本、平台、设备和其他信息，请参阅最新支持矩阵。

  有关安装、配置和使用 Microsoft Exchange Server 的信息，请参见 Microsoft Exchange Server 文档。

- Microsoft 管理控制台 (MMC) 3.0 或更高版本
- .NET Framework 4.5
- Internet 信息服务 (IIS) 6.0 或更高版本

Data Protector 软件
安装以下 Data Protector 组件：

- Data Protector MS Exchange Server 2010+ 集成 组件
- 所有 Microsoft Exchange Server 系统上的 Data Protector MS Exchange Server 2010+ 集成 组件

确保已安装并配置了 Data Protector 备份解决方案，如安装和集成部分中所述。

其他非 **Data Protector** 软件和服务

- 安装 Windows PowerShell 1.0 或更高版本（Windows Management Framework Core 包）
- 不支持除英语以外的 PowerShell 本地化（Windows OS 必须使用英语本地化）。
- 将 TCP/IP 端口 60000（默认）在 Granular Recovery Web 服务上保持空闲。
- 将防火墙配置为允许新端口。

支持的环境

该扩展可与不同 Microsoft Exchange Server 环境中的 Microsoft Exchange Server 集成。

- 独立的 Microsoft Exchange Server 系统（独立环境）
- 多个 Microsoft Exchange 邮箱服务器系统（多个服务器系统）
- Microsoft Exchange Server 的数据库可用性组环境（DAG 环境）

根据 Microsoft Exchange Server 环境，按如下方式安装扩展：

独立环境

所有 Microsoft Exchange Server 服务和数据均安装在单个 Microsoft Exchange 邮箱服务器上，这在小规模环境中已足够。将 MS Exchange Granular Recovery Extension 组件安装到 Exchange 邮箱服务器系统。

多个 **Exchange Server** 系统的环境

您的环境包含多个 Microsoft Exchange Server 数据库。将 MS Exchange Granular Recovery Extension 组件安装到要恢复单个项目的 Exchange 邮箱服务器系统中。

DAG 环境

您的环境最多包含 16 个 Microsoft Exchange 邮箱服务器系统。将 MS Exchange Granular Recovery Extension 组件安装到任何 Microsoft Exchange Server 邮箱角色的系统节点。安装该组件之后，Granular Recovery Extension 图形用户界面 (GUI) 将为 DAG 环境中的所有邮箱服务器节点显示所有邮箱数据库对象。该扩展将自动考虑 DAG 环境的动态行为。

有关 Microsoft Exchange Server 概念的详细信息，请参见 Microsoft Exchange Server 文档。

适用于 Microsoft SharePoint Server 的 Granular Recovery Extension (GRE)

Microsoft 软件包：

安装以下各项:

- Windows Management Framework Core 包
- Microsoft PowerShell 2.0 或更高版本
- Microsoft SQL Server 2008 包:
  - Microsoft SQL Server Native Client
  - Microsoft Core XML Services (MSXML) 6.0
  - Microsoft SQL Server 2008 管理对象集合
- Microsoft SQL Server 2012 包:

- Microsoft SQL Server Native Client
- Microsoft Core XML Services (MSXML) 6.0 或更高版本
- Microsoft SQL Server 2012 管理对象集合

- Microsoft SQL Server 2014 包:
  - Microsoft SQL Server Native Client
  - Microsoft Core XML Services (MSXML) 6.0 或更高版本
  - Microsoft SQL Server 2014 管理对象集合
- Microsoft SQL Server 2016 包:
  - Microsoft SQL Server Native Client
  - Microsoft Core XML Services (MSXML) 6.0 或更高版本
  - Microsoft SQL Server 2016 管理对象集合
- 必须在所有已至少启用以下其中一项服务的 Microsoft SharePoint Server 系统上安装这些包：
  - 管理中心
  - Microsoft SharePoint Foundation Web 应用程序 (Microsoft SharePoint Server 2010/2013)
- 每个 SharePoint Server 系统上只能安装一个版本的 Microsoft SQL Server 管理对象集合。
  - 此 Microsoft SQL Server 管理对象集合的版本号必须与 SharePoint 场所使用的 SQL Server 版本号相同。
  - 如果系统上安装了多个版本的 Microsoft SQL Server 管理对象集合，请删除所有版本，但与 SQL Server 版本相同的版本除外。
  - 可以从以下网站下载包: http://www.microsoft.com/downloads/en/default.aspx。搜索 **Feature Pack for Microsoft SQL Server 2008**、 **Feature Pack for Microsoft SQL Server 2012**、 **Feature Pack for Microsoft SQL Server 2014** 或 **Feature Pack for Microsoft SQL Server 2016**。

Data Protector 软件
安装以下 Data Protector 组件：

- 确保已安装并配置了 Data Protector 备份解决方案，如安装或集成部分中所述。
- 此外，请确保在所有已至少启用以下服务之一的 Microsoft SharePoint Server 系统上安装 Data Protector 用户界面 组件:

SAP R/3 客户机

- 确保安装并配置以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 软件
  - SQL*Plus
- 假设 SAP R/3 Database Server 已启动并正在运行。

Data Protector SAP R/3 集成备份规范与先前版本的 Data Protector 完全兼容。Data Protector 可以运行由先前 Data Protector 版本创建的所有备份规范。在较早版本的 Data Protector 上，无法使用由当前版本的 Data Protector 创建的备份规范。

适用于 VMware vSphere Web 客户机的 GRE

- 您计划用于执行恢复操作的虚拟机必须安装 VMware 工具 4.x 或更高版本。可以从 http://www.vmware.com/download 网页下载 VMware 工具安装包。
- 仅支持远程安装适用于 VMware vSphere 的 Data Protector Granular Recovery Extension Web 客户机。
- 为确保扩展的功能正常，请不要在同一客户机系统上同时安装和配置 VMware vCenter Server 系统和装载代理系统。
- 确保 VMware Granular Recovery Extension 代理 、虚拟环境集成代理 和 Data Protector Cell Manager 为同一版本。不支持混合代理版本。
- 要使用扩展，需要安装和配置以下系统：
  - **Data Protector** 单元和客户机
  - VMware vCenter Server 系统
  - 装载代理系统

GRE 插件可通过 HTML5 GRE Web 插件用户界面进行访问。

P9000 XP 磁盘阵列系列与 Microsoft SQL Server 集成

应用程序系统上必须安装 Microsoft SQL Server。用户数据库必须位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。但是，如果系统数据库也安装在磁盘阵列上，它们必须安装在不同于用户数据库的其他源卷上。

P9000 XP 磁盘阵列系列与 Oracle Server 集成

- 在应用程序系统上，以及使用备份集 ZDB 方法的备份系统上，必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 备份系统上的 Oracle 软件必须安装在与应用程序系统相同的目录中。二进制文件应与应用程序系统上的二进制文件相同。实现方法有，从

应用程序系统将文件和系统环境复制到备份系统，或者使用与应用程序系统上相同的安装参数在备份系统上全新安装 Oracle 二进制文件。

- 应用程序系统上的 Oracle 数据文件必须安装在镜像到备份系统的 P9000 XP 磁盘阵列系列 LDEV 上。

  在使用备份集方法的情况下，如果一些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

  根据 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 的位置，有以下两个可能选项：

  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于不同于 Oracle 数据文件的其他卷组 (如果使用了 LVM) 或源卷。

    默认情况下，此类配置启用即时恢复。

  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于与 Oracle 数据文件相同 的卷组 (如果使用了 LVM) 或源卷。

    默认情况下，此类配置不启用即时恢复。可以通过设置 ZDB_ORA_INCLUDE_CF_OLF 、 ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECK CONF_IR omnirc 选项启用即时恢复。有关详细信息，请参阅 Data Protector 零宕机时间备份集成部分。

  Oracle 归档重做日志文件不一定要位于源卷上。

P9000 XP 磁盘阵列系列与 SAP R/3 集成

- 在应用程序系统上必须安装和配置以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话（BRBACKUP 在备份系统上启动，而不是在应用程序系统上），请配置备份系统。有关详细信息，请参阅 Oracle 的 SAP 数据库部分 (拆分镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件必须位于磁盘阵列上。
  - 对于联机备份，控制文件和联机重做日志不一定要位于磁盘阵列上。联机 SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须位于磁盘阵列上。
  - 对于脱机备份，控制文件和联机重做日志必须位于磁盘阵列上。
  - 归档重做日志文件不一定要位于磁盘阵列上。

  如果 Oracle 控制文件、联机重做日志和 Oracle SPFILE 位于与 Oracle 数据文件相同的 LVM 卷组或源卷上，请设置 Data Protector ZDB_ORA_NO_CHECKCONF_IR 、 ZDB_ORA_INCLUDE_CF_OLF 和 ZDB_ORA_INCLUDE_SPF omnirc 选项。否则，将无法运行“ZDB 到磁盘”和“ZDB 到磁盘 + 磁带”会话。有关详细信息，请参阅 Data Protector 零宕机时间备份集成部分。

  注意: 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

  UNIX 系统： 如果在原始分区（原始磁盘或原始逻辑卷）上安装 Oracle 数据库，请确保应用程序系统和备份系统上的卷/磁盘组名称相同。
- 在 UNIX 系统上，确保应用程序系统上存在以下用户：
  - oraORACLE_SID 具有主组 dba
  - ORACLE_SID adm 在 UNIX 组中 sapsys
- SAP R/3 软件必须正确安装在应用程序系统上。

  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  注意: 目录的位置取决于环境（UNIX 系统）或注册表（Windows 系统）变量。有关详细信息，请参见 SAP R/3 文档。

  - ORACLE_HOME /dbs （UNIX 系统）

    ORACLE_HOME \database (Windows 系统) - Oracle 和 SAP R/3 配置文件
  - ORACLE_HOME /bin or （UNIX 系统）

    ORACLE_HOME \bin (Windows 系统) - Oracle 二进制文件
  - SAPDATA_HOME /sapbackup （UNIX 系统）

    SAPDATA_HOME \sapbackup (Windows 系统) -

    带有 BRBACKUP 日志文件的 SAPBACKUP 目录
  - *SAPDATA_HOME* /saparch (UNIX 系统)

    SAPDATA_HOME \saparch (Windows 系统) - SAPARCH

    带有 BRARCHIVE 日志文件的 SAPARCH 目录
  - SAPDATA_HOME /sapreorg （UNIX 系统）

    SAPDATA_HOME \sapreorg (Windows 系统)
  - SAPDATA_HOME /sapcheck （UNIX 系统）

SAPDATA_HOME \sapcheck（Windows 系统）

- SAPDATA_HOME /saptrace （UNIX 系统）

  SAPDATA_HOME \saptrace（Windows 系统）

- /usr/sap/ORACLE_SID/SYS/exe/run （UNIX 系统）

  c:\Oracle\ORACLE_SID\sys\exe\run （Windows 系统）

注意: 如果计划执行即时恢复，请确保 sapbackup 、 saparch 和 sapreorg 目录位于不同于 Oracle 数据文件的其他源卷上。

UNIX 系统

在 UNIX 系统上，如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。在 UNIX 系统上，目录 /usr/sap/ORACLE_SID/SYS/exe/run 必须由 UNIX 用户 ora *ORACLE_SID* 所有。SAP R/3 文件的所有者必须为 UNIX 用户 ora *ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba 。例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID* adm 所有。

UNIX 示例

如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于:

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011 brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

P9000 XP 磁盘阵列系列与 Microsoft Exchange Server 集成

镜像到备份系统的 P9000 XP 磁盘阵列系列卷 (LDEV) 上的应用程序系统上必须安装 Microsoft Exchange Server 数据库。镜像可以是 BC P9000 XP 或 CA P9000 XP 和安装在文件系统上的数据库。以下对象必须位于被镜像的卷上：

- Microsoft Information Store (MIS)
- （可选）Key Management Service (KMS)
- (可选) Site Replication Service (SRS)

为了能够备份事务日志，请禁用 Microsoft Exchange Server 上的“循环日志记录”。

P9000 XP 磁盘阵列系列与 Microsoft SQL Server 集成

应用程序系统上必须安装 Microsoft SQL Server。用户数据库必须位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。但是，如果系统数据库也安装在磁盘阵列上，它们必须安装在不同于用户数据库的其他源卷上。

非 HPE 存储阵列与 Oracle Server 的集成

- 在应用程序系统上，以及使用备份集 ZDB 方法的备份系统上，必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus

  备份系统上的 Oracle 软件必须安装在与应用程序系统相同的目录中。二进制文件应与应用程序系统上的二进制文件相同。实现方法有，从应用程序系统将文件和系统环境复制到备份系统，或者使用与应用程序系统上相同的安装参数在备份系统上全新安装 Oracle 二进制文件。
- 应用程序系统上的 Oracle 数据文件必须安装在将使用已安装的 Storage Provider（通过 SMI-S 代理）进行复制的源卷上。

  根据 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 的位置，有以下两个可能选项：
  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于不同于 Oracle 数据文件的其他卷组 (如果使用了 LVM) 或源卷。
  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于与 Oracle 数据文件相同 的卷组 (如果使用了 LVM) 或源卷。

  Oracle 归档重做日志文件不一定要位于源卷上。

  如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

与 SAP R/3 的非 HPE 存储阵列集成

- 在应用程序系统上必须安装以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话（BRBACKUP 在备份系统上启动，而不是在应用程序系统上），请配置备份系统。有关详细信息，请参阅 Oracle 的 SAP 数据库部分 (拆分镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件必须驻留在存储系统上。
  - 对于联机备份，控制文件和联机重做日志不必驻留在存储系统上。联机 SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须

驻留在存储系统上。

- 对于脱机备份，控制文件和联机重做日志必须位于存储系统上。
- 归档重做日志文件不必驻留在存储系统上。

注意: 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

UNIX 系统： 如果在原始分区（原始磁盘或原始逻辑卷）上安装 Oracle 数据库，请确保应用程序系统和备份系统上的卷/磁盘组名称相同。

- 在 UNIX 系统上，确保应用程序系统上存在以下用户：
  - oraORACLE_SID 具有主组 dba
  - ORACLE_SID adm 在 UNIX 组中 sapsys
- SAP R/3 软件必须正确安装在应用程序系统上。

  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  注意**:** 目录的位置取决于环境（UNIX 系统）或注册表（Windows 系统）变量。有关详细信息，请参见 SAP R/3 文档。
  - ORACLE_HOME /dbs（UNIX 系统）*ORACLE_HOME*\database（Windows 系统）- Oracle 和 SAP 配置文件
  - ORACLE_HOME /bin（UNIX 系统）*ORACLE_HOME*\bin（Windows 系统）- Oracle 二进制文件
  - SAPDATA_HOME /sapbackup（UNIX 系统）*SAPDATA_HOME*\sapbackup（Windows 系统）- 带有 BRBACKUP 日志文件的 SAPBACKUP 目录
  - SAPDATA_HOME /saparch（UNIX 系统）SAPDATA_HOME\saparch（Windows 系统）- 带有 BRARCHIVE 日志文件的 SAPARCH 目录
  - SAPDATA_HOME /sapreorg（UNIX 系统）*SAPDATA_HOME*\sapreorg（Windows 系统）
  - SAPDATA_HOME /sapcheck（UNIX 系统）*SAPDATA_HOME*\sapcheck（Windows 系统）
  - SAPDATA_HOME /saptrace（UNIX 系统）SAPDATA_HOME\saptrace（Windows 系统）
  - /usr/sap/ORACLE_SID/SYS/exe/run （UNIX 系统）

    c:\Oracle\ORACLE_SID\sys\exe\run （Windows 系统）

  UNIX 系统

  在 UNIX 系统上，如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。在 UNIX 系统上，目录 /usr/sap/ORACLE_SID/SYS/exe/run 必须由 UNIX 用户 ora *ORACLE_SID* 所有。SAP R/3 文件的所有者必须为 UNIX 用户 ora *ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba。例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID*adm 所有。

  UNIX 示例

  如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于:

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011 brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

与 Microsoft SQL Server 的非 HPE 存储阵列集成

应用程序系统上必须安装 Microsoft SQL Server。用户数据库必须位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。但是，如果系统数据库也安装在磁盘阵列上，它们必须安装在不同于用户数据库的其他源卷上。

安装 Data Protector 服务器

本节提供有关安装 Data Protector 服务器的信息:

以非群集模式安装 Cell Manager

以下各节提供有关如何在 Windows 和 UNIX 服务器上安装 Cell Manager 的逐步说明。

在 Windows 系统上安装

执行以下步骤，在 Windows 系统上安装新的 Cell Manager 实例:

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 setup.exe 文件。
2. 按照安装向导操作，并仔细阅读许可协议。如果接受协议的条款，则单击**下一步 (Next)** 继续。
3. 查看“过时信息”页面中的详细信息，然后单击“我了解对所支持平台的更改”，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在“安装类型”页中，选择 **Cell Manager**，然后单击“下一步”以安装 Data Protector Cell Manager 软件。
5. 提供 Data Protector 服务运行所使用的帐户的用户名和密码。

   单击**下一步 (Next)** 继续。
6. 单击**下一步 (Next)** 将 Data Protector 安装到默认安装文件夹中。

   或者单击“更改 (Change)”打开“更改当前目标文件夹 (Change Current Destination Folder)”或“更改当前程序数据目标文件夹 (Change Current Program Data Destination Folder)”对话框，然后根据需要更改安装文件夹。程序数据安装文件夹的路径不应超过 80 个字符。
7. 在“组件选择”页中，选择要安装的组件。

   默认情况下选择了“磁盘代理”、“常规介质代理”、“用户界面”和“安装服务器”。单击“下一步”。
8. 查看先决条件检查状态。Data Protector 安装程序将检查可用内存、主机名和主机名/NetBIOS 长度。如果这些检查中的任何一个失败，安装程序将显示“其中一个先决条件未满足。安装将退出。 ”消息并退出安装。解决问题，然后重新开始安装。有关详细信息，请参见 Data Protector 安装程序检查。

   单击**下一步 (Next)** 继续。
9. 查看以下安全选项：
   - 启用安全数据通信：此选项启用安全的数据通信。
   - 启用审核日志：此选项启用审核日志。您可以选择保留审核日志的期限（月）。默认情况下，审核日志保留时间设置为 90 个月。
     - 审核日志保留：此选项指定在清除之前将审核日志文件保留多长时间（月数）。每月清除一次审核日志，这意味着在指定的月份数后将删除整个月的会话信息。默认情况下，审核日志将保留 90 个月。如果该值设置为 0，则禁用审核日志清除。指定审核日志保留最大值是没有限制的，但是，Micro Focus 建议将该值限制为 99 年（1188 个月）。

   单击**下一步 (Next)** 继续。

   这些选项会为新安装默认选中。如果要从旧版本的 Data Protector 升级，则基于源版本中全局变量“EnableSecureDataCommunication” 和 “AuditLogEnable” 的值来启用/禁用安全数据通信和审核日志。

   Micro Focus 建议启用安全的通信和审核日志保留。如果您未选择任何一个或两个选项，则会显示以下消息： Are you sure you want to proceed? By not selecting these options, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By not using this option, you understand and agree to assume all associated risks and hold Micro Focus harmless for the same.

   - 单击“是”继续，而无需执行任何操作。
   - 单击“否”以选择安全选项。单击“下一步” 继续。
10. 此外，还可以更改 Data Protector IDB 和应用程序服务器所使用的用户帐户，以及这些服务所使用的端口。

    单击“下一步”。
11. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，“最初，允许新注册的 Data Protector 可执行文件按需打开入站端口选项”已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的客户机的 Data Protector，必须在 Windows 防火墙中启用 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。

    单击“下一步”。
12. 组件摘要列表随即显示。单击**安装**开始安装选定组件。这可能需要几分钟时间。
13. “安装状态”页面随即显示。单击“下一步”。
14. 如果已经安装了“用户界面”组件，并要在设置后立即使用 Data Protector GUI 启动，则请选择“启动 Data Protector GUI”。

    单击**完成**。

在典型安装中，Cell Manager 文件位于 Data_Protector_home 目录和 Data_Protector_program_data 中。

> **注意:**在使用 Windows Defender 的系统中安装 Cell Manager 时，Data_Protector_program_data 文件夹将在安装期间添加到 Windows Defender 排除列表中。安装后，将从排除列表中删除 Data_Protector_program_data 文件夹。

软件仓库位于 Data_Protector_program_data\Depot 目录中。

重要说明建议通过命令位置在操作系统配置中扩展相应环境变量值来从任何目录中调用 Data Protector 命令。Data Protector 文档中的步骤假设值已经扩展。

Cell Manager 系统上运行以下进程:

crs	Data Protector 单元请求服务器 (CRS) 服务在 Cell Manager 系统上运行，并在系统上安装 Cell Manager 软件后启动。CRS 负责启动和控制单元中的备份和还原会话。它在 *Data_Protector_home*\bin 目录中运行。
mmd	Data Protector 介质管理后台程序 (MMD) 服务在 Cell Manager 系统上运行，并在系统上安装 Cell Manager 软件后启动。MMD 管理设备和介质管理操作。它在 *Data_Protector_home*\bin 目录中运行。
omniinet	通过 Data Protector 客户机服务，Cell Manager 能够在其他系统上启动代理。Data Protector 单元中的所有系统上都必须运行 Data Protector Inet 服务。它在 *Data_Protector_home*\bin 目录中运行。
kms	Data Protector 密钥管理服务器 (KMS) 服务在 Cell Manager 系统上运行，并在系统上安装 Cell Manager 软件后启动。KMS 为 Data Protector 加密功能提供密钥管理。它在 *Data_Protector_home*\bin 目录中运行。
hpdp-idb	Data Protector 内部数据库服务 (hpdp-idb) 是 IDB 在其中运行的服务。此服务可供需要内部数据库中的信息的进程在 Cell Manager 上以本机方式进行访问。仅在将有关传输的介质管理信息从 Cell Manager 上的 IDB 传输到 Manager-of-Manager (MoM) 上的 IDB 上时，才能远程访问此服务。
hpdp-idb-cp	Data Protector 内部数据库连接池程序 (hpdp-idb-cp) 服务提供了一系列到 hpdb-idb 的开放连接，可以根据需要使用这些连接，无需为每个请求打开一个新连接，从而确保 hpdp-idb 连接的可扩展性。服务在 Cell Manager 上运行，仅可供本地进程访问。
hpdp-as	Data Protector 应用程序服务器 (hpdp-as) 服务用于通过 HTTPS 连接 (Web 服务) 将 GUI 连接到 IDB。在 Cell Manager 上运行，具有到 hpdp-idb-cp 服务的本地连接。

提示如果 Data Protector GUI 未提供相应的编码，您可以安装附加的代码页转换表来正确显示文件名。有关详细步骤，请参见操作系统文档。

如果安装不成功，请确保满足“安装”检查的以下要求:

- Service Pack 版本
- nslookup ，以便 Data Protector 能够展开主机名
- 磁盘空间
- 管理权限

下面的步骤

在此阶段，将安装 Cell Manager，以及适用于 Windows 的安装服务器 (如果已选择)。下一步的任务是：

1. 如果具备混合备份环境，则安装适用于 UNIX 的安装服务器。如果 UNIX 系统不需要安装服务器，则跳过该步骤。
2. 将软件分发到客户机上。

安装在 Linux 系统上

如果在同一系统上安装 Cell Manager 和安装服务器，则可以执行 omnisetup.sh -CM -IS ，在一个步骤中执行安装。

有关 omnisetup.sh 命令的说明，请参阅 tar 包中的 README 文件或 omnisetup.sh 命令页。

要在 Linux 系统上安装 Cell Manager，请执行以下步骤:

1. 复制 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。

LOCAL_INSTALL

platform_dir /DP_DEPOT

其中，*platform_dir* 为 linux_x86_64（对于 Linux 系统）:

2. 转到 LOCAL_INSTALL 目录并执行 ./omnisetup.sh -CM 。

安装完成时，核心 Data Protector 软件位于 /opt/omni/bin 目录中，安装服务器位于 /opt/omni/databases/vendor 目录中。以下列表显示了 Data Protector 子目录及其内容：

/opt/omni/bin	用户命令
/opt/omni/help/C	帮助
/opt/omni/lbin	管理命令、命令行实用程序
/opt/omni/sbin	管理命令、命令行实用程序
/opt/omni/sbin/install	安装脚本
/etc/opt/omni	配置数据
/opt/omni/lib	用于压缩、数据编码和设备处理的共享库
/opt/omni/doc/C	指南采用电子 PDF 格式
/var/opt/omni/log /var/opt/omni/server/log	日志文件
/opt/omni/lib/nls/C	消息编目文件
/opt/omni/lib/man	手册页面
/var/opt/omni/tmp	临时文件
/var/opt/omni/server/db80	IDB 文件 有关详细信息，请参阅 Data Protector 帮助索引: “IDB, 目录位置”。
/opt/omni/AppServer	Data Protector 应用程序服务器。
/opt/omni/idb	Data Protector 内部数据库。
/opt/omni/jre	用于 Data Protector 的 Java 运行时环境。

在 Linux 系统上使用 rpm 安装 Cell Manager

Linux 上的本机安装步骤“仅”适用于使用有限的一组远程安装包安装安装服务器。

1. 复制 Linux 上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到 linux_x86_64/DP_DEPOT 目录。
3. 要安装组件，请执行：

   rpm -i package_name-A.10.30-1.x86_64.rpm

   其中 *package_name* 是相应的子产品包的名称。

   必须安装以下组件：

OB2-CORE	Data Protector 核心软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库。
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境。
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-DISPATCHER	作业控制引擎调度程序
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件。
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。

OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 指南和 WebHelp 格式的《Data Protector 帮助》。

重要说明Linux 上的组件相互依赖。应以上面列出的顺序安装这些组件。

4. 重新启动 Data Protector 服务：

   omnisv stop

   omnisv start

配置自动启动和关闭

Data Protector 安装过程会配置每次系统重新启动时所有 Data Protector 进程的自动启动和关闭。该配置的有些部分与操作系统有关。

它会自动配置以下文件：

Linux 系统：

/etc/init.d/omni
/etc/rcinit_level.d/K10omni
/etc/rcinit_level.d/S90omni

安装完成时，在 Cell Manager 上会有以下进程在运行:

/opt/omni/lbin/crs	Data Protector 单元请求服务器 (CRS) 服务在 Cell Manager 系统上运行，并在系统上安装 Cell Manager 软件后启动。CRS 负责启动和控制单元中的备份和还原会话。
/opt/omni/lbin/mmd	Data Protector 介质管理后台程序 (MMD) 服务在 Cell Manager 上运行，并在系统上安装 Cell Manager 软件后启动。MMD 管理设备和介质管理操作。
/opt/omni/lbin/kms	Data Protector 密钥管理服务器 (KMS) 服务在 Cell Manager 上运行，并且在系统上安装 Cell Manager 软件时启动该服务。KMS 为 Data Protector 加密功能提供密钥管理。
/opt/omni/idb/bin/postgres	Data Protector 内部数据库服务 (hpdp-idb) 是用于运行 IDB 的服务。此服务可供需要内部数据库中的信息的进程在 Cell Manager 上以本机方式进行访问。仅在将有关传输的介质管理信息从 Cell Manager 上的 IDB 传输到 Manager-of-Manager (MoM) 上的 IDB 上时，才能远程访问此服务。
/opt/omni/idb/bin/pgbouncer	Data Protector 内部数据库连接池程序 (hpdp-idb-cp) 服务提供了一系列到 hpdb-idb 的开放连接，可以根据需要使用这些连接，而无需为每个请求打开一个新连接，从而确保 hpdp-idb 连接的可扩展性。服务在 Cell Manager 上运行，仅可供本地进程访问。
/opt/omni/AppServer/bin/standalone.sh	Data Protector 应用程序服务器 (hpdp-as) 服务用于通过 HTTPS 连接 (Web 服务) 将 GUI 连接到 IDB。在 Cell Manager 上运行，具有到 hpdp-idb-cp 服务的本地连接。

设置环境变量

使用 Data Protector 之前，建议您在操作系统配置中扩展特定环境变量的值:

- 要使 Data Protector 手册页可从任何位置进行查看，请添加 /opt/omni/lib/man 到 MANPATH 变量。
- 要使 Data Protector 命令可从任何目录调用，请添加命令位置到 PATH 变量。Data Protector 文档中的步骤假设变量值已经扩展。命令位置列在 omniintro 命令页中。

下面的步骤

在此阶段，将安装 Cell Manager，以及适用于 UNIX 系统的安装服务器 (如果已选择)。下一步的任务是：

1. 安装安装服务器。请参阅以非群集模式安装安装服务器或以群集模式安装安装服务器。
2. 将软件分发到客户机上。请参阅安装 Data Protector 客户机。

以群集模式安装 Cell Manager

本主题包含以下几节:

HPE Serviceguard for Linux

Data Protector 支持 HPE Serviceguard (SG) for Linux。使用在 Linux 系统中安装 Cell Manager 的标准过程安装群集中的所有主机。

安装后，决定哪些系统将作为主 Cell Manager，哪些系统将作为辅助 Cell Manager。按以下顺序配置所安装的主 Cell Manager、辅助 Cell Manager 和 Cell Manager 包:

1. 配置主 Cell Manager
2. 配置辅助 Cell Manager
3. 配置 Cell Manager 包

配置主 Cell Manager

完成以下步骤以配置主 Cell Manager：

1. 在两个 Cell Manager 均可访问的共享磁盘上创建卷组。如果要使用 ob2 磁盘作为群集锁磁盘，则应已为其创建了卷组。
   a. 为新卷组创建一个目录：

      mkdir vg_name

      vg_name 是 /dev 目录的一个子目录中的卷组的路径名。

   b. 列出系统中现有的所有卷组，以检查哪些次要编号正在使用中：

      ll /dev/*/group

   c. 为卷组创建组文件：

      mknod vg_name/group c 64 0xNN0000

      NN 是可用的次要编号。

   d. 在 Data Protector Cell Manager 使用的磁盘上创建物理卷：

      pvcreate -f pv_path ...

      pv_path 与 pvcreate 命令一起使用，指 /dev/rdsk 目录的子目录中的物理卷的字符 (原始) 设备路径名称 (例如物理卷 c0t1d0 的 character pv_path 为 /dev/rdsk/c0t1d0)。

   e. 创建新的卷组：

      vgcreate vg_name pv_path ...

      pv_path 与 vgcreate 命令一起使用，指分配到新卷组的物理卷的块设备路径名称。位于 /dev/dsk 目录的子目录中（例如物理卷 c0t1d0 的 block pv_path 为 /dev/dsk/c0t1d0 ）。

2. 为此组创建逻辑卷。
   a. 为卷组创建新的逻辑卷：

      lvcreate -L lv_size -n lv_name vg_name

      此处提供 /etc/opt/omni 和 /var/opt/omni Data Protector 目录。

      lv_size 是表示分区大小的数字（以 MB 为单位）。

      lv_name 是逻辑卷的名称。

   b. 在逻辑卷上创建日记文件系统：

      newfs -F FStype lv_path

      FStype 指定要在其上进行操作的文件系统类型。

      lv_path 是逻辑卷的字符（原始）特殊设备路径名称。

3. 根据群集文档设置卷组属性。
   a. 从常规模式取消激活卷组：

      vgchange -a n vg_name

   b. 标记供群集使用的卷组：

      vgchange -a y vg_name

4. 创建一个装载点目录（例如 /omni_shared ），然后将逻辑卷装载到此目录：
   a. mkdir shared_dirname
   b. mount lv_path shared_dirname

5. 卸载装载点目录：

   umount shared_dirname

6. 取消激活所创建的卷组：

   vgchange -a n vg_name

7. 导出在主 Cell Manager 上创建的卷组。

   a. 从 system1 导出 LVM 配置信息：

      vgexport -p -m mapfile vg_name

      在这里， mapfile 指定必须将逻辑卷名称和编号写入到的文件的路径名。

   b. 将映射文件传输到 system2：

      rcp mapfile second_system: mapfile

8. 启动群集：

   cmruncl

9. 激活卷组。

   vgchange -a y vg_name

10. 将逻辑卷装载到装载点目录（例如， /omni_shared ）。

    mount lv_path /omni_shared

11. 修改 /etc/opt/omni/server/sg/sg.conf 模板文件。

    SHARED_DISK_ROOT 选项应包含装载点目录的名称（例如 SHARED DISK ROOT=/omni_shared ）。

    CS_SERVICE_HOSTNAME 选项应包含虚拟 Cell Manager 的名称，因为网络已知该名称。群集中的每个包都需要有自己的虚拟 IP 地址及其网络名称（例如 CS_SERVICE HOSTNAME=ob2cl.company.com ）。

12. 配置主 Cell Manager。使用虚拟 IP 地址创建虚拟网络接口 (例如: ifconfig lan0:1 16.57.73.10)，以便激活虚拟 IP 地址。运行脚本时，确保当前位置不在 /etc/opt/omni/ 或 /var/opt/omni/ 目录或其子目录中。还要确保 /etc/opt/omni/ 或 /var/opt/omni/ 中没有装载的子目录。运行：

    /opt/omni/sbin/install/omniforsg.ksh -primary

    注意，运行此脚本之后，已停止 Data Protector 服务，并且随后将重新启动该服务。

    执行脚本后禁用虚拟网络接口 (示例: ifconfig lan0:1 down)。

13. 卸载装载点目录：

    umount dirname

14. 停用卷组：

    vgchange -a n vg_name

配置辅助 Cell Manager

完成以下步骤以配置辅助 Cell Manager：

1. 创建要导入的卷组，并将其导入。

   a. 为新卷组创建一个目录：

      mkdir vg_name

      > **注意** vg_name 是 /dev 目录的子目录包含的卷组的路径名。

   b. 列出系统中现有的所有卷组，以检查哪些次要编号正在使用中：

      ll /dev/*/group

   c. 为卷组创建组文件：

      mknod vg_name/group c 64 0xNN0000

      > **注意** NN 是可用的次要编号。

d. 导入卷组：

vgimport -m mapfile -v vg_name pv_path ...

> **注意** mapfile 是要从中读取逻辑卷名称和编号的文件的名称。
>
> pv_path 是物理卷的块设备路径名称。

2. 设置卷组属性。
   a. 从常规模式取消激活卷组：

      vgchange -a n vg_name

   b. 标记供群集使用的卷组：

      vgchange -a y vg_name

3. 创建装载点目录（与主 Cell Manager 上创建的相同），然后将逻辑卷装载到此目录。
4. 卸载装载点目录：

   umount shared_dirname

5. 取消激活所导入的卷组：

   vgchange -a n vg_name

6. 激活卷组。

   vgchange -a y vg_name

7. 将逻辑卷装载到装载点目录。

   mount lv_path /omni_shared

8. 配置辅助 Cell Manager：

   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname

   其中 dirname 表示装载点或共享目录（例如 /omni_shared ）。

9. 卸载装载点目录：

   umount /omni_shared

10. 停用卷组：

    vgchange -a n vg_name

配置 Cell Manager 包

在主 Cell Manager 节点上执行以下步骤：

1. 检查群集配置文件（例如 cluster.conf ）是否有错误：

   cmcheckconf -C /etc/cmcluster/cluster.conf

   如果有错误，则修复这些错误。

   如果没有错误，则启用该配置：

   cmapplyconf -C /etc/cmcluster/cluster.conf

2. 启动群集（如果尚未启动）：

   cmruncl

3. 创建和修改 Data Protector 群集包文件（配置和控制）。对于模块化包，创建并修改单个群集包文件（配置）。
   a. 在 /etc/cmcluster 目录中创建将容纳 Data Protector 包的目录:

      mkdir /etc/cmcluster/ob2cl

   b. 更改为 /etc/cmcluster/ob2cl 目录：

      cd /etc/cmcluster/ob2cl

   c. 对于旧包，在 Data Protector 包目录中创建包配置文件：

      cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf
      对于模块化包，使用该命令：
      cmmakepkg -m sg/all ob2cl.conf

d. 只需要针对旧包执行此步骤。在 Data Protector 包目录中创建包控制文件：
cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl 。

e. 修改 Data Protector 包配置文件 (例如， /etc/cmcluster/ob2cl/ob2cl.conf)。在 Data Protector 模块化包配置文件中，修改以下字段：

例如：

package_name	ob2cl
run_script_timeout	600
halt_script_timeout	600
script_log_file	/usr/local/cmcluster/conf/ob2cl/ob2cl.log

子网设置如下所示：

例如：

monitored_subnet	10.81.0.0
ip_subnet	10.81.0.0
ip_address	10.81.8.46

注意 monitored_subnet 是包括群集节点的子网。

ip_subnet 是包括 Data Protector Cell Manager 虚拟服务器 IP 的子网。

ip_address 是 Data Protector Cell Manager 虚拟服务器 IP。

Data Protector 服务设置如下所示：

例如：

service_name	dp_svc
service_cmd	/opt/omni/sbin/csfailover.ksh start
service_restart	None
service_fail_fast_enabled	no
service_halt_timeout	300

service_cmd 必须设置为 /opt/omni/sbin/csfailover.ksh start 。

Data Protector 共享的文件系统信息如下所示：

例如：

vg	DP
fs_name	/dev/DP/vol
fs_directory	/DPCLUS
fs_type	ext3
fs_mount_opt	-o rw
fs_umount_opt	""
fs_fsck_opt	""

在 Data Protector 旧包配置文件中，修改以下字段：

PACKAGE_NAME

NODE_NAME

RUN_SCRIPT （与 Data Protector 包控制文件相同。）

HALT_SCRIPT （与 Data Protector 包控制文件相同。）

MONITORED_SUBNET

SERVICE_NAME （您可以输入任何名称，但在控制文件中也必须使用相同名称。）

SERVICE_FAIL_FAST_ENABLED

SERVICE_HALT_TIMEOUT

例如：

PACKAGE_NAME	ob2cl
NODE_NAME	onca
NODE_NAME	pardus
RUN_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl

HALT_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
MONITORED_SUBNET	10.17.0.0
SERVICE_NAME	omni_sv
SERVICE_FAIL_FAST_ENABLED	NO
SERVICE_HALT_TIMEOUT	300

只需要针对旧包执行此步骤。修改 Data Protector 包控制文件 (例如， /etc/cmcluster/ob2cl/ob2cl.cntl)。在 Data Protector 旧包控制文件中，修改以下字段：

VG [n]

LV [n]

FS [n]

FS_MOUNT_OPT [n]

IP

SUBNET

SERVICE_NAME （与配置文件中使用的相同。）

SERVICE_CMD（必须为：/opt/omni/sbin/csfailover.ksh start ）

例如：

VG[0]	vg_dp
LV[0]	/dev/vg_dp/dp_share
FS[0]	/DP_SHARE
FS_MOUNT_OPT[0]	-o rw
FS_TYPE[0]	vxfs
IP[0]	10.17.17.69
SUBNET[0]	10.17.0.0
SERVICE_NAME[0]	omni_sv
SERVICE_CMD[0]	/opt/omni/sbin/csfailover.ksh start

4. 检查和传播 Data Protector 群集包文件。
    1. 对于旧包，将包控制文件复制到群集中称为 system2 的另一个节点:

        remsh system2 "mkdir /etc/cmcluster/ob2cl" rcp /etc/cmcluster/ob2cl/ob2cl.cntl system2: /etc/cmcluster/ob2cl/ob2cl.cntl
    2. 在所有群集节点上将 Data Protector 共享磁盘作为（先前创建的）群集卷组：

        vgchange -a y vg_name
    3. 检查 Data Protector 包：

        cmcheckconf -P /etc/cmcluster/ob2cl/ob2cl.conf
        如果检查成功，则添加 Data Protector 包： cmapplyconf -P /etc/cmcluster/ob2cl/ob2cl.conf
    4. 启动包：

    cmrunpkg ob2cl
    此时应形成群集，并且 Data Protector Cell Manager 包应正常运行。

下面的步骤

完成安装之后，必须将虚拟服务器（在群集包中指定的主机名）导入 Data Protector 单元。

Veritas InfoScale Availability

Data Protector 支持 Veritas InfoScale Availability for Linux。使用在 Linux 系统中安装 Cell Manager 的标准过程安装群集中的所有主机。

如果您已配置 Data Protector 服务组 IP，使用该 IP 进行许可。如果您在配置 Data Protector 服务组时未使用 IP 地址，使用 Veritas Cluster IP 进行许可。

安装后，决定哪些系统将作为主 Cell Manager，哪些系统将作为辅助 Cell Manager。按以下顺序配置所安装的主 Cell Manager、辅助 Cell Manager 和 Cell Manager 群集服务组:

1. 配置主 Cell Manager
2. 配置辅助 Cell Manager
3. 配置 Cell Manager 包

配置主 Cell Manager

完成以下步骤以配置主 Cell Manager：

1. 在主节点上启动 Data Protector 服务组。
2. 修改 /etc/opt/omni/server/sg/sg.conf 模板文件。

   SHARED_DISK_ROOT 选项应包含装载点目录的名称（例如 SHARED DISK ROOT=/omni_shared ）。

   CS_SERVICE_HOSTNAME 选项必须包含虚拟 Cell Manager 的名称，因为网络已知该名称。(例如，CS_SERVICE HOSTNAME=dpvcs.company.com)
3. 配置主 Cell Manager。确保不从 /etc/opt/omni/ 或 /var/opt/omni/ 目录或其子目录执行脚本。还要确保 /etc/opt/omni/ 或 /var/opt/omni/ 目录中未装载子目录。请执行以下命令：

   /opt/omni/sbin/install/omniforsg.ksh -primary

   运行此脚本之后，已停止 Data Protector 服务，并且随后将重新启动该服务。

配置辅助 Cell Manager

完成以下步骤以配置辅助 Cell Manager：

1. 将 Data Protector 服务组切换到辅助节点。
2. 配置辅助 Cell Manager：

   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname

   其中 dirname 表示装载点或共享目录 (例如 /omni_shared)。

配置 Cell Manager 群集服务组

完成以下步骤以配置 Cell Manager 群集服务组：

1. 将 Data Protector 服务组切换回到主节点。
2. 添加群集应用程序资源，该资源将用于监视和控制 Data Protector 服务至 Data Protector 服务组并使用 vcsfailover.ksh 脚本作为应用程序监控或控制程序。例如，

   Application dpapp (

   StartProgram = "/opt/omni/sbin/vcsfailover.ksh start"

   StopProgram = "/opt/omni/sbin/vcsfailover.ksh stop"

   CleanProgram = "/opt/omni/sbin/vcsfailover.ksh stop"

   MonitorProgram = "/opt/omni/sbin/vcsfailover.ksh monitor"

)

   如果 vcsfailover.ksh 脚本需要自定义，必须创建该脚本的副本并用作监视或控制程序。在升级或更新期间，原始脚本被覆盖，必须通过新引入的更改（如有）手动更新自定义的脚本。
3. 创建 Data Protector 应用程序资源。

   使 Data Protector 应用程序资源依赖于装载和虚拟服务器 IP 字段。
4. 启用并启动 Data Protector 应用程序资源。

下面的步骤

完成安装之后：

- 要备份虚拟服务器，应该将其导入到单元。
- 要备份物理节点，也应该将其导入单元。

Microsoft 群集服务器

如果 Cell Manager 需要以群集感知模式运行，请注意应对许可证使用 Cell Manager 的虚拟服务器 IP 地址。

在安装群集感知 Cell Manager 之前，执行以下步骤:

1. 为 Data Protector 应用程序安装创建群集组和资源。
2. 创建共享文件夹，并提供访问该文件夹需要的对群集节点、域管理员和群集资源的共享权限。
3. 检查可能的所有者以便进行故障转移。

> **注意:**在使用 Windows Defender 的系统中安装 Cell Manager 时，Data_Protector_program_data 文件夹将在安装期间添加到 Windows Defender 排除列表中。安装后，将从排除列表中删除 Data_Protector_program_data 文件夹。

本地安装

群集感知 Data Protector Cell Manager 必须从安装包进行本地安装。请执行以下操作：

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 setup.exe 文件。
2. 按照安装向导操作，并仔细阅读许可协议。如果接受协议的条款，则单击**下一步 (Next)** 继续。
3. 查看“过时信息”页面中的详细信息，然后单击“我了解对所支持平台的更改”，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在“安装类型”页中，选择 **Cell Manager**，然后单击“下一步”以安装 Data Protector Cell Manager 软件。
5. 安装程序会自动检测它是否是在群集环境中运行。选择**安装群集感知 Cell Manager** 以启用群集安装程序。

   选择群集组、虚拟主机名，以及 Data Protector 共享文件和数据块将驻留的文件群集资源。

   创建共享文件夹，并提供访问该文件夹需要的对群集节点、域管理员和群集资源的完全控制权限。

   如果选择**仅在该节点安装 Cell Manager**，Cell Manager 将*不是*以群集感知模式运行。
6. 输入将用于启动 Data Protector 服务的帐户的用户名和密码。
7. 单击**下一步 (Next)** 将 Data Protector 安装到默认安装文件夹中。

   或者单击**更改 (Change)** 打开“更改当前目标文件夹 (Change Current Destination Folder)”或“更改当前程序数据目标文件夹 (Change Current Program Data Destination Folder)”对话框，然后根据需要更改安装文件夹。指向程序数据安装文件夹的路径不得超过 80 个字符。
8. 在“组件选择”窗口中，选择要在所有群集节点和群集虚拟服务器上安装的组件。单击“下一步”。

   此时将自动安装 MS 群集支持文件。

   选定组件将安装到所有群集节点上。
9. 查看先决条件检查状态。Data Protector 安装程序将检查可用内存、主机名和主机名/NetBIOS 长度。如果这些检查中的任何一个失败，安装程序将显示“其中一个先决条件未满足。安装将退出。 ”消息并退出安装。解决问题，然后重新开始安装。有关详细信息，请参见 Data Protector 安装程序检查。

   单击**下一步 (Next)** 继续。
10. 查看以下安全选项：
    - 启用安全数据通信：此选项启用安全的数据通信。
    - 启用审核日志：此选项启用审核日志。您可以选择保留审核日志的期限（月）。默认情况下，审核日志保留时间设置为 90 个月。
      - 审核日志保留：此选项指定在清除之前将审核日志文件保留多长时间（月数）。每月清除一次审核日志，这意味着在指定的月份数后将删除整个月的会话信息。默认情况下，审核日志将保留 90 个月。如果该值设置为 0，则禁用审核日志清除。指定审核日志保留最大值是没有限制的，但是，Micro Focus 建议将该值限制为 99 年（1188 个月）。

    单击**下一步 (Next)** 继续。

    这些选项会为新安装默认选中。如果要从 Data Protector 版本升级，则基于源版本中全局变量 “EnableSecureDataCommunication” 和 “AuditLogEnable” 的值来启用/禁用安全数据通信和审核日志。

    Micro Focus 建议启用安全的通信和审核日志保留。如果您未选择任何一个或两个选项，则会显示以下消息： Are you sure you want to proceed? By not selecting these options, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By not using this option, you understand and agree to assume all associated risks and hold Micro Focus harmless for the same.

    - 单击“是”继续，而无需执行任何操作。
    - 单击“否”以选择安全选项。单击“下一步” 继续。
11. (可选) 通过 Data Protector 服务“内部数据库服务”和 Application Server 更改用户帐户或所用的端口。

    单击“下一步”。
12. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，“最初，允许新注册的 Data Protector 可执行文件按需打开入站端口选项”已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的客户机的 Data Protector，必须在 Windows 防火墙中启用 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。

    单击“下一步”。
13. 此时会显示组件选择摘要页面。单击“安装”。
14. 此时会显示“安装设置”页。单击“下一步”。
15. 如果已经安装了 “用户界面”组件，并要在设置后立即使用 Data Protector GUI 启动，则请选择“启动 Data Protector GUI”。
16. 单击“完成”完成安装。

安装适用于 Windows 2012 和 Windows 2012 R2 群集的群集感知 Cell Manager

1. 在不属于群集一部分的计算机上安装 Data Protector 安装服务器。
2. 在其上应用最新的补丁。安装服务器的 ‘\DP_Program_data\Depot’ 中的仓库可用于在 Windows 2012 和 2012 R2 系统中安装群集感知 Cell Manager。
3. 将仓库复制到任一群集节点，并从本地磁盘开始安装。
4. 或者，也可以使用网络共享访问仓库，并从该共享开始安装。对于此步骤，需要考虑以下各项：
   - 安装服务器应当与群集位于相同的域中。
   - 不应使用管理（隐藏）共享（ \\hostname or IP address of IS\c$\... ），因为在某些情况下，它们不可从其他群集节点访问。因此，应当使用正常路径（ \\hostname or IP address of IS\depot ），且所有群集节点均应共享该路径。
   - 群集节点应当无需任何密码即可连接到正常的网络路径。

- 正常的网络路径应当可从浏览器访问，且无需提供凭据。如果提示需要凭据，请输入凭据并选择“记住凭据”。

在带 Veritas Volume Manager 的 Microsoft Cluster Server 上安装 Data Protector

要在带有 Veritas Volume Manager 的 Microsoft Cluster Server (MSCS) 上安装 Data Protector，请先按照在 MSCS 上安装 Data Protector 的常规过程进行操作。安装完成后，还需要一些额外的步骤，以使 Data Protector Inet 服务能区别本地磁盘资源，以及使用自己的资源驱动程序，而不是使用 Microsoft 资源驱动程序的群集磁盘资源:

1. 在 Cell Manager 上执行 omnisv -maintenance 命令以启动维护模式。
2. 按如下所示定义值为 Volume Manager Disk Group 的新环境变量 OB2CLUSTERDISKTYPES ，或者在两个群集节点上设置 omnirc 选项:

   OB2CLUSTERDISKTYPES=Volume Manager Disk Group

   要指定更多专有磁盘资源 (如 NetRAID4 磁盘)，只需将资源类型名称附加到 OB2CLUSTERDISKTYPES 环境变量值即可:

   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
3. 通过执行 omnisv -maintenance —stop 命令退出维护模式。

完成安装过程之后，可以检查 Data Protector 软件是否已正确安装。请执行以下操作：

1. 检查在每个群集节点上，是否为 Data Protector Inet 服务分配了群集服务帐户。确保 Data Protector admin 用户组中也添加了同一用户。登录帐户类型应设置为“本帐户”。
2. 请执行以下命令：

   omnirsh host INFO_CLUS

   其中，*host* 是群集虚拟服务器的名称 (区分大小写)。输出将会列出群集中的系统的名称，以及虚拟服务器的名称。如果输出返回 0 “NONE” ，则说明 Data Protector 不是以群集感知模式安装的。
3. 启动 Data Protector GUI，选择“客户机”上下文，然后单击“MS 群集”。可以看到“结果区域”中列出新安装的系统。

如果需要，请更改运行 Data Protector Inet 和 CRS 服务的帐户。

下面的步骤

完成安装之后，必须将虚拟服务器主机名（群集感知应用程序）导入 Data Protector 单元。

更改 Inet 和 CRS 帐户

如果需要，请更改运行 Data Protector Inet 和 CRS 服务的帐户。

以非群集模式安装安装服务器

安装服务器可以安装在 Cell Manager 系统上或任何通过 LAN 与 Cell Manager 连接的受支持系统上。要将安装服务器保留在独立于 Cell Manager 的系统上，请在本地安装相应的软件仓库。本节介绍详细的过程。

在 Windows 系统上安装

要安装适用于 Windows 系统的安装服务器，请执行以下操作:

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 setup.exe 文件。
2. 按照安装向导操作，并仔细阅读许可协议。如果接受协议的条款，则单击**下一步 (Next)** 继续。
3. 查看“过时信息”页面中的详细信息，然后单击“我了解对所支持平台的更改”，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在“安装类型”页面中，选择“安装服务器”，然后单击“下一步”，安装 Data Protector 软件仓库。
5. 单击“下一步”，在默认文件夹中安装 Data Protector。

   否则，单击**更改**打开“更改当前目标文件夹”窗口并输入新的路径。
6. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，“最初，允许新注册的 Data Protector 可执行文件按需打开入站端口选项”已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的客户机的 Data Protector，必须在 Windows 防火墙中启用 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。

   单击“下一步”。
7. 组件摘要列表随即显示。单击**安装**开始安装选定组件。这可能需要几分钟时间。
8. “安装状态”页随即显示。单击“下一步”。
9. 单击**完成**。

安装完成后，默认情况下将此软件安装到 Data_Protector_program_data\Depot 目录中。该软件设置为共享，以便可以从网络上访问它。

为确保安装文件在从安装服务器复制到新客户机期间不会发生更改，安装服务器和客户机之间的通信使用会话管理块 (Session Management Block, SMB) 网络文件协议。

安装服务器会在第一次远程安装期间设置 SMB 数据包签名。将应用以下策略：

- Microsoft 网络客户机：数字签名通信（始终）
- Microsoft 网络服务器：数字签名通信（始终）

在以下项中，**RequireSecuritySignature** 参数的注册表值将设置为 1：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

远程安装期间会显示以下消息：

Verifying SMB signing at DP IS computer and if necessary starting it...

If SMB related services could not be restarted after making the changes, following message will be displayed

[Critical] SMB (session message block) signing setup failed, please restart DP IS computer and retry.

Do restart the Installation server and retry the installation.

启用 SMB 签名后，如果用户要通过 SMB 从安装服务器主机连接到另一个主机，那么另一个主机也应当启用 SMB 签名。

在第一次远程安装期间，安装服务器禁用 SMBv1。在以下项中，SMB1 参数的以下注册表值将设置为 0：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

如果进行更改后未重新启动与 SMB 相关的服务，则会显示以下消息：

[Critical] SMBv1 disabling failed, please restart Installation Server and retry.

要解决此问题，请重新启动安装服务器，然后重试安装。

下面的步骤
此时，您应当已在网络上安装了适用于 Windows 的安装服务器。现在应执行以下任务：

1. 如果已安装独立的 (例如，不在 Cell Manager 上) 安装服务器，必须将该系统手动添加 (导入) 到 Data Protector 单元中。
2. 如果具有混合备份环境，则安装适用于 Linux 的安装服务器。
3. 将软件分发到客户机上。

安装在 Linux 系统上

要在 Linux 系统上安装安装服务器，请执行以下操作:

1. 复制 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。

   LOCAL_INSTALL

   platform_dir/DP_DEPOT

   其中，*platform_dir* 为： linux_x86_64 (对于 Linux 系统)。

2. 转到 LOCAL_INSTALL 目录并执行：./omnisetup.sh -IS 。

   有关 omnisetup.sh 命令的说明，请参阅 omnisetup.sh 命令页。

安装完成时，Linux 的软件仓库位于 /opt/omni/databases/vendor 目录中。

omnisetup.sh 命令安装含有所有包的安装服务器。要仅安装这些包的一部分，请使用 rpm (适用于 Linux)。

在 Linux 系统上使用 rpm 安装安装服务器

要在 Linux 系统上安装安装服务器，请执行以下操作:

1. 复制 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到包含安装存档的目录 (在此例中是 linux_x86_64/DP_DEPOT)。
3. 对于每个组件，请执行：

   rpm -i package_name-A.10.30-1.x86_64.rpm

   产品中包括以下与 Installation Server 安装相关的组件 (*package_name*)：

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装安装服务器，则已安装该软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器核心软件。
OB2-CFP	适用于 Linux 平台的公用安装服务器核心软件。
OB2-TS-CFP	适用于平台的公用安装服务器技术堆栈软件
OB2-DAP	适用于所有 UNIX 系统的磁盘代理远程安装包。
OB2-MAP	适用于所有 UNIX 系统的介质代理远程安装包。
OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于 Linux 系统的单元控制台远程安装包。

如果是安装独立的安装服务器 (即不在 Cell Manager 上) 且要使用用户界面:

OB2-CC	单元控制台软件。它包含命令行界面。

4. 安装完这些组件后，使用 rpm 为所有将远程安装的组件安装远程安装包。例如：

OB2-INTGP	Data Protector 集成核心软件。该组件为安装集成所必需。

OB2-TS-PEGP	PEGASUS 技术堆栈组件。
OB2-OR8P	Oracle Integration 组件。
OB2-MYSQLP	MySQL 集成组件。
OB2-POSTGRESQLP	PostgreSQL 集成组件。
OB2-SAPP	SAP Integration 组件。
OB2-SAPDBP	SAP MaxDB 集成组件。
OB2-SAPHANAP	SAP HANA 集成组件。
OB2-INFP	Informix Integration 组件。
OB2-LOTP	Lotus Notes/Domino Integration 组件。
OB2-SYBP	Sybase Integration 组件。
OB2-DB2P	DB2 Integration 组件。
OB2-SMISAP	3PAR SMI-S 代理组件。
OB2-SSEAP	P9000 XP 代理组件。
OB2-NETAPPP	NetApp Storage Provider 组件。
OB2-VEPAP	虚拟环境保护代理组件。
OB2-SODAP	StoreOnce Software 重复数据删除组件。
OB2-AUTODRP	自动灾难恢复组件。
OB2-VMWAREGRE-AGENTP	VMware Granular Recovery Extension 组件。
OB2-DOCSP	英语文档 (指南、帮助) (English Documentation (Guides, Help)) 组件。
OB2-FRAP	法语文档 (指南、帮助) (French Documentation (Guides, Help)) 组件。
OB2-JPNP	日语文档 (指南、帮助) (Japanese Documentation (Guides, Help)) 组件。
OB2-CHSP	简体中文文档（指南和帮助）组件。

安装完成时，Linux 的软件仓库位于 /opt/omni/databases/vendor 目录中。

如果不在网络中安装适用于 Linux 的安装服务器，则必须从 Linux 安装包 (tar) 本地安装每个 Linux 客户机。此外，也无法为 Data Protector 客户机上的组件打补丁。

下面的步骤

至此，您应该已在网络中安装了适用于 Linux 的安装服务器。下一步的任务是：

1. 如果将安装服务器安装在不同于 Cell Manager 的系统上，则必须将系统手动添加 (导入) 到 Data Protector 单元中。

   > **注意**导入安装服务器后，Cell Manager 上的 /etc/opt/omni/server/cell/installation_servers 文件将更新以列出已安装的远程安装包。该文件可用于在 CLI 中检查可用的远程安装包。为保持该文件最新，每当安装或删除远程安装包后应导出再导入安装服务器。即使安装服务器安装在与 Cell Manager 相同的系统上，此方法也适用。

2. 将软件分发到客户机上。请参阅安装 Data Protector 客户机。

以群集模式安装安装服务器

本主题包含以下几节:

- Serviceguard 群集节点
- Symantec Veritas 群集节点

Serviceguard 群集节点

如果进行远程安装，则可以在辅助 Serviceguard 节点上安装安装服务器并使用。有关详细信息，请参阅以非群集模式安装安装服务器。

如果在将主节点配置为群集感知 Cell Manager 之前对安装服务器进行安装，请确保将安装服务器安装在每个辅助群集节点上。在配置主节点期间，会使用虚拟服务器名称导入安装服务器。如果安装服务器并未在每个群集节点上安装，则必须从安装服务器的列表中导出安装服务器的虚拟服务器名称。另外，在群集感知 Cell Manager 的配置完成之后，必须导入每个相应的物理群集节点名称。

Symantec Veritas 群集节点

可以在辅助 Symantec Veritas Cluster Server 节点上安装安装服务器并使用，以进行远程安装。有关详细信息，请参阅以非群集模式安装安装服务器。

如果在将主节点配置为群集感知 Cell Manager 之前对安装服务器进行安装，请确保将安装服务器安装在每个辅助群集节点上。在配置主节点期间，会使用虚拟服务器名称导入安装服务器。如果安装服务器并未在每个群集节点上安装，则必须从安装服务器的列表中导出安装服务器的虚拟服务器名称。另外，在群集感知 Cell Manager 的配置完成之后，必须导入每个相应的物理群集节点名称。

安装报告服务器

Data Protector 现在提供各种集成报告，可帮助您管理和计划备份环境。这些集成报告可使用 Data Protector GUI 中“主页”上下文中的“报告”选项进行访问。

要使用报告功能，请在未用作 Data Protector Cell Manager 的 Linux 或 Windows 服务器上安装报告服务器。有关受支持的操作系统版本的更多信息，请参见支持矩阵。

Data Protector 报告服务器包含在 Data Protector Express、Data Protector Premium 和基于容量的许可证中。它可以作为基于功能的许可证的单独许可证使用。

安装报告服务器软件

您可以在未安装 Cell Manager 的 Windows 或 Linux 服务器上安装报告服务器软件。

先决条件

安装报告服务器的先决条件与 Cell Manager 相同。 如果要在 Linux 服务器上安装报告服务器，则必须创建 **rsdb** 用户，并且必须针对 **rsdb** 和 **root** 用户调整打开文件限制。有关 Cell Manager 和打开文件限制的要求的详细信息，请参阅准备安装。

> 要允许导入报告服务器，请在防火墙中打开报告服务器端口 (默认值为 8443) 和 Cell Manager 应用程序服务器端口 (默认值为 7116)。

在 Windows 上安装

要在 Windows 上安装报告服务器，请完成以下步骤:

1. 将下载的安装包 (zip 文件) 复制到 Windows 服务器上，然后将文件提取到本地目录。注意在 Windows 服务器上安装之前，请确保 C:\ProgramData\Omniback 文件夹是 Windows Defender 设置的一部分。
2. 浏览到适用于您平台的文件夹，然后运行 **setup.exe** 文件。这将启动安装向导。
3. 阅读许可协议并选择“我接受许可协议中的条款”。单击“下一步”。
4. 在“安装类型”页中选择“报告服务器”。单击“下一步”。
5. 单击“更改”以更改安装路径，或者单击“下一步”在默认路径中安装报告服务器。单击“下一步”。
6. 在“帐户信息”页中输入用户帐户的用户名和密码。单击“下一步”。
7. 在“报告信息”页中，输入报告服务器的用户名、密码、端口以及报告服务器数据库的端口。单击“下一步”。
8. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，“最初，允许新注册的 Data Protector 可执行文件按需打开入站端口”选项已选中。单击“下一步”。
9. 单击组件选择摘要页中的“安装”进行安装。您可以单击“返回”转到上一页以更改您的选择。“安装状态”页随即显示。单击“下一步”。
10. 单击“安装完成”页中的“完成”以完成安装。

在 Linux 上安装

要使用 root 访问权限在 Linux 上安装 Data Protector 报告服务器，请完成以下步骤:

1. 下载 Micro_Focus_DP_10.x0_Linux_DP_A10x0_GPLx86_64.tar.gz 包并将其提取到临时文件夹。
2. 提取安装包 (.tar 文件)。运行以下命令: tar -xvzf Micro_Focus_DP_10.x0_Linux_DP_A10x0_GPLx86_64.tar.gz
3. 使用以下命令创建用户帐户 **rsdb**: useradd -m rsdb
4. 修改 /etc/security/limits.conf 以包括
   - 对于 **root** 用户: 软限制为 8192 个文件，硬限制为 16384 个文件或更多
   - 对于 **rsdb** 用户: 软限制为 8192 个文件，硬限制为 16384 个文件或更多
5. 安装报告服务器软件。
   - 从临时文件夹运行命令 ./LOCAL_INSTALL/omnisetup.sh -RS 。此时会安装以下 RPM:
     - OB2-CORE-A.10.x0-1.x86_64.rpm
     - OB2-TS-JRE-A.10.x0-1.x86_64.rpm
     - OB2-RS-IDB-A.10.x0-1.x86_64.rpm
     - OB2-RS-REST-A.10.x0-1.x86_64.rpm
     - OB2-TS-AS-A.10.x0-1.x86_64.rpm
6. 输入报告服务器的用户名、密码和端口号以及报告服务器数据库的端口号。
7. 出现“是否要继续安装?”提示时，输入“Y”以完成安装。

静默安装

使用与上述相同的步骤，但使用命令 ./LOCAL_INSTALL/omnisetup.sh -RS -reportingusername <*username*> -reportingpasswd <*password*> -reportingport <*serverportnumber*> -reportingdbport <*dbportnumber*> ，其中

- [-reportingusername <*username*>] 是报告服务器用户名。
- [-reportingpasswd <*password*>] 是报告服务器密码。确保使用符合密码策略的复杂密码。
- [-reportingport <*serverportnumber*>] 是报告服务器端口 (可选)。如果未指定端口号，则使用默认服务器端口号 **8443**。
- [-reportingdbport <*dbportnumber*>] 是报告数据库端口 (可选)。如果未指定端口号，则使用默认数据库端口号 **5432**。

相关主题

有关设置报告服务器以查看和生成集成报告的信息，请参阅设置集成报告。

安装 Data Protector 客户机

您可以通过使用安装服务器进行分发来“远程”安装 Data Protector 客户机，或者通过相应的安装包 (zip/tar) 进行“本地”安装。

使用 Linux 安装服务器来安装 Data Protector 是适用于 UNIX 客户机的首选方法。尽管 UNIX 客户机可以本地安装 Data Protector，但是由于不使用安装服务器将没有支持的过程可以为 UNIX 客户机打补丁，因此建议不要这么做。由于对 UNIX 客户机打补丁需要安装服务器，因此建议使用同一安装服务器在 UNIX 客户机上先安装 Data Protector。

Windows 安装服务器在远程安装期间以客户机的端口 445 作为目标，而 Linux 安装服务器以客户机的端口 22 (安全远程安装) 或端口 512/514 (非安全远程安装) 作为目标。在安装服务器端，短端口用于与这些目标端口建立连接。

已经安装完客户机之后，建议通过在每个客户机上添加命令位置到相应的环境变量来从任何目录调用 Data Protector 命令。Data Protector 文档中的步骤假设变量值已经扩展。

在安装并导入 Data Protector 客户机到单元后，强烈建议对安装进行验证，以防止出现无法保证客户机访问的情况。有关验证客户机安装的过程，请参阅验证 Data Protector 客户机安装。

安装 Data Protector 客户机系统

客户机系统	安装类型和参考
Windows	远程和本地安装；请参阅安装 Windows 客户机
HP-UX	远程和本地安装；请参阅安装 HP-UX 客户机
Solaris	远程和本地安装；请参见安装 Solaris 客户机
Linux	远程和本地安装；请参阅安装 Linux 客户机
IBM AIX	远程和本地安装；请参阅安装 IBM AIX 客户机
OpenVMS	本地安装；请参阅安装 OpenVMS 客户机
其他 UNIX 系统	本地安装；请参阅在 UNIX 系统上进行本地安装
DAS Media Agent 客户机	远程和本地安装；请参阅安装 ADIC/GRAU 库介质代理。
ACS Media Agent 客户机	远程和本地安装；请参阅安装 ADIC/GRAU 库介质代理

集成客户机

Data Protector 集成是一些软件组件，可让您通过 Data Protector 备份数据库应用程序。运行数据库应用程序的系统的安装方式与任意 Windows 或 UNIX 客户机系统相同，前提是选择了相应的软件组件（例如，用于备份 Microsoft Exchange Server 数据库的 MS Exchange Integration 组件和用于备份 Oracle 数据库的 Oracle Integration 组件等）。

安装集成

软件应用程序或磁盘阵列系列	参考
Microsoft Exchange Server	请参阅安装 Microsoft Exchange Server 客户机。
Microsoft SQL Server	请参阅安装 Microsoft SQL Server 客户机
Microsoft SharePoint Server	请参阅安装 Microsoft SharePoint Server 客户机
Microsoft Volume Shadow Copy Service (VSS)	请参阅安装 Microsoft 卷影复制服务客户机。
Sybase Server	请参阅安装 Sybase Server 客户机
Informix Server	请参阅安装 Informix Server 客户机
SAP R/3	请参阅安装 SAP R/3 客户机
SAP MaxDB	请参阅安装 SAP MaxDB 客户机
SAP HANA Appliance	请参阅安装 SAP HANA Appliance 客户机
Oracle Server	请参阅安装 Oracle Server 客户机
MySQL	请参阅安装 MySQL 客户机
PostgreSQL	请参阅安装 PostgreSQL 客户机
IBM DB2 UDB	请参阅安装 IBM DB2 UDB 客户机
Lotus Notes/Domino Server	请参阅安装 Lotus Notes/Domino Server 客户机
VMware	请参阅安装 VMware 客户机
Microsoft Hyper-V	请参阅安装 Microsoft Hyper-V 客户机
Network Data Management Protocol (NDMP) Server	请参阅安装 NDMP 服务器客户机
P9000 XP 磁盘阵列系列	请参阅安装 P9000 XP 磁盘阵列系列客户机
3PAR StoreServ Storage	请参阅安装 3PAR StoreServ Storage 客户机
NetApp 存储提供程序	请参阅安装存储阵列的存储提供程序

Data Protector 组件

可以在现有客户机系统和 Cell Manager 上安装其他 Data Protector 软件组件。组件可以从远程或本地添加。

有关支持的平台的最新信息，请参阅最新支持矩阵。

以下是可供选择的 Data Protector 组件及其说明:

用户界面	用户界面组件包含 Windows 系统上的 Data Protector 图形用户界面和 Windows 与 Linux 系统上的部分命令行界面。访问 Data Protector Cell Manager 需要使用该软件，必须至少将该软件安装到用于管理单元的系统上。
英语文档（指南、帮助）	这是 Data Protector 英语文档文件集。
法语文档（指南、帮助）	这是 Data Protector 法语文档文件集。
日语文档（指南、帮助）	这是 Data Protector 日语文档文件集。
简体中文文档（指南和帮助）	这是 Data Protector 简体中文文件文件集。
Manager-of-Managers 用户界面	Manager-of-Managers 用户界面包含 Data Protector 图形用户界面。该软件用于访问 Data Protector Manager-of-Managers 功能和控制多单元环境。“Manager-of-Managers 用户界面”和“管理器用户界面”可用作公共应用程序。
磁盘代理	具有需要使用 Data Protector 进行备份的磁盘的系统上必须安装磁盘代理组件。
常规介质代理	连接了备份设备或有权访问库机械手并通过 Data Protector 进行管理的系统上必须安装常规介质代理组件。
自动灾难恢复	在需要使用自动灾难恢复方法支持恢复的系统上，以及需要为增强型自动灾难恢复 (EADR) 或一键式灾难恢复 (OBDR) 准备 DR CD ISO 映像来为灾难恢复提供自动准备的系统上，必须安装自动灾难恢复组件。
SAP R/3 集成	具有需要使用 Data Protector 备份的 SAP R/3 数据库的系统上必须安装 SAP R/3 集成组件。
SAP MaxDB 集成	具有需要使用 Data Protector 备份的 SAP MaxDB 数据库的系统上必须安装 SAP MaxDB 集成组件。
SAP HANA 集成	必须在代表或组成您要使用 Data Protector 保护的 SAP HANA Appliance 上安装 SAP HANA Integration 组件。
Oracle 集成	具有需要使用 Data Protector 进行备份的 Oracle 数据库的系统上必须安装 Oracle 集成组件。
MySQL 集成	必须在具有需要使用 Data Protector 进行备份的 MySQL 数据库的系统上安装 MySQL 集成组件。
虚拟环境集成 **(适用于Data Protector Express)**	虚拟环境集成组件必须安装在将用作备份主机的系统上，以使用 Data Protector 虚拟环境集成控制虚拟机的备份和还原。
DB2 集成	具有需要使用 Data Protector 进行备份的 DB2 Server 的所有系统上必须安装 DB2 集成组件。
Sybase 集成	具有需要使用 Data Protector 进行备份的 Sybase 数据库的系统上必须安装 Sybase 集成组件。
Informix 集成	具有需要使用 Data Protector 进行备份的 Informix Server 的系统上必须安装 Informix 集成组件。
MS Exchange 集成	还必须在将要使用 Data Protector Microsoft Exchange Single Mailbox 集成进行备份的 Microsoft Exchange Server 2010 系统上安装 MS Exchange 集成组件。
MS Exchange Server 2010+ 集成 (MS Exchange Server 2010 Integration)	必须将 MS Exchange Server 2010+ 集成组件安装到计划使用 Data Protector Microsoft Exchange Server 2010 集成进行备份的 Microsoft Exchange Server 2010 或 Microsoft Exchange Server 2013 系统。
MS SQL 集成	具有需要使用 Data Protector 进行备份的 Microsoft SQL Server 数据库的系统上必须安装 MS SQL 集成组件。
MS SharePoint 2010/2013 集成	必须在需要使用 Data Protector 进行备份的 Microsoft SharePoint Server 2010/2013 系统上安装 MS SharePoint 2010/2013 集成组件。
MS Volume Shadow Copy 集成	在要运行由卷影复制服务协调的备份的 Windows Server 系统上必须安装 MS 卷影复制服务集成组件。
P6000/3PAR SMI-S 代理	P6000/3PAR SMI-S 代理组件必须同时安装在应用程序系统和备份系统上，以将 Data Protector 与 3PAR StoreServ Storage 集成。
P9000 XP 代理	P9000 XP 代理组件必须同时安装到应用程序系统和备份系统，以将 Data Protector 与 P9000 XP 磁盘阵列系列集成。
3PAR VSS 代理	3PAR VSS 代理组件必须同时安装在应用程序系统和备份系统上，以将 Data Protector 与 3PAR StoreServ Storage （在其配置中，应用程序系统和备份系统均为 Windows 系统，并且您要使用卷影复制服务备份及还原数据) 集成。
NetApp 存储提供程序	应用程序系统和备份系统上的 NetApp 存储提供程序，可将 Data Protector 与 NetApp 存储集成。进行虚拟环境集成时，此组件必须仅安装在备份系统上。NetApp Storage Provider 组件是 Data Protector SMI-S 代理的插件。
NDMP 介质代理	必须在需要通过 NDMP 服务器将数据备份到 NDMP 专用驱动器的所有系统上安装 NDMP 介质代理组件。
Lotus 集成	在 Data Protector 单元中具有计划使用 Data Protector 进行备份的 Lotus Notes/Domino Server 数据库的所有系统上必须安装 Lotus 集成组件。
MS Exchange Granular Recovery Extension	要启用精细复原功能，则必须每个 Microsoft Exchange Server 系统上安装适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension。在 Microsoft Exchange Server 的数据库可用性组 (DAG) 环境中，它必须安装在 DAG 的所有 Exchange Server 系统上。
MS SharePoint Granular Recovery Extension	必须在 Microsoft SharePoint Server Central Administration 系统上安装适用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension 。

VMware Granular Recovery Extension (GRE) HTML5 Web 插件 **(适用于 Data Protector Express)**	要启用 VMware 虚拟机的粒度恢复功能，则必须在 VMware Virtual Server 系统上安装 Data Protector VMware GRE HTML5 Web 插件组件。在使用 Web 插件进行文件恢复操作之前，必须先配置 Data Protector GRE 环境。
VMware Granular Recovery Extension 代理 **(适用于 Data Protector Express)**	要启用 VMware 虚拟机的存储和精细复原，则必须在装载代理系统上安装 Data Protector VMware Granular Recovery Extension Agent 组件。仅支持远程安装。

注意不能在同一系统上安装常规介质代理和 NDMP 介质代理。

Data Protector 服务

Data Protector 使用以下服务：

Inet	备份客户机服务
CRS	Cell Manager 服务
hpdp-idb	内部数据库服务
hpdp-idb-cp	内部数据库连接池程序
hpdp-as	应用程序服务器

默认情况下， Inet 和 hpdp-* 服务在本地系统帐户下运行， CRS 在管理员帐户下运行。

注意 inet -version 命令返回 Inet 版本作为基本主要版本而不是次要版本或补丁版本。

您可以为其中任一服务更改帐户信息。但是，以下是新帐户必须满足的最低要求：

服务	资源	服务所需的最低资源权限
CRS	Data_Protector_program_data	完全访问权限
	HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII	完全访问权限
Inet	备份和还原	-
	取得所有权	-

安装 Windows 客户机

通过使用安装服务器分发软件，可以在本地或远程安装 Data Protector 客户机。在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。

限制

- 由于 Windows 操作系统强加的安全限制，您只能将热修复 (HF) 远程部署到与安装服务器位于同一域中的客户机。
- 当远程安装客户机到 Windows Server 2008 或者 Windows Server 2012 时，可使用以下某个帐户：
  - 远程系统上的内置管理员帐户。必须启用该帐户，并且禁用*管理批准模式*。
  - 域用户帐户，它是远程系统上本地管理员用户组的成员。
- Windows 目录共享信息只能还原到安装有 Data Protector 磁盘代理的 Windows 系统上。如果不符合此要求，目录仍可还原，但磁盘代理会忽略目录共享信息。
- 在 Windows 客户机上一次只能运行一个 CONFIGURATION 备份。
- Data Protector 要求计算机名称和解析主机名的名称相同。
- 在 Windows 平台上不支持使用安全 shell (SSH) 进行远程安装。
- 本地安全 shell 安装支持基于密钥的认证。不支持其他认证模式。
- 不支持使用 VSS 功能备份网络共享卷。
- Windows 系统上的 GUI 在树形结构视图中可以显示最多 64000 个项目（一个目录中的文件、库中的插槽等等）。
- 在 Windows 上安装 Data Protector 群集集成时使用的文件群集资源的名称不得为 omniback。
- 使用备份规范编辑器浏览 Windows 客户机时，Windows 用户界面会列出处于联机和脱机状态的 Informix Server 数据库空间。要检查数据库，请使用 onstat -d 命令。可用数据库标有 PO 标志。
- 在 Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 系统上，执行网络共享备份的用户必须是操作系统“备份操作员”用户组的成员，且必须添加到运行磁盘代理的系统上的 Inet 配置中 (使用 omniinetpasswd -add)。在群集环境中，必须在两个节点上配置用户。
- 在 Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 系统上，不支持广播消息发送方法。
- 从 32 位 Windows 系统目录中备份的目录共享信息，不能还原到 64 位 Windows 系统，反之亦然。在这样的备份情境中，选定的目录及其内容会如您所期望地进行恢复，但不会还原其目录共享信息。
- 仅可在 Windows Server 2008 系统上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 只能在 Windows 2008 Server 系统上通过网络引导目标系统。
- Data Protector 灾难恢复 GUI 仅在 Windows 2008 Server 系统上可用。在其他 Windows 系统上，控制台界面可用。
- 备份网络共享卷时，共享名中无法使用 IPv6 地址。
- 如果以网络安全模式启动 Windows 系统，Data Protector Inet 服务将无法启动。

Windows 64 位限制

- 支持将原始 Microsoft Windows 安装 CD-ROM 用于自动系统恢复 (ASR)。
- 无法使用 Data Protector OB2_Snap 管理单元将 Data Protector GUI 与 Microsoft 管理控制台 (MMC) 相集成。
- Data Protector 在基于 Itanium 2 处理器架构的 Windows 系统上不支持 Java Web 报告功能，因为此平台上不支持 Java 运行时环境。
- 在 AMD64/Intel EM64T 系统上，仅支持使用 Microsoft Outlook Express 而不是 Microsoft Outlook 发送通过 MAPI 交互的电子邮件通知和报告。

Windows Server 2012 限制

- 不支持使用 Resilient File System (ReFS) 格式化的卷的文件系统备份。而是使用磁盘映像备份。
- 不使用 VSS 的 SMB 文件共享功能，也能支持网络共享磁盘备份。

在本地安装

可以通过 Windows 安装包 (zip) 在本地安装 Windows 客户机：

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 setup.exe 文件。
2. 按照安装向导操作，并仔细阅读许可协议。单击**下一步 (Next)** 继续。
3. 在“安装类型”页中，选择**客户机**。对于 Itanium 客户机，将会自动选择该类型。
4. 输入 Cell Manager 的名称。

   如果 Cell Manager 使用默认 5565 之外的端口，则更改端口号。通过单击“检查响应”可测试 Cell Manager 是否活动并使用所选端口。

   如果在安装期间指定了 Cell Manager，则作为安装的一部分，将在客户机中配置 Cell Manager 证书，但不会执行导入。

   单击“下一步”。
5. 单击“下一步”，在默认文件夹中安装 Data Protector。

   否则，单击**更改**打开“更改当前目标文件夹”页面并输入路径。
6. 选择要安装的 Data Protector 组件。单击“下一步”。
7. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，“最初，允许新注册的 **Data Protector** 可执行文件按需打开入站端口”选项已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的客户机的 Data Protector，必须在 Windows 防火墙中启用 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。

   单击“下一步”。
8. 此时会显示组件选择摘要页面。单击**安装 (Install)** 安装选定组件。
9. “安装状态”页随即显示。单击“下一步”。

10. 如果已经安装了“用户界面”组件，并要在设置后立即使用 Data Protector GUI 启动，则请选择“启动 Data Protector GUI”。
11. 单击**完成**。

导入本地安装的客户机

导入表示在安装 Data Protector 软件之后手动将计算机添加到单元中。添加到 Data Protector 单元后，系统将变为 Data Protector 客户机。

一个客户机只能是一个单元的成员。如果希望将客户机移动到其他单元，则首先将其从当前单元*导出*，然后将其*导入*到新单元。

配置客户机以执行导入

此过程仅在本地安装过程中未指定 Cell Manager 名称的情况下适用。本地安装完成之后，在客户机端执行以下命令： omnicc –secure_comm –configure_peer <Cell manager hostname>

此步骤可为客户机配置 Cell Manager 证书。对于本地安装的客户机，这是强制步骤。重新导入删除的客户机也需要此命令。

该命令提示用来显示 Cell Manager 证书指纹的 **y/n** 选项。输入 **y** 将成功完成配置。如果要配置客户机而不执行任何验证，请将 -accept_host 命令附加到以下命令中：omnicc –secure_comm –configure_peer <Cell manager hostname> -accept_host 使用 accept_host 命令时，控制台不会提示 **y/n** 选项。

使用 GUI 导入客户机系统

当用户选择**接受指纹**选项时，不会显示指纹窗口，主机会被接受，而无需用户确认。如果不选择此选项，则会显示指纹窗口，用户必须手动接受指纹选项。

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 输入客户机的名称或浏览网络以选择要导入的客户机（仅在 Windows GUI 上）。

   如果导入配置有多个 LAN 卡的客户机，请选择**虚拟主机**选项。选择该选项后，必须导入同一系统的所有名称。

   如果导入 NDMP 客户机，请选择 **NDMP 服务器**选项并单击**下一步**。指定 NDMP 服务器的相关信息。

   如果要导入 HP OpenVMS 客户机，则在“名称 ”文本框中键入 OpenVMS 客户机的 TCP/IP 名称。

   如果将导入 Microsoft Exchange Server DAG 虚拟主机以进行 Data Protector Microsoft Exchange Server 2010 集成，请选择“虚拟主机”。

   如果要为 Data Protector Virtual 环境集成导入客户机，可以选择适用于独立 VMware ESX(i) Server 系统的 **VMware ESX(i)**、适用于 VMware vCenter Server 系统的 **VMware vCenter**，也可以选择适用于 Microsoft Hyper-V 系统的 **Hyper-V**。单击**下一步**并指定登录凭据。
4. 单击“下一步”。
5. 单击**完成 (Finish)** 以导入客户机。

所导入客户机的名称将显示在结果区域中。

使用 CLI 导入客户机系统

omnicc –import_host 命令用于导入 Data Protector 客户机，而 omnicc –import_cs 命令用于导入外部 Cell Manager。将 –virtual 添加到命令，以进行虚拟客户机导入。

该命令提示用来显示 Cell Manager 证书指纹的 **y/n** 选项。输入 **y** 将成功完成配置。如果用户要配置客户机而不执行任何验证，请将 -accept_host 附加到命令中。

MOM 配置中的 Cell Manager

不同版本的 Cell Manager 不得为 MOM 配置的一部分。应遵循以下步骤，以在 MOM 配置中包括 Cell Manager:

1. 应使用以下命令，通过 MOM 服务器配置 Cell Manager:

   omnicc -secure_comm -configure_peer <MOM server>

   此命令在 Cell Manager 中配置 MOM 服务器。提示 MOM 服务器指纹，用户需要接受指纹。
2. 从 MOM GUI 导入 Cell Manager。此操作提示 Cell Manager 证书指纹，用户需要接受该指纹。

在本地安装安装服务器

如遇下述情况，则必须向单元添加一个安装服务器:

- 如果作为独立的 Linux 安装服务器安装，例如未安装在 Cell Manager 上。

  在这种情况下，只有将安装服务器添加到单元后，才能在单元中远程安装客户机。
- 如果安装在 Cell Manager 上，但是您也想将其用于在其他单元中执行远程安装。那么必须将其添加到其他单元 (使用连接到其他单元的 Cell Manager 的 GUI)。

与客户机不同，安装服务器可以是多个单元的成员。因此，不必将其从一个单元删除（导出），即可添加（导入）到另一个单元。

配置安装服务器

请运行以下命令配置安装服务器主机：omnicc -secure_comm -configure_peer <CM host name>

导入安装服务器

导入安装服务器的过程与导入客户机的过程类似。使用 Data Protector GUI (连接到将添加安装服务器的单元的 Cell Manager) 执行此任务时，请执行以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击 **Installation Server**，然后单击**导入 Installation Server** 启动向导。
3. 输入或选择要导入的系统的名称。单击“完成”导入安装服务器。

在 Windows/Linux 上将安装服务器导入 Cell Manager 的示例

如果 **hostname1.company.net** 为 Cell Manager，并且 **hostname2.company.net** 为安装服务器，则在安装服务器上运行以下命令：

```
omnicc -secure_comm -configure_peer hostname1.company.net
```

```
[root@hostname2 etc]# omnicc -secure_comm -configure_peer hostname1.company.net
```

```
- Please use the
```

```
fingerprint to validate the certificate manually!
```

```
Certificate information:
```

```
- Hostname:hostname1.company.net
```

```
- Valid: from Sep 24 06:25:52 2016 GMT until Sep 22 06:25:52 2026 GMT
```

```
- Fingerprint: e9:2a:3f:ed:af:10:c1:f7:7h:67:69:4b:4d:51:87:25:6h:79:gr:78
```

```
Do you want to continue (y/n)?y
```

```
Host 'hostname1.company.net' configured for secure configuration successfully.
```

现在，在 Cell Manager 上，使用以下命令重新导入安装服务器，因为必须交换并验证证书。

```
omnicc -import_is HostName [-accept_host]
```

```
C:\Program Files\OmniBack\bin>omnicc -import_is hostname2.company.net
```

```
- Please use the fingerprint to validate the certificate manually!
```

```
Certificate information:
```

```
- Hostname:hostname2.company.net
```

```
- Valid: from Aug 24 07:26:15 2016 GMT until Aug 22 07:26:15 2026 GMT
```

```
- Fingerprint: f5:3b:3h:gb:cf:10:d1:f7:7d:67:60:5b:4d:51:87:76:6h:51:rg:89
```

```
Do you want to continue (y/n)?y
```

```
Import host successful.
```

将备份设备与 Windows 系统连接

安装介质代理组件之后，可以通过执行以下步骤将备份设备与 Windows 系统进行连接：

1. 为要连接的备份设备的驱动器和控制设备（机械手）查找可用的 SCSI 地址（在 Windows 上称作 SCSI 目标 ID。
2. 为驱动器和控制设备（机械手）设置未使用的 SCSI Target ID。根据设备类型，通常可以通过设备上的开关来完成设置。有关详细信息，请参见设备自带的文档。

   有关受支持的设备的信息，请参阅 https://softwaresupport.softwaregrp.com。
3. 关闭计算机，并将备份设备与系统连接。
4. 开启设备，然后开启计算机，并等待启动过程完成。
5. 要验证系统是否正确识别新的备份设备，可以在 Data_Protector_home\bin 目录中运行 devbra -dev 命令。

   查看命令输出列出的新设备。例如， devbra -dev 命令可能会生成以下输出：

   - 如果设备的磁带驱动程序已加载：

     HP:C1533A

     tape3:0:4:0

     DDS

     ...

     第一行代表设备规范，第二行是设备文件名。

     路径格式指示 DDS 磁带设备的驱动器实例编号为 3，连接到 SCSI 总线 0，SCSI 目标 ID 4 和 LUN 编号 0。
   - 如果设备的磁带驱动程序未加载：

     HP:C1533A

     scsi1:0:4:0

     DDS

     ...

     第一行代表设备规范，第二行提供设备文件名。

     路径格式指示 DDS 磁带设备连接到 SCSI 端口 1、SCSI 总线 0，磁带驱动器具有 SCSI 目标 ID 4 和 LUN 编号 0。

下面的步骤

在此阶段，您应当已经安装了客户机组件，并连接了备份设备，从而能够配置备份设备和介质池。有关配置任务的详细信息，请参阅《Data Protector 帮助》索引: “配置, 备份设备”。

安装 HP-UX 客户机

可以使用适用于 Linux 的 安装服务器远程安装 HP-UX 客户机，或者从 UNIX 安装包 (tar) 本地安装。

以下限制适用：

- 不支持从磁盘映像中还原单个文件。
- 在使用新的永久多路径和与路径无关的设备特殊文件 (DSF) 命名方式的 HP-UX 11.31 上，如果系统上禁用了旧的 DSF，则无法使用引用旧的 DSF 的备份规范。此时，应重新配置设备和更新备份规范以使用新的 DSF 命名方式。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。

远程安装

使用 Data Protector 图形用户界面从适用于 Linux 的安装服务器将客户机软件安装到客户机上。

进行远程安装之后，客户机系统会自动成为 Data Protector 单元的成员。

如果在客户机上已安装了介质代理，则必须将备份设备与系统进行物理连接。要确定对应于您所用设备类型的设备驱动程序是否已构建到内核中，在运行备份之前，请先检查内核配置。

在本地安装

在安装服务器上

如果在您的环境中未安装适用于 Linux 的安装服务器，则必须从 Linux 安装包 (tar) 执行本地安装。有关本地安装的步骤，请参见安装服务器的本地安装。

在客户机上

进行本地安装之后，必须将客户机系统手动导入单元中。请参阅导入本地安装的客户机。

群集感知客户机

对于安装群集感知客户机，还存在一些其他先决条件和步骤。

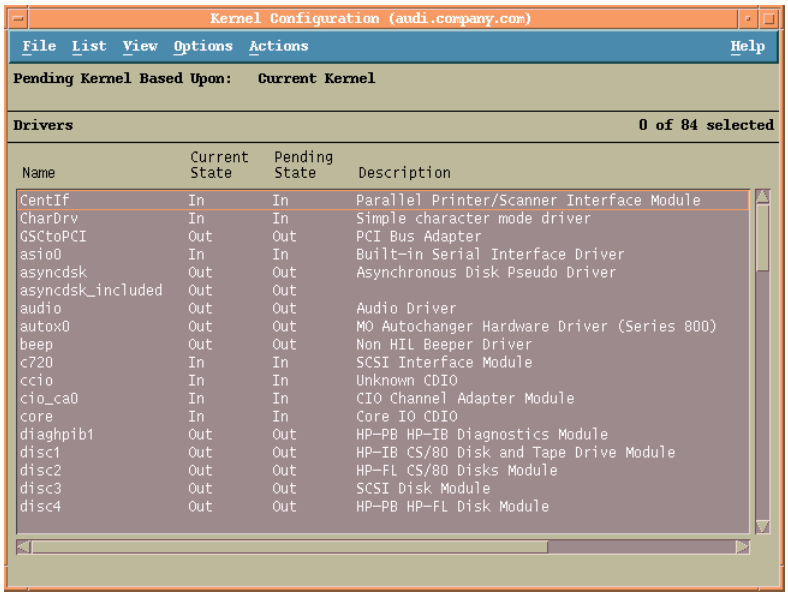
检查 HP-UX 上的内核配置

以下过程说明如何使用 *System Administration Manager (SAM)* 实用程序在 HP-UX 11.x 上检查和构建内核配置。

按照以下过程使用 *System Administration Manager (SAM)* 实用程序构建内核配置:

1. 以 root 用户身份登录，然后打开终端并输入 sam。
2. 在 **System Administration Manager** 窗口中，双击**内核配置 (Kernel Configuration)**，然后双击**驱动程序 (Drivers)**。
3. 在**内核配置 (Kernel Configuration)** 窗口中，验证以下方面：
   - 您将要使用的设备的驱动程序必须列在已安装驱动程序中。请参阅内核配置窗口。如果要查找的驱动程序未列出，则必须使用 /usr/sbin/swinstall 实用程序安装它。例如：
     - 如果将磁带设备与系统连接，则磁带设备驱动程序对于磁带设备是必需的，因此必须安装它。例如，对于通用 SCSI 磁带驱动器 (如 DLT 或 LTO)，需要使用 stape 驱动程序；对于 DDS 设备，需要使用 tape2 驱动程序。
     - 要控制磁带库设备中的机械手，需要名为 sctl 或 spt 的 SCSI 直通驱动程序，或者名为 schgr 的自动更换器机械手驱动程序 (具体取决于硬件)。

内核配置窗口



- **当前状态 (Current State)** 列中显示的驱动程序状态必须设置为**包含 (In)**。如果状态值设置为**不包含 (Out)**，则执行以下操作：
  1. 在列表中选择驱动程序。单击“操作”并选择“将驱动程序添加到内核中”。在**挂起状态**列中，状态将设置为 In.

     对于**当前状态 (Current State)** 为**包含 (In)** 的每个驱动程序重复该操作。
  2. 单击“操作”并选择“创建新内核”来应用更改，也就是将“挂起内核”构建为“当前内核”。执行该操作之后，需要重新启动系统。

将所有必需驱动程序构建到内核中之后，您可以继续操作，即将备份设备与系统连接。

将备份设备与 HP-UX 系统连接

1. 确定驱动器和控制设备（机械手）的可用 SCSI 地址。使用 /usr/sbin/ioscan -f 系统命令。
2. 在设备上设置 SCSI 地址。根据设备类型，通常可以通过设备上的开关来完成设置。有关详细信息，请参见设备自带的文档。

   有关支持的设备的详细信息，请参阅最新支持矩阵。
3. 将设备与系统连接，开启设备，然后开启计算机，并等待启动过程完成。设备文件通常在启动过程期间创建。
4. 验证系统是否正确识别新的备份设备。使用 ioscan 实用程序:

   /usr/sbin/ioscan -fn

   从而可以查看针对每个已连接备份设备列出的设备文件。如果在启动过程期间未自动创建设备文件，则必须手动创建它。

完成安装过程，并将备份设备与系统正确连接之后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解有关配置设备和介质池，或其他 Data Protector 配置任务的详细信息。

安装 Solaris 客户机

可以通过 UNIX 安装包 (tar) 在本地安装 Solaris 客户机。

以下限制适用：

- 如果在 pre- 或 post-exec 中使用 csh 脚本，必须在以下解释器规范行中指定 -b 选项： #!/bin/csh -b
- 在 Solaris 上，/tmp 是交换区域中的虚拟文件系统。如果备份规范中包括 /tmp 目录，则将其作为空目录来备份。如果还原此类备份，必须于还原前在客户机上配置交换区域，否则不能重新创建 /tmp 目录。
- 不支持备份和还原 Veritas Cluster File System (CFS) 上的访问控制列表 (ACL)。
- 在 Solaris 上，由于使用许多块大小不同的介质，检测非 Data Protector 介质类型的介质不可靠。不要依赖 Data Protector 来识别外来介质。

变通方法：为防止 Data Protector 对不能正确识别的介质自动进行初始化，请将 InitOnLoosePolicy 全局选项设置为 0 。这样，所有介质必须手动初始化。

- 磁头清洁磁带在 DDS 库中无法识别。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。

在本地安装

您必须从 UNIX 安装包 (tar) 中执行本地安装。相关说明，请参阅在 UNIX 系统上进行本地安装。

安装后配置

在客户机系统上安装介质代理组件之后，必须检查配置以确定所需的变更，具体取决于将使用的平台和设备类型。

- 如果您的 Solaris 系统是已打补丁的 Solaris 10 系统，磁带设备驱动程序可能已默认支持您的设备。要对此进行检查，请使用 strings 命令。

  例如，如果要检查您的 DAT-72 设备是否无需额外的配置步骤即可使用，请执行以下命令:

  Solaris (SPARC) 系统：

  strings /kernel/drv/sparcv9/st | grep HP

  Solaris (x86_64) 系统:

  strings /kernel/drv/st | grep HP

  检查命令输出。如果输出中显示了您的设备，则不需要额外的步骤。反之，则按照以下的说明进行操作。

- 对于 DAT (4 毫米) 设备，需要在 /kernel/drv/st.conf 文件中添加以下行:

  tape-config-list =

  ```
  "HP HP35470A", "HP DDS 4mm DAT", "HP-data1", "HP HP35480A", "HP DDS-DC 4mm DAT", "HP-data1", "HP C1533A", "HP DDS2 4mm DAT", "HP-data2", "HP C1537A", "HP DDS3 4mm DAT", "HP-data3", "HP C1553A", "HP DDS2 4mm DATloader", "HP-data2", "HP C1557A", "HP DDS3 4mm DATloader", "HP-data3"; HP-data1 = 1,0x34,0,0x8019,3,0x00,0x13,0x03,2; HP-data2 = 1,0x34,0,0x8239,4,0x0,0,0x13,0x24,0x3,3; HP-data3 = 1,0x34,0,0x8239,4,0x0,0,0x13,0x24,0x3,3;
  ```

重要说明这些数据条目不同于支持人员通常建议的默认条目。请准确指定这些行，否则 Data Protector 将无法使用您的驱动器。

- 对于 DLT、DLT1、SuperDLT、LTO1、LTO2 和 STK9840 设备，需要在 /kernel/drv/st.conf 文件中添加以下行:

  tape-config-list =

  ```
  "HP Ultrium 1-SCSI", "HP Ultrium 1-SCSI", "LTO-data", "HP Ultrium 2-SCSI", "HP_LTO", "HP-LTO2", "DEC DLT2000", "Digital DLT2000", "DLT2k-data", "Quantum DLT4000","Quantum DLT4000", "DLT4k-data", "QUANTUM DLT7000", "Quantum DLT7000", "DLT7k-data", "QUANTUM DLT8000", "Quantum DLT8000", "DLT8k-data", "HP C9264CB-VS80","HP DLT vs80 DLTloader","HP_data1" "QUANTUM SuperDLT1", "QUANTUM SuperDLT", "SDLT-data", "TANDBERGSuperDLT1", "TANDBERG SuperDLT", "SDL-data", "STK 9840", "STK 9840", "CLASS_9840";
  ```

  ```
  DLT2k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT4k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT7k-data = 1,0x38,0,0x8639,4,0x82,0x83,0x84,0x85,3; DLT8k-data = 1,0x77,0,0x1D639,4,0x84,0x85,0x88,0x89,3; HP_data1 = 1,0x3a,0,0x8639,4,0x40,0x86,0x87,0x7f,0; LTO-data = 1,0x7a,0,0x1d679,4,0x00,0x00,0x00,0x40,3; HP-LTO2 = 1,0x7a,0,0xd639,4,0x00,0x00,0x00,0x42,3; SDLT-data = 1,0x79,0,0x8639,4,0x90,0x91,0x90,0x91,3; CLASS_9840 = 1,0x78,0,0x1d679,1,0x00,0;
  ```

- 对于 StorageWorks 12000e (48AL) 自动加载器 (C1553A)，除了 /kernel/drv/st.conf 文件中的数据条目之外，还需要添加以下条目:

```
name="st" class="scsi" target=ID lun=0; name="st" class="scsi" target=ID lun=1;
```

将 *ID* 符号替换为自动加载器的 SCSI 地址，并将自动加载器选项号设置为 5（开关位于设备的后面板上），并将驱动器的 DIP 开关设置为 11111001（开关位于自动加载器的底部）。

> 注意StorageWorks 12000e 库没有用于拾取器设备的专用 SCSI ID，但它通过相同的 SCSI ID 接收数据驱动器存取命令和拾取器命令。但是，数据驱动器存取命令必须定向到 SCSI lun=0，拾取器命令必须定向到 SCSI lun=1。

对于所有其他设备，请检查 st.conf.templ 模板 (位于 /opt/omni/spt) 来确定 st.conf 文件中的必需条目。它只是一个模板文件，不能代替 st.conf 文件。

- 对于每一个要使用的磁带设备，检查文件 /kernel/drv/st.conf 中是否存在以下行并在必要时添加该行。用设备地址替换 ID 占位符:

  SCSI 设备：

  ```
  name="st" class="scsi" target=ID lun=0;
  ```

  光纤通道设备：

  ```
  name="st" parent="fp" target=ID
  ```

  注意， parent 参数的值可能因磁带设备的不同而有所不同。有关详细信息，请参见您的磁带设备文档。

- 要在 Solaris 10 (SPARC、x86、x64) 上控制 SCSI 交换器设备，则应配置内置 sgen 驱动程序，然后安装 SCSI 设备。请遵循以下步骤：

  1. 打开文件 /kernel/drv/sgen.conf 。

     如果文件中显示了参数 device-type-config-list ，则将更换器设备引用添加到已存在的行中，例如:

     ```
     device-type-config-list=”scanner”, "changer";
     ```

     如果尚未定义参数，则将以下行添加到文件：

     ```
     device-type-config-list="changer";
     ```

  2. 对于每一个要控制的 SCSI 交换器设备，检查文件 /kernel/drv/sgen.conf 中是否存在以下行且在必要时添加。用设备地址替换 ID 占位符:

     ```
     name="sgen" class="scsi" target=ID lun=0;
     ```

  3. 在此阶段，您已准备好安装 SCSI 设备。在安装之前，必须为交换器设备的每个驱动器和机械手（拾取器）分配正确的 SCSI 地址。系统的任何其他设备不能使用所选的地址。

     要检查 SCSI 配置，通过以下命令（特定于 SPARC 系统的步骤）关闭系统：

     ```
     shutdown -i0
     ```

     然后在 ok 提示符处运行 probe-scsi-all 命令来检查所分配的地址:

     ```
     ok probe-scsi-all
     ```

     完成之后，使用以下命令重新启动系统：

     ```
     ok boot -r
     ```

     要准备系统以使用 SCSI 设备，按照下例中所示的步骤执行：

     a. 编辑 /kernel/drv/st.conf 来设置设备参数以使用所分配的 SCSI 端口。有关详细信息，请参见设备文档。仅当磁带设备驱动程序默认不支持您的设备时修改 tape-config-list 参数。

     b. 编辑 /kernel/drv/sgen.conf 来设置 ADIC SCSI 控制设备，以使用所分配的 SCSI 端口 4。将 ADIC SCSI Exchanger 驱动器的以下数据添加到 /kernel/drv/sgen.conf 文件:

        ```
        name="sgen" class= "scsi" target=4 lun=0;
        ```

修改 /kernel/drv/sgen.conf 文件 (Solaris 10) 后，即可将备份设备物理连接到系统。

将备份设备与 Solaris 系统连接

1. 创建 reconfigure 文件:

   ```
   touch /reconfigure
   ```

2. 通过输入 $shutdown -i0 命令关闭系统，然后关闭计算机，并将设备与 SCSI 总线进行物理连接。检查是否有任何其他设备在使用您为设备选择的 SCSI 地址。

> **注意**在 Solaris 系统上，Data Protector 不会自动识别清洗带。如果 Data Protector 检测到并在 StorageWorks 12000e (48AL) 设备中插入清洗带，则磁带驱动程序会进入未定义状态，可能需要您重新启动系统。请在 Data Protector 发出清洗带请求时，手动加载清洗带。

3. 如果您的系统是 Solaris (SPARC)，可通过按 Stop-A 键来重新开启系统和中断启动过程。
4. 通过在 ok 提示符处输入 probe-scsi-all 命令验证是否正确识别了新设备:

   ```
   ok > probe-scsi-all
   ```

   然后，输入：

   ```
   ok > go
   ```

   继续。
5. 在此阶段，设备应当正确工作。对于驱动器，设备文件必须位于 /dev/rmt 目录中；对于 SCSI 控制设备 (拾取器)，设备文件必须位于 /dev 目录中。

   > **注意**在 Solaris 10 上，从来没有创建过这样的链接。在这种情况下，创建符号链接以将合适的设备文件加入到 /dev/rsstNum ，其中 Num 是您选择的一个数字。例如：
   >
   > 当使用 sst 时：
   >
   > ```
   > ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4
   > ```
   >
   > 当使用 sgen 时：
   >
   > ```
   > ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /dev/rsst4
   > ```

   您可以使用 Data Protector uma 实用程序验证设备。要检查前面示例的 SCSI 交换器设备的拾取器（使用 SCSI 端口 4），请输入：

   ```
   echo “inq”|/opt/omni/lbin/uma -ioctl /dev/rsst4
   ```

   拾取器必须将自身标识为 SCSI-2 设备库。可以通过强制该库初始化自身来检查该库。命令为：

   ```
   echo “init”|/opt/omni/lbin/uma -ioctl /dev/rsst4
   ```

请确保使用伯克利样式的设备文件；在此例中，对于磁带驱动器使用 /dev/rmt/0cbn（不是 /dev/rmt/0h），对于 SCSI 控制文件 (拾取器) 使用 /dev/rsst4 。

下面的步骤

完成安装步骤并且将备份设备与 Solaris 客户机正确连接之后，如需有关配置备份设备、介质池和其他配置任务的其他信息，请参阅《Data Protector 帮助》索引: “配置, 备份设备”。

安装 Linux 客户机

可以使用适用于 Linux 的 安装服务器远程安装 Linux 客户机系统，或者从 UNIX 安装包 (tar) 本地安装。

以下限制适用：

- 完全支持 LOFS 文件系统。但是，如果在相同的文件系统内装载目录，则 Data Protector 不能识别 LOFS 装载的目录。这会导致重复备份数据。
- 不支持跨文件系统还原 ACL（文件权限属性）。例如，从 VxFS 文件系统备份的 ACL 不能还原到 UFS 文件系统，反之亦然。但是，不含 ACL 的文件对象可以还原到其他文件系统。
- 不支持跨平台还原 ACL。存在此限制是由于不同操作系统有不同的内部 ACL 数据结构。
- 修改 ACL 条目不会影响文件对象的修改时间，因此增量备份期间不会备份该文件对象（及修改过的 ACL）。
- GUI 在树形结构视图中可以显示最多 64000 个项目 (一个目录中的文件、库中的插槽等等)。
- 不支持包含引号的文件名。
- 在 Linux 系统上从 ext2 转换为 ext3 文件系统后，日记变为可见，在该文件系统的 root 目录下显示为 .journal 文件。如果未装载该文件系统，日记将不可见，而且也不会显示在文件系统中。
  由于 Linux 操作系统的限制，不要删除、备份和从备份中还原此 .journal 文件。
- 如果使用访问控制列表 (ACL) 在 32 位和 64 位 Linux 系统之间执行备份和还原操作（例如，在 32 位 Linux 系统执行备份，在 64 位 Linux 系统上执行还原），则不能还原 ACL 条目。
- 在 Linux 系统上，还原所有者不是 root 用户的符号链接前，请确保链接所有者对要还原链接的路径中的所有目录都具有执行权限。否则，还原会话将失败。
- 如果启用 SELinux，将不支持“灾难恢复”（“增强型自动灾难恢复”或“一键式灾难恢复”）。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。

Serviceguard 群集

对于 Serviceguard 群集，Data Protector 代理 (磁盘代理、介质代理) 必须单独安装在“每个群集节点”(本地磁盘) 而不是共享磁盘上。

安装之后，需要将*虚拟主机*（应用程序包）作为客户机导入单元中。因此，应用程序包（例如 Oracle）必须使用它的*虚拟 IP* 在群集上运行。在导入客户机之前，使用命令 cmviewcl -v 来检查这一点。

您可以使用被动节点来安装安装服务器。

Novell Open Enterprise Server

在 Novell Open Enterprise Server (OES) 系统上，Data Protector 会自动安装 OES 感知磁盘代理。但是，存在一些特定于 Novell OES 的方面：

- 如果在 32 位 SUSE Linux Enterprise Server (SLES) 上安装 Novell OES，则在系统上安装 Data Protector Linux 客户机之后，必须同时升级 Data Protector 客户机。

  请注意，在升级过程中，新的 Novell OES 感知磁盘代理将被远程安装到客户机系统上。

- 如果从 SLES 中删除了 Novell OES 组件，则必须重新安装 Data Protector 客户机。

远程安装

使用 Data Protector 图形用户界面，通过将 Data Protector 组件从适用于 Linux 的安装服务器分发到 Linux 系统来远程安装 Linux 客户机系统。有关分发软件的逐步式过程，请参见远程安装。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

在带有 /tmp 目录的 Linux 计算机上进行远程安装

如果 /tmp 是使用 noexec 装载的，则支持远程安装。要在 /tmp 目录中装载了 noexec 的 Linux 客户机系统上进行远程安装，请在安装服务器上设置 omnirc 变量 OB2NOEXEC=1 。

在本地安装

如果在您的环境中未安装适用于 Linux 的安装服务器，则必须从 UNIX 安装包 (tar) 执行本地安装。

在带有 /tmp 目录的 Linux 计算机上进行本地安装

如果 /tmp 是使用 noexec 装载的，则支持本地安装。要在 /tmp 目录中装载了 noexec 的 Linux 客户机系统上进行本地安装，请在系统上设置本地变量 OB2NOEXEC=1 。

将备份设备与 Linux 系统连接

在 Linux 客户机上安装介质代理组件之后，请执行以下步骤将备份设备与系统进行连接：

1. 运行 cat /proc/scsi/scsi 命令来确定可用于驱动器和控制设备 (机械手) 的 SCSI 地址。
2. 在设备上设置 SCSI 地址。根据设备类型，通常可以通过设备上的开关切换来完成设置。有关详细信息，请参见设备自带的文档。

   有关受支持的设备的详细信息，请参阅 https://softwaresupport.softwaregrp.com。
3. 将设备与系统连接，开启设备，然后开启计算机，并等待启动过程完成。设备文件将在启动过程期间创建。

   在 Red Hat Enterprise Linux 系统上，当新设备与系统连接时，启动过程中将会启动应用程序 Kudzu。按任意键启动该应用程序，然后单击“配置”按钮。
4. 要验证系统是否正确识别新的备份设备，请先运行 cat /proc/scsi/scsi ，然后运行 dmesg |grep scsi 。此时会列出每个已连接备份设备的设备文件。

   示例

   对于机械手， dmesg |grep scsi 命令的输出为:

   ```
   Detected scsi generic sg2 at scsi2, channel 0, id 4, lun 0, type 8
   ```

   对于驱动器，输出为：

   ```
   Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
   ```
5. 在 /dev 目录中创建设备文件。要检查是否创建了指向设备文件的链接，请执行：

   ```
   ll /dev | grep device_file
   ```

   例如：

   ```
   ll /dev | grep sg2
   ```

   该命令的输出为：

   ```
   lrwxrwxrwx 1 root root 3 Nov 27 2001 sg2 -> sgc
   ```

   其中， /dev/sg2 是指向设备文件 /dev/sgc 的链接。这意味着，对于机械手，Data Protector 使用的设备文件为 /dev/sgc ，对于驱动器，它使用的设备文件为 /dev/st0 。机械手的设备文件为 sga 、 sgb 、 sgc … sgh ，驱动器的设备文件为 st0 、 st1 … st7 。

下面的步骤

完成安装过程，并将备份设备与 Linux 客户机系统正确连接之后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”，了解有关配置备份设备、介质池，或其他配置任务的信息。

安装 IBM AIX 客户机

可以通过 UNIX 安装包 (tar) 在本地安装 IBM AIX 客户机。

在启动安装进程之前，先确定需要在客户机系统上安装哪些组件。

IBM HACMP Cluster

在适用于 AIX 的 IBM 高可用性群集多处理环境中，在所有群集节点上安装 Data Protector 磁盘代理 组件。有关如何在安装了群集感知应用程序数据库的群集环境中安装 Data Protector 的信息，请参阅安装 Data Protector 集成客户机。

安装之后，将群集节点和“虚拟服务器”(虚拟环境包 IP 地址) 导入 Data Protector 单元。

在本地安装

您必须从 UNIX 安装包 (tar) 中执行本地安装。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

将备份设备与 AIX 客户机连接

在 AIX 客户机上安装介质代理组件之后，执行以下步骤：

1. 关闭计算机，并将备份设备与 SCSI 总线进行连接。检查是否有任何其他设备在使用为备份设备选择的同一 SCSI 地址。
2. 开启计算机，并等待启动过程完成。启动 AIX 系统 smit 管理工具，并验证系统是否正确识别新的备份设备。

   使用 smit 将设备的默认块大小更改为 0 (可变块大小)。
3. 从 /dev 目录中选择相应的设备文件，并配置 Data Protector 备份设备。

   请仅使用非重绕样式的设备文件。例如，选择 /dev/rmt0.1 而非 /dev/rmt0 。

下面的步骤

完成安装过程，并将备份设备与 AIX 系统正确连接之后，配置备份设备、介质池或完成其他 Data Protector 配置任务。

UNIX 系统上的本地安装

可以通过 UNIX 安装包 (tar) 在本地安装 Data Protector 客户机：

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。

OpenVMS 客户机可以本地安装。不支持远程安装。

以下先决条件适用:

- 有关系统要求、磁盘空间要求、受支持的平台、处理器和 Data Protector 组件的信息，请参阅支持矩阵。
- 您必须具有每个目标系统上的 root 权限。
- 安装必须使用 POSIX shell (sh)。

您也可以使用以下步骤在本地升级 UNIX 客户机。脚本将会检测先前的安装，并提示您执行升级。

本地安装 UNIX 客户机

1. 复制 HP-UX 或 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 在 LOCAL_INSTALL 目录中，执行 omnisetup.sh 命令。
   命令的语法如下：
   omnisetup.sh [-source directory] [-server name] [-install component_list] 其中:
   - *目录*是提取安装包所在的位置。如果未指定，则使用当前目录。
   - *name* 是要将客户机导入到的 Cell Manager 单元的完整主机名。如果未指定，则不会自动将客户机导入单元。I在升级 Cell Manager 或安装服务器上的客户机时，不需要指定 -install component_list 。在此情况下，安装程序在升级前将选择与系统上已安装的组件相同的组件，而不会发出提示。
   - *component_list* 是要安装的组件代码的逗号分隔列表。不允许有空格。如果未指定 -install 参数，则安装程序会对在系统上安装每个可用组件分别给出提示。在升级客户机的情况下，安装程序在升级前将选择与系统上已安装的组件相同的组件，而不会发出提示。

下表显示了组件的列表。准确的组件列表取决于组件在特定系统上是否可用。

Data Protector 组件代码

组件代码	组件
cc	用户界面
da	磁盘代理
ma	常规介质代理
ndmp	NDMP 介质代理
informix	Informix 集成
lotus	Lotus 集成
oracle8	Oracle 集成
mysql	MySQL 集成
postgresql	PostgreSQL 集成
vepa	虚拟环境集成
sybase	Sybase 集成
sap	SAP R/3 集成
sapdb	SAP MaxDB 集成
saphana	SA HANA 集成
db2	DB2 集成
smisa	3PAR SMI-S 代理
ssea	P9000 XP 代理
netapp	NetApp 存储提供程序
StoreOnceSoftware	StoreOnce Software Deduplication
autodr	自动灾难恢复
docs	英语文档（指南、帮助）
fra_ls	法语文档（指南、帮助）
jpn_ls	日语文档（指南、帮助）
chs_ls	简体中文文档（指南和帮助）

示例

以下示例显示了如何在客户机上安装“磁盘代理”、“常规介质代理”、“用户界面”和“Informix 集成”组件，并且使用 Cell Manager computer.company.com 将该客户机自动导入到单元中:
./omnisetup.sh -server computer.company.com -install da,ma,cc,informix

1. 如果安装完成，并且客户机导入到 Data Protector 单元中，安装程序将会通知您。

CORE 组件在首次选择安装任意软件组件时安装。

CORE-INTEG 组件在首次选择安装或重新安装任意集成软件组件时安装。

从硬盘运行安装

要将安装包复制到计算机，并且从硬盘运行 UNIX 客户机的安装或升级，则至少要复制 hpux/DP_DEPOT 和 LOCAL_INSTALL 目录。

Linux 仓库不支持本地安装。即使在 Linux 系统上，也必须复制 UNIX 仓库。

例如，如果将安装包复制到 /var/dp80 ，则目录必须是 /var/dp10 的子目录:

- # pwd
- /var/dp80
- # ls
- DP_DEPOT
- LOCAL_INSTALL

将其复制到硬盘之后，更改为 LOCAL_INSTALL 目录并执行以下命令:
omnisetup.sh [-server name] [-install component_list]

例如： ./omnisetup.sh -install da

请注意，如果将 DP_DEPOT 目录复制到其他目录 (例如，由于硬盘空间限制)，则还需要使用 -source 选项。

下面的步骤

如果在安装期间未指定 Cell Manager 的名称，客户机将不会被导入单元中。在这种情况下，应使用 Data Protector 图形用户界面导入它。

安装 OpenVMS 客户机

- OpenVMS 客户机的安装过程必须在受支持的 OpenVMS 系统上本地执行。不支持远程安装。
- 产品只能安装在系统磁盘上的 SYS$COMMON:[OMNI] 中。
- 在 OpenVMS 上不能显示补丁级别。

您可以在运行 OpenVMS 的系统上安装 Data Protector 磁盘代理和用户界面 (仅命令行界面)。

有关更多特定于 OpenVMS 的信息，请参见OpenVMS 发行说明，它位于 OpenVMS 上的默认帮助文档目录中，例如：SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTES 。

安装过程

安装过程可以通过 Data Protector Windows 安装程序包 (zip) 执行。

在 OpenVMS 系统上安装 Data Protector 客户机

1. 如果已经有 PCSI 安装文件，则转至步骤 2。要获取 PCSI 安装文件，请在 OpenVMS Server 上提取安装程序包，并将其复制到所需位置。您也可以从 Windows 系统通过 ftp 获取 PCSI 文件。
2. 运行以下命令：

   ```
   $ PRODUCT INSTALL DP /SOURCE=device:[directory]
   ```

   其中， device:[directory] 是 .PCSI 安装文件的位置。
3. 通过对提示回答 YES 来确认工具包的版本:

   示例

   ```
   The following product has been selected: AXPVMS DP A08.00-xx Layered Product Do you want to continue? [YES]
   ```
4. 选择要安装的软件组件。采用默认选择，这样将会安装磁盘代理和用户界面。您也可以单独选择每个组件。

   对于每个选定产品和对于可能安装的任意产品，可能会要求您选择一些选项（如果有），以满足软件依赖关系要求。

   示例

   ```
   HP IA64VMS DP A08.00-xx: HP OpenVMS IA64 Data Protector V8.00

   (c) COPYRIGHT MICRO FOCUS COMPANY 2018

   Do you want the defaults for all options? [YES] NO

   Do you wish to install Disk Agent for this client node?

   [YES] YES

   Do you wish to install Command Language Interface for this client node?

   [YES] YES

   Do you want to review the options?

   [NO] YES

   HP IA64VMS DP X08.00-xx: HP OpenVMS IA64 Data Protector V8.00 [Installed]

   Do you wish to install Disk Agent for this client node?

   YES

   Do you wish to install Command Language Interface for this client node?

   YES

   Are you satisfied with these options?

   [YES] YES
   ```

   Data Protector 目录和文件的默认且唯一的位置为：

   ```
   SYS$SYSDEVICE:[VMS$COMMON.OMNI]
   ```

   目录结构将会自动创建，文件将放在该目录树中。

   Data Protector 启动和关闭命令过程将放入

   ```
   SYS$SYSDEVICE:[VMS$COMMON.SYS$STARTUP]
   ```

   对于 OpenVMS 客户机，总是存在四个文件，只有选择 CLI 选项时，才会存在第五个文件。有关的 5 个文件为：

   - SYS$STARTUP:OMNI$STARTUP.COM 它是启动该节点上的 Data Protector 的命令过程。
   - SYS$STARTUP:OMNI$SYSTARTUP.COM 它是定义 OMNI$ROOT 逻辑名称的命令过程。该客户机所需的任何其他逻辑名称可以添加到该

命令过程中。

- SYS$STARTUP:OMNI$SHUTDOWN.COM 它是关闭该节点上的 Data Protector 的命令过程。
- OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM 它是用于启动 TCP/IP INET 进程的命令过程，然后该进程会执行由 Cell Manager 发送的命令。
- OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM 它是定义调用 Data Protector CLI 所需符号的命令过程。只有在安装期间选择 CLI 选项时，系统上才会存在该文件。

  请针对所有将使用 CLI 界面的用户，从 login.com 过程执行该命令过程。在该过程中会定义几个正确执行 CLI 命令所必需的逻辑名称。

5. 在 SYS$MANAGER:SYSTARTUP_VMS.COM 中插入以下行:

   @sys$startup:omni$startup.com

6. 在 SYS$MANAGER:SYSHUTDWN.COM 中插入以下行:

   @sys$startup:omni$shutdown.com

7. 确保可以从 OpenVMS 客户机连接 Cell Manager 的所有可能的 TCP/IP 别名。
8. 使用 Data Protector 图形用户界面将 OpenVMS 客户机导入 Data Protector 单元。

在安装期间会创建名为 OMNIADMIN 的帐户。 OMNI 服务使用该帐户运行。

该帐户的登录目录为 OMNI$ROOT:[LOG]，它保存 Data Protector 组件每次启动的日志文件 OMNI$STARTUP_INET.LOG 。该日志文件包含执行请求的进程的名称、所用 Data Protector 映像的名称，以及请求的选项。

任何意外错误都记录在该目录中的 DEBUG.LOG 中。

> **注意**在 OpenVMS 8.3 和更高版本上，Data Protector 安装会显示以下消息： %PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0800 -XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit is not signed and therefore has no manifest file 要避免发出该警告，请使用 /OPTION=NOVALIDATE_KIT 运行产品安装命令。

> **注意**如果需要将 OpenVMS 客户机的默认 TCP 端口从 5565 更改为 5555，请编辑 sys$startup:omni$startup.com 文件。

在群集环境中安装

如果使用公用系统磁盘，则客户机软件只需安装一次。但是，对于每个节点，需要执行 OMNI$STARTUP.COM 过程，节点才可用作 Data Protector 客户机。如果使用的不是公用系统磁盘，则需要在每台客户机上安装客户机软件。

如果使用群集 TCP/IP 别名，并且如果使用群集公用系统磁盘，则可以为别名定义客户机。定义别名客户机后，不需要配置各个客户机节点。您可以选择客户机定义或别名定义以在群集中运行备份和还原。根据您的配置，保存或还原可能可以使用，也可能不能使用到磁带设备或磁带库的直接路径。

磁盘代理配置

OpenVMS 上的 Data Protector 磁盘代理支持装载的 FILES-11 ODS-2 和 ODS-5 磁盘卷。不需要配置 OpenVMS 磁盘代理。但是，在设置将使用它的备份规范时，需要记住几点。下面介绍这几点：

- 输入 GUI 或传递给 CLI 的文件规范必须使用 UNIX 样式语法，例如：

  /disk/directory1/directory2/.../filename.ext.n

  - 字符串必须以斜杠开头，后跟磁盘、目录和文件名，中间用斜杠分隔。
  - 不要在磁盘名称后面加冒号。
  - 版本号前面应该用句点，而不是分号。
  - OpenVMS 文件的文件规范不区分大小写，驻留在 ODS-5 磁盘上的文件除外。

示例

OpenVMS 文件规范：

```
$1$DGA100:[USERS.DOE]LOGIN.COM;1
```

必须使用以下形式指定给 Data Protector：

```
/$1$DGA100/USERS/DOE/LOGIN.COM.1
```

> **注意**没有隐式版本号。必须始终指定版本号，且仅备份指定的文件版本。对于一些允许使用通配符的选项，可以将版本号替换为星号 '*'。要在备份中包括文件的所有版本，则应在 GUI 中进行选择，或者在 CLI 中在 -only 选项下包括文件规范，并使用通配符作为版本号，如下:
> ```
> /DKA1/dir1/filename.txt.*
> ```

命令行界面

在 OpenVMS 上使用 Data Protector 命令行界面之前，必须先运行 CLI 命令设置过程，如下：

```
$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM
```

下面的步骤

有关其他配置任务的信息，请参阅《Data Protector 帮助》索引: "OpenVMS"。

远程安装

远程安装

每次执行远程安装时，都需要通过 GUI 访问安装服务器。用户界面组件可安装在 Cell Manager 上 (虽然这不是必需的)。明智的做法是在多台系统上安装用户界面，这样就可以从不同的位置访问 Cell Manager。可以从适用于 Windows 的安装服务器将客户机软件分发到任何 Windows 系统。Windows 系统必须通过 Data Protector Windows 安装程序包 (zip) 进行本地安装。可以从适用于 UNIX 系统的安装服务器将客户机软件远程安装到 HP-UX、Solaris、Linux、AIX 以及其他受支持的 UNIX 操作系统上。有关受支持平台的列表，请参阅 Data Protector 支持矩阵。尽管在本地安装客户机不需要安装服务器，但保持客户机补丁更新需要它。对于不支持远程安装的 UNIX 操作系统，可以从 Data Protector UNIX 安装包 (tar) 本地安装 UNIX 客户机。

使用 Data Protector 用户界面将软件分发到客户机上。支持跨平台客户机安装。

先决条件

- 有关安装的先决条件和建议，请参见介绍特定客户机安装过程的章节。
- 有关受支持平台、Data Protector 组件和磁盘空间要求的信息，请参阅最新支持矩阵。
- 此时，您应当已在网络上安装了 Cell Manager 和安装服务器。
- 在适用于 Windows 的安装服务器上，本地操作系统“管理员”用户组中的某个用户帐户在远程安装期间由安装服务器使用: 运行以下命令以设置安装服务器用户:

  ```
  omniinetpasswd -inst_srv_user User@Domain
  ```

  安装服务器系统上的本地管理员帐户已足够，但如果域帐户是本地管理员组的一部分，则该帐户也可以使用。
- 关于全新远程安装，适用于 Windows 的安装服务器必须驻留在共享目录中，从而在网络上可见。
- *Windows 2012 :* 要远程安装到 Windows 2012 系统，请完成以下步骤之一:

  在“安装服务器主机”上配置作为远程主机管理员的域用户 (omniinetpasswd -inst_srv_user)。在此帐户下启动远程安装，并在无其他用户干预的情况下建立到远程主机的连接。

  或

  在**远程主机**上的防火墙内阻止以下服务。

  - 远程服务管理 (RPC)
  - 远程服务管理 (RPC-EPMAP)

  或

  关闭“安装服务器主机”上的 RPC/TCP (客户机端)。

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
  ```

  ```
  DWORD SCMApiConnectionParam = 0x80000000
  ```

  合并 SCMApiConnectionParam 注册表值和掩码值 0x80000000 。

  > **注意**不需要重新启动系统。

配置防火墙以成功进行远程安装

用安装服务器安装新的 Data Protector 客户机或升级较旧的 Data Protector 客户机时，将在远程计算机上启动安装代理。安装服务器随即通过 Data Protector 单元端口（默认是 5555/5565）连接到该代理。但是，如果客户机上正在运行 Microsoft 防火墙或任何第三方防火墙软件，就无法建立连接，安装将失败。要解决此问题，请执行以下步骤之一：

- 将 Windows 防火墙配置为允许通过特定端口连接。
- 对于 Microsoft 防火墙: 如果在安装服务器上设置了 omnirc 选项 OB2FWPASSTHRU ，则安装代理将自动向 Windows 防火墙注册，且安装继续正常进行。
- *Linux 系统 :* 出于安全原因，建议使用安全 shell 进行 Data Protector 远程安装。配置 SSH 时，将使用无密码身份验证，否则将提示用户输入凭据。

  要使用安全 shell，请在客户机和安装服务器上安装并设置 OpenSSH。如果对私钥加密，则在安装服务器上安装并设置 keychain。

> **注意**您无法将软件分发到另一个 Data Protector 单元中的客户机上。但是，如果具有独立的安装服务器，可以将它导入多个单元。然后，可以通过依次使用与每个 Cell Manager 连接的 GUI 在每个不同单元中分发软件。

- *管理员帐户 :* 要使用属于**远程主机**上管理员组成员的本地用户（远程主机已启用 UAC），则在远程主机上完成以下任一步骤：

禁用用户帐户控制 (UAC)

> **注意**需要重新启动系统。

或

设置注册表值：

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

DWORD LocalAccountTokenFilterPolicy = 1

> **注意**不需要重新启动系统。

使用安全 shell 进行远程安装

通过安全 shell 以安全方式安装 Data Protector 组件，可以帮助您保护客户机和安装服务器。通过以下方式实现高级保护：

- 通过公钥-私钥对机制以安全方式为客户机验证安装服务器用户。
- 通过网络发送加密的安装包。

> **注意**只有 UNIX 系统支持安全 shell 安装。

设置 OpenSSH

在客户机和安装服务器上同时安装并设置 OpenSSH:

1. 确保系统上安装了 OpenSSH。有关详细信息，请参见操作系统文档或分发文档。

   如果 OpenSSH 包不是 OS 分发的一部分，则需要从 http://www.openssh.org 下载 OpenSSH，然后将其同时安装在 Data Protector 客户机和安装服务器上。

   或者，在 HP-UX 上，可以使用 HP-UX Secure Shell。

   > **注意**安全 shell 安装的默认位置为 /opt/ssh 。

2. 在安装服务器上，运行 ssh-keygen 以生成公钥-私钥对。在 Installation Server 上保留私钥，同时将公钥传输到客户机。请注意，如果使用加密私钥 (即受密码保护)，则需要在安装服务器上设置 keychain。

   有关 ssh-keygen 的信息，请参阅 http://man.openbsd.org/ssh-keygen。

3. 使用名称 authorized_keys 将公钥存储在客户机的 $HOME/.ssh 目录中。

   > **注意** $HOME/.ssh 通常是 root 用户的主目录。

   要设置 SSH 协议版本 (SSH1 或 SSH2)，请修改以下文件中的 protocol 参数:

   1. 在安装服务器上:

      ssh_install_directory /ssh/etc/ssh_config

      ssh 命令将使用该文件。

   2. 在客户机上：

      ssh_install_directory /ssh/etc/sshd_config

      ssh 后台程序 (sshd) 将使用该命令。

   请注意，这两个文件必须同步。

> 注意默认的 SSH 协议版本为 SSH2。

4. 在客户机上，启动 ssh 后台程序:

   ssh_install_directory /ssh/sbin/sshd

5. 通过运行以下命令，将客户机添加到已知主机的列表 (位于安装服务器上的 $HOME/.ssh/known_hosts 中) 中:

   ssh root@client_host

   其中， client_host 必须为完全限定 DNS 名称，例如:

   ssh root@client1.company.com

设置 keychain

keychain 是一个工具，利用它可以在解密私钥时无需手动提供通行密码。只有私钥进行加密的情况下才需要它。要设置 keychain，请完成以下步骤:

1. 将 keychain 从 http://www.funtoo.org/Keychain 下载到安装服务器。
2. 在 $HOME/.profile 中添加以下两行:

   HP-UX 和 Solaris 系统：

   keychain_install_directory /keychain-keychain_version/keychain $HOME/.ssh/private_key

   . $HOME/.keychain/'hostname'-sh

   Linux 系统：

   /usr/bin/keychain $HOME/.ssh/private_key

   . $HOME/.keychain/'hostname'-sh

3. 在安装服务器上，将 OB2_ENCRYPT_PVT_KEY omnirc 选项设置为 1。有关 omnirc 选项的详细信息，请参阅《Data Protector 故障诊断指南》。

   如果因执行此命令失败而无法执行安全 shell 安装，将发出一个警告。但是，将使用标准 Data Protector 远程安装方法继续安装。

下面的步骤

设置 OpenSSH 和 keychain 后，使用 GUI，或使用 CLI 通过运行 ob2install 命令向单元中添加客户机。

> **注意**如果因为执行命令发生失败而无法执行安全 shell 安装，则会发出一条警告消息。但是，安装将继续使用标准 Data Protector 远程安装方法。

向单元添加客户机

要将 Data Protector 软件分发到不在 Data Protector 单元中的客户机上，请完成以下步骤:

1. 单击“开始”>“程序”>“Data Protector”>“Data Protector Manager”启动 Data Protector GUI。

   > **注意**有关 Data Protector 图形用户界面的详细信息，请参阅 Data Protector 图形用户界面和《Data Protector 帮助》。

2. 在 Data Protector Manager 中，切换到**客户机 (Clients)** 环境。
3. 在“范围窗格”中，右键单击**客户机**，然后单击**添加客户机**。
4. 如果配置了多个安装服务器，则选择要安装的客户机的平台 (UNIX 或 Windows) 和用于安装客户机的安装服务器。单击“下一步”。
5. 键入客户机的名称，或搜索要安装的客户机（仅限于 Windows GUI 中）。单击“下一步”。
6. 选择要安装的 Data Protector 组件。请注意，您只能选择一种介质代理。
7. 要更改安装的默认用户帐户和目标目录（仅限于 Windows 中），请单击**选项 (Options)**。
8. 如果已选择多个客户机并且要在每个客户机上安装不同组件，请单击**为各个客户机分别指定组件**，然后单击**下一步**。单独为每个客户机选择要安装的组件。
9. 单击“下一步”。
10. 单击**完成 (Finish)** 开始安装。
11. 在安装过程中和受到请求时，提供所需的数据（用户名、密码和（在 Windows 上还需提供）域）来访问特定客户机系统，然后单击**确定**。

在系统上安装 Data Protector 软件并将系统添加到 Data Protector 单元中之后，它会成为 Data Protector 客户机。

> **注意**在客户机系统上开始使用 Data Protector GUI 之前，将该系统的某个用户添加到相应的 Data Protector 用户组。有关步骤和可用用户权限的说明，请参阅 Data Protector 帮助。

> **注意**密码缓存功能用于推送安装、添加组件和升级。

密码缓存

如果管理员/root 用户在所有主机中具有相同的凭据，则输入一个主机的凭据就足够了，因为其他客户机使用相同的凭据。这适用于推送安装、添加组件和客户机升级。

- **CLI**: 对于 ob2install 命令，可以为第一个主机输入凭据，其余主机则留为 "-"，这些主机将使用相同的凭据。
- **GUI**: 第一个主机的凭据将用于其余客户机。

如果特定主机具有不同的凭据，系统会提示用户输入新凭据。在推送安装中，新输入的凭据将用于其余客户机。

以下是推送安装中凭据的使用顺序:

- ob2install 命令中输入文件的凭据 (适用于 linux 和 hp-ux 计算机) - 必须为第一个客户机输入凭据。
- 缓存的凭据 - 为先前成功的客户机输入的凭据。
- 出现提示时输入的凭据。

除非输入文件中没有凭据且缓存凭据失败，否则，系统不会提示用户输入密码来连接客户机。此功能默认情况下已启用。可以通过设置全局变量 `UseCommonCred=0` 来禁用此功能。

故障诊断

完成远程安装时，可以使用 GUI 通过单击**操作 (Actions)** 和**重新启动失败的客户机 (Restart Failed Clients)** 来重新启动任意失败的安装过程。

安装 ADIC/GRAU 库介质代理

Data Protector 提供专用的 ADIC/GRAU 策略，用于将 ADIC/GRAU 库配置为 Data Protector 备份设备。您需要在将与 ADIC/GRAU 库中的驱动器物理连接的每个系统上安装 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)。此外，对于多主机配置，必须在控制 ADIC/GRAU 库机械手的系统上安装 Data Protector 介质代理。请注意，多主机配置是库和驱动器不连接到同一计算机的配置。

对于 ADIC/GRAU 库，安装了介质代理软件并通过 GRAU/ADIC DAS 服务器访问库机械手的每个系统称作 **DAS 客户机**。

> **注意**您需要特别的许可证，具体取决于在 StorageTek 库中使用的驱动器和插槽数量。

连接库驱动器

将库驱动器与要安装介质代理软件的系统进行物理连接。

有关受支持 ADIC/GRAU 库的详细信息，请参阅 https://softwaresupport.softwaregrp.com。

准备 Data Protector 客户机以使用 ADIC/GRAU 库

以下步骤与配置 ADIC/GRAU 库有关，应在安装介质代理软件之前完成它们：

1. 如果 DAS 服务器基于 OS/2，则在配置 DData Protector ADIC/GRAU 备份设备之前，请创建/更新 DAS 服务器计算机上的 C:\DAS\ETC\CONFIG 文件。在该文件中，必须定义所有 DAS 客户机的列表。对于 Data Protector，这意味着必须在文件中定义每个可以控制库机械手的 Data Protector 客户机。

   每个 DAS 客户机都用唯一的客户机名称（无空格）进行标识，例如 DP_C1 。例如， C:\DAS\ETC\CONFIG 文件的内容应类似如下:

   ```
   client client_name = DP_C1, # hostname = AMU,"client1" ip_address = 19.18.17.15, requests = complete, options = (avc,dismount),
   volumes = ((ALL)), drives = ((ALL)), inserts = ((ALL)), ejects = ((ALL)), scratchpools = ((ALL))
   ```

2. 在安装有需要访问 ADIC/GRAU DAS 库机械手的 Data Protector 介质代理的每个 Data Protector 客户机上，编辑 omnirc 文件并设置以下选项:

DAS_CLIENT	在 DAS 服务器上定义的唯一 GRAU 客户机名称。例如，如果客户机名称为 "DP_C1"，则 omnirc 文件中的相应行为 DAS_CLIENT=DP_C1.
DAS_SERVER	DAS 服务器的名称。

3. 您必须确定 ADIC/GRAU 库插槽分配策略的配置方式（静态或动态）。有关如何检查所用分配策略是何种类型的信息，请参见AMU 参考手册。

   静态策略对于每个 volser 具有专用的插槽，而动态分配策略则随机分配插槽。根据已设置的策略，您需要相应地配置 Data Protector。

   如果配置了静态分配策略，则需要向控制库机械手的系统中添加以下 omnirc 选项：

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

   > **注意**它适用于 HP-UX 和 Windows。

   有关 ADIC/GRAU 库配置的更多问题，请与当地 ADIC/GRAU 支持人员联系，或者查看 ADIC/GRAU 文档。

安装介质代理来使用 ADIC/GRAU 库

安装过程包含以下步骤：

1. 使用 Data Protector 图形用户界面和安装服务器，将介质代理组件分发到客户机。
2. 安装 ADIC/GRAU 库：
   - 在 Windows 系统上，执行以下操作：
     a. 将 aci.dll 、 winrpc32.dll 和 ezrpc32.dll 库复制到 Data_Protector_home\bin 目录。（这三个库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上或 AMU-PC 上的 C:\DAS\AMU\ 目录中可以找到它们。）
     b. 同时将这三个文件复制到 %SystemRoot%\system32 目录中。
     c. 将 Portinst 和 Portmapper service 复制到 DAS 客户机上。（这些必需文件是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上可以找到它们。）
     d. 在“控制面板”中，依次转至“管理工具”和“服务”，并启动 portinst 来安装 portmapper 。DAS 客户机需要重新启动才能运行 portmapper 服务。
     e. 重新启动系统之后，检查是否 portmapper 和两个 rpc services 都在运行 (在“控制面板”中，依次转至“管理工具”和“服务”)，并检查服务的状态。
   - 在 HP-UX 系统上，将 libaci.sl 共享库复制到 /opt/omni/lib 目录中。您必须具有访问该目录的权限。请确保共享库对于所有用户（root、组和其他对象）都具有读取和执行权限。 libaci.sl 共享库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上可以找到它。
   - 在 AIX 系统上，将 libaci.o 共享库复制到 /usr/omni/lib 目录中。您必须具有访问该目录的权限。请确保共享库对于所有用户（root、组和其他对象）都具有读取和执行权限。 libaci.o 共享库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上可以找到它。

在此阶段，应已连接了硬件并正确安装了 DAS 软件。

从默认的 Data Protector 管理命令位置，执行 devbra -dev 命令来检查库驱动器是否与系统正确连接。

查看库驱动器和列表中显示的相应设备文件。

下面的步骤

安装介质代理并将 ADIC/GRAU 库与系统进行物理连接之后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”，了解有关其他配置任务 (例如配置备份设备和介质池) 的信息。

安装 StorageTek 库介质代理

Data Protector 提供一个专用的 StorageTek ACS 库策略，用于将 StorageTek ACS 库配置为 Data Protector 备份设备。您需要在将与 StorageTek 库中的驱动器物理连接的每个系统上安装 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)。此外，对于多主机配置，必须在控制 StorageTek 库机械手的系统上安装 Data Protector 介质代理。请注意，多主机配置是库和驱动器不连接到同一计算机的配置。

对于 STK ACS 集成，安装了介质代理软件并通过 STK ACS 服务器访问库机械手的每个系统称作 **ACS 客户机**。

> **注意**您需要特别的许可证，具体取决于在 StorageTek 库中使用的驱动器和插槽数量。

连接库驱动器

将库驱动器与要安装介质代理软件的系统进行物理连接。

有关支持的 STK 库的详细信息，请参阅最新支持矩阵。

有关如何将备份设备与系统进行物理连接的信息，请参阅 StorageTek 库随附的文档。

有关如何将备份设备与受支持的 Windows 系统进行物理连接的信息，请参阅 StorageTek 库随附的文档。

安装介质代理来使用 StorageTek 库

1. 使用 Data Protector 图形用户界面和适用于 UNIX 系统的安装服务器将介质代理组件分发到客户机上。
2. 为每个 ACS 客户机启动 ACS ssi 后台程序:

   Windows 系统：

   安装 LibAttach 服务。有关详细信息，请参见 ACS 文档。请确保在 LibAttach 服务配置期间输入相应的 ACSLS 主机名。成功配置之后，LibAttach 服务将自动启动，并且每次系统重新启动之后也会自动启动。

   HP-UX、Solaris 和 Linux 系统：

   运行以下命令：

   ```
   /opt/omni/acs/ssi.sh start ACS_LS_Hostname
   ```

   AIX 系统：

   运行以下命令：

   ```
   /usr/omni/acs/ssi.sh start ACS_LS_Hostname
   ```

   > **注意**安装 LibAttach 服务之后，检查 libattach\bin 目录是否已自动添加到系统路径。如果未添加，则手动添加它。

   有关 LibAttach 服务的详细信息，请参阅 StorageTek 库随附的文档。
3. 从默认的 Data Protector 管理命令位置，执行 devbra -dev 命令来检查库驱动器是否正确连接到系统。

   可以看到列表中显示库驱动器和相应的设备文件/SCSI 地址。

下面的步骤

安装介质代理并将 StorageTek 库与系统进行物理连接之后，请参阅《Data Protector 帮助》索引：“配置，备份设备”，了解有关其他配置任务（例如配置备份设备和介质池） 的信息。

安装群集感知客户机

在安装群集感知客户机时，请注意以下重要事项:

- 所有群集节点上都必须安装 Data Protector 群集感知客户机。
- 不支持在 Windows 上的群集感知 Cell Manager 中添加组件。但是，支持在客户机上添加组件。

Serviceguard

在安装 Serviceguard 之前，请确保 **hpdp** 用户具有相同的 UID 和 GID。安装过程是在 UNIX 客户机上安装 Data Protector 的标准过程。有关详细说明，请参阅安装 HP-UX 客户机和安装 Linux 客户机。

Symantec Veritas

此安装步骤是在客户机系统上安装 Data Protector 的标准步骤。有关详细说明，请参阅安装客户机。

Microsoft 群集服务器

群集感知的 Data Protector 客户机必须在每个群集节点上通过安装包在本地进行安装。群集节点（Data Protector 群集客户机）会在安装期间被导入指定的单元。之后，您需要导入虚拟服务器名称。

执行安装需要群集 Administrator 帐户。除此之外，群集客户机安装与普通 Windows 客户机的安装方式相同。此时将自动安装 MS 群集支持文件。

有关如何本地安装 Data Protector Windows 客户机系统的信息，请参阅安装 Windows 客户机。

Data Protector 安装会报告检测到群集。选择**以群集感知模式安装客户机 (Install client in cluster-aware mode)**。

如果要安装 Data Protector Oracle 集成，则必须在所有群集节点上和 Oracle 资源组的虚拟服务器上执行安装步骤。

> **注意**您可以将群集感知客户机导入使用标准 Cell Manager 或群集感知 Cell Manager 管理的 Data Protector 单元。

IBM HACMP 群集

要在群集节点上安装 Data Protector 组件，请使用在 UNIX 系统上安装 Data Protector 的标准步骤。

安装 Data Protector 集成客户机

> 注意: 有关最新和更新的安装信息，请参阅联机文档。

Data Protector 集成是一些软件组件，通过它们可以使用 Data Protector 运行数据库应用程序 (例如 Oracle Server 或 Microsoft Exchange Server) 的联机备份。Data Protector ZDB 集成是一些软件组件，通过它们可以运行使用磁盘阵列的零宕机时间备份和即时恢复。

运行数据库应用程序的系统称作“集成客户机”；使用 ZDB 磁盘阵列备份和存储数据的系统称作“ZDB 集成客户机”。按照 Windows 或 UNIX 系统上的任何其他客户机的相同安装过程安装此类客户机，假设已选择合适的软件组件 (例如，用于备份 Microsoft Exchange Server 数据库的 MS Exchange Integration 组件)。

可以使用适用于 Windows 或 UNIX 的 安装服务器远程安装集成客户机，或者从 Windows 或 UNIX 安装包 (zip/tar) 本地安装。

有关特定集成客户机的详细信息，请参见以下相应章节：

> 注意Data Protector Express 仅支持安装 Microsoft Hyper-V 客户机和 VMWare 客户机。

- 安装 Microsoft Exchange Server 客户机
- 安装 Microsoft SQL Server 客户机
- 安装 Microsoft SharePoint Server 客户机
- 安装 Microsoft 卷影复制服务客户机
- 安装 Sybase Server 客户机
- 安装 Informix Server 客户机
- 安装 SAP R/3 客户机
- 安装 SAP MaxDB 客户机
- 安装 SAP HANA Appliance 客户机
- 安装 Oracle Server 客户机
- 安装 MySQL 客户机
- 安装 PostgreSQL 客户机
- 安装 IBM DB2 UDB 客户机
- 安装 Lotus Notes/Domino Server 客户机
- 安装 VMware 客户机
- 安装 Microsoft Hyper-V 客户机
- 安装 NDMP Server 客户机

已经安装完集成客户机之后，建议通过在每个客户机上将命令位置添加到相应的环境变量来从任何目录调用 Data Protector 命令。Data Protector 文档中的步骤假设变量值已经扩展。命令位置列在《Data Protector 命令行界面参考》和 omniintro 手册页中的 omniintro 参考页中。

安装后，另请参阅 Data Protector 集成部分、Data Protector 零宕机时间备份管理员部分 或 Data Protector 零宕机时间备份集成部分来配置 Data Protector集成客户机。

远程安装

使用 Data Protector 图形用户界面从安装服务器将客户机软件安装到客户机上。

进行远程安装之后，客户机系统会自动成为 Data Protector 单元的成员。

本地安装

如果所在环境中未安装相应操作系统的安装服务器，则必须通过 Windows 或 UNIX 安装包 (zip/tar) 执行本地安装，具体取决于客户机要安装到的平台。

如果在安装期间未选择 Cell Manager，则必须在本地安装之后将客户机系统手动导入单元中。请参阅导入本地安装的客户机。

安装群集感知集成

Data Protector 群集感知集成客户机必须在每个群集节点上通过安装程序包在本地进行安装。在本地客户机设置和安装的过程中，除了安装其他客户机软件组件之外，还要安装相应的集成软件组件（如 Oracle Integration 或 P6000 / 3PAR SMI-S Agent ）。

您还可以在 Data Protector Cell Manager 上安装群集感知数据库应用程序和 ZDB 代理。在 Cell Manager 安装期间，请选择相应的集成软件

组件。

安装过程取决于安装集成客户机的群集环境。

有关创建群集的详细信息，请参阅《Data Protector 帮助》索引: "cluster, Serviceguard" 和 Data Protector 概念部分。

下面的步骤

安装完成后，请参阅《Data Protector 集成部分》了解有关配置集成的信息。

安装 3PAR StoreServ Storage 客户机

要将 3PAR StoreServ Storage 与 Data Protector 进行集成，请在应用程序和备份系统上安装以下 Data Protector 软件组件:

- P6000 / 3PAR SMI-S Agent

如果要使用卷影复制服务备份和恢复对象，您还需要具备以下组件：

- MS Volume Shadow Copy Integration
- 3PAR VSS Agent

不论是何种操作系统，要执行“ZDB 到磁盘 + 磁带”或“ZDB 到磁带”会话，则还要在备份系统上安装以下 Data Protector 软件组件：

- General Media Agent

安装存储阵列的存储提供程序

This feature is available in the Premium Edition

Data Protector 使用适用于存储阵列的存储提供程序与以下 ZDB 存储阵列集成: NetApp storage。此存储提供程序组件是 Data Protector SMI-S Agent 的插件。它通过 SMI-S Agent 启用相应存储的 ZDB 功能。在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- 根据所使用的存储，安装适用于存储阵列的存储提供程序组件之一 (NetApp Storage Provider).

要执行“ZDB 到磁带”会话，请在备份系统上安装以下 Data Protector 软件组件：

- General Media Agent

与其他应用程序集成

要安装 Data Protector 存储阵列与数据库应用程序的集成或与虚拟环境的集成，请在适用的系统上安装特定于特定集成的 Data Protector 组件，并执行特定于该集成的安装任务。您可以安装与 VMware、Oracle Server、SAP R/3 和 Microsoft SQL Server 的存储阵列集成。请参阅最新的支持矩阵，检查支持存储阵列与特定数据库应用程序或虚拟环境集成的哪些组合。

安装或卸载更改后的块驱动程序

Data Protector 支持 Windows Server 2012 及更高版本的基于块的增量备份。在执行基于块的增量备份之前，必须在以下一个位置安装更改后的块驱动程序:

- 已安装 Cell Manager 的 Windows 系统
- 已安装 Data Protector 磁盘代理的 Windows 客户机

关于更改后的块驱动程序

更改后的块驱动程序是 Windows 卷过滤器驱动程序，可跟踪系统上现有 NTFS 卷的更改后的块。在基于块的增量备份过程中，驱动程序会识别可用于备份的增量数据。在执行任何基于块的增量备份之前，必须先安装此驱动程序。

驱动程序连续监视系统中的所有 NTFS 卷，以识别这些卷上的已修改块。在基于块的备份会话期间，会话消息将通知更改后的块驱动程序是否正在配置选择用于备份的卷。

重要说明:

- 要完成驱动程序的安装或卸载，必须在安装或卸载驱动程序后重新引导系统。
- 当新的 NTFS 卷添加到系统中或受监视的 NTFS 卷大小更改时，必须重新配置驱动程序。

安装更改后的块驱动程序

在已安装 Data Protector 磁盘代理的 Windows 客户机上安装更改后的块驱动程序之前，必须将 Windows 客户机连接到 Cell Manager。

要安装更改后的块驱动程序，请在要安装驱动程序的系统上运行以下命令:

```
omnicc  -chgblkdrvr_install [-force]
```

使用强制选项 [-force] 来安装驱动程序，系统不提示您进行任何其他输入。

重要说明: 为了完成驱动程序的安装，必须在安装驱动程序后重新引导系统。

查看更改后的块驱动程序的安装状态

要查看是否已安装更改后的块驱动程序，请在系统上运行以下命令:

```
omnicc  -chgblkdrvr_status
```

重要说明: 如果您在安装驱动程序后未重新引导系统，则驱动程序安装未完成，并且状态命令显示以下消息: 驱动程序已安装在系统上，但系统尚未重新引导。为了完成驱动程序的安装，必须重新引导系统。

卸载更改后的块驱动程序

要卸载更改后的块驱动程序，请在要卸载驱动程序的系统上运行以下命令:

```
omnicc  -chgblkdrvr_uninstall
```

重要说明: 为了完成驱动程序的卸载，必须在卸载驱动程序后重新引导系统。

重新配置更改后的块驱动程序

要重新配置更改后的块驱动程序，必须先卸载更改后的块驱动程序，然后在 DA 客户机主机系统上重新安装更改后的块驱动程序。在以下情况下，需要重新配置更改后的块驱动程序。

- 需要为基于块的增量备份配置的新 NTFS 卷将添加到已安装更改后的块驱动程序的系统中。除非您重新配置驱动程序，否则已安装的更改后的块驱动程序不会监视这些新添加的 NTFS 卷。
- 由于卷缩小或扩大操作，更改后的块驱动程序所监视的 NTFS 卷的大小可能会有所更改。

影响:

在 DA 客户机系统上重新配置更改后的块驱动程序等同于全新安装驱动程序，这会影响所有已受监视的卷。建议您在源卷上没有更改或更改很少的情况下重新配置更改后的块驱动程序。如果在重新配置期间发生任何源更改，最好对所有卷 (新添加和已受监视的卷) 执行完整备份。

相关主题

- 有关 omnicc 命令的详细信息，请参阅 omnicc。

迁移 **HP-UX Cell Manager**

从 Data Protector 版本 2019.08 (10.50) 开始，Data Protector 不支持将 **HP-UX** 用作 Cell Manager 和安装服务器的平台。Data Protector 继续支持将 **HP-UX** 作为客户机的平台。如果当前环境包含安装在 **HP-UX** 系统上的 Cell Manager，请将 Cell Manager 从 **HP-UX** 系统迁移到 Linux 系统。

要将 Cell Manager 从 **HP-UX** 迁移到 Linux，源 **HP-UX** Cell Manager 和目标 Linux Cell Manager 必须安装 Data Protector 2019.05 (10.40)。

有关从 **HP-UX** 迁移到 Linux 的信息，请参阅:

- 迁移 'HP-UX' Cell Manager
- 从 'HP-UX' 到 Linux Cell Manager 迁移期间要执行的任务

安装后任务

验证 Data Protector 安装

安装 Data Protector 后，可以使用 Data Protector 图形用户界面来验证安装。查看以下部分以确保 Data Protector 软件组件是否已在 Cell Manager 或客户机系统上启动并运行。

验证 Data Protector 安装包括以下内容:

- 检查 Cell Manager 和客户机系统上的 DNS 配置，并确保 Cell Manager 和客户机系统上 omnicheck -dns 命令的结果与指定的系统匹配。
- 检查客户机上安装的软件组件。
- 将某个软件组件安装所需要的文件列表与客户机上已安装的文件进行比较。
- 验证某个软件组件所需要的每个只读文件的校验和 。

先决条件

必须具有适用于客户机系统类型 (Unix、Windows) 的安装服务器。

步骤

1. 在“上下文列表”中，单击**客户机**。
2. 在范围窗格中，展开**客户机**，右键单击 Cell Manager 或客户机系统，然后单击**检查安装**以打开向导。
3. 此时将列出相同类型 (Unix 系统或 Windows 系统) 的所有客户机系统。
4. 遵循向导以验证单元中系统的安装。有关详细信息，请参阅《 **Data Protector** 帮助》。
   “检查安装”窗口随即打开，其中显示了安装结果。

有关如何使用 Data Protector CLI 在 Linux/UNIX 系统上验证安装的信息，请参阅 ob2install 手册页。

从防病毒扫描中排除目录或进程

将防病毒解决方案与 Data Protector 结合使用时，请遵循一般准则以避免在备份或还原期间应用程序中断和性能下降。有关详细信息，请参阅防病毒排除。

卸载 Data Protector

如果您的系统配置更改，则可能要从系统中卸载 Data Protector 软件或删除部分软件组件。

卸载是从系统中删除所有 Data Protector 软件组件，其中包括 Cell Manager 计算机上的配置对此系统的引用。受保护的备份对象根据配置的保留期限保留在内部数据库 (IDB) 和备份介质中，并且可以还原到其他客户端系统。但是，默认情况下，Data Protector 配置数据 (包括自签名证书) 会保留在系统中，因为将来升级 Data Protector 时可能需要这些数据。如果在重新安装后需要生成新证书，请按照“Data Protector 管理员”一章中“在 Data Protector 中重新生成证书”一节所述的步骤进行操作，生成证书并将其分发给客户机。

要在卸载 Data Protector 软件后删除配置数据，请删除安装了 Data Protector 的目录。

如果 Data Protector 安装目录中有其他数据，请确保在卸载 Data Protector 前将这些数据复制到其他位置。否则，卸载过程中将删除这些数据。

从单元中卸载 Data Protector 软件需要以下步骤：

1. 使用 GUI 卸载 Data Protector 客户机软件。请参阅卸载 Data Protector 客户机。
2. 卸载 Data Protector Cell Manager 和安装服务器。请参阅卸载 Cell Manager 和安装服务器。

您也可以不用卸载 Cell Manager 或客户机即卸载 Data Protector 软件组件。在 UNIX 上，还可以手动删除 Data Protector 软件。请参阅在 UNIX 上手动删除 Data Protector 软件。

先决条件

从计算机中卸载 Data Protector 软件前，请检查以下内容：

- 确保计算机的所有相关参考都已从备份规范中删除。否则，Data Protector 将尝试备份未知的系统，而此部分备份规范将会失败。有关如何修改备份规范的说明，请参阅《Data Protector 帮助》索引：“修改，备份规范”。
- 确保要卸载的系统上没有连接和配置备份设备或磁盘阵列。导出系统后，Data Protector 不再能够使用原单元中的备份设备或磁盘列阵。
- 在卸载之前，确保关闭所有未处理的 GRE 开机请求。此外，确保完成或中止正在进行中的实时迁移会话。

卸载 Data Protector 客户机

> **注意**远程卸载过程要求为正在卸载其 Data Protector 软件的平台安装安装服务器。

在 Data Protector GUI 中远程卸载客户机

1. 在“上下文列表 (Context List)”中，切换到**客户机 (Clients)** 上下文。
2. 在“范围窗格”中，展开**客户机**，右键单击要卸载的客户机，然后单击**删除**。此时会询问您是否要同时卸载 Data Protector 软件。
3. 单击**是 (Yes)** 从客户机中卸载所有软件组件，然后单击**完成 (Finish)**。

客户机将从“结果区域”的列表中删除，Data Protector 软件将从硬盘中删除。

请注意，Data Protector 配置数据将保留在客户机系统中。要删除配置数据，请删除安装了 Data Protector 的目录。

卸载群集客户机 如果您的 Data Protector 环境中具有群集感知客户机，您要将其卸载，则必须在本地执行此操作。此过程与卸载 Cell Manager 或安装服务器的情况相同。请参阅卸载 Cell Manager 和安装服务器。群集客户机将从“结果区域”的列表中删除，Data Protector 软件将从其硬盘中删除。

OpenVMS 客户机 无法使用安装服务器远程删除 Data Protector OpenVMS 客户机。必须在本地卸载它。

从 OpenVMS 系统中卸载 Data Protector 客户机

1. 首先使用 Data Protector GUI 从 Data Protector 单元中导出相关的客户机，如从单元导出客户机中所述。

   当询问是否要同时卸载 Data Protector 软件时，选择“否”。

2. 要删除实际的 Data Protector 客户机软件，请登录到 OpenVMS 客户机上的 SYSTEM 帐户并执行以下命令：$ PRODUCT REMOVE DP。对于出现的提示请选择 YES。

> **重要说明**这将关闭 Data Protector 服务并删除 OpenVMS 系统上所有与 Data Protector 关联的目录、文件和帐户。

卸载 Cell Manager 和安装服务器

本节介绍从 Windows 和 Linux 系统上卸载 Data Protector Cell Manager 和安装服务器软件的步骤。

从 Windows 系统中卸载

要从 Windows 系统中卸载 Data Protector 软件，请完成以下步骤:

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 在 Windows 控制面板中，单击**添加/删除程序**。
3. 根据您是否希望在系统上留下配置数据，将应用不同的操作：

> **重要说明**如果卸载后在系统中保留 Data Protector 配置数据，以后又安装了低于所卸载版本的 Data Protector Cell Manager，请注意这些配置数据将不可用。
>
> 要成功安装较低版本，请在安装期间选择将删除配置数据的选项。

   - 要卸载 Data Protector 并将 Data Protector 配置数据保留在系统中，请选择“Data Protector”并单击“删除”。
   - 要卸载 Data Protector 并删除 Data Protector 配置数据，请选择“Data Protector”，单击“更改”，然后单击“下一步”。在“程序维护 (Program Maintenance)”对话框中，选择**删除 (Remove)**。选择**永久删除配置数据**并单击**下一步**。

4. 卸载完成后，单击**完成**退出向导。

卸载在 Serviceguard 上配置的 Cell Manager 和/或安装服务器

如果您的 Cell Manager 和/或安装服务器是在 Serviceguard 群集上配置的，请执行以下步骤来卸载软件。

主节点

登录到主节点，并执行以下步骤：

1. 停止 Data Protector 包：

   cmhaltpkg PackageName

   其中 PackageName 表示群集包名称。

   例如：

   cmhaltpkg ob2cl

2. 停用卷组的群集模式：

   vgchange -c n *vg_name*

   （其中 vg_name 代表位于 /dev 目录的子目录中的卷组的路径名）。

   例如：

   vgchange -c n /dev/vg_ob2cm

3. 激活卷组：

   vgchange -a y -q y *vg_name*

   例如：

   vgchange -a y -q y /dev/vg_ob2cm

4. 将逻辑卷装载为共享磁盘：

   mount *lv_pathshared_disk*

   （其中 lv_path 代表逻辑卷的路径名，shared_disk 代表装载点或共享目录）。

   例如：

   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared

5. 使用 swremove 实用程序删除 Data Protector。
6. 删除软链接：

   rm /etc/opt/omni

   rm /var/opt/omni

7. 删除备份目录：

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

8. 删除 Data Protector 目录及其内容：

rm -rf /opt/omni

9. 卸载共享磁盘：

   umount *shared_disk*

   例如：

   umount /omni_shared

10. 停用卷组：

    vgchange -a n *vg_name*

    例如：

    vgchange -a n /dev/vg_ob2cm

辅助节点

登录到辅助节点，并执行以下步骤：

1. 激活卷组：

   vgchange -a y *vg_name*

2. 装载共享磁盘：

   mount *lv_path shared_disk*

3. 使用 swremove 实用程序删除 Data Protector。
4. 删除软链接：

   rm /etc/opt/omni

   rm /var/opt/omni

5. 删除备份目录：

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

6. 删除 Data Protector 目录及其内容：

   rm -rf /opt/omni

7. 删除共享文件系统中的目录：

   rm -rf shared_disk/etc_opt_omni

   rm -rf shared_disk/var_opt_omni

   例如：

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/etc_opt_omni

8. 卸载共享磁盘：

   umount *shared_disk*

9. 停用卷组：

   vgchange -a n *vg_name*

已将 Data Protector 从系统中完全删除。

卸载在 Veritas Cluster Server 上配置的 Cell Manager 和/或安装服务器

如果 Cell Manager 和/或安装服务器是在 Veritas Cluster Server 上配置的，请执行以下步骤来卸载软件。

主节点

登录到主节点，并执行以下步骤：

1. 使 Data Protector 应用程序资源脱机。
2. 禁用 Data Protector 应用程序资源。
3. 卸载 Data Protector。
4. 删除软链接：

rm /etc/opt/omni

rm /var/opt/omni

5. 删除备份目录：

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

6. 删除 Data Protector 目录及其内容：

   rm -rf /opt/omni

辅助节点

登录到辅助节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到辅助节点。
2. 卸载 Data Protector。
3. 删除软链接：

   rm /etc/opt/omni

   rm /var/opt/omni

4. 删除备份目录：

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

5. 删除 Data Protector 目录及其内容：

   rm -rf /opt/omni

6. 删除共享文件系统中的目录：

   rm -rf shared_disk/etc_opt_omni

   rm -rf shared_disk/var_opt_omni

   例如：

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/var_opt_omni

   已将 Data Protector 从系统中完全删除。

从 Linux 系统中卸载

先决条件

- 使用 omnisetup.sh -bundlerem 命令删除已安装的所有 Data Protector 补丁包。

Cell Manager

适用于 Linux 的 Cell Manager 始终使用 omnisetup.sh 命令在本地安装。因此，必须使用 rpm 实用程序在本地将其卸载。

> **重要说明**如果卸载后在系统中保留 Data Protector 配置数据，以后又安装了低于所卸载版本的 Data Protector Cell Manager，请注意这些配置数据将不可用。
> 要成功安装较低版本，请在卸载后从系统中删除剩余的 Data Protector 目录。

要卸载 Data Protector Cell Manager，请按如下方式继续操作:

1. 确保已终止所有 Data Protector 会话并退出图形用户界面。
2. 输入 rpm -qa | grep OB2 命令，列出 Cell Manager 上安装的所有 Data Protector 组件。

   与 Cell Manager 关联的组件如下:

OB2-CORE	Data Protector 核心软件

OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-DISPATCHER	作业控制引擎调度程序
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。
OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 部分和 WebHelp 格式的《Data Protector 帮助》。

如果系统上还安装了 Data Protector 客户机或安装服务器，则其他组件也将列出。

> **注意**要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 `rpm -e package name` 命令删除上一步中提到的组件并按提示继续。

安装服务器

Linux 上适用于 UNIX 的安装服务器始终使用 `omnisetup.sh` 命令在本地安装。因此，必须使用 `rpm` 实用程序在本地将其卸载。

要卸载 Data Protector 安装服务器，请按如下方式继续操作:

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 输入 `rpm -qa | grep OB2` 命令，列出所有 Data Protector 组件和安装服务器系统上存储的远程安装包。

   与安装服务器关联的组件和远程安装包如下:

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装安装服务器，则已安装该软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器核心软件。
OB2-CFP	适用于所有 UNIX 平台的公用安装服务器核心软件。
OB2-TS-CFP	适用于所有 UNIX 平台的公用安装服务器技术堆栈软件
OB2-DAP	适用于所有 UNIX 系统的磁盘代理远程安装包
OB2-MAP	适用于所有 UNIX 系统的介质代理远程安装包。

OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于所有 UNIX 系统的单元控制台远程安装包。

如果系统上安装了其他 Data Protector 组件，则其他组件也将列出。

> **注意**要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 rpm -e package name 命令删除上一步中提到的组件并按提示继续。

在 UNIX 上手动删除 Data Protector 软件

卸载 UNIX 客户机前，应先将其从单元中导出。

Linux 系统

要手动从 Linux 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni
```

```
rm -fr /etc/opt/omni
```

```
rm -fr /opt/omni
```

Solaris 系统

要手动从 Solaris 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni
```

```
rm -fr /etc/opt/omni
```

```
rm -fr /opt/omni
```

其他 UNIX 系统

使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /usr/omni
```

卸载报告服务器

在 Windows 上卸载报告服务器

完成以下步骤，从 Windows 系统卸载报告服务器软件。

1. 浏览程序列表，选择并右键单击“报告软件”，然后选择“卸载”。
2. 在“程序维护”页中选择“删除”。单击“下一步”。报告软件将会卸载。

在 Linux 上卸载报告服务器

完成以下步骤，从 Linux 系统卸载报告服务器软件。

1. 使用 root 用户凭据登录 Linux 系统。
2. 浏览到 local_install DEPOT 所提取到的文件夹，然后运行以下命令以卸载报告软件:
   sh LOCAL_INSTALL/omnisetup.sh -Delete
   卸载完成后，将显示以下消息:
   Data Protector software successfully uninstalled. Removing all Data Protector directories, including configuration data and IDB files

许可证

本主题包含以下相关信息:

- 新引入的许可证密钥
- Data Protector 许可检查和报告
- 获取和安装 Data Protector 密码
- Data Protector 产品结构和许可证

概述

您必须拥有许可证密钥才能使用 Data Protector 产品。首次安装时，Data Protector 将获得一个即开即用（试用）许可证。试用许可证的有效期为 90 天。在 90 天的试用期到期之前，您必须获取永久许可证才能继续使用 Data Protector。要获取永久许可证，请参阅获取许可证一节。Data Protector 不再显示已到期或无效的许可证。

本主题说明以下几节:

- 许可证类型 -
  - “基于功能的许可”基于功能和备份目标。
  - **基于容量（高级版）的许可**基于受 Data Protector 保护的原始源数据的数量。
  - **基于插座（精简版）的许可**基于用于虚拟机监控程序 (ESX，Hyper-V 节点) 的处理器。
- 选择许可证类型 - 本节说明基于功能的许可证和基于容量 (高级版) 的许可证之间的区别。同一个客户可以利用功能模型和容量模型，但不能在同一个 Cell Manager 或 MoM 环境中将这两个模型结合使用。
- 获取许可证 - 本节提供有关获取新的许可证密钥和请求密码的详细信息。
- 集中式许可 - 通过 Data Protector，可为整个多单元环境配置中央许可，从而简化许可证管理。
- 许可报告 - Data Protector 许可证会被检查，如果丢失，则会在各种 Data Protector 操作期间进行报告。

许可证类型

Data Protector 支持以下许可模式:

- 基于功能的许可: 基于功能和备份目标。基于功能的许可也称为传统许可。
- 基于容量 (高级版) 的许可: 基于受 Data Protector 保护的原始源数据的数量。容量以“前端千吉字节”或前端 TB 为单位。Data Protector 使用 1024 作为计算千吉字节值 (也称为 TiB) 的乘数。例如：1 TB = 1024 GB。
- 基于插座 (精简版) 的许可: 基于用于虚拟机监控程序 (ESX，Hyper-V节点) 的处理器。通过托管虚拟机的物理机上的插座 (处理器) 数量来衡量许可证。

基于功能的许可

Data Protector 产品结构和基于功能的许可模型包含三个主要类别：

与 Cell Manager 相关的许可证

- **Starter Pack**：

  Data Protector Starter Pack 包含：

  - 指定的平台（Windows 和 Linux）上的一个 Cell Manager。
  - 任何平台上无线数量的备份客户机（代理）（仅用于文件系统备份）。
  - 一个驱动器许可证（一个驱动器，此案例中是一个磁带驱动器）
  - 库（最多包含 60 个插槽）
  - 系统灾难恢复选项
  - 基本报告（通过 Data Protector GUI 和 Web 提供）

报告服务器许可证

使用 DP 用户界面浏览 Data Protector 基于 Web 的报告需要报告服务器许可证。

- 您可以浏览任何 Cell Manager 的所有可用 Web 报告。
- 每个 Cell Manager 只能使用一个许可证。
- 如果使用 Manager-of-Manager 进行中央许可，则必须为许可证分配多个值。

备份目标

- **驱动器扩展和库扩展**:
  - 备份驱动器扩展 - 包含用于在一个 Data Protector 单元中管理更多驱动器（加上 Starter Pack 中可管理的一个驱动器）的许可证
  - 库扩展 - 包含用于在一个 Data Protector 单元中管理磁带库（包含更多物理可用的插槽，加上 Starter Pack 中可用的插槽）的使用许可证 (LTU)。

如果在单元中配置的任何项目具有基于源的许可证的对象，则会检查是否有所需的基于实体的许可证及其数量。如果许可证数量少于配置的项目，则 Data Protector 会发出通知。如果在 SAN 环境中为多个 Data Protector 客户机配置了一个备份设备，则必须使用多路径功能以便 Data Protector 将其识别为单备份设备。以下备份目标按照容量进行许可：

- 适用于 1 TB 和 10 TB 的 UNIX 零宕机时间备份
- UNIX 零宕机时间备份非阵列 1 TB
- 适用于 1 TB 和 10 TB 的 UNIX 即时恢复
- 适用于 1 TB 和 10 TB 的 Linux 零宕机时间备份
- Linux 零宕机时间备份非阵列 1 TB
- 适用于 1 TB 和 10 TB 的 Linux 即时恢复

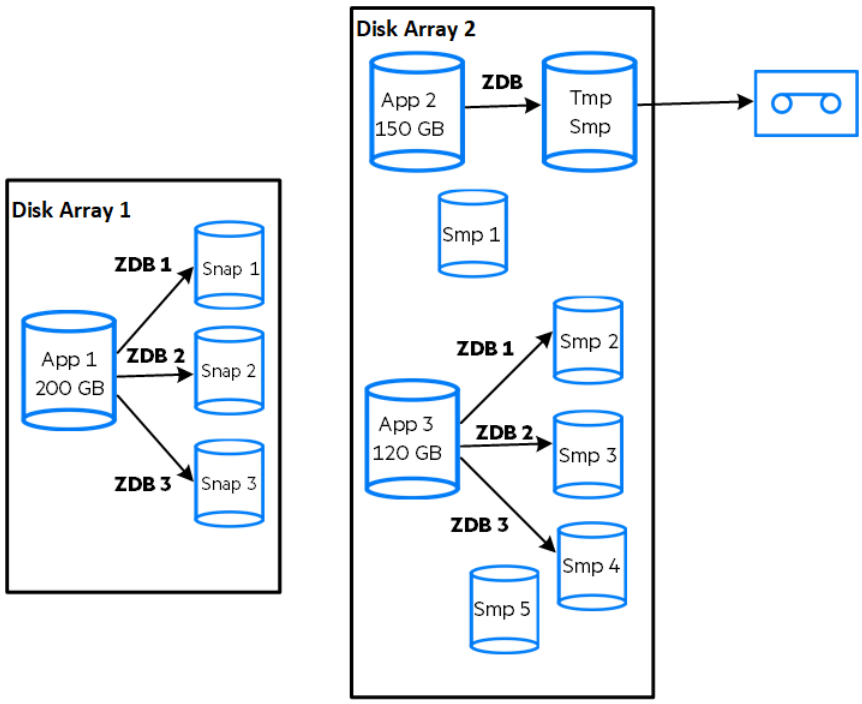
- 适用于 1 TB 和 10 TB 的 Windows 零宕机时间备份
- Windows 零宕机时间备份非阵列 1 TB
- 适用于 1 TB 和 10 TB 的 Windows 即时恢复
- 使用 NDMP 直接备份，适用于 1 TB 和 10 TB
- 高级备份到磁盘，适用于 1 TB、10 TB 和 100 TB
- 备份到 IAP 扩展，适用于 1 TB

检查基于容量的备份目标的许可证（除高级备份到磁盘许可证外）时，会将已备份的逻辑单元上的总磁盘空间量与安装的许可证的容量进行比较。以这种方式进行许可检查是为了即使在许可的容量用尽后也可执行即时恢复或备份。在这些情况下，会在备份会话期间显示警告消息，通知您已超出许可的容量。已用磁盘的容量是基于在每次 ZDB 备份会话期间收集的历史信息进行计算的。计算的时间间隔是二十四小时。Data Protector 基于过去二十四小时内所有会话中使用的磁盘来计算已用磁盘容量，并将计算的容量与许可的容量相比较。如果违反许可，则会在备份期间发出警告消息。此外，许可证报告工具每天运行，如果超出许可容量，则会向 Data Protector 事件日志写入通知。

应用于备份目标的已用容量计算

已用容量计算会计算过去二十四小时内使用的每个磁盘阵列的许可容量。在指定时间间隔内使用过两次或多次的磁盘仅计为一次。磁盘阵列单元使用从每个阵列获取的标识号进行标识。阵列标识号的使用意味着可以知道某阵列已被计入。如果已经运行包括即时恢复的 ZDB 备份，则将为每个磁盘阵列 ZDB 使用的容量以及每个磁盘阵列用于即时恢复的容量计算每个原始单元的总容量。例如，假定有两个磁盘阵列的情况。在一个阵列上有单个磁盘 (App.1)，它有 200 GB 的容量用于数据保护。一天触发三次的备份会话中，每个会话都附带了即时恢复选项。每次保留三个复本，这些复本轮流用于即时恢复用途。在另一个磁盘阵列上有两个磁盘（App.2 和 App.3），分别有 150 GB 和 120 GB 的容量。在 App.2 磁盘上每天运行一次备份，数据移动到磁带后即删除快照。在 App.3 上，每天运行三次备份，并循环五个不同的复本以进行即时恢复。

已用容量计算方法



ZDB 已用容量的计算包括过去二十四小时内用于备份会话的所有磁盘 200 GB (App.1) + 150 GB (App.2) + 120 GB (App.3) = 470 GB。即时恢复已用容量的计算包括将数据用于即时恢复的 ZDB 会话的源容量。同一磁盘仅计算一次 200 GB (App.1) + 120 GB (App.3) = 320 GB。

到磁盘的高级备份许可证

到磁盘的高级备份许可证在备份到 Data Protector 文件库时不可获缺，并且可代替驱动器许可证用于虚拟磁带库 (VTL)。

- Data Protector 文件库的可用本机容量是磁盘上用于文件库的可用大小，如文件系统所报告。
  - 虚拟完整备份以及要合并到合成或虚拟完整备份中的增量备份必须存储在 Data Protector 文件库中，这需要此许可证。
- 如果 Data Protector 独占使用 VTL，则建议许可与 VTL 的物理容量匹配的容量，也称为可用本机容量。
  - 虚拟磁带库 (VTL) 的可用本机容量是磁盘上所有受保护的 Data Protector 备份消耗的虚拟磁带库大小，如 VTL 所报告。
  - 对于每个 VTL，可以选择使用“备份到磁盘”还是“备份到磁带驱动器”许可模式。在一个 VTL 内，一定不能混合这两种概念。
  - 如果 VTL 具有将备份数据从磁盘缓存迁移到其他磁盘或磁带的内置功能，则需要完全许可迁移的存储容量。由 VTL 单独控制的磁带库不需要驱动器和带库许可证，但是*物理磁带库中所有磁带的已用容量需要获得许可*。但是，如果 Data Protector 对象复制功能已用于将备份数据迁移到其他磁盘或磁带，则此方法不适用。
  - 默认情况下，Data Protector 将 VTL 设备视为普通库（例如 SCSI II 库），不会利用基于容量的许可。要启用基于容量的许可，必须在设备配置期间将设备标记为 VTL。
- 对于使用 Manager-of-Manager (MoM) 的中央许可，需要使用“到磁盘的高级备份”功能为每个单元分配至少 1 TB 的空间。

由于目前的虚拟磁带库以及某些托管 Data Protector 文件库的文件服务器缺少工具和界面，Data Protector 无法报告所需要的许可证数量。您需要按照许可定义，进行一致的容量许可。

示例 如果使用 omniupload 命令通过命令行界面 (CLI) 配置一个名为 "VTL_2011" 的虚拟磁带库，则必须在配置文件中指定字符串 VTLCAPACITY 的估计库容量。此估计值随后会在许可证检查程序报告中加总为“到磁盘的高级备份”的已用许可证容量。估计的虚拟带库容量消耗值 (VTLCAPACITY) (TB) 必须为整数，以避免出现错误消息“ Invalid VTL capacity specified”。在目录 "C:\Temp" 下名为 "libVTL.txt" 的配置文件中，键入估计的库容量，例如 11 ，然后执行: omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt 若要验证库配置，请执行： omnidownload -library VTL_2011

```
#omnidownload -library VTL_2011 NAME "VTL2011" DESCRIPTION "" HOST computer.company.com POLICY SCSI-II TYPE DDS LIBVIRTUAL VTLCAPACITY 11 IOCTLSERIAL "" CONTROL "SCSI address" REPOSITORY "SCSI repository" MGMTCONSOLEURL ""
```

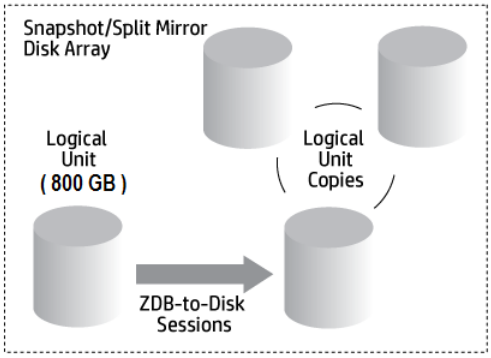
许可证检查程序会报告正在使用的许可证容量，即文件库 (FL) 的已用磁盘空间与虚拟磁带库中的估计磁盘空间大小之和。例如，用 2 TB 磁盘空间进行 FL 备份，VTL 上的磁盘容量为 10 TB，则所用总容量为 12 TB。如果仅安装了 5 TB 的许可证容量，则会收到通知，说明还需要 7 个“高级备份到磁盘，适用于 1 TB”许可证。

```
#omnicc –check_licenses –detail ---------- 许可证类别：到磁盘的高级备份，适用于 1 TB 已安装的许可证容量：5 TB 使用中的许可证容量：12.0 TB 需要的附加许可证容量: 7 TB 摘要 ------- 描述 需要的许可证 到磁盘的高级备份，适用于 1 TB 7 个 受保护数据总量 1 TB
```

基于许可容量的备份目标示例

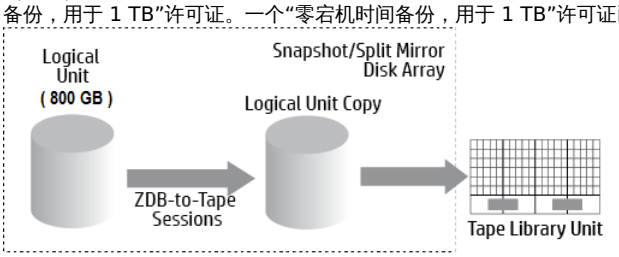
本节举例说明了基于容量的许可是如何计算的。

- **示例 1** 显示在 ZDB 到磁盘会话中一天备份三次某个 800 GB 逻辑单元中的数据的情形。**ZDB 到磁盘会话**

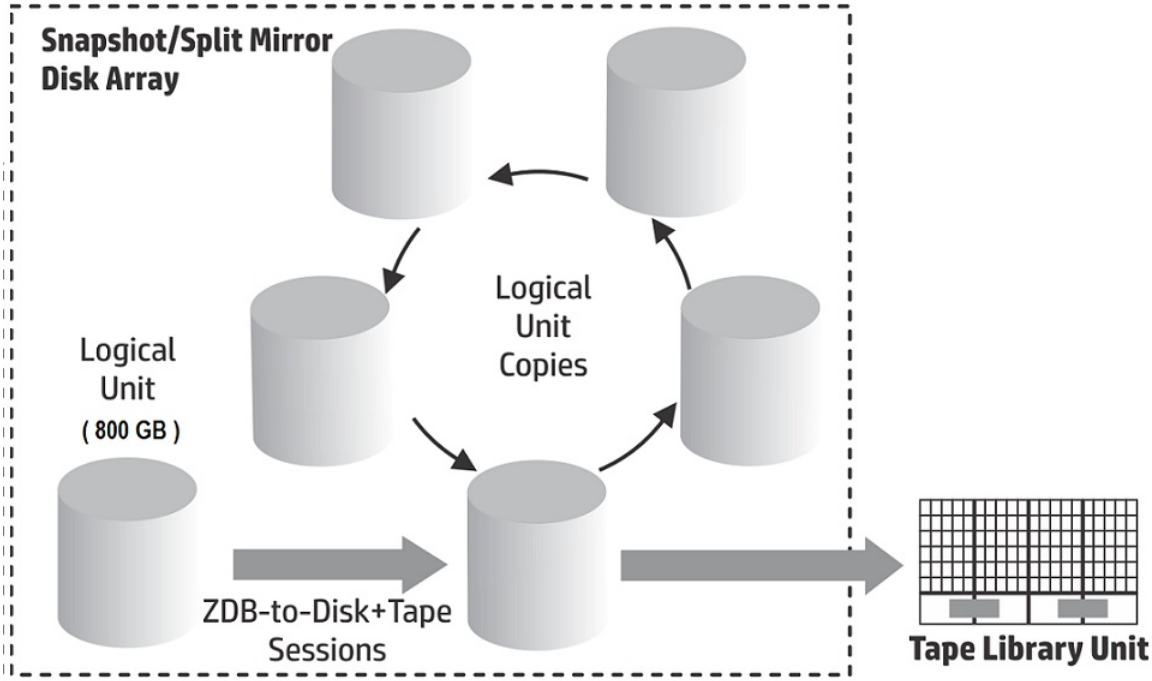


三个拆分镜像或快照副本 (复本) 进行循环，并保留用于即时恢复。基于容量的许可的计算方法如下：一个 800 GB 的逻辑单元用于“ZDB 到磁盘”会话：1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。为即时恢复保留同一 800 GB 逻辑单元的三个复本。请注意，这是源卷的容量，不是作为许可证主体的复本的容量：1 x 800 GB = 0.8 TB，对于“即时恢复，用于 1 TB”许可证。一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够。

- **示例 2** 显示在 ZDB 到磁带会话中一天备份两次某个 800 GB 逻辑单元中的数据的情形。因此，不必为即时恢复保留分割镜像或快照副本（复本）。基于容量的许可的计算方法如下：一个 800 GB 的逻辑单元用于“ZDB 到磁盘”会话：1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。一个“零宕机时间备份，用于 1 TB”许可证已足够。**ZDB 到磁带会话**



- **示例 3** ZDB 到磁盘 + 磁带会话显示的情形为: 在 ZDB 到磁盘 + 磁带会话中一天备份三次某个 800 GB 逻辑单元中的数据。五个分割镜像或快照副本（复本）进行循环，并保留用于即时恢复。基于容量的许可的计算方法如下：一个 800 GB 逻辑单元用于“ZDB 到磁盘 + 磁带”会话：1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。出于即时恢复目的，保留同一 800 GB 逻辑单元的五个复本。请注意，这是源卷的容量，不是作为许可证主体的复本的容量：1 x 800 GB = 0.8 TB，对于“即时恢复，用于 1 TB”许可证。一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够。**ZDB 到磁盘 + 磁带会话**



- **示例 4** 一个 200 GB 的逻辑单元、一个 500 GB 的逻辑单元、一个 120 GB 的逻辑单元和一个 300 GB 的逻辑单元用于 ZDB 会话: 1 x 200 GB + 1 x 500 GB + 1 x 120 GB + 1 x 300 GB = 1.12 TB 对于“零宕机时间备份，用于 1 TB 许可证”。保留一个 200 GB 的逻辑单元、一个 120 GB 的逻辑单元和一个 300 GB 的逻辑单元的拆分镜像或快照副本用于即时恢复：1 x 200 GB + 1 x 120 GB + 1 x 300 GB = 0.62 TB 对于“即时恢复，用于 1 TB”许可证。一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够，前提是ZDB 到磁盘会话中的三个示例在单元中通过ZDB 到磁盘 + 磁带会话配置。

功能扩展

- 联机备份 – 能够在应用程序正在运行时备份应用程序服务器和虚拟环境。
- 用于一个 UNIX 系统的联机扩展和用于一个 Windows/Linux 系统的联机扩展
- Manager-of-Managers 功能。
- 具有超过 60 个介质插槽的带库。
- 适用于一个客户机系统的 Data Protector 加密扩展
- NDMP 备份。
- 用于一个数据库服务器的 Granular Recovery Extension。
- 零宕机时间备份 (ZDB) - 能够为存储系统备份基于阵列的快照。
- 即时恢复 (IR) - 能够从基于阵列的快照创建备份并从该备份恢复。
- 高级备份到磁盘 – 包含用于 1 TB 备份磁盘存储的许可证。每千兆字节 (TB) 备份磁盘存储的可用本机容量都需要一次该许可证。执行备份到 Data Protector 文件库以及备份到“Data Protector 备份到磁盘设备类型”操作时需要此许可证，而且您可以使用此许可证而非驱动器许可证来备份到虚拟磁带库。

基于容量 (高级版) 的许可

基于容量的产品结构基于受 Data Protector 保护的主数据卷，且支持无限制地使用企业保护功能。容量以“前端千吉字节”或前端 TB 为单位。前端千吉字节的总量定义为 Cell Manager 中所有要备份的系统中的数据总量。对于每个系统，以最大完整数据量（即受保护的源数据量）进行度量。此许可证模型可应用到现有基础架构。新的基础架构会自动包含到同一个许可证中。

基于容量的许可 (CBL) 在计算费用时将所有受保护的数据包括在内，并且无法区分用于备份的当前许可证类型和原始许可证类型。可以将备份中不包含的系统 (不再存在) 复制到单独的介质，然后可以从 Cell Manager 系统导出该介质。

IDB 对象不包含在 CBL 计算中。

> **注意**从 Data Protector 2018.11 开始，容量计算在当前日期之前 90 天内执行。

使用基于容量的许可时，以下模块是许可结构的一部分:

- Cell Managers 和 Manager of Managers
- 磁带驱动器和带库
- 联机备份和 Granular Recovery Extension
- DP 扩展联机备份
- Data Protector 零宕机时间备份 (ZDB)
- 零宕机时间备份和即时恢复
- 高级备份到磁盘和 NDMP

- 加密软件
- 报告服务器

不包含的产品以及与基于容量的许可分开销售的产品如下：

- Data Protector Management Pack，包含适用于 Operations Manager 和 Microsoft Systems Center 的 DP Smart 插件

基于容量的许可证报告

在基于容量的许可模式下，Data Protector 仅会列出基于容量的许可证的数量 (粒度为 1 TB)，以及未包括在基于容量的许可证范围内的许可证，即软件加密扩展。不会显示基于容量的许可所涵盖的基于功能的许可证。

```
#omnicc -check_license -detail
```

```
警告: Calculation of total protected data size may take some time.
```

```
Report generated : 03/03/2016 1:48:27 AM 许可证模式 : 服务器 许可证服务器 : host.domain.com ---------- 许可证类别 : 适用于一个客户机系统的加密扩展 已安装的许可证 : 0 已使用的许可证 : 0 需要的其他许可证 : 0 ---------- 许可证类别 : Data Protector - 基于每 TB 软件的容量 已安装的许可证容量 : 9 TB 使用中的许可证容量 : 0 TB 需要的附加许可证容量: 0 TB ---------- . . . 摘要 ------- 许可已涵盖。 受保护的数据总计 : 5 TB ---------- 备份类型 | 受保护的数据总计 | ---------- MS 文件系统 | 1024 GB MS SQL | 1024 GB SAP | 1024 GB UNIX 文件系统 | 1024 GB vProtect_Exchange | 1024 GB ----------
```

Total Protected Data（受保护的总数据）定义为正在从所有系统备份的聚合数据量。每个系统的 Total Protected Data（受保护的总数据）等于以下内容之和：

- 文件系统（包括合成备份）和虚拟环境备份的每个对象的最大完整备份之和。
- 每个应用程序集成备份的每个数据集的最大完整备份。
- 从所有导入的 vProtect 服务器获取的 Exchange 备份容量之和。“备份类型”显示为 **vProtect_Exchange**。

每个文件系统和虚拟环境的唯一对象是在备份时创建的实际对象。实际对象可以是装载点、虚拟机或虚拟机磁盘。每个应用程序集成的唯一数据集都按照不同的方式（通常为数据库实例或服务器名称）标识。

限制

以下限制适用：

- 在使用多个不同的代理备份相同数据时，会对备份进行多次计算。下面是双重计算的几个类似示例：
  - 使用 VSS 的数据库文件系统备份，同一个数据库的应用程序集成代理备份。
  - 虚拟主机的虚拟环境集成备份，以及在虚拟机（主机）内部运行的文件系统代理备份。
- 当在外部重新配置 Oracle 备份对象名称格式时，这可能会导致不从新对象名称解析数据库名称。在计算受保护的总数据量时，类似的对象大小可能无法正确处理。

  对于重新配置的格式，仍必须包括定义为 <DBID_*.dbf 的 Oracle 数据库名称，以便在计算受保护的总数据大小时正确地添加 Oracle 对象。
- 当前，Data Protector 中没有任何方法可用于检测通过虚拟环境代理和已安装的磁带客户机（在 VM、VEPA 和磁带客户机中运行）备份的 VMware VM 是否正在使用相同数据运行。
- 这两种许可模式无法在同一 Data Protector 单元中共存。
- 在 MoM 环境中，不能混用这两种许可模式。
- 使用先前版本的 Data Protector 创建的虚拟磁带库的库容量 (VTLCAPACITY) 在升级到最新版本之后，默认设置为 1 TB。必须通过图形用户界面 (GUI) 或通过命令行界面 (CLI) 手动输入估计的库容量值。

基于插座 (精简版) 的许可

使用基于插座的许可 (SBL)，基于用于虚拟机监控程序的处理器使用许可证。许可证与托管虚拟机的物理机上的插座 (处理器) 数量相关联。可以从仪表板、Data Protector GUI 和 CLI 获取每个 Cell Manager 使用的插座数量的列表。虚拟机监控程序中的处理器插座、CPU 插座或 CPU 插槽位于主板上。CPU 插座计数等于 ESX(i) 服务器上的物理处理器的数量，具体取决于服务器的型号和配置。CPU 插座数量因硬件制造商而异。

SBL 包含与虚拟机相关的所有 Data Protector 功能。3PAR、VSS 高级阵列集成加密等具有的功能也可用于虚拟环境。还支持高级 VMWare 操作，如 Granular Recovery Extension、PowerOn 和 Live Migrate。

要升级到 Data Protector 高级版，请安装高级版许可证密钥。

选择许可证类型

同一个客户可以利用基于功能的模型和容量模型，但不能在同一个 Cell Manager 或 MoM 环境中将这两个模型结合使用。列出的补充产品不受此限制约束，因为这些许可证可与 Data Protector 基于功能的许可方法和基于容量的许可方法结合使用。支持从传统产品结构迁移到基于容量的产品结构: 有关详细信息，请联系授权销售代表。这两种许可模型对任何环境规模均有效。

基于功能的许可和基于容量 (高级版) 的许可证之间的区别

- 基于功能的许可提供更低的入门成本，但已启用的功能较少；而容量许可已启用大部分功能，它是一个“随增长付费”模型。
- 基于功能的许可要求每个 Cell Manager 和磁带驱动器等具有单独的许可证，并要求用户先记录现有环境再选择需要许可哪些备份软件功能来保护其环境。
- 灵活性更大 – 容量许可仅需一个许可证即可保护客户机上所有需要受保护的数据。
- 需要关注的另一个问题是：如果您计划将数据保留很长一段时间，并且数据将发生大量更改但容量不一定会增长，这也可能导致该备选的基于容量的模型随着时间的推移产生更多成本。

为什么要使用基于功能的许可？

- 提供更低的入门成本，但已启用的功能较少
- 如果组织内的数据持续以适当速度增长，则使用基于功能的许可方法可能更具有成本效益

为什么要使用基于容量（高级版）的许可?

- 基于受 Data Protector 保护的生产数据量
- 可容纳多个备份副本，而不会增加许可证成本
- 允许无限制地使用企业保护功能
- 它是一个永久许可证，并且可转移到新的服务器、存储和应用程序等。
- 它是一个高度可扩展且成本不太高昂的“随增长付费”许可模型，可改善 OPEX 管理并简化规模估算

获取许可证

在本节，您将了解有关为 Data Protector 获取新许可证密钥并为现有许可证密钥请求新密码的信息。

获取新许可证密钥

在 Data Protector 9.x 之前获得的许可证密钥与 Data Protector 10.00 或更高版本不兼容。如果要从 Data Protector 9.x 或更早版本升级到 Data Protector 10.00 或更高版本，请获取新的许可证密钥。

从 Data Protector 10.00 或更高版本获得的许可证密钥可用于所有后续发行版。

对于新购买的许可证，在请求许可证密钥时您必须选择 Data Protector 的产品版本来匹配您的安装。

升级以后，将使用期限为 90 天的即开即用许可证密钥运行 Data Protector。该行为将与采用即开即用许可证密钥的全新安装相同。一旦安装至少一个新许可证密钥，将关闭即开即用许可证密钥，并且仅可识别已安装的有效密钥。在升级后仅可激活即开即用许可证密钥一次。

升级以后，现有许可证仍与新（即开即用）密码一起报告为无效。要避免出现此情况，请重命名（但不要删除）文件 lic.dat ：

- Windows 系统：转到目录 Data_Protector_program_data\Config\server\Cell 并重命名以下文件：

```
ren lic.dat lic.bak
```

- Linux 系统：转到目录 /etc/opt/omni/server/cell 并重命名以下文件：
  mv lic.dat lic.bak

升级现有许可证

如果您已经是 Data Protector 的用户，为了将您的旧许可证密码升级到 Data Protector 的最新版本，您必须具有有效的支持协议，其中涵盖了您正在使用的许可证数量和类型。

在收到新许可证密钥之后，应将其与已安装在 Data Protector 环境中的许可证密钥的数量和类型进行比较。只有在确认拥有所需 Data Protector 版本的有效许可证密钥之后，才可升级软件。

如果收到的新许可证密钥少于或不同于实际安装在 Data Protector 环境中的密钥，则不应升级到 Data Protector 的最新版本。由于缺少许可证密钥，Data Protector 环境可能不再运行。

首先，联系您的销售代表或合作伙伴，以确定需执行哪些步骤来消除支持合同所涵盖的功能许可证与当前使用的实际许可证 (在早期 Data Protector 版本中使用的许可证) 之间的差异。

安装 Data Protector 产品后，可以使用 90 天。90 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

在 Cell Manager 上更改许可证后，取消注册并重新注册报告软件，使新许可证生效。

> **注意**CRS 将对应用程序服务器的许可证数据进行 GET REST API 调用。如果应用程序服务器启动较慢，CRS 将重试 GET REST API 调用 30 次。将全局变量 LicenseWaitForAppServer 设置为在两次调用之间间隔 10 秒再重试。

将许可证移至另一 Cell Manager 系统

在以下某种情况下，您必须联系 *Password Delivery Center*:

- 如果希望移动到其他 Cell Manager 系统。
- 如果打算将安装在 Cell Manager 上但当前并未在单元中使用的许可证移动到其他 Data Protector 单元。

UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到其他平台。所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。

要在不同的 Cell Manager 之间移动许可证，请完成以下步骤:

1. 为每个新的 Cell Manager 填写一份“许可证移动表单”，并将其发送至 *Password Delivery Center*。如果要移动无法再购买的产品的许可证，请使用以前版本的产品自带的*许可证移动表单*。请参阅 Data Protector 许可表单。

   在表单上，必须指定要从现有 Cell Manager 移动的许可证的数量。

   或者，访问密码交付中心网站并使许可证联机移动。

2. 删除以下文件：

   - Windows 系统： Data_Protector_program_data\config\server\cell\lic.dat
   - Linux 系统： /etc/opt/omni/server/cell/lic.dat

3. 填写“许可证移动表单”并将其发送至 *Password Delivery Center (PDC)* 后，即可就从法律上迫使您从当前 Cell Manager 中删除所有 Data Protector 密码。

4. 安装新密码。对于每个新的 Cell Manager，您都将收到一个密码。如果许可证仍留在当前 Cell Manager 上，则您还将收到一个新密码用于当前 Cell Manager。这个新密码将替换当前 Cell Manager 上的当前密码项。

集中式许可

所有许可证都保留在 Manager-of-Managers (MoM) Manager 系统上。虽然许可证仍然是在 MoM 管理器配置的，但是它们会被分配到特定单元。UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到其他平台。所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。MoM 功能允许在 MoM 单元间移动（重分配）许可证。如果是安装新的 Data Protector 许可证，请确保先检查 MoM 功能再请求许可证。如果您决定以后使用中央许可，则必须完成移动许可证的步骤。作为 100 TB 许可证的一部分，您将收到单个许可证密钥。您无法从 Webware 或许可获取多个密钥。要使用此单个许可证密钥，您必须在 MoM 环境中使用集中式许可。您不需要额外购买 1 TB LTU，相反，即使需要 100 GB，也会为每个 Cell Manager 分配 1 TB LTU。MoM 功能允许中央许可。这意味着您可以在 MoM Manager 上安装所有许可证，然后将它们分配到属于 MoM 单元的各个 Cell Manager。以后可以在 MoM 单元间移动（重分配）许可证。

许可证报告

Data Protector 许可证会被检查，如果丢失，则会在多种 Data Protector 操作期间进行报告，例如:

- 作为 Data Protector 检查和维护机制的一部分，许可证会得到检查，如果丢失，则会在 Data Protector 事件日志中进行报告。Data Protector 事件日志位于 Cell Manager 上的 Data_Protector_program_data\log\server\Ob2EventLog.txt (Windows 系统) 或 /var/opt/omni/server/log/Ob2EventLog.txt (Linux 系统)。
- 启动 Data Protector 会话后，将检查许可证，如果缺少，则报告。

按需许可证报告

要从单元生成有关许可信息的报告，请执行： omnicc -check_licenses [-detail] 如果指定了 -detail 选项，则生成详细的报告。许可证检查程序会为单元中的每个许可证返回以下信息：许可证名称、安装的许可证、使用的许可证、受保护的总数据 (TB) 和需要的其他许可证（容量）。如果未指定 -detail 选项，则命令返回是否涵盖 Data Protector 许可的相关信息。命令将返回信息：生成报告的时间、许可模式、许可证服务器以及受保护的总数据 (TB)。请注意，对于驱动器扩展所用许可证，许可证检查程序返回有关配置的驱动器和建议的其他许可证的相关信息。在任何时候，您需要的许可证数量与所使用的驱动器数量一样。此数量通常是已配置的驱动器的总数，以允许同时使用所有驱动器。请注意，命令不会列出许可证的失效日期。报告的生成可能需要一些时间，具体取决于环境和安装的许可证数量。要获取有关许可证失效日期的信息，请执行： omnicc -password_info 在配置有 CMMDB 的 MoM 环境中，当为属于库和驱动器的项目生成许可证报告时，必须在安装有 CMMDB 的 Cell Manager 上运行 omnicc 命令。

许可证迁移

支持合同中的 Data Protector 8.1 及更高版本的客户可免费收到最新 Data Protector 版本，其中包括支持合同中所有许可证的新许可证密钥。Data Protector 不会显示已过期的或不用于同一个产品版本的许可证。在此处，可以根据有效支持合同 (SAID) 下载您有权访问的软件和许可证密钥。可以查看与 SAID 关联的所有软件，选中所需 Data Protector 版本前面的复选框并单击“获取更新”。请注意，Data Protector 10.00 旁边显示消息“需要新许可证密钥”。将显示以下三个选项卡：

- **获取软件**：用于下载软件。
- **获取许可证**：可获取映射到 Data Protector 9.00 或更高版本的 LTU 的许可证。
- **获取文档**：可下载产品文档。

当您单击“获取许可证”链接时，会直接将您指向更新订单“软件许可证门户”，在这里您可以获取与服务协议标识符 (SAID) 上数量一致的 LTU 许可证密钥。

Data Protector 许可表单

本节讨论 Data Protector 许可表单。填写完成后可使用以下某种方法订购永久密码：

- 使用联机 *Password Delivery Center* 站点订购永久密码。
- 打印在 Cell Manager 系统和安装介质上的以下文件中包含的许可表单的电子版:

  Linux 系统： /opt/omni/doc/C/license_forms_UNIX

***Windows** 安装程序包：* DriveLetter:Docs\license_forms.txt

或使用电子文件将您的邮件内容“复制”并“粘贴”到 *Password Delivery Center (PDC)*。

请确保清楚地输入信息且记住必需字段。下面简单描述一下许可表单中必须填写的常规字段：

个人数据	该字段包含客户信息，包括新密码的发送对象。
许可数据	提供有关 Data Protector 单元的许可信息。
当前 Cell Manager	输入有关当前 Cell Manager 的必要信息。
新 Cell Manager	输入有关新 Cell Manager 的必要信息。
订单号	输入打印在*权利证书*上的*订单号*。需要“Cell Manager”以验证您有权请求永久密码。
IP 地址	该字段定义 *Password Delivery Center* 将为哪些系统生成密码。如果要使用中央许可（仅限 MoM 环境），那么该系统必须是 MoM 管理器系统。 如果 Cell Manager 具有多个 LAN 卡，则可以输入任何一个 IP 地址。建议输入主 IP 地址。 如果您的 Data Protector 在 ServiceGuard 或 Microsoft Cluster 环境中，则输入虚拟服务器的 IP 地址。
Password Delivery Center 传真号码	有关联系信息，请参见产品随附的*权利证书*。
产品许可证类型	在“产品号”旁边的字段中，输入要在该 Cell Manager 上安装的许可证数量。该数量可以是随*订单号*购买的许可证的全部或一部分。

Data Protector 产品结构和许可证

要更改 Cell Manager 的 IP 地址、移动 Cell Manager 到另一个系统或者将许可证从一个单元移动到另一个单元 (而不使用 MoM 功能)，应联系 *Password Delivery Center (PDC)* 以便更新许可证。有关联系 Password Delivery Center 的信息，请参阅“获取和安装永久密码”部分。

许可证密码

安装 Data Protector 产品后，可以使用 90 天。90 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

密码考虑事项

考虑以下事项以帮助确定合适的密码数量：

- 即开即用密码是内置的。每次在新安装和将现有 Data Protector 升级到 Data Protector 9.00 或更高版本后将提供为期 90 天的该密码，在这 90 天内您无需安装任何额外许可证密码，并且可为您提供完整的产品功能，以供您评估。

  在 90 天后，即开即用密码到期，除非安装永久许可证密钥，否则产品将停止工作。

  在安装首个常规许可证密钥之后，完整产品的评估期将终止。一旦已至少安装了一个许可证密钥后，仅可使用已安装许可证密钥对应的功能。

- 可将永久许可证移动到其他 Cell Manager。但是，需要使用“许可证移动表单”并将它们发送至 Password Delivery Center (PDC)。
- 密码安装在 Cell Manager 上且对整个单元有效。
- Manager-of-Managers (MoM) 功能中包含中央许可。如果您为多个单元购买了多个许可证，则可以将所有许可证都安装在 MoM 系统上。
- 您需要每个单元使用一个 Cell Manager 许可证。
- 执行 Data Protector 配置任务或启动备份会话时，软件会定期检查许可证密钥或密码。
- 即开即用密码可用于任何系统上，而评估密码和永久密码只能用于为其请求许可证的 Cell Manager 系统上。

Data Protector 密码

Data Protector 许可需要以下某种密码：

- 即开即用密码

  首次安装时会在产品中创建即开即用密码。在 Data Protector 支持的任何系统上安装软件后，可以使用软件 90 天。在此期间内，您必须从 *Password Delivery Center (PDC)* 请求永久密码，然后安装该密码。

  对于现有的 Data Protector 安装，在升级到 Data Protector 9.00 或更高版本后，您的安装将使用即开即用密码运行 90 天。在此期间内，您必须从有效支持协议中所指定的 Password Delivery Center 请求新的永久密码。无法升级未包括在支持协议中的旧许可证。

- 永久密码

  Data Protector 产品自带了一个“权利证书”许可证，它授权您获取永久密码。如果您已购买所有需要的许可证，则永久密码允许您根据备份策略配置 Data Protector 单元。在请求永久密码前，必须确定 Cell Manager 系统并了解单元配置要求。

- 紧急密码

  如果由于紧急情况，当前安装的密码与当前系统配置不匹配，则可使用紧急或后备密码。它们允许在任何系统上操作 120 天。

  紧急密码由支持组织发布。它们必须由 人员请求，且仅发布给这些人员。请咨询支持联系人或查看许可站点。

  紧急密码的目的是当原始系统配置进行重构时，或移动到新的永久安装后启用备份操作。如果要移动许可证，您需要填写许可证移动表格并将其发送到 *Password Delivery Center (PDC)*。

获取永久密码

完成以下步骤，以获取永久密码:

1. 收集永久密码*请求表单*所需的信息。请参阅“Data Protector 许可表单”查找表单位置并获取关于如何填写表单的说明。
2. *Password Delivery Center* 将使用您发送请求的方式发送您的永久密码。例如，如果您通过电子邮件发送请求，那么您将通过电子邮件收到永久密码。
3. 执行以下某个操作：
   - 访问联机 *Password Delivery Center* 站点。
   - 填写“永久密码请求表单”并使用以下某种方式将其发送至 *Password Delivery Center* (请参阅产品自带的权利证书以获取传真号码、电话号码、电子邮件地址和工作时间):
     - 将表单传真至 *Password Delivery Center*
     - 发送电子邮件至 *Password Delivery Center*

       可以使用 Cell Manager 和安装介质上以下文件中包含的电子版许可表单:

       - 在 Windows Cell Manager 上: Data_Protector_home\Docs\license_forms.txt
       - 在 Linux Cell Manager 上： /opt/omni/doc/C/license_forms_UNIX
       - 在 Windows 安装程序包上： Disk_Label:\Docs\license_forms.txt

       将邮件内容“复制”和“粘贴”到 *Password Delivery Center (PDC)*。

       您将在发送*永久密码请求表单*后 24 小时内收到永久密码。

安装永久密码

本节介绍安装 *Password Delivery Center (PDC)* 发送的永久密码的步骤。**先决条件：**您必须已收到 *Password Delivery Center* 发送的永久密码，且必须在 Cell Manager 上安装 Data Protector 用户界面。密码安装在整个单元上且对整个单元有效。

使用 GUI

要使用 Data Protector GUI 安装永久密码，请继续执行以下步骤:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击“Data Protector 单元”并单击“添加许可证”。
3. 严格按照密码证书上所示输入或复制密码。

   一个密码由长度可变的 4 个字符组构成，以空格分隔，后面跟一个字符串。请确保此序列中没有换行符或回车符。以下是一个密码的示例：

   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ 2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23T X ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for Linux"

   键入密码后，请检查以下内容：
   - 确保在屏幕上正确显示密码。
   - 确保开头和结尾都没有空格，也没有多余字符。
   - 仔细检查 "1"（数字 1）字符和 "l"（字母 l）字符。
   - 仔细检查字符“O”（大写字母 O）和字符“0”（数字 0）。
   - 确保大小写使用正确。密码区分大小写。

   单击**确定**。

密码将写入 Cell Manager 上的以下文件:

- Windows 系统： Data_Protector_program_data\Config\server\Cell\lic.dat
- Linux 系统： /etc/opt/omni/server/cell/lic.dat

使用 CLI

要使用 Data Protector CLI 安装永久密码，请继续执行以下步骤:

1. 登录到 Cell Manager。
2. 请执行以下命令：

   omnicc -install_license password

   password 字符串必须严格按照密码证书上的显示准确输入。它必须是单行格式，不能包含任何嵌入的回车。密码必须在引号里。如果密码还包括在引号中的说明，则该说明的引号前必须有反斜杠。

在 Cell Manager 上还可以将密码附加到以下文件:

- Windows 系统： Data_Protector_program_data\config\server\cell\lic.dat
- Linux 系统： /etc/opt/omni/server/cell/lic.dat

如果文件不存在，请使用编辑器 (例如 vi 或 Notepad) 创建文件。有关密码示例，请参阅图形用户界面步骤中的步骤 3。

验证密码

使用 Data Protector GUI 和 CLI 验证密码。

使用 GUI

要验证安装的许可证密码是否正确，请在 Data Protector GUI 中继续执行以下步骤:

1. 在“帮助”菜单中，单击**许可证...**。
2. 单击**许可证**选项卡。所有安装的许可证都会显示出来。单击**密码信息**选项卡以查看已安装的有效密码的详细信息。无效的密码将被标记为已过期或已删除。

   整个弹出窗口及各个列可调整大小。

使用 CLI

要验证安装的许可证密码是否正确，请使用以下命令： omnicc -password_info 此命令显示所有安装的许可证。如果输入的密码错误，会将其列出并标注 Password could not be decoded.

查找安装的许可证数量

使用 Data Protector GUI 和 CLI 查找安装的许可证数量。

使用 GUI

安装永久密码后，可以检查当前在 Cell Manager 上安装的许可证数量:

1. 启动 Data Protector 管理器。
2. 在菜单栏中，单击**帮助**，然后单击**许可证...**。此时将打开“关于管理器”窗口，显示安装的许可证。

使用 CLI

如果使用命令行，请执行如下步骤：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -query
   ```

此时将显示一个列出了当前安装的许可证的表。

使用 Linux 系统本机工具安装和升级

本主题介绍如何使用本机安装工具 rpm 在 Linux 系统上安装和升级 Data Protector。

在 Linux 系统上使用本机工具安装

建议使用 omnisetup.sh 安装 Data Protector。Linux 上的本机安装步骤仅适用于使用有限的一组远程安装包安装安装服务器。

在 Linux 系统上使用 rpm 安装 Cell Manager

要在 Linux 系统上安装 Cell Manager，请完成以下步骤:

1. 复制 Linux 上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到 linux_x86_64/DP_DEPOT 目录。
3. 要安装组件，请执行：

```
rpm -i package_name -A.10.30-1.x86_64.rpm
```

其中 package_name 是相应的子产品包的名称。必须安装以下组件：

OB2-CORE	Data Protector 核心软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库。
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境。
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-DISPATCHER	作业控制引擎调度程序
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件。
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。
OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包含 Data Protector 文档。

> **重要说明**Linux 上的组件相互依赖。应以上面列出的顺序安装这些组件。

4. 重新启动 Data Protector 服务：

```
omnisv stop omnisv start
```

在 Linux 系统上使用 rpm 安装安装服务器

在 Linux 本地安装

要在 Linux 系统上安装适用于 Linux 的安装服务器，请完成以下步骤:

1. 复制 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到包含安装存档的目录 (在此例中是 linux_x86_64/DP_DEPOT)。
3. 对于每个组件，请执行：

```
rpm -i package_name -A.10.30-1.x86_64.rpm
```

产品中包括以下与安装服务器安装相关的组件 (package_name):

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装安装服务器，则已安装该软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器核心软件。
OB2-CFP	适用于所有 Linux 平台的公用安装服务器核心软件。
OB2-TS-CFP	适用于所有 Linux 平台的公用安装服务器技术堆栈软件
OB2-DAP	适用于所有 Linux 系统的磁盘代理远程安装包。
OB2-MAP	适用于所有 Linux 系统的介质代理远程安装包。
OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于所有 Linux 系统的单元控制台远程安装包。

如果是安装独立的安装服务器 (即不在 Cell Manager 上) 且要使用用户界面:

OB2-CC	单元控制台软件。它包含命令行界面。

4. 安装完这些组件后，使用 rpm 为所有将远程安装的组件安装远程安装包。例如：

OB2-INTGP	Data Protector 集成核心软件。该组件为安装集成所必需
OB2-TS-PEGP	PEGASUS 技术堆栈组件。
OB2-OR8P	Oracle Integration 组件。
OB2-MYSQLP	MySQL 集成组件。
OB2-POSTGRESQLP	PostgreSQL 集成组件。
OB2-SAPP	SAP Integration 组件。
OB2-SAPDBP	SAP MaxDB 集成组件。
OB2-SAPHANAP	SAP HANA 集成组件。
OB2-INFP	Informix Integration 组件。
OB2-LOTP	Lotus Notes/Domino Integration 组件。
OB2-SYBP	Sybase Integration 组件。
OB2-DB2P	DB2 Integration 组件。
OB2-SMISAP	P6000/ 3PAR SMI-S 代理组件。
OB2-SSEAP	P9000 XP 代理组件。
OB2-NETAPPP	NetApp Storage Provider 组件。
OB2-VEPAP	虚拟环境保护代理组件。
OB2-SODAP	StoreOnce Software 重复数据删除组件。
OB2-AUTODRP	自动灾难恢复组件。
OB2-VMWAREGRE-AGENTP	VMware Granular Recovery Extension 组件。
OB2-DOCSP	英文文档组件。
OB2-FRAP	法语文档组件。
OB2-JPNP	日文文档组件。
OB2-CHSP	简体中文文档组件。

安装完成时，Linux 的软件仓库位于 /opt/omni/databases/vendor 目录中。

重要说明将 Data Protector 安装到链接目录中，例如:

```
/opt/omni/ -> /prefix/opt/omni/ /etc/opt/omni/ -> /prefix/etc/opt/omni/ /var/opt/omni/ -> /prefix /var/opt/omni/
```

必须在安装前创建链接并确保目标目录存在。

下面的步骤

至此，您应该已在网络中安装了适用于 Linux 的安装服务器。现在应执行以下任务：

1. 如果已安装独立的安装服务器 (即不在 Cell Manager 上)，则必须手动将系统添加 (导入) 到 Data Protector 单元中。导入安装服务器后，Cell Manager 上的 /etc/opt/omni/server/cell/installation_servers 文件将更新以列出已安装的远程安装包。该文件可用于在 CLI 中检查可用的远程安装包。为保持该文件最新，每当安装或删除远程安装包后应导出再导入安装服务器。即使安装服务器安装在与 Cell Manager 相同的系统上，此方法也适用。
2. 如果 Data Protector 单元中有 Windows 系统，请安装适用于 Windows 的安装服务器。
3. 将软件分发到客户机上。

安装客户机

在安装 Cell Manager 或安装服务器期间没有安装客户机。必须使用 omnisetup.sh 或从 Data Protector GUI 远程安装组件来安装客户机。

在 Linux 系统上使用 rpm 升级 Data Protector

要升级 Linux Cell Manager 或安装服务器，请卸载产品的旧版本并安装新版本。

在 Cell Manager 升级期间不升级 Cell Manager 系统上安装的客户机组件，必须使用 omnisetup.sh 或从安装服务器中远程安装组件来升级这些组件。

要使用 rpm 升级 Data Protector，请完成以下步骤:

1. 1. 将 omnimigrate.pl 脚本从安装包复制到临时目录:

```
cp –p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI -CS/opt/omni/sbin/omnimigrate.pl/tmp
```

2. 使用 omnimigrate.pl 命令导出 IDB：

```
/opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir /var/opt/omni/server/exported -export
```

2. 以 root 身份登录，然后通过执行 omnisv -stop 命令停止 Data Protector 服务。输入 ps -ef | grep omni 以验证是否已关闭所有服务。
   执行 ps -ef | grep omni 命令后必须没有 Data Protector 服务列出。
3. 使用 rpm 卸载 Data Protector。
   在此步骤中会保留配置文件和数据库。
4. 运行 rpm -q 命令以验证是否已卸载旧版本的 Data Protector。旧版本的 Data Protector 不应被列出。
   验证数据库和配置文件是否还在。以下目录应还在且包含二进制文件：
   - /opt/omni
   - /var/opt/omni
   - /etc/opt/omni
5. 如果要升级 Cell Manager，请使用 rpm 安装 Cell Manager。
   如果升级安装服务器，请使用 Linux 安装包。

系统准备和维护任务

本主题介绍超出本主题范畴，但对安装过程有很大影响的任务的一些附加信息。这些任务包括系统准备和维护任务。

Linux 系统上的网络配置

在 Linux 系统上安装 Data Protector 时，Data Protector Inet 注册为网络服务。这通常需要执行以下步骤：

- 修改 /etc/services 文件，用于注册 Data Protector Inet 将要侦听的端口。
- 在系统的 inetd 后台程序或其等效后台程序 (xinetd、systemd 或 launchd) 中注册 Data Protector Inet。

修改网络配置时，初始 Data Protector Inet 配置可能会变成未完成或处于无效状态。由于将 IPv6 支持添加到网络服务的系统特定设置，每当您添加或移除 Internet 协议版本 6 (IPv6) 网络接口时就会发生此问题。其他情况下也可能会发生此问题。

为了更新 Data Protector Inet 配置，可以使用 **dpsvcsetup.sh** 实用程序。此实用程序 (也可用于安装，收集所需信息并相应地更新系统配置) 位于目录 /opt/omni/sbin (Solaris 和 Linux 系统) 中。

- 要更新 Data Protector Inet 配置，请执行：
  dpsvcsetup.sh -update
- 要将 Data Protector Inet 注册为网络服务，请执行：
  dpsvcsetup.sh -install
- 要将 Data Protector Inet 取消注册为网络服务，请执行：
  dpsvcsetup.sh -uninstall.

检查 TCP/IP 设置

TCP/IP 配置过程的一个重要方面是设置主机名解析机制。网络中的每个系统都必须能够解析 Cell Manager 的地址以及连接了介质代理和物理介质设备的所有客户机的地址。Cell Manager 必须能够解析单元中所有客户机的名称。

安装 TCP/IP 协议后，可以使用 ping 和 **ipconfig**/**ifconfig** 命令来验证 TCP/IP 配置。

请注意，在某些系统上，不能对 IPv6 地址使用 ping 命令，而应使用 ping6 命令。

检查 TCP/IP 设置

要检查TCP/IP设置，请完成以下步骤:

1. 在命令行处运行：
   Windows 系统: ipconfig /all
   Linux 系统： ifconfig interface 或 ifconfig -a or nestat -i, (取决于系统)。为网络适配器设置的 TCP/IP 配置和地址的精确信息。检查 IP 地址和子网掩码是否设置正确。
2. 键入 ping your_IP_address 以确认软件的安装和配置。默认情况下，应该收到四个响应包。
3. 键入 ping default_gateway
   网关应处于您所在的子网中。如果未能 ping 到网关，请检查网关 IP 地址是否正确，并且网关是否正在运行。
4. 如果前面的步骤都成功，那么就可以测试名称解析。运行 ping 命令时输入系统的名称，以测试 hosts 文件和/或 DNS。例如，如果计算机名称为 computer，域名为 company.com，则需输入: ping computer.company.com。

   如果此命令不起作用，则确认“TCP/IP 属性”窗口中的域名正确。还应该检查主机文件和 DNS。以两种方式确保要作为 Cell Manager 的系统和要作为客户机的系统的名称解析正常运行:

   > **注意**使用 hosts 文件进行名称解析时，上述测试不保证名称解析工作正确。在这种情况下，可能要在安装 Data Protector 后使用 DNS 检查工具。

   > **重要说明**如果上方指定的名称解析不起作用，则无法正确安装 Data Protector。

   另请注意，Windows 计算机名必须与主机名相同。

   - 在 Cell Manager 上，可以 ping 每个客户机。
   - 在客户机上，可以 ping Cell Manager 和装有介质代理的每个客户机。
5. 安装 Data Protector 并且创建 Data Protector 单元之后，可以使用 DNS 检查工具确认 Cell Manager 和装有介质代理的每个客户机正确解析与单元中所有其他客户机的 DNS 连接，反之亦然。可以通过执行 omnicheck -dns 命令实现此目的。失败的检查以及失败检查的数量将列出。

更改默认的 Data Protector 端口

请参阅以下小节:

更改默认的 Data Protector Inet 端口

Data ProtectorInet 服务（进程）（该进程启动备份和还原所需要的其他进程）应在 Data Protector 单元中的每台系统上使用相同的端口号。

默认情况下，Inet 使用端口号 5555/5565。要验证此特定端口没有被其他程序使用，请检查本地 /etc/services 文件（Linux 系统）或在本地调用 netstat -a command 之后的输出（Windows 系统）。如果端口已由其他程序占用，必须重新配置 Inet 以使用未用的端口。必须在单元的每个系统上完成此重新配置，以便单元中的所有系统均使用相同的端口。

一旦在 Cell Manager（还用作 Installation Server）或独立的安装服务器上进行此更改之后，使用此安装服务器远程安装的所有客户机均将自动使用新的端口。因此，在建立单元时更改 Inet 端口最轻松。

> ⚠ **警告**请勿更改系统上为灾难恢复准备的默认 Inet 侦听端口。反之，如果此类系统受到灾难打击，灾难恢复进程可能会失败。

Linux 系统

要在将成为 Cell Manager、安装服务器或 Data Protector 客户机的 Linux 系统上更改 Inet 端口，请执行以下步骤:

- 创建 /tmp/omni_tmp/socket.dat 文件，创建时指定所需的端口号。

要在已成为 Cell Manager、安装服务器或 Data Protector 客户机的 Linux 系统上更改 Inet 端口，请执行以下步骤:

1. 编辑 /etc/services 文件。默认情况下，此文件应包含以下条目：
   omni 5565/tcp # DATA-PROTECTOR
   将端口号 5565 替换为某个未使用的端口号。
2. 如果系统上存在文件 /etc/opt/omni/client/customize/socket 和 /opt/omni/newconfig/etc/opt/omni/client/customize/socket ，则将所需的端口号更新到其内容中。
3. 通过使用 kill -HUP inetd_pid 命令终止相关进程，重新启动 Inet 服务。要确定进程 ID (inetd_pid)，请运行 ps -ef 命令。
4. 如果正在 Cell Manager 上重新配置 Inet，请为端口全局选项设置新值。
5. 如果正在 Cell Manager 上重新配置 Inet，请重新启动 Data Protector 服务：

```
omnisv stop   omnisv start
```

Windows 系统

更改 Windows 系统上将成为 Cell Manager、安装服务器或 Data Protector 客户机的 Inet **端口**

1. 在命令行上，运行 regedit 打开注册表编辑器。
2. 在注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\
   OpenView\OmniBackII\Common 下，创建注册表项 InetPort:
   注册表项名称：InetPort
   注册表项类型：REG_SZ（字符串）
   注册表项的值：PortNumber

要在已成为 Cell Manager、安装服务器或 Data Protector 客户机的 Windows 系统上更改 **Inet** 端口，请执行以下步骤:

1. 在命令行上，运行 regedit 打开注册表编辑器。
2. 依次展开“HKEY_LOCAL_MACHINE”、“SOFTWARE”、“Hewlett-Packard”、“OpenView”和“OmniBack”，然后选择“Common”。
3. 单击 **InetPort** 打开“编辑字符串”对话框。在“数值数据”文本框中，输入未用的端口号。必须在 Common 文件夹的 Parameters 子文件夹中完成相同操作。
4. 在 Windows 控制面板中，打开“管理工具”、“服务”，选择“Data Protector Inet”服务，然后通过单击工具栏上的“重新启动”图标重新启动该服务。

OpenVMS 系统

要在将成为 Data Protector 客户机的 OpenVMS 系统上更改 **Inet** 端口，请执行以下步骤:

1. 停止 Data Protector 服务。使用 @SYS$STARTUP:OMNI$SHUTDOWN.COM 命令。
2. 编辑 sys$startup:omni$startup.com 文件，将默认 TCP 端口从 5565 更改为 5555。
3. 启动 Data Protector 服务。使用 @SYS$STARTUP:OMNI$STARTUP.COM 命令。

在 Linux 系统中更改默认的 Data Protector IDB 端口和用户帐户

在 Linux 系统上，安装由 omnisetup.sh 脚本执行且不是交互式的。在启动安装之前必须先更改文件 /tmp/omni_tmp/DP.dat 文件中的端口值。

以下端口条目与 IDB 服务相对应：

- Data Protector IDB (hpdp-idb) 服务端口: PGPORT
- Data Protector IDB 连接池程序 (hpdp-idb-cp) 端口: PGCPORT
- Data Protector 应用程序服务器 (hpdp-as) 服务端口: APPSSPORT
- Data Protector 应用程序服务器 (hpdp-as) 管理端口: APPSNATIVEMGTPORT

通过设置变量 PGOSUSER，可以更改运行 IDB 所使用的默认用户帐户。DP.dat 文件示例：

```
PGPORT=7112 PGCPPORT=7113 PGOSUSER=hpdp APPSSPORT=7116 APPSNATIVEMGTPORT=7119
```

准备在 Windows 系统中运行的 Microsoft Server Cluster 以安装 Data Protector

要使用 Windows 系统中运行的 Microsoft Cluster Service (MSCS) 服务器群集安装群集感知 Data Protector，需要提前准备该群集。如果未准备，可能会导致备份本地的 CONFIGURATION 对象（该对象必须在准备期间予以备份，以便进行灾难恢复）会话失败，甚至有可能导致数据丢失。

先决条件

- 请确保您已使用域用户帐户登录到系统。域用户帐户必须是本地 Administrators 组的成员。

准备过程

若要正确准备群集以安装 Data Protector，请执行以下操作：

1. 在两个群集节点上，启动 Windows Firewall，并为文件和打印机共享 (File and Printer Sharing) 程序启用例外。
2. 在活动的群集节点中，启动“故障转移群集管理 (Failover Cluster Management)”，并验证 quorum 资源中的见证磁盘是否已联机。如果该资源已脱机，请将它联机。
   仅在活动的群集节点中执行以下步骤。
3. 如果正在准备尚未配置多数节点集 (MNS) 的群集，请启动 Windows 资源管理器，并将 WitnessDiskLetter :\\Cluster 文件夹的所有权更改为本地 Administrators 组。在“群集的高级安全性设置 (Advanced Security Settings for Cluster)”窗口中更改所有权时，请确保已选中**替换子容器及对象的所有者 (Replace owner on subcontainers and objects)** 选项。在“Windows 安全性”对话框中，单击“是”确认建议操作，然后再单击“是”来确认通知。
4. 如果正在准备尚未配置 MNS 的群集，请在 Windows 资源管理器中，将针对 SYSTEM 和本地 Administrators 组将 WitnessDiskLetter:\Cluster 文件夹的权限更改为允许完全控制。
5. 如果在准备一个将执行 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理 (Failover Cluster Management)”中添加群集访问点 (Cluster Access Point) 资源。选择**添加资源 (Add a resource)**，然后单击**1- 客户机访问点 (1- Client Access Point)** 以启动“新建资源 (New Resource)”向导。
   a. 在“客户机访问点 (Client Access Point)”窗格中，在“名称 (Name)”文本框中输入虚拟服务器的网络名称。
   b. 在“地址 (Address)”文本框中，输入虚拟服务器的 IP 地址。
6. 如果在准备一个将执行 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理 (Failover Cluster Management)”中，将一个共享文件夹添加到群集。单击“添加共享文件夹”以启动“设置共享文件夹”向导:
   a. 在“共享文件夹位置 (Shared Folder Location)”窗格上的“位置 (Location)”文本框中，输入目录路径。请确保所选目录具有足够的可用空间，可以存储在 Data Protector 安装过程中创建的数据。单击“下一步”。
   b. 在“NTFS 权限 (NTFS Permissions)”、“共享协议 (Share Protocols)”和“SMB 设置 (SMB Settings)”窗格中，保留默认选项值不变。单击**下一步 (Next)**，移到下一个窗格。
   c. 在“SMB 权限”窗格上，选中“管理员具有完全控制权，其他所有用户和组只有读写访问权”**选项**。单击“下一步”。

      > 注意**:** 要成功安装或升级群集感知 Data Protector，请确保 NT-AUTHORITY\SYSTEM 有权访问 MS 群集中的共享目录。您可以在安装或升级完成后删除此权限。

   d. 在“DFS 名称空间发布 (DFS Namespace Publishing)”中，保留默认选项值。单击“下一步”。
   e. 在“查看设置”和“创建共享”窗格中，单击“创建”。

在带有 Veritas Volume Manager 的 Microsoft Cluster Server 上安装 Data Protector

要在带有 Veritas Volume Manager 的 Microsoft Cluster Server (MSCS) 上安装 Data Protector，请先按照在 MSCS 上安装 Data Protector 的常规过程进行操作。

安装完成后，还需要一些额外的步骤，以使 Data Protector Inet 服务能区别本地磁盘资源，以及使用自己的资源驱动程序，而不是使用 Microsoft 资源驱动程序的群集磁盘资源：

1. 通过在 Cell Manager 上执行 omnisv -maintenance 命令启动维护模式。
2. 如下定义值为 Volume Manager Disk Group 的新系统环境变量 OB2CLUSTERDISKTYPES，或者设置两个群集节点上的 omnirc 选项：OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   要指定更多专有磁盘资源（如 NetRAID4 磁盘），只需将资源类型名称追加到 OB2CLUSTERDISKTYPES 环境变量值即可：OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
3. 通过执行 omnisv -maintenance -stop 命令退出维护模式。

准备 NIS 服务器

此过程将使 NIS 服务器能识别 Data Protector Cell Manager

添加 Data Protector 信息

要将 Data Protector 信息添加到 NIS 服务器，请完成下面的步骤:

1. 作为 root 登录到 NIS 服务器。
2. 如果通过 NIS 管理 /etc/services 文件，将下面的行追加到 /etc/services 文件
   omni 5565/tcp # Data Protector for Data Protector inet server
   如果端口 5565 不可用，将其替换成其他端口。

如果通过 NIS 管理 /etc/inetd.conf 文件，将下面的行追加到 /etc/inetd.conf 文件：
#Data Protector
omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log

3. 运行下面的命令，使 NIS 服务器读取文件并更新配置。
   cd /var/yp; make

> **注意**在 NIS 环境中，nsswitch.conf 文件可定义不同配置文件在将来的使用顺序。例如，可以定义是在本地计算机还是 NIS 服务器上使用 /etc/inetd.conf 文件。还可以在该文件中插入语句，声明由 nsswitch.conf 文件来控制保留名称的位置。请参见手册页获得详细信息。
>
> 如果已经安装了 Data Protector，必须准备 NIS 服务器，然后在同时作为 Data Protector 客户机的每台 NIS 客户机上，使用命令 kill -HUP pid 停止相关的进程以便重新启动 Inet 服务。

故障诊断

- 如果在 NIS 环境中安装 Data Protector 后，Data Protector Inet 服务未启动，请检查 **/etc/nsswitch.conf** 文件。
  如果找到下面一行：
  services: nis [NOTFOUND=RETURN] files
  将该行替换为：
  services: nis [NOTFOUND=CONTINUE] files。

更改 Cell Manager 名称

安装 Data Protector 后，它将使用当前主机名作为 Cell Manager 名称。如果更改 Cell Manager 的主机名，需要手动更新 Data Protector 文件。

> **重要说明:**
>
> - 使用新的 Cell Manager 名称更新客户机信息。更改 Cell Manager 主机名之前，从单元中导出客户机以更新名称。
> - Cell Manager 名称更改后，旧证书将不起作用。在客户机中，您需要重新配置安全的通信证书: omnicc -secure_comm -reconfigure_peer CMname。
> - 必须修改使用旧 Cell Manager 名称配置的所有设备和备份规范，以反映正确的名称。

在 Linux 系统上 - 独立

在 Linux Cell Manager 上 (独立)，执行以下操作:

1. 更改计算机名称或域名。

   > **注意**确保新主机名能够由 DNS 在两个方向上解析。如果名称解析不起作用，请不要继续此过程。

2. 从 Cell Manager 取消注册报告服务器。
3. 执行命令 /opt/omni/bin/perl /opt/omni/sbin/omnicellnamechange.pl --newcmhost *<new_cell_manager_name>*

   > **注意**成功执行该命令之后，使用旧域或客户机的用户仍会出现在“用户”上下文或 omniusers –list 命令中。要在 UserList 文件和“用户”上下文之间保持同步，请使用 omniusers –remove 命令或从“用户”上下文中删除旧域或旧客户机中的用户。

4. 编辑以下文件中的 Cell Manager 名称条目 (如果存在):
   - /etc/opt/omni/server/cell/lic_server
   - /etc/opt/omni/server/cell/mmdb_server
5. 在执行该命令之后，重新向 Cell Manager 注册报告服务器。
6. 使用 Data Protector GUI 连接到 Cell Manager，并接受新证书。
7. 如果磁带设备连接到 Cell Manager，请导航到设备和介质，然后在磁带设备的属性中更改主机名。
8. 对于所配置的文件设备：
   1. 要查看所配置的设备，使用以下命令：
      "omnidownload -list_libraries [-detail]" 和 "omnidownload -dev_info"
   2. 要修改“库”中的主机名，请导航到 # omnidownload -library <LIBRARY_NAME> >/tmp/file_lib.txt 并按如下方式编辑 file_lib.txt 文件:
      # omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt
   3. 要修改“设备”中的主机名，请导航到 # omnidownload -device <DRIVE_NAME> >/tmp/writer_0.txt 并按如下方式编辑 writer_0.txt 文件:
      # omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt

9. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
10. 更改受到主机名更改影响的其他备份规范。
11. 根据以下目录中的 Cell Server 主机名更改更新 UNIX 或 LINUX 客户机：
    /etc/opt/omni/client/cell_server
12. 根据注册表中的 Cell Server 主机名更改更新 Windows 客户机：
    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer
13. 检查以下配置文件中是否存在旧主机名：
    # grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"
    注意: 可以在以下位置查看旧主机名：/etc/opt/omni/server/dr/p1s -> 如果过去存储了系统恢复数据。
    /etc/opt/omni/server/certificates -> 旧证书 /etc/opt/omni/client/certificates -> 旧证书
14. 检查 IDB 内容并将其导出到以下文件：
    /opt/omni/sbin/omnidbutil -writedb /tmp <ENTER>
    dpidb.dat 文件包含内部数据库的主要部分。旧主机名仍保留在如下表格中：

    dp_frontend_application dp_catalog_object dp_catalog_object_datastream (in case the old device name(s) contain the old hostname) dp_management_session dp_medmng_library (in case the current device name(s) contain the old hostname) dp_medmng_media_pool (in case the old pool name(s) contain the old hostname) dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

在 Linux 系统上 - 群集

在 Linux Cell Manager 上 (群集)，执行以下步骤:

1. 更改计算机名称或域名。

   注意确保新主机名能够由 DNS、所有成员在两个方向上解析。如果名称解析不起作用，请不要继续此过程。

2. 在 Data Protector 包上禁用故障转移。
3. 使用 <新的 Cell Manager 名称> 编辑 /etc/opt/omni/server/install/sg/sg.conf file 文件中的条目。
4. 从 Cell Manager 取消注册报告服务器。
5. 执行命令 /opt/omni/bin/perl /opt/omni/sbin/omnicellnamechange.pl --newcmhost <*new_cell_manager_name*>

   注意成功执行该命令之后，使用旧域或客户机的用户仍会出现在“用户”上下文或 omniusers –list 命令中。要在 UserList 文件和“用户”上下文之间保持同步，请使用 omniusers –remove 命令或从“用户”上下文中删除旧域或旧客户机中的用户。

6. 编辑以下文件中的 Cell Manager 名称条目 (如果存在):
   - /etc/opt/omni/server/cell/lic_server
   - /etc/opt/omni/server/cell/mmdb_server
7. 在执行该命令之后，重新向 Cell Manager 注册报告服务器。
8. 使用 Data Protector GUI 连接到 Cell Manager，并接受新证书。
9. 如果磁带设备连接到 Cell Manager，请导航到设备和介质，然后在磁带设备的属性中更改主机名。
10. 对于所配置的文件设备：
    1. 要查看所配置的设备，使用以下命令：
       "omnidownload -list_libraries [-detail]" 和 "omnidownload -dev_info"
    2. 要修改“库”中的主机名，请导航到 # omnidownload -library <*LIBRARY_NAME*> >/tmp/file_lib.txt 并按如下方式编辑 file_lib.txt 文件:
       # omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt
    3. 要修改“设备”中的主机名，请导航到 # omnidownload -device <DRIVE_NAME> >/tmp/writer_0.txt 并按如下方式编辑 writer_0.txt 文件:
       # omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt
11. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
12. 更改受到主机名更改影响的其他备份规范。
13. 根据以下目录中的 Cell Server 主机名更改来更新 UNIX 或 Linux 客户机/节点:
    /etc/opt/omni/client/cell_server
14. 根据注册表中的 Cell Server 主机名更改更新 Windows 客户机：
    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer
15. 检查以下配置文件中是否存在旧主机名：
    # grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"
    注意: 可以在以下位置查看旧主机名：/etc/opt/omni/server/dr/p1s -> 如果过去存储了系统恢复数据。
    /etc/opt/omni/server/certificates -> 旧证书 /etc/opt/omni/client/certificates -> 旧证书
16. 检查 IDB 内容并将其导出到以下文件：
    /opt/omni/sbin/omnidbutil -writedb /tmp <ENTER>
    dpidb.dat 文件包含内部数据库的主要部分。旧主机名仍保留在如下表格中：

    dp_frontend_application dp_catalog_object dp_catalog_object_datastream (in case the old device name(s) contain the old hostname) dp_management_session dp_medmng_library (in case the current device name(s) contain the old hostname) dp_medmng_media_pool (in case the old pool name(s) contain the old hostname) dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

在 Windows 系统上 - 独立

在 Windows Cell Manager 上 (独立)，执行以下操作:

1. 更改计算机名称或域名。

> **注意**确保新主机名能够由 DNS 在两个方向上解析。如果名称解析不起作用，请不要继续此过程。

2. 从 Cell Manager 取消注册报告服务器。
3. 请执行以下命令:
   <DP_HOME>/perl <DP_HOME>/omnicellnamechange.pl --newcmhost <new_cell_manager_name>
   For example:C:\Program Files\Omniback\bin\perl C:\Program Files\Omniback\bin\omnicellnamechange.pl --newcmhost <new_cell_manager_name>

> **注意**成功执行该命令之后，使用旧域或客户机的用户仍会出现在“用户”上下文或 omniusers –list 命令中。要在 UserList 文件和“用户”上下文之间保持同步，请使用 omniusers –remove 命令或从“用户”上下文中删除旧域或旧客户机中的用户。

4. 编辑以下文件中的 Cell Manager 名称条目 (如果存在):
   - C:\ProgramData\OmniBack\Config\Server\cell\ lic_server
   - C:\ProgramData\OmniBack\Config\Server\cell\ mmdb_server
5. 在执行该命令之后，重新向 Cell Manager 注册报告服务器。
6. 使用 Data Protector GUI 连接到 Cell Manager，并接受新证书。
7. 如果磁带设备连接到 Cell Manager，请导航到**设备和介质**，然后在磁带设备的属性中更改主机名。
8. 对于所配置的文件设备：
   1. 要查看所配置的设备，使用以下命令：
      "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"
   2. 要修改“库”中的主机名，请导航到 "omnidownload -library <LIBRARY_NAME> > c:\temp\file_lib.txt" 并按如下方式编辑 file_lib.txt 文件: omniupload -modify_library <LIBRARY_NAME> -file c:\temp\file_lib.txt
   3. 要修改“设备”中的主机名，请导航到 "omnidownload -device <Device Name> > c:\temp\device.txt" 并按如下方式编辑 device.txt 文件: omniupload -modify_device <Device Name> -file c:\temp\device.txt
9. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
10. 更改受到主机名更改影响的其他备份规范。
11. 根据以下目录中的 Cell Server 主机名更改更新 UNIX 或 Linux 客户机：

```
/etc/opt/omni/client/cell_server
```

12. 根据注册表中的 Cell Server 主机名更改更新 Windows 客户机：

```
HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer
```

13. 使用 Windows 的“在文件中查找”选项检查以下文件，以搜索旧主机名：Data_Protector_program_data\Config

> **注意**可以在以下位置查看旧主机名：
> - Data_Protector_program_data\Config\Server\dr：如果过去存储了系统恢复数据。
> - Data_Protector_program_data\Config\Server\certificates：旧证书
> - Data_Protector_program_data\Config\client\certificates：旧证书。

14. 检查 IDB 内容并将其导出到以下文件： omnidbutil -writedb e:\idb_export <ENTER>

> **注意**dpidb.dat 文件包含内部数据库的主要部分。旧主机名仍保留在如下表格中：
> - dp_frontend_application
> - dp_catalog_object
> - dp_catalog_object_datastream (如果旧设备名称包含旧主机名)
> - dp_management_session
> - dp_medmng_library (如果当前设备名称包含旧主机名)
> - dp_medmng_media_pool (如果旧池名称包含旧主机名)
> - dp_medmng_cartridge (如果旧池名称包含旧主机名)

在 Windows 系统上 - 群集

在 Windows 系统上 (群集)，执行以下操作:

1. 停止角色和所有群集服务。
2. 在以下位置更改名称:
   1. 角色名称
   2. 文件服务器名称
   3. 服务器名称

> **注意**确保新主机名由 DNS 进行解析，而且可从所有节点访问文件共享。如果名称解析不起作用，请不要继续此过程。

3. 更改以下文件中的 DNS 条目:
   <*drive*>\Windows\System32\drivers\etc\hosts
4. 从 Cell Manager 取消注册报告服务器。
5. 请执行以下命令:
   <DP_HOME>/perl <DP_HOME>/omnicellnamechange.pl --newcmhost <new_cell_manager_name>
   For example:C:\Program Files\Omniback\bin\perl C:\Program Files\Omniback\bin\omnicellnamechange.pl --newcmhost <new_cell_manager_name>

> **注意**成功执行该命令之后，使用旧域或客户机的用户仍会出现在“用户”上下文或 omniusers –list 命令中。要在 UserList 文件和“用户”上下文之间保持同步，请使用 omniusers –remove 命令或从“用户”上下文中删除旧域或旧客户机中的用户。

6. 编辑以下文件中的 Cell Manager 名称条目 (如果存在):
   - C:\ProgramData\OmniBack\Config\Server\cell\ lic_server
   - C:\ProgramData\OmniBack\Config\Server\cell\ mmdb_server
7. 在执行该命令之后，重新向 Cell Manager 注册报告服务器。
8. 使用 Data Protector GUI 连接到 Cell Manager，并接受新证书。
9. 如果磁带设备连接到 Cell Manager，请导航到“设备和介质”，然后在磁带设备的属性中更改主机名。
10. 如果文件设备连接到 Cell Manager:
    1. 查看配置的设备。使用以下命令:
       - omnidownload -list_libraries [-detail]
       - omnidownload -dev_info
    2. 修改库中的主机名。
       1. 将库复制到临时文件。使用 omnidownload -library <*LIBRARY_NAME*>> c:\temp\file_lib.txt 命令。
       2. 编辑库文件。使用以下命令: omniupload -modify_library <*LIBRARY_NAME*> -file c:\temp\file_lib.txt
    3. 修改设备中的主机名。
       1. 将设备信息复制到临时位置。使用命令 omnidownload -device <*Device Name*>> c:\temp\device.txt.
       2. 编辑 **device.txt** 文件。使用以下命令: omniupload -modify_device <*Device Name*> -file c:\temp\device.txt
11. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
12. 更改受到主机名更改影响的其他备份规范。
13. 在以下文件中更新 UNIX 或 Linux 客户机的 Cell Server 主机名更改: /etc/opt/omni/client/cell_server
14. 在以下注册表中更新 Windows 客户机的 Cell Server 主机名更改: HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack II\Site\CellServer
15. 使用 Windows 的“在文件中查找”选项检查以下文件，以搜索旧主机名: Data_Protector_program_data\Config

> **注意**可以在以下位置查看旧主机名：
> - Data_Protector_program_data\Config\Server\dr：如果过去存储了系统恢复数据。
> - Data_Protector_program_data\Config\Server\certificates：旧证书
> - Data_Protector_program_data\Config\client\certificates：旧证书。

16. 检查 IDB 内容并将其导出到以下文件： omnidbutil -writedb e:\idb_export <ENTER>

> **注意**dpidb.dat 文件包含内部数据库的主要部分。旧主机名仍保留在如下表格中：
> - dp_frontend_application
> - dp_catalog_object
> - dp_catalog_object_datastream (如果旧设备名称包含旧主机名)
> - dp_management_session
> - dp_medmng_library (如果当前设备名称包含旧主机名)
> - dp_medmng_media_pool (如果旧池名称包含旧主机名)
> - dp_medmng_cartridge (如果旧池名称包含旧主机名)

在 Windows Cell Manager 上运行大量备份会话

要在 Windows Cell Manager 上运行大量备份会话，您应在 Windows 注册表中调整桌面堆限制。桌面堆由以下注册表项控制：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows
```

此注册表项的默认值如下所示：

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
```

Data Protector 受 SharedSection 参数影响，该参数包括以下值:

- 1024: 所有桌面通用的共享堆大小。要避免出现与桌面堆耗尽相关的问题，不得更改此值。
- 20480: 与交互式窗口站关联的每个桌面的桌面堆大小。
- 768: 与非交互式窗口站关联的每个桌面的桌面堆大小。

应将 SharedSection 参数的第三个值 (768) 设置为 20480。修改的 Windows 注册表项值将如下所示：
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,20480 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16 请勿设置非常高的值，因为值以千字节为单位。

设置新值后，必须重新启动系统。

Upgrade

This section guides you with information to upgrade to the latest version of Data Protector.

Upgrade workflow

Data Protector allows you to directly upgrade to Data Protector 10.03 or later versions, without a need to upgrade to an interim version. In order to successfully upgrade from an earlier version to the latest version of Data Protector, complete the steps in this upgrade workflow:

1. Prepare to upgrade.
   1. Download the latest software from https://entitlement.microfocus.com/mysoftware/index.
   2. Meet the system requirements.
      - See Upgrade prerequisites or Preinstall tasks
      - Review supported and discontinued platforms and versions. See the latest Support Matrix.
   3. Disable encrypted control communication (ECC) on all clients and the Cell Manager if you are upgrading from Data Protector 9.x and earlier.
2. Update licenses.
   - License keys obtained prior to Data Protector 9.x are not compatible with Data Protector 10.00 or later releases. If you are upgrading from Data Protector 9.x or earlier releases to Data Protector 10.00 or later releases, obtain new license keys.
   - License keys obtained for Data Protector 10.00 or later work with all subsequent releases.

   After the upgrade, Data Protector will run with a 90 days Instant-On password. This behavior is identical to a fresh installation with an Instant-On password. See Obtain a license for more information.

3. Set up port addresses.
   - The `omnirc` parameter `OB2PORTRANGE(SPEC)` defines a range of ports to be used by Data Protector agents. These ports must be outside the firewall/DMZ setting of your network. From Data Protector 10.xx, the INET port has changed to a new Data Protector-only associated IANA-recognized port of 5565/TCP. This port will be used in fresh Data Protector 10.xx installations (and all subsequent upgrades) by default. In an upgrade situation, it is recommended to have both 5555 and 5565 ports open until all clients are upgraded.
     If your current Data Protector version used port 5555, the upgraded version will continue to use port 5555.
   - You also have to consider checking existing firewall settings after upgrading to Data Protector 10.00 or later releases as some ports (like 5555) might only be opened in one direction. Change this to bi-directional behavior.
4. Upgrade the Cell Manager. Complete the following:
   1. Check for proper DNS names and bi-directional FQDN resolution before you begin the upgrade process. Use the command `omnicheck -dns -host <CellManager>` to ensure DNS is resolved correctly.

      > **Important** Having incorrect DNS names results in issues with certificate creation process. You may have to recreate certificate on every system separately after resolving DNS issues.

      Ensure the following:

      - The Cell Manager's host name starts with an alphabet or a numeric.
      - The Cell Manager's host name does not contain an underscore (_).
      - The Cell Manager's host name is not single character.
      - The length of the short host name or the host name component in the FQDN is less than 15 characters on the Windows platform.
      - The host name retrieved from the OS matches the Cell Manager's host name as recorded by Data Protector.
      - The Cell Manager's host name FQDN is present in **standalone.xml** file.
      - The Cell Manager's host name FQDN is present in the **client webservice.properties** file.
   2. Upgrade the Cell Manager.
      1. Run database consistency checks
      2. Follow the steps in the Upgrade Cell Manager section.
   3. Migrate users.

      When the Cell Manager is upgraded, all the existing users are migrated automatically. No manual intervention is required.

      If user migration fails during the upgrade process, complete the following:

      1. Check if the appserver service is running using the `omnisv -status` command.
      2. Run the following command to migrate the existing users:
         - Windows: `<DP_HOME>\bin\perl.exe <DP_HOME>\bin\userMigrate.pl`
         - Linux: `/opt/omni/bin/perl /opt/omni/sbin/userMigrate.pl`
   4. Migrate schedules.

      When the Cell Manager is upgraded, all existing schedules are migrated automatically. No manual intervention is required. See the Migrate schedules from previous versions section for information.

5. Enable secure peering between the Cell Manager and the Installation Server/client.

   Run the command `omnicc -secure_comm -configure_peer` on both Cell Manager and Installation Server/client. Repeat this step for all the Installation Servers and clients in your cell. See omnicc command page for more information on command usage.

   - Execute the `omnicc -secure_comm -configure_peer <CellManagerHostname>` command on both Cell Manager and the client.

This configures the client with a Cell Manager certificate. Now, run the omnicc -secure_comm -configure_peer <*ClientHostname*> command on the Cell Manager to establish two-way "secure communication" between the Cell Manager and the client.

6. Create a dedicated user with web access. Data Protector 10.03 and later versions provide web access to all users by default. Use the naming convention **user|group|client** when you create a new user. Using the name **<any>** for an user is not supported.
7. Upgrade Installation Server.

   You can upgrade Installation Server in the following scenarios:

   - Cell Manager and Installation Server is on the same host:

     If Cell Manager and Installation Server are on the same host, then no additional steps are needed to import the Installation Server in the environment. As they are co-exists on the same host, there is no need to establish secure peering.

   - Cell Manager and Installation Server are on different hosts:

     If the Cell Manager and Installation Servers are on different hosts, upgrade the Cell Manager first, and then upgrade the Installation Server.

     > **Note** Establish secure peering between the Cell Manager and Installation Server hosts. If one Installation Server is imported in multiple Cell Managers, then establish secure peerting between the respective Cell Manager and Installation Server host pairs.

     To upgrade Installation Server, follow the steps in the Upgrade Installation Server section.

8. Install or upgrade clients. The following options are available for installing or upgrading clients:
   - Push install Windows clients:
     - Windows Clients use the Session Message Block (SMB) protocol to obtain the installation sources from the Data Protector Installation Server. Data Protector uses it to copy data from the Installation Server to the client during the initial client push installation or later upgrade, and to manipulate services on the client.
     - Starting with Data Protector 10.03, the Installation Server host system is modified so that the SMB Server and Client are both modified to request SMB signing. It is now mandatory to specify valid user credentials (if requested) during any kind of remote push operation including upgrades.
     - The SMB signing implies that files copied from the <InstallationServerHost>\OmniBack shares are copied to clients from the Installation Server with signed and verified packages. This improves Data Protector security as signed SMB traffic provides data integrity, as clients are given secure data during the installation and data cannot be changed by attackers.
     - Starting with Data Protector 10.60, the Installation Server host system is modified so that the SMBv1 is disabled. This improves Data Protector security.
   - Push install UNIX and Linux clients
     - Linux clients were using **rsh** and **rexec** on Installation Servers to push packages to be locally installed on clients, if not already configured to SSH. Starting with Data Protector 10.03, Data Protector uses SSH as the default mechanism to send and install software on new clients.
     - SSH is a much more secure protocol compared to rsh and rexec, which both send and receive data in an unencrypted format. SSH sends data encrypted and is widely regarded as one of the most secure protocols.
     - The mutual exchange certificates (public keys) between a Cell Manager and client will happen over this secure SSH channel.
     - Starting with Data Protector 10.04, it is also possible to install/upgrade clients with a non-root user account. The non-root user needs to have "sudo" permission. See Configure sudo access for more information.
   - Local install:
     - Starting with Data Protector 10.03, clients and Cell Managers are configured are set up for secure peering. The omnicc -secure_comm -configure_peer command is run on the clients (when installed locally) to authenticate them with the Cell Manager. The secure peering has to be set up on both Cell Manager and clients.
     - This secure peering between Cell Managers and clients improves security as the identity of each is first reviewed and then verified.
   - Import clients manually after local installation:
     - Clients have to be imported when the Cell Manager name is not specified during the local installation. After the local installation is complete, execute the omnicc -secure_comm -configure_peer <*CellManagerHostname*> command on both Cell Manager and the client. This configures the client with a Cell Manager certificate. This is a mandatory step for locally installed clients. Run the omnicc -secure_comm -configure_peer <*ClientHostname*> command on the Cell Manager to establish two-way trust between the Cell Manager and the client.

     You can also use the omnicc -secure_comm -configure_peer <*CellManagerHostname*> command for re-importing a deleted client.

   To install clients, see Install Data Protector clients

   To upgrade clients, see Upgrade Data Protector clients

9. Post upgrade
   - After upgrading Data Protector and VMware GRE, un-register and re-register the GRE plugin onto your vCenter Server(s). Specify the web user credentials (created earlier) if VMware GRE prompts for Cell Manager credentials.
   - See the Post upgrade section.
10. Troubleshoot upgrade.

    For resolving issues during Data Protector upgrade, see Troubleshoot upgrade issues topic.

See also the following for upgrading Data Protector:

- Upgrade Data Protector in cluster-mode
- Upgrade from Single Server Edition

Upgrade prerequisites

Meet the upgrade prerequisites

Cell Manager hostname checks

Prior to starting the upgrade, ensure that the following infrastructural prerequisite conditions are met:

- The Cell Manager's host name as obtained from the omnidbutil –show_cell_name command output matches the FQDN of the host as recorded in the DNS.
- The Cell Manager's host name starts with an alphabet or a numeral.
- The Cell Manager's host name does not contain an underscore (_).
- The Cell Manager's host name is not single character.
- The length of the short host name or the host name component in the FQDN is less than 15 characters on the Windows platform.
- The host name retrieved from the OS matches the Cell Manager's host name as recorded by Data Protector. This check is excluded in a cluster setup.
- The Cell Manager's host name FQDN is present in **standalone.xml** file.
- The Cell Manager's host name FQDN is present in the **client webservice.properties** file.

Other prerequisites

- Ensure you have appropriate licenses before you begin upgrade.
  - License keys obtained prior to Data Protector 9.x are not compatible with Data Protector 10.00 or later releases. If you are upgrading from Data Protector 9.x or earlier releases to Data Protector 10.00 or later releases, obtain new license keys.
  - License keys and existing passwords generated for Data Protector 10.xx release works with all Data Protector 10.xx, 2018.xx, and 2019.xx releases. If you are upgrading from a version earlier than Data Protector 10.00, obtain compatible license keys.

  You must have a valid active support agreement in place in order to be eligible for new license passwords according to the type and quantity of licenses listed in your support agreement.

  Before you start the upgrade, check the quantity and type of license keys installed in your Data Protector environment and compare it to the quantity and type of licenses listed in your support agreement.

  If you have fewer or different licenses listed in your support agreement than actually installed in your environment, you should not start the upgrade. Otherwise you risk that your Data Protector environment is no longer operational due to missing license keys. Instead, contact your sales representative or partner first to determine what steps are needed to close the gap in the licensed functionality covered by the support contract and the actual licenses currently in use with Data Protector versions older than Data Protector 10.00.

- (Applies to CM upgrades from DP 10.03 or later versions) Ensure that the omniusers -list command produces a valid output. The upgrade wizard runs this command as part of the upgrade precheck. If this command fails, the upgrade cannot proceed.
- *Applies to CM upgrades from DP 2020.08 or earlier.* To ensure that all existing LDAP groups and users are available after the upgrade, you must disable LDAPS configuration through the Keycloak console before starting the upgrade. Open the Keycloak console, go to **User Federation** > **Settings** and turn off the **Enabled** option.
- A POSIX shell (sh) is required for the installation.
- You must have root permissions to perform the upgrade.
- Set the kernel parameter shmmax (maximum size of a shared memory segment) to at least 2.5 GB. To check the configuration, execute: cat /proc/sys/kernel/shmmax
- Ensure that the following ports are open for Inet:
  - Fresh Data Protector installation - 5565
  - Upgraded Data Protector installation - 5555
- (Applies to upgrades from versions earlier than DP 2020.05 (DP 10.70)) Ensure that the 3612 port is free for Internal Database (IDB) upgrade.
- It is recommended to have a successful full IDB backup with protection in the last 3 days with an active protection of at least 7 days.
- (Applies to Windows installation only)The upgrade user should have Read, Write, and Edit permissions on the IDB configuration folder:(Data_Protector_program_data/omniback/server/db80).
- (Applies to CM installed on virtual machines only) It is recommended to take a snapshot of the Cell Manager virtual machine before initiating the upgrade.
- Disable Encrypted Control Communication (ECC) on all clients and the Cell Manager if you are upgrading from Data Protector 9.x and earlier versions. It is also recommended to disable ECC if you have previously upgraded from a Data Protector 9.x version. As ECC was supported in 9.x versions, a DP 10.x system that was previously upgraded from a 9.x version with ECC enabled inherits it, causing the upgrade to fail.

  If you are upgrading from a 9.x system, use the omnicc command to disable ECC. If you are upgrading from a 10.x version, do the following to disable ECC:
  - Set the Encryption option to 0 in cell_info file.
  - Remove or rename the config folder available at the following location: <ProgramData>/omniback/Config/Server
  - Remove or rename the config folder available at the following location: <ProgramData>/omniback/Config/client
- Ensure that the tablespace location of IDB Postgres database is same as PGDATA_IDB value mentioned in idb.config file. Also ensure that the tablespace location of JCE in Postgres is same as PGDATA_JCE value mentioned in idb.config file. The

location of the idb.config file is as follows:
Windows
<DP_SDATA_DIR>\server\idb\idb.config
Linux
/etc/opt/omni/server/idb/idb.config

- For information about supported and discontinued platforms and versions, see the latest Support Matrix.

  On platforms where the Cell Manager is no longer supported, first migrate the Cell Manager to a supported platform and then upgrade to the latest version of Data Protector.

  As an unsupported functional area, the Data Protector Java graphical user interface is not supplied in this release of Data Protector. If there are UNIX systems in your Data Protector cell that have the Data Protector Java graphical user interface installed, during the cell upgrade process, you need to choose other systems that will take the role of Data Protector graphical user interface clients. These clients should run on operating systems supported by the original (native) Data Protector graphical user interface.

- The bc command line calculator must be installed on the target client, for remote installation or upgrade of Linux clients with minimal OS installation.

- After the upgrade, the Cell Manager, and Installation Server must have the same Data Protector version installed. Although older Data Protector Disk Agent and Media Agent versions are supported in the same cell, it is highly recommended that the clients also have the same version of Data Protector components installed.

- After the upgrade of a multiple-cell (MoM) environment, all Cell Managers must have the same Data Protector version installed.

- With Data Protector 10.00, JBoss 7.1 is replaced with WildFly 10. During the Data Protector upgrade, the following JBoss configurations are automatically migrated to WildFly:

  - Logger levels and formats
  - LDAP configuration
  - PostgreSQL credentials

  > **Important** Any changes made in JBoss 7.1 standalone.xml file, apart from the configurations listed above, must be manually added in the WildFly configuration file after upgrade.

  Note that during upgrade, Data Protector creates a backup for the old JBoss configuration files in the Data_Protector_program_data folder. By default, the files are available at the following location:

  - Linux: /etc/opt/omni/server/AppServer_<versionNo>
  - Windows: Data_Protector_program_data\OmniBack\Config\Server\AppServer_<versionNo>

- Run database consistency checks on the existing IDB to validate data consistency prior to the upgrade.

- Perform a backup of the existing Cell Manager system and the Internal Database (IDB).

- Before upgrading, ensure that all GRE Power On open requests are closed. Additionally, make sure that the Live Migrate sessions that are in progress, are completed or aborted.
- *Applies if you are upgrading from DP 2019.08*. If the omnidbutil -enable_common_criteria_mode command has been executed in your 2019.08 environment , you must disable it before upgrading to a later version. To disable, run the following command:
  omnidbutil -disable_common_criteria_mode
- If you are following any of the following upgrade paths:
  - From Data Protector 9.x to any Data Protector 10.x version
  - From Data Protector 10.00 to Data Protector 10.40 or higher versions

  and want to use a backup from an older Data Protector version to perform Disaster Recovery, then you have one of the following options to plan ISO creation:
  - Create ISO image immediately after the Disaster Recovery backup and then perform the upgrade
  - Use the media creation host of the older Data Protector version in which the backup was performed to create the ISO image in the upgraded version.

  If you are upgrading from Data Protector 10.40 to any higher version, no special planning is needed for ISO creation for Disaster Recovery.

Limitations

The following limitations apply:

- Changing the Cell Manager platform during the upgrade is not supported. Upgrades are only supported on the same Cell Manager platform (Linux to Linux or Windows to Windows).

  If your platform is discontinued, migrate the Cell Manager to a supported platform first and then upgrade to the new version.

- In a UNIX environment: The only Data Protector processes that can be running before performing an upgrade are from Data Protector services. To do this, stop the Data Protector services, terminate any running process and restart the services.

- The Internal Database restore is supported only from the same minor-minor Data Protector version, in which the Internal Database was backed up. This is because of the Internal Database schema changes that are present in new releases.

- If you want to restore the Internal Database that was backed up in an earlier Data Protector version, reinstall the particular version, import the Internal Database backup medium, and then perform the restore.
- If the stores created using an older Data Protector version are not visible after upgrading, then you should restart the client (where stores reside).

Related topics

- For additional information about system preparation and maintenance tasks that are beyond the scope of this topic but strongly influence the upgrade procedure, see System preparation and maintenance tasks.

Upgrade Cell Manager and Installation server

To upgrade the Installation Server and Cell Manager on Windows and Linux platforms, consider the following:

- Windows:
  - Installation Server needs to be upgraded first even if it is a client to a Cell Manager.
  - Installation Server and Cell Manager are upgraded manually.
  - After installation or upgrade procedure, the Installation Server is secured and no other host can communicate through Data Protector processes.
  - Once the Cell Manager is installed or upgraded, on the Installation Server configure the Cell Manager host for accepting the requests from the Cell Manager using the following command:

    omnicc -secure_comm -configure_peer {Hostname1 [HostName2 ...]} [-accept_host]

  - Once secure communication is configured, import the Installation Server using Data Protector GUI or CLI.
- Linux:
  - If the Installation Server and Cell Manager are installed on the same system, it is upgraded automatically when the omnisetup.sh command is executed. If the Installation Server is installed on a separate system, you must manually upgrade the Installation server before upgrading the Cell Manager. For more information, see Upgrade Installation Server.
  - Upgrade of Cell Manager happens through Installation Server.
  - After the upgrade of Linux Installation Server, on the Installation Server host configure encryption for the cell manager using the following command:

    omnicc -secure_comm -configure_peer {Hostname1 [HostName2 ...]} [-accept_host]

  - Once secure communication is configured, import the Installation Server using Data Protector GUI or CLI.

Validate data consistency before upgrade

Before you proceed with the upgrade, it is highly recommended to perform several consistency checks to validate data consistency in the existing IDB.

To run database consistency checks, complete the following steps:

1. Run omnidbcheck.

   This command validates data consistency in the following areas:

   - Database connection (omnidbcheck -connection)
   - Schema consistency (omnidbcheck -schema_consistency)
   - Datafiles consistency (omnidbcheck -verify_db_files)
   - DCBF

2. Run omnidbcheck -dc.

   This command validates your DataCatalog consistency.

   If the data is consistent, both checks respond with Status - Ok on all fields. Perform a backup of the existing Cell Manager system and the IDB.

   If any inconsistencies are detected, it is highly advised to first fix those problems and then perform the upgrade.

Upgrade Cell Manager

- If the Linux Installation Server and Cell Manager are installed on the same system, it is upgraded automatically when the omnisetup.sh command is executed. If the Linux Installation Server is installed on a separate system, you must manually upgrade the Installation server before upgrading the Cell Manager. For more information, see Upgrade Installation Server.
  - On Linux, this command directly upgrades the installed components using the rpm utility.
- All client components installed on the Installation Server are automatically upgraded when omnisetup.sh is used.
- The upgrade procedure for the Cell Manager configured on Serviceguard differs from the upgrade procedure for the Cell Manager not running in the Serviceguard environment.

Upgrade Cell Manager - Linux

To upgrade the Linux Cell Manager, complete the following steps:

1. Before you begin, we recommend the following:
   - Take a full IDB backup with protection.
   - Take a snapshot of the Cell Manager virtual machine before initiating the upgrade (*Applies to CM installed on virtual machines only).*
   - For upgrade of Cell Manager from version 2019.12 (10.60) or prior, ensure the availability of port 3612 for the IDB upgrade.
2. Copy the downloaded Linux installation package (tar) in the server that has an existing Cell Manager installation, and extract the contents to a local directory.

   LOCAL_INSTALL

platform_dir/DP_DEPOT

Where platform_dir is linux_x86_64 for Linux systems.

3. Go to the directory where you have extracted the contents and execute:

   ./omnisetup.sh

   After the previous version of Data Protector is detected, the upgrade procedure is automatically started.
   The following message is displayed:

   Before initiating an upgrade, it is highly recommended that you create and validate a rollback plan in case a failure is encountered. The plan co uld include (but may not be limited to) backups, disaster recovery and snapshots. For more information, please consult Data Protector documen tation and support personnel.
   Do you want the setup to resume Cell Manager upgrade?[Y/N]

   Enter Y to proceed or enter N to exit the upgrade.
   The upgrade begins with the upgrade of Internal Database (IDB). Data Protector performs system and database checks as part of the upgrade. These checks take a few minutes to complete, depending on the database size and system performance.

   The following checks are performed:
   - **IDB Consistency Check**: This includes Database connection, Schema consistency, and Data files consistency checks.
   - **IDB Port Check**: This check applies for upgrade of Cell Manager from version 2019.12 (10.60) or prior. For this check to pass, port 3612 must be free.
   - **IDB Backup Check**: This checks for IDB backup that completed successfully within the last 3 days with an active protection of at least 7 days. Check fails if no successful IDB backup exists and displays the following message:

     IDB check failed, are you sure you want to continue: Y/N

     If you want to ignore the check and proceed, enter Y. If you want to abort the upgrade, enter N.

   To perform a clean installation (the database of previous version will be deleted), uninstall the old version and restart the installation.

As soon as the procedure is completed, you can start using Data Protector.

If you want to perform a backup after upgrading Cell Manager from any DP version to DP 2019.08 or later, run the following command to calculate and update Total Protected Data in 'DP_CATALOG_CBL' table:

/opt/omni/sbin/omnidbutil -update_total_protected_data

For the description of the omnisetup.sh command, see the omnisetup.sh command page.

Next steps

> **Note** Make sure to execute the commands in a new command prompt after the upgrade.

- After the upgrade is complete, validate the data consistency by running omnidbcheck and omnidbcheck -dc again. See Validate data consistency before upgrade.
- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See Check configuration changes.
- You must manually adjust the library capacity (VTLCAPACITY) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade by default set to 1 TB. See Check configuration changes.
- On SUSE Linux Enterprise Server (x86-64) the maximum size of database files can exceed the default maximum size of 2 GB. Consequently, during an upgrade to Data Protector 2018.09 or later, a warning message is displayed with an advice to adjust the maximum size of database files. This adjustment should be done after the upgrade, as it may take a significant amount of time, depending on the database size. See Troubleshoot upgrade issues.

Upgrade Cell Manager - Windows

To upgrade the Windows Cell Manager and Installation Server, follow the procedure described below:

In addition, it is recommended to:

1. Before you begin, ensure that the following prerequisites are met:
   - For upgrade of Cell Manager from version 2019.12 (10.60) or prior, ensure the availability of port 3612 for the IDB upgrade.
   - The upgrade user should have Read, Write, and Edit permissions on the IDB configuration folder (Data Protector_program_data/omniback/server/db80).
   - Take a full IDB backup with protection.
   - Take a snapshot of the Cell Manager virtual machine before initiating the upgrade (*applies to CM installed on virtual machines only).*
2. Run omnidbcheck. This command validates data consistency in the following areas:
   - Database connection
   - Schema consistency
   - Datafiles consistency

- DCBF

3. Run `omnisv –stop` to stop all Data Protector services that are running. Make sure other services such as Data Protector Telemetry Client service and Data Protector Filter Listener service are shut down and put in manual mode.
4. Download **Process Explorer** from the following site and put this on the cell server that will be upgraded: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
5. Run **Process explorer** and click **Find** which has only **Find handle or dll**. Search for `omniback`. This will find all processes that have any `omniback` directory opened. Remove all processes from this list before proceeding. Reboot system if necessary and then check **Process explorer** again. Once there are no processes showing up in **Process Explorer**, then proceed to start with the setup.
6. Start all the Data Protector services using the `omnisv -start` command. Make sure all the services are up and running before starting the installation.
7. Copy the downloaded installation package (zip) on a Windows system and extract to local directory. Run the `\Windows\x8664\setup.exe` command. Setup detects the previous Data Protector installation. Click **Next** to start the upgrade.
8. The upgrade begins with the upgrade of Internal Database (IDB). Data Protector performs system and database checks as part of the upgrade. These checks take a few minutes to complete, depending on the database size and system performance. The following checks are performed:
   - **IDB consistency check**: This includes Database connection, Schema consistency, and Data files consistency checks.
   - **IDB Port check**: This check applies for upgrade of Cell Manager from version 2019.12 (10.60) or prior. For this check to pass, port 3612 must be free.
   - **IDB Backup Check**: This checks for IDB backup that completed successfully within the last 3 days with an active protection of at least 7 days. If you want to ignore the check and proceed, select the **Ignore IDB Backup check** check box.
9. Click **Next**.
10. In the **Component Selection** page, the components previously installed on the system are selected.

    You can change the component set by selecting or deselecting additional components. Click **Next**.
11. Optionally, change the user account or the ports used by the Data Protector Internal Database Service and Application Server.

    Click **Next**.
12. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup registers all necessary Data Protector executables. By default, the **Initially, allow newly registered** Data Protector **executables to open inbound ports as needed** option is selected. If you do not want to enable Data Protector to open ports at the moment, deselect the option. For proper functioning of Data Protector with previous version clients, the Data Protector rules in Windows firewall must be enabled. Rules for the OmniInet Service executable, Application Server port and Internal Database Service port will always be enabled, regardless of the choice.

    Click **Next**.
13. The component summary list is displayed. Click **Install** to perform the upgrade.

    Upgrades from 6.20 and 7.00 to 9.00 or later:

    - A Command Prompt window opens and the software begins the IDB migration to the new database format by exporting the older IDB.
    - This Command Prompt window remains open during the export of the older IDB and displays status messages. The IDB export may take several minutes to complete.
    - As the upgrade proceeds, an additional Command Prompt window opens to display the status of the import of the IDB configuration information and data into Data Protector 9.00 or later.

    Upgrades from Data Protector 8.1x and later:

    - The IDB updates automatically; no Command Prompt windows are opened.
    - The **Installation status** page is displayed. Click **Next**.
14. To start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

> **Note** This step is performed only for a Cell Manager upgrade. If the Installation Server installed on a client other than the Cell Manager is being upgraded, this step does not occur.

15. Click **Finish**.

As soon as the procedure is completed, you can start using Data Protector.

If you want to perform a backup after upgrading Cell Manager from any DP version to DP 2019.08 or later, run the following command to calculate and update Total Protected Data in 'DP_CATALOG_CBL' table:

```
Program Files\OmniBack\bin\omnidbutil -update_total_protected_data
```

Microsoft Cluster Server

The upgrade procedure for the Cell Manager, running in the Microsoft Cluster Server environment, is different from the upgrade procedure for the Cell Manager not configured for use with Microsoft Cluster Server. The detailed steps you need to follow are described in Upgrade the Cell Manager configured on Microsoft Cluster Server.

You cannot upgrade Data Protector directly if the installation path:

- contains non-ASCII characters
- contains the characters "@ " or "# "
- contains a directory that ends with the character "!"
- is longer than 80 characters.

Troubleshoot Cell Manager upgrade issues

- Issue: **Upgrading fails if the previous version of the product is installed in a long path**

  For workaround, see Upgrading fails if the previous version of the product is installed in a long path

- Issue: **Upgrading fails if the previous version of the product is installed in a path with unsupported characters**

  For workaround, see Upgrading fails if the previous version of the product is installed in a path with unsupported characters.

- Issue: **Upgrade in secondary node on Linux**

  During Cell Manger upgrade to 10.00 in cluster environment on passive node, following message will be displayed:

  Error code : 302 error description :

  Operation failed!

  Could not update telemetry details. Please run

  /opt/omni/sbin/omnidbutil -set_telemetry_details -customer_name <name> -proxy_URL <URL> -proxy_port <port> -proxy_user <user> -proxy_passwd <password> -update_frequency <frequency> to update the details.

  No user intervention required.

Upgrade Installation Server

Upgrade Installation Server - Linux

To upgrade the Linux Installation Server, follow the procedure described below:

1. Copy the downloaded installation package (tar) to a Linux system where Installation Server is installed, and extract the contents to a local directory.

   LOCAL_INSTALL

   platform_dir/DP_DEPOT

   Where `platform_dir` is `linux_x86_64` for Linux systems.

2. Go to the directory where you have extracted the contents, and execute the following command:

   ./omnisetup.sh

As soon as the procedure is completed, you can start using Data Protector.

For the description of the `omnisetup.sh` command, see the omnisetup.sh page.

Next steps

Once the Installation Server system is upgraded, check if you have to apply any modifications to your configuration files. See Check configuration changes.

Upgrade Installation Server - Windows

The Windows Installation Server is upgraded automatically during the upgrade procedure if it is installed on the same system as the Cell Manager. The old Installation Server depot is removed and if the Installation Server component is selected during the installation, the new Installation Server depot is copied to its place.

If the Installation Server is installed together with the Data Protector client, and this client is upgraded remotely (using the Data Protector GUI), the Installation Server is upgraded as well.

> **Important** Re-import the upgraded Installation Server after the installation procedure has finished. For details, see Import Installation Server.

The steps for upgrading Installation Server on Windows is same as upgrading Cell Manager on Windows. To upgrade Installation Server, complete the steps in the Upgrade Cell Manager - Windows section.

Manual local upgrade on Linux systems

Normally, you can upgrade Data Protector 8.1 and later on Linux Cell Manager and Installation Server by executing the omnisetup.sh command, which performs an automated upgrade procedure. However, you can also perform the upgrade manually.

After upgrading the client manually, run the following omnicc command in the Cell Manager to update the client information:

```
omnicc -update_host [hostname] -accept_host
```

To update all the clients information which are part of the cell, run the following command:

```
omnicc –update_all -accept_host
```

Upgrade Data Protector on Linux systems using rpm

To upgrade the Linux Cell Manager or Installation Server, uninstall the old version and install the new version of the product.

Client components that are installed on the Cell Manager system are *not* upgraded during a Cell Manager upgrade and must be upgraded either by using omnisetup.sh or by remotely installing the components from the Installation Server.

To upgrade Data Protector using rpm, complete the following steps:

1. a. Copy the omnimigrate.pl script from the installation package to a temporary directory:

   ```
   cp –p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omnimigrate.pl /tmp
   ```

   b. Export the IDB using the omnimigrate.pl command:

   ```
   /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir /var/opt/omni/server/exported -export
   ```

2. Log in as root and stop the Data Protector services executing the omnisv -stop command.

   Type ps -ef | grep omni to verify whether all the services have been shut down. There must be no Data Protector services listed after executing the ps -ef | grep omni command.

3. Uninstall Data Protector using rpm.

   The configuration files and the database are preserved during this procedure.

4. Run the rpm -q command to verify that you uninstalled the old version of Data Protector. Old versions of Data Protector should not be listed.

   Verify that the database and configuration files are still present. The following directories should still exist and contain binaries:

   - /opt/omni
   - /var/opt/omni
   - /etc/opt/omni

5. If you are upgrading a Cell Manager, use rpm to install the Cell Manager.

   If you are upgrading an Installation Server, use the Linux installation package.

Next steps

> **Note** Make sure to execute the commands in a new command prompt after the upgrade.

- After the upgrade is complete, validate the data consistency by running omnidbcheck and omnidbcheck -dc commands again. See Validate data consistency before upgrade.
- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See Checking configuration changes.
- You must manually adjust the library capacity (VTLCAPACITY) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade by default set to 1 TB. See Checking configuration changes.

Check configuration changes

Global options file

During the upgrade, the contents of the *old* global options file are merged with the contents of the *new (default)* global options file on the Cell Manager, located at:

- Windows systems: Data_Protector_program_data\NewConfig\Server\Options
- Linux systems: /opt/omni/newconfig/etc/opt/omni/server/options

The *merged* file global resides at the same location on the Cell Manager as the old one and is used by the upgraded version of the product. The *old* global options file is renamed to global.1 , global.2 , and so on, depending on the number of upgrades performed.

The following applies when the merged file is created:

- Global options that were active (uncommented) in the old file remain active in the merged file. The following comment, stating that the value of the option was copied from the old file, is added to the merged file:

  ```
  Option=Value # Data Protector <''upgraded_version_number''> # This value was automatically copied from previous version.
  ```

- Global options that are not used anymore, are commented (made inactive) in the merged file and added the following comment stating that the option is no longer in use:

  ```
  #Option=Value # Data Protector <''source_version_number''> # This value is no longer in use.
  ```

- Global options with values, not supported anymore, are commented (made inactive) in the merged file. The following comment is added, containing a template line (DefaultValue) and stating the previous value of this option:

  ```
  # Option=DefaultValue # Data Protector <''upgraded_version_number''> # This variable cannot be transferred automatically. # The previous setting was: # Option=Value
  ```

- Comments are not transferred to the newly merged file.

Descriptions of the new options are in the merged global options file.

Post upgrade steps

The following list summarizes the steps you must perform manually once the upgrade procedure has successfully completed:

- Omnirc options

  After upgrading the Cell Manager and Installation Server systems, you may want to edit the omnirc file.

- Command line

  You may need to make adjustments for your scripts that invoke Data Protector commands:

  - The omnidbrestore command is replaced with the extended omnioffl r command that provides the same functionality. Until you replace the omnidbrestore command lines with the omnioffl r command lines, you can use the script omnidbrestore.pl that is supplied for your convenience. It recognizes the same set of options as omnioffl r . Invocations of the script should be in the following format where OMNIOFFLR_OPTIONS are omnioffl r command options without the -idb option:

    Windows systems: perl omnidbrestore.pl OMNIOFFLR_OPTIONS

    Linux systems: omnidbrestore.pl OMNIOFFLR_OPTIONS

- Verify that the hosts file contains the fully qualified domain names (FQDNs) in the computer.company.com format. If needed, update the file accordingly. The file resides at the following location:

  Windows systems: %SystemRoot%\system32\drivers\etc\

  Linux systems: /etc/hosts

- Changed default block size of backup devices

  Pay attention to an increased default block size for physical backup devices and other device types in device configuration wizard. Specific use cases, for example, object copying, object mirroring, and object consolidation, require careful selection of backup device block sizes. Devices configured with the default block size may not meet such use case requirements when used in conjunction with devices configured with the default block size in an earlier product version.

- If you have upgraded from DP 2020.08 or later versions, you must enable secure LDAP configuration using the Keycloak console. After enabling secure LDAP, All the LDAP groups and users from the older DP version will be available in the upgraded DP version.

Non-converted IDB parts after an upgrade from Data Protector 6.20 or 7.00

To ensure an efficient upgrade, the Data Protector upgrade process does not automatically upgrade (convert) specific parts of the Internal Database to the new format. The non-converted parts are nevertheless actively used in the new product version. Files constituting these IDB parts are located in the following directory:

- Windows systems: Data_Protector_program_data\db40
- Linux systems: /var/opt/omni/server/db40

This directory continues to be used until either of the following happens:

- Catalog protection expires for all backup data that was referenced in the DCBF of the earlier product version at the time of upgrade.
- Migration of the legacy DCBF to the new format is triggered using the omnimigrate.pl command.

> ⚠ **Caution** The above-mentioned directory should not be manually removed. Failing to do so may result in a data loss.

Next steps

Once the Cell Manager and Installation Servers are installed and all required modifications implemented, it is recommended that you distribute the software to clients. See Upgrading the clients.

Upgrade clients

On platforms where remote installation is supported, it is recommended that you upgrade the clients remotely.

Upgrade clients remotely

On Linux systems, you must upgrade the already present components before you add new components. After new components are added, the components from previous versions are not displayed by Data Protector. In this case, you have to reinstall them.

> **Note** If a client is not part of any Cell Manager, the remote upgrade of the client is not possible.

Upgrade clients locally

If you do not have an Installation Server installed on your network, or if for some reason you cannot distribute the Data Protector software to a client system, Data Protector clients can be upgraded locally.

To upgrade Windows clients locally, see Install Windows clients.

To upgrade UNIX clients locally, see Local install on UNIX systems.

Upgrade-related operating system specific tasks

Upgrading Windows and Linux clients

During an upgrade, the enhanced incremental backup database is not migrated to the new release version. The old enhanced incremental backup repository is deleted from the directory Data_Protector_home\enhincrdb\MountPoint (Windows systems) or /var/opt/omni/enhincrdb (Linux systems). During the first full backup after the client upgrade, a new repository is created at the same location. Ensure the type if your first backup performed after the upgrade is full.

Upgrading Linux clients

If the xinetd service is used instead of inetd, the /etc/xinetd.d/omni file is *not* replaced and thus the settings remain unchanged. To check if the xinetd service is running, run the ps -e | grep xinetd command.

To replace your settings with the default Data Protector settings or to replace a corrupted file, remove the file and remotely upgrade any Data Protector software component from the Data Protector GUI. The /etc/xinetd.d/omni file is then installed with the default settings.

> **Important** By replacing the /etc/xinetd.d/omni file, your modifications are lost. To retain your modifications, create a backup copy in advance and manually transfer the settings to the newly installed file after the upgrade.

Upgrade Solaris 8 to Solaris 9 systems

Starting with Data Protector 7.00, upgrading the operating system on the Data Protector Disk Agent clients from Solaris 8 to Solaris 9 is no longer supported.

If you still have Disk Agent (DA) of an earlier Data Protector version installed on Solaris 8, to upgrade the operating system to Solaris 9, follow instructions in the Install section of the earlier product version.

Upgrade clients configured on Serviceguard

If you are upgrading the client that uses Serviceguard, and if the Data Protector integration component to be upgraded is installed on the same node as the Cell Manager, first upgrade the physical nodes, and then perform the following:

1. Export the virtual host by executing:

   omnicc -export_host *virtual_hostname*

2. Re-import the virtual host by executing:

   omnicc -import_host *virtual_hostname* -virtual

Upgrade integration clients

If you are upgrading a Data Protector client that has the integration installed (such as the integration for Oracle, SAP R/3, or Microsoft Volume Shadow Copy Service, the Automatic Disaster Recovery module, the integration for Microsoft Exchange Server, Microsoft SQL Server, P9000 XP Disk Array Family, and so on), follow the steps described in sections below to successfully perform the upgrade:

- For instructions on how to upgrade the Oracle integration, see Upgrade the Oracle integration.
- For instructions on how to upgrade the SAP R/3 integration, see Upgrade the SAP R/3 integration.
- For instructions on how to upgrade the Microsoft Volume Shadow Copy Service integration, see Upgrade the Microsoft Volume Shadow Copy Service integration.
- For instructions on how to upgrade the Virtual Environment integration, see Upgrade the Virtual Environment integration.
- For instructions on how to upgrade the Microsoft Exchange Server, Microsoft SQL Server, P9000 XP Disk Array Family, or any other integration, see Upgrade other integrations.

Upgrade the Oracle integration

The clients that have the Oracle integration installed are upgraded either locally, by running the omnisetup.sh -install oracle8 command (Linux systems) or the setup.exe command (Windows systems), or remotely, by remotely installing the Oracle integration agent to the client using the Data Protector GUI. Note that on Linux, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the -install oracle8 option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

When the user has installed Container Database (CDB) on Data Protector 9.0x version and upgrades to the latest Data Protector version then he needs to reconfigure Oracle integration to get the new functionality.

User root is no longer required

On UNIX clients, the Data Protector Oracle Server integration no longer configures, checks the configuration of, and browses Oracle databases under the user root. Now, these operations run under the operating system user account that you specify in a backup specification. Therefore, you can safely remove the user root from the Data Protector user group.

> **Note** For ZDB and instant recovery sessions, the user root is still required.

After the upgrade, it is also recommended to perform a configuration check for each Oracle database, during which Data Protector copies the operating system user account (backup owner) from the backup specification to the corresponding Data Protector Oracle database configuration file.

If the configuration check is not performed, the configuration file is not updated. In such cases, during restore, Data Protector browses Oracle databases under the backup owner of the last backup session. If such a backup session has not been created in the last three months, the root user is used as the last option.

Configuring an Oracle instance for instant recovery

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you must either reconfigure the Oracle instance or set the ZDB_ORA_INCLUDE_CF_OLF , ZDB_ORA_INCLUDE_SPF , and ZDB_ORA_NO_CHECKCONF_IR omnirc options.

Oracle ASM configurations using 3PAR StoreServ Storage

To enable support for creation of consistent replicas of the Oracle Server data in 3PAR StoreServ Storage configurations in which Automatic Storage Management (ASM) is used, you need to upgrade both Data Protector components, the Oracle Integration and the 3PAR SMI-S Agent, on the application system as well as on the backup system.

Upgrade the SAP R/3 integration

The clients that have the SAP R/3 integration installed are upgraded either locally, by executing the omnisetup.sh -install sap command (Linux systems) or the setup.exe command (Windows systems), or remotely, by remotely installing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that on Linux, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the -install sap option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

SAP compliant ZDB sessions

SAP standards recommend that BRBACKUP is started on the backup system during ZDB sessions (SAP compliant ZDB sessions). Data Protector enables you to comply with these standards. First, configure the backup system as described in the SAP section for Oracle (split mirror backup, software configuration) and install the Data Protector SAP R/3 Integration component on the backup system. Then, configure Data Protector for SAP compliant ZDB sessions.

Configuring an Oracle instance for instant recovery

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you have three options:

- Reconfigure the Oracle instance.
- Set the ZDB_ORA_INCLUDE_CF_OLF , ZDB_ORA_INCLUDE_SPF , and ZDB_ORA_NO_CHECKCONF_IR omnirc options.
- Configure Data Protector to start BRBACKUP on the backup system (SAP compliant ZDB sessions).

Upgrade the Microsoft Volume Shadow Copy Service integration

Instant recovery-enabled backup sessions after upgrading from Data Protector 6.20 , Data Protector 7.00, and Data Protector 8.00 and later

After you upgraded the VSS integration from an older version of Data Protector, you need to resolve the source volumes on the application system if you will perform the ZDB-to-disk and ZDB-to-disk+tape sessions. Otherwise, the ZDB-to-disk sessions will fail and ZDB-to-disk+tape session will complete only with backups to tape not leaving the replicas on the disk array. Execute the resolve operation from any VSS client in the cell as follows:

```
omnidbvss –resolve {–apphost ApplicationSystem | –all}
```

Upgrade the Virtual Environment integration

When upgrading the Data Protector Virtual Environment integration component from the Data Protector version 6.20 or earlier, run the following command after the new version has been installed on the corresponding clients:

```
vepa_util.exe ––upgrade-cell_info
```

This is needed due to a change in password encoding in the cell_info file. It will re-encode the passwords used by the Virtual Environment integration, first creating a cell_info.bak file.

Upgrade other integrations

If the Data Protector client has the Microsoft Exchange Server, Microsoft SQL Server, P9000 XP Disk Array Family, or any other integration installed, upgrade such client either locally, using the omnisetup.sh -install *component_list* command (Linux systems) or the setup.exe command (Windows systems), or remotely, using the Data Protector GUI. For a list of the Data Protector component codes, see Local install on UNIX systems. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the -install *component_list* option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

Upgrade in a MoM environment

You can upgrade a MoM Environment sequentially. However, note that you cannot use **distributed file media format** with your file libraries until all Cell Managers have been upgraded to Data Protector 9.00 or later.

To upgrade your MoM environment, you need to upgrade the MoM Manager system first.

To upgrade your MoM environment, proceed as follows:

1. Upgrade the MoM Manager/CMMDB Server to the latest Data Protector version.

   During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with the old Cell Managers.

2. Upgrade each client Cell Manager in a MoM environment.
3. Upgrade clients with configured devices.
4. Upgrade clients with application integrations.

   After this part of the upgrade is finished, you can backup and restore filesystems and integrations with the latest Data Protector version MoM GUI.

Once MoM Manager is upgraded, run the following command on the MoM Manager for all the nodes of the non-windows cluster aware Cell Managers which are not upgraded:

```
omnicc -secure_comm -configure_for_cm <cluster node name>
```

This is only temporary measure till the respective Cell Manager is upgraded.

Once the Cell Manager is upgraded, run the following command to remove the node configuration for all the nodes of the upgraded Cell Manager:

omnicc -secure_comm -remove_peer <cluster node name>

After this is done, all Cell Managers of the previous versions, which have not been upgraded yet, are able to access the Central MMDB and central licensing, perform backups, but other MoM functionality is not available. Note that device sharing between the upgraded MoM cell and the cells with earlier versions of the product installed is not supported. During the upgrade of a MoM environment, none of the Cell Managers in the MoM environment should be operational.

Configure Data Protector users

In the MoM environment, ensure the following:

- The MOM server user is added in all Cell Manager and password is set for the MoM server user.
- All respective Cell Manager users are added in the MOM server client and their password is set in the MoM server.

See Configure Data Protector users for information on adding users.

Support for earlier agent versions

When you upgrade a Data Protector cell, ensure that you upgrade all the required Data Protector components on all the clients in the cell. This is required to ensure the availability of the latest Data Protector features on all the clients in the cell.
For example: Upgrading a cell might take some considerable time depending on the numbers of clients in the cell. While the clients are still being upgraded, you might run into issues with GUI or CLI if you use an older client with the upgraded Cell Manager. To avoid such issues, you must ensure that the client is upgraded to a version that matches the upgraded Cell Manager version.

Nevertheless, Disk Agent and Media Agent components of an earlier Data Protector version are supported in the upgraded cell with the following constraints:

- The earlier product version is still supported as an independent product. To check the announced end-of-support dates for products, see https://softwaresupport.softwaregrp.com.
- Support is limited to the feature set of the earlier Data Protector version.
- If you are performing operations involving clients on different systems, all agents of the same type (for example Media Agents) must be of the same version.
- Earlier Media Agent component versions are not supported in combination with NDMP servers.
- A file system backup can be sourced from multiple Disk Agents with different versions and the Backup Server deduplication is supported with different versions of the Media Agent. The Disk and Media agent versions could be lower than or equal to the Cell Manager version. However, the source deduplication requires the same versions of Disk Agents and Media Agents, which can be lower than or equal to the Cell Manager version.
- For the Data Protector StoreOnce software store, the Disk Agent and Media Agent must be the same version. However, this version can be lower than or equal to the Cell Manager version.
- If one Data Protector component on a client is upgraded, all other components have to be upgraded as well.
- Lower versions of Integration agents are not supported with the latest Cell Manager version.

If you encounter problems establishing a connection with agents of an earlier product version, consider upgrading to the latest Data Protector version as the first resolution step.

Migrate users

When you upgrade to the latest Data Protector version, all existing users are migrated automatically. No manual intervention is required.
If user migration fails during the upgrade process:

1. Check if the appserver service is running using command `omnisv -status`.
2. Run the following command to migrate the existing users:
   - Windows: *<DP_HOME>*\bin\perl.exe *<DP_HOME>*\bin\userMigrate.pl
   - Linux: /opt/omni/bin/perl /opt/omni/sbin/userMigrate.pl

Migrate schedules from previous versions

When you upgrade to a latest version of Data Protector, all existing schedules are migrated automatically to the new web-based scheduler. No manual intervention is required.

During upgrade, all your existing schedule files are appended with `.migrate` suffix.

For example, in an earlier Data Protector version, if you had a backup specification schedule with the name `WeeklyBackup`, the file name will be modified as `WeeklyBackup.migrate` during upgrade. If migration fails, the files are not renamed.

If the schedules are not migrated correctly, you may be asked to provide these `.migrate` files to Support for troubleshooting.

The migrated schedule files are available at the following location:

Specification Type	Schedule path
Backup schedules	• Windows: Data Protector_program_data\OmniBack\Config\Server\amoschedules • Linux: /var/opt/omni/server/amoschedules
Integration schedules	• Windows: Data Protector_program_data\OmniBack\Config\Server\Barschedules • Linux: /var/opt/omni/server/Barschedules
Copy operation schedules	• Windows: Data Protector_program_data\OmniBack\Config\Server\copylists\scheduled\schedules • Linux: /var/opt/omni/server/copylists/scheduled/schedules
Consolidation operation schedules	• Windows: Data Protector_program_data\OmniBack\Config\Server\consolidationlists\scheduled\schedules • Linux: /var/opt/omni/server/consolidationlists/scheduled/schedules
Verification operation schedule	• Windows: Data Protector_program_data\OmniBack\Config\Server\verificationlists\scheduled\schedules • Linux: /var/opt/omni/server/verificationlists/scheduled/schedules
Report group schedules	• Windows: Data Protector_program_data\OmniBack\Config\Server\rptschedules • Linux: /var/opt/omni/server/rptschedules

If schedule migration fails during the upgrade process, you can manually run the following command to successfully migrate the existing schedules to the new scheduler:

```
omnidbutil -migrate_schedules
```

The schedules added in previous versions of Data Protector did not have a name attribute associated with them. As a result, after migration, the name for the migrated schedules appears as **...**. You can edit these schedule and provide a name to the schedule.

Upgrade Reporting Server

This section describes how you can upgrade the Reporting Server on Windows and Linux platforms.

Upgrade on Windows

If an already existing version is detected when installing the Reporting Server on a Windows machine, the existing components are removed and the new components are installed.

Upgrade on Linux

Run the following command to upgrade the Reporting Server:

```
./omnisetup.sh -RS
```

The installer checks if the reporting server software is already installed. If yes, then it checks if a higher version of the reporting software is available in the downloaded DP DEPOT package. If a higher version is available, the installer then upgrades the software. If a higher version is not available, the installer exits by displaying the message that the reporting software is already installed

Upgrade Data Protector clients

After upgrading the Cell Manager, you must also upgrade the existing clients to enable secure communication for the clients. You can upgrade the Data Protector (DP) Clients either manually or through the Installation Server

Upgrade Data Protector Client through Installation Server

Data Protector clients with version DP 2018.09 (DP 10.20) and later use INET by default. When upgrading from these versions, the upgrade process doesn't prompt for credentials. However, while upgrading the following DP client versions that use either Server Message Block (SMB) or SSH communication, the client upgrade process by default prompts you for credentials.

- **Windows clients:** Uses Server Message Block (SMB) communication for DP versions 10.10, 10.04, 10.03, 10.02, and versions older than DP 10.01.
- **Linux clients:** Uses SSH communication for DP version 10.02 and versions older than DP 10.00 (DP 2018.09).

To avoid being prompted for credentials during the upgrade of these clients, set the `omnirc` variable **OB2UPGRADEOVERINET** on the installation server to 1. Setting this variable forces some clients to upgrade over INET as indicated in the following table:

DP client version	Client OS type	Default communication	Communication used after enabling OB2UPGRADEOVERINET	Prompt for credentials after enabling OB2UPGRADEOVERINET
Older than 9.07	Windows	SMB	INET	No
9.07 to 10.00	Windows	SMB	SMB	Yes
10.03 10.04 10.10 (DP 2018.09)	Windows	SMB	SMB	Yes
10.02	Windows	SMB	SMB	Yes
	Linux	SSH	SSH	No (for password-less SSH)
Older than 10.00	Linux	SSH	INET	No

Note: For upgrade through SMB or SSH, the upgrade process prompts for credentials on all Windows clients and on Linux clients that don't have password-less SSH configured.

For DP clients that upgrade over INET by default, you can force either SMB (for Windows clients) or SSH (for Linux clients) communication by setting the `omnirc` variable **OB2RESTRICTUPGRADEOVERINET** to **1** on the installation server.

Remote upgrade on Linux client systems with /tmp directory

You can perform remote upgrading of a client having `/tmp` directory with `noexec` mounted. To remotely upgrade the Linux client system, replace the INET binary on that system. Raise a service request with Micro Focus support for the modified INET binary of the required client version.

You must apply this modified INET binary provided as a hotfix on the system by setting the omnirc variable `OB2NOEXEC=1` on the Installation Server and then proceed with the upgrade.

Upgrade clients manually

As a part of post upgrade step the self-signed certificate and keys are created.

Later as a part post upgrade or install step, the following command is executed on the client to configure Cell Manager certificate on the client to make Cell Manager to access the client.

```
omnicc -secure_comm -configure_peer {Hostname1 [HostName2 ...]} [-accept_host]
```

The user is prompted for thumbprint verification, after the user accepts the request, the Cell Manager certificate and thumbprint is configured. The import happens from CLI or GUI.

As part of import, the thumbprint of the client is displayed to the user. Once the user accepts the thumbprint, the client certificate and thumbprint is configured on the Cell Manager.

For cluster clients same logic applies and when importing, the appropriate details are configured.

If you upgrade Data Protector on client systems that are part of a cluster, or cluster based integrations, such as Exchange DAG and MS SQL high availability, the virtual entity (“Virtual Host” client type or cluster) will not show upgraded Data Protector

version, instead it still shows the older Data Protector version; you must re-import the virtual entity to the Cell Manager for it to show upgraded version.

Local upgrade on Linux machines with /tmp directory

If /tmp directory is mounted with noexec, local upgrade is supported. To locally upgrade on a Linux client system mounted with noexec on `/tmp` directory, set the global variable `OB2NOEXEC=1` on the system.

MOM clients

MOM upgrade

When MOM server is upgraded, self-signed certificates are generated for the MOM server, all the clients and client Cell Manager are put into exception configuration. So the MOM setup continues to work. If MOM GUI is in separate host which is not part of MOM cell manager, and if it is not yet upgraded, then the MOM GUI host needs to be added to the exception list by executing following command on the mom server host.

```
omnicc -secure_comm -configure_for_gui {Hostname1 [HostName2 ...] | -all_peers}
```

After the MOM GUI is also upgraded, then both MOM GUI and MOM server hosts needs to be configured for secure communication of each other by using the following command:

```
omnicc -secure_comm -configure_peer {Hostname1 [HostName2 ...]} [-accept_host]
```

Once the client Cell Managers are upgraded, configure certificates of client Cell Manager and MOM server on each others side.

New MOM setup

For new MOM setup, MOM GUI client and MOM server needs to be mutually configured with certificates of each other.

Moving clients between Cell Manager of the MOM

Before moving a client from old Cell Manager to new Cell Manager, run the following command on the client to configure the certificate of the new Cell Manager:

```
omnicc -secure_comm -configure_peer {Hostname1 [HostName2 ...]} [-accept_host]
```

During this the older Cell Manager certificate is removed automatically.

Cluster setups

Cluster aware client installation or upgrade through Installation Server

Push installation or upgrade automatically configures the Cell Manager certificate on the client and client certificate on the Cell Manager.

All the nodes are upgraded and configured before importing or updating the virtual server.

Cluster aware client installation or upgrade manually on the client side

Configure all the nodes as normal clients and import the virtual server as **virtual host** type.

Before importing the client nodes, the Cell Manager certificate needs to be configured on each node using the following command if not done already during installation:

```
omnicc -secure_comm -configure_peer <cell manager>
```

When importing individual nodes, the certificate is displayed for user confirmation. Before importing the virtual server name, all the nodes needs to be imported as normal clients.

MS clusters

On each client node, the Cell Manager certificate should be configured. This should happen automatically as part of installation, when the cell server is specified during the installation. Or else this can be done manually using the following `omnicc` command:

```
omnicc -secure_comm -configure_peer <cell manager>
```

On the Cell Manager, each node certificate along with `omnicc` command needs to be configured by using the following command:

```
omnicc -secure_comm -configure_peer <node1 node2 ...>
```

OpenVMS or MacOS clients

Upgrade OpenVMS client

Follow the below steps when upgrading an OpenVMS client:

1. Remove the existing Data Protector client by running `PRODUCT REMOVE DP`
2. Install the new Data Protector client by running `PRODUCT INSTALL DP`

> **Note** After removing the product and installing it again, INET will use port 5565 instead of port 5555.

Similar to ECC in the past Secure Communication (SSC) is not supported for the OpenVMS and MacOS client platforms. Only MacOS client can be push installed and for that `bmsetup` process is changed accordingly and does not have any additional steps.

New client import

Use one of the following commands to import OpenVMS or MacOS clients from the Cell Manager:

```
omnicc -import_mac_host HostName [-virtual]
```

```
omnicc -import_openvms_host HostName [-virtual]
```

Existing clients

When the Cell Manager is upgraded, an exception is configured for all clients. MacOS or OpenVMS clients do not support secure communication and therefore their exception is maintained forever. No additional steps are required.

Upgrade Data Protector in cluster-mode

To upgrade Data Protector in cluster-mode, perform the steps listed in the following sections.

Upgrade the Cell Manager configured in Serviceguard

During an upgrade procedure, only the database is upgraded, and the previous version of the product is removed. The latest version of Data Protector is installed with the default selection of agents, and other agents are removed. To obtain a configuration equivalent to the state before the upgrade, you must manually select any other agents during the upgrade procedure or reinstall them afterwards on each physical node.

The upgrade procedure from previous versions of Data Protector to the latest version of Data Protector consists of upgrading the primary and secondary nodes. Follow the instructions in the order they are presented in the sections below.

Prerequisites

- The Data Protector services on the Serviceguard secondary node(s) should not be running.

  This ensures the upgrade uses the IDB exported during the upgrade of the primary node and avoids an additional IDB export.

- Cluster management IP package for Data Protector has to be started/stopped whenever the ob2cl package is started/stopped, if the cluster management IP package for Data Protector is configured as a separate package other than ob2cl package.

Primary node

Log on to the primary node and perform the procedure:

1. Stop the old Data Protector package by running the cmhaltpkg *PackageName* command (where *PackageName* is the name of the cluster package). For example:

   ```
   cmhaltpkg ob2cl
   ```

2. Activate the volume group.

   - Linux
     1. Add tag using the command vgchange --addtag *hostname*

        Where *hostname* is the hostname of the primary node.

        For example: vgchange --addtag clusterserver1

     2. Activate volume group using the command vgchange -a y *VGName*

        Where *VGName* is name of the volume group.

        For example: vgchange –a y /dev/vg_ob2cm

3. Mount the logical volume to the shared disk:

   ```
   mount LVPathSharedDisk
   ```

   The LVPath parameter is the path name of the logical volume, and SharedDisk is the mount point or a shared directory. For example:

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

4. Start the Data Protector services:

   ```
   omnisv -start
   ```

5. Upgrade the Cell Manager. Ensure that the ob2cl package is stopped and VIP package is up and running.

6. Stop the Data Protector services:

   ```
   omnisv -stop
   ```

7. Dismount the shared disk:

   ```
   umount SharedDisk
   ```

   For example:

   ```
   umount /omni_shared
   ```

8. Deactivate the volume group.

   - Linux
     1. Deactivate the volume group using the command:
        vgchange -a n *VGName*

        Where *VGName* is name of the volume group.

        For example: vgchange -a n /dev/vg_ob2cm

2. Delete the tag using the command vgchange --deltag *hostname*

   Where *hostname* is the hostname of the primary node.

   For example: vgchange --deltag clusterserver1

Secondary node

Log on to the secondary node and perform the procedure:

1. Activate the volume group.
   - Linux
     1. Add tag using the command vgchange --addtag *hostname*

        Where *hostname* is the hostname of the secondary node.

        For example: vgchange --addtag clusterserver2

     2. Activate volume group using the command vgchange -a y *VGName*

        Where *VGName* is name of the volume group.

        For example: vgchange –a y /dev/vg_ob2cm
2. Mount the logical volume to the shared disk:

   mount LVPathSharedDisk
3. Upgrade the Cell Manager.
4. Rename the csfailover.sh and mafailover.ksh startup scripts in the /etc/opt/omni/server/sg directory (for example, to csfailover_DP70.sh and mafailover_DP70.ksh) and copy the new csfailover.sh and the mafailover.ksh scripts from the /opt/omni/newconfig/etc/opt/omni/server/sg directory to the /etc/opt/omni/server/sg directory.

   If you customized your old startup scripts, reimplement the changes also in the new startup scripts.
5. Stop the Data Protector services:

   omnisv -stop
6. Dismount the shared disk:

   umount SharedDisk
7. Deactivate the volume group.
   - Linux
     1. Deactivate the volume group using the command:
        vgchange -a n *VGName*

        Where *VGName* is name of the volume group.

        For example: vgchange -a n /dev/vg_ob2cm
     2. Delete the tag using the command vgchange --deltag *hostname*

        Where *hostname* is the hostname of the primary node.

        For example: vgchange --deltag clusterserver2

Primary node

Log on to the primary node again and perform the procedure:

1. Start the Data Protector package:

   cmrunpkg *PackageName*

   For example: cmrunpkg ob2cl
2. Configure the Cell Manager. Make sure not to be positioned in the /etc/opt/omni or /var/opt/omni directory or their subdirectories when running the script. Make also sure to have no mounted subdirectories in the /etc/opt/omni or /var/opt/omni . Execute:

   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade

   At the end of omniforsg.ksh -primary –upgrade command execution, notice the set of commands to be executed to create LDAP user, migrate schedules, and create java user. Run them on the primary node after the secondary node is upgraded and cluster services are up.
3. Stop the Data Protector package:

   cmhaltpkg *PackageName*

   For example: cmhaltpkg ob2cl

Secondary node

Log on to the secondary node again and perform the procedure:

1. Start the Data Protector package:

   cmrunpkg *PackageName*

   For example: cmrunpkg ob2cl

2. Configure the Cell Manager. Make sure not to be positioned in the /etc/opt/omni or /var/opt/omni directory or their subdirectories when running the script. Ensure no subdirectories are mounted in the /etc/opt/omni or /var/opt/omni directory. Execute:

   /opt/omni/sbin/install/omniforsg.ksh -secondary -upgrade

   At the end of omniforsg.ksh -primary –upgrade command execution, notice the set of commands to be executed to create LDAP user, migrate schedules, and create java user. Run them on the primary node after the cluster services are up.

3. Stop the Data Protector package:

   cmhaltpkg *PackageName*

   For example: cmhaltpkg ob2cl

Primary node

Log on to the primary node once again and perform the procedure:

1. Start the Data Protector package:

   cmrunpkg *PackageName*

   For example: cmrunpkg ob2cl

   Make sure that the package switching and switching for nodes options are enabled.

2. Execute the commands which were noticed at the end of secondary node upgrade.

Note All requests coming from the Cell Managers are logged in the /var/opt/omni/log/inet.log file on the Data Protector clients. To prevent unnecessary log entries, secure the clients.

Upgrade the Cell Manager configured on Microsoft Cluster Server

Upgrade of the Cell Manager on Microsoft Cluster Server (MSCS) is performed locally, from the Windows installation package.

Prerequisites

- The upgrade option is supported only if the previously installed Data Protector software is the Cell Manager installed in cluster-aware mode. If a system in the cluster has the Data Protector software installed as non-cluster-aware, you must uninstall it prior to starting the setup.

Upgrade procedure

To perform the upgrade, proceed as follows:

1. Copy the downloaded installation package on a Windows system, and extract the files to a temporary location. Run the setup.exe file available in \Windows \x8664 location. It is recommended to start the setup on the currently active virtual server node.

   Setup automatically detects the previous version of the product and prompts you to upgrade.

   Click **Next** to continue.

2. Data Protector automatically selects the components that were installed.

   Click **Next**.

3. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup registers all necessary Data Protector executables. By default, the **Initially, allow newly registered Data Protector executables to open inbound ports as needed** option is selected. If you do not want to enable Data Protector to open ports at the moment, deselect the option. For proper functioning of Data Protector with previous version of the clients, the Data Protector rules in Windows firewall must be enabled. Rules for the OmniInet Service executable, Application Server port and Internal Database Service port will always be enabled, regardless of the choice.

   Click **Next**.

4. Optionally, change the user account used by the Data Protector IDB and HTTPS Application Server and the ports used by these services.

   Click **Next**.

5. The component selection summary list is displayed. Click **Install** to perform the upgrade.

   A Command Prompt window opens and the software begins the IDB migration to the new database format by exporting the older IDB.

   This Command Prompt window remains open during the export of the older IDB and displays status messages. The IDB export may take several minutes to complete.

   As the upgrade proceeds, an additional Command Prompt window opens to display the status of the import of the IDB configuration information and data into Data Protector.

   Upgrades from 8.00 and later:

   The IDB updates automatically; no Command Prompt windows are opened.

   Note that after the upgrade, every node has the same component set.

6. The **Installation status** page is displayed. Click **Next**.
7. To start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

   If the English Documentation (Guides, Help) component has been upgraded or newly installed, to view the Data Protector Product Announcements, Software Notes, and References immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

   Click **Finish**.

Note If you are upgrading cluster-aware clients, first upgrade every cluster node separately, and then re-import the virtual server. The remote upgrade is not supported.

Upgrading the Cell Manager configured in Symantec Veritas Cluster Server

During an upgrade procedure, only the database is upgraded, and the previous version of the product is removed. Data Protector is installed with the default selection of agents, and other agents are removed. To obtain a configuration equivalent to the state before the upgrade, you must manually select any other agents during the upgrade procedure or reinstall them afterwards on each physical node.

Prerequisites

The Data Protector services on the Symantec Veritas Cluster Server secondary node(s) should not be running.

The upgrade procedure from previous versions of Data Protector consists of upgrading the primary and secondary nodes. Follow the instructions in the order they are presented in the sections below.

Primary node

Log on to the primary node and perform the following steps:

1. Take the Data Protector application resource offline.
2. Disable the Data Protector application resource.
3. Start the Data Protector services:

   ```
   omnisv -start
   ```

4. Upgrade the Cell Manager.
5. If you have customized the monitoring script used by the Data Protector Application resource, re-implement the changes provided by the newly installed /opt/omni/sbin/vcsfailover.ksh script in your customized script.
6. Stop the Data Protector services:

   ```
   omnisv -stop
   ```

Secondary node

Log on to the secondary node and perform the following steps:

1. Switch over the Data Protector service group to the secondary node.
2. Upgrade the Cell Manager.
3. If you have customized the monitoring script used by Data Protector Application resource, re-implement the changes provided by the newly installed /opt/omni/sbin/vcsfailover.ksh script in your customized script.
4. Stop the Data Protector services:

   ```
   omnisv -stop
   ```

Primary node

Log on to the primary node again and perform the following steps:

1. Switch over the Data Protector service group to the primary node.
2. Enable the Data Protector application resource.
3. Bring the Data Protector application resource online.
4. Configure the Cell Manager. Ensure that the script is not executed from /etc/opt/omni or /var/opt/omni directory or their sub-directories. Also, ensure that sub-directories are not mounted in the /etc/opt/omni or /var/opt/omni directory. Execute the following command:

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
   ```

Secondary node

Log on to the secondary node again and perform the following steps:

1. Switch over the Data Protector service group to the secondary node.
2. Configure the Cell Manager. Ensure that the script is not executed from /etc/opt/omni or /var/opt/omni directory or their sub-directories. Also, ensure that sub-directories are not mounted in the /etc/opt/omni or /var/opt/omni directory. Execute the following command:

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary -upgrade
   ```

Primary node

Log on to the primary node once again and perform the following steps:

1. Switch over the Data Protector service group to the primary node.
2. If you have the Installation Server in the same service group as the Cell Manager, import the Installation Server virtual hostname:

   ```
   omnicc -import_is VirtualHostname
   ```

Note All requests coming from the Cell Managers are logged in the /var/opt/omni/log/inet.log file on the Data Protector clients. To prevent unnecessary log entries, secure the clients. See Security considerations for information on how to secure a cell.

Upgrade from Single Server Edition

You can perform the upgrade from one of the following:

- From earlier versions of the Single Server Edition (SSE) to Data Protector 2020.08 Single Server Edition. For details, see Upgrading from earlier versions of SSE to Data Protector 2020.08 SSE.
- From Data Protector 2020.08 Single Server Edition to Data Protector 2020.08. For details, see Upgrading from Data Protector 2020.08 SSE to Data Protector 2020.08

Upgrade from earlier versions of SSE to Data Protector 2020.08 SSE

The upgrade procedure from earlier versions of SSE to Data Protector 2020.08 SSE is the same as the upgrade procedure from earlier versions of Data Protector to Data Protector 2020.08.

Upgrade from Data Protector 2020.08 SSE to Data Protector 2020.08

You need to have a license to perform the upgrade from Data Protector 2020.08 Single Server Edition to Data Protector 2020.08.

The upgrade from Data Protector 2020.08 Single Server Edition to Data Protector 2020.08 is offered for two possible scenarios:

- If you have the Data Protector Single Server Edition installed on one system (Cell Manager) only. See Upgrade the Cell Manager.
- If you have the Data Protector Single Server Edition installed on multiple systems and you want to merge these cells. See Upgrade from multiple installations.

Note To upgrade from a previous version of the Single Server Edition to a fullData Protector installation, first upgrade your Single Server Edition to the full installation of the same version level.

Upgrade the Cell Manager

To upgrade the Single Server Edition Cell Manager, do the following:

1. Remove the Single Server Edition license:

   Windows systems:

   del Data_Protector_program_data\Config\server\Cell\lic.dat

   Linux systems:

   rm /etc/opt/omni/server/cell/lic.dat

2. Start the Data Protector GUI and add a permanent password.

Upgrade from multiple installations

To upgrade the Data Protector Single Server Edition installed on multiple systems, proceed as follows:

1. Select one of the existing Single Server Edition systems to be the new Cell Manager.
2. Upgrade the selected Cell Manager by performing the following:
   a. Remove the Single Server Edition license:

      del Data_Protector_program_data\Config\server\Cell\lic.dat (on Windows systems) or

      rm /etc/opt/omni/server/cell/lic.dat (on Linux systems)

   b. Start the Data Protector GUI and add a permanent password.
3. Import the other Single Server Edition systems into the newly created Cell Manager system as clients using the GUI.
4. Uninstall the Data Protector Single Server Edition from the other systems.
5. Import the media to the new Cell Manager.

   For information about importing media, see the Data Protector Help index: “importing, media”.

集成

本节介绍如何配置、备份和还原以下集成:

供应商或类型	应用程序
IBM	• DB2 UDB 集成 • Informix Server 集成 • Lotus Notes/Domino Server 集成
Micro Focus	• 业务价值仪表板集成 • Operations Orchestration 集成
Microsoft	• Microsoft 365 Exchange 在线集成 • 基于 Microsoft SharePoint Server VSS 的解决方案 • Microsoft Exchange Server 集成 • Microsoft SharePoint Server 集成 • Microsoft SQL Server 集成 • Microsoft Volume Shadow Copy Service
NetApp	• NDMP 集成 • NetApp ONTAP C 模式 • NetApp SnapManager 解决方案
Oracle	• MySQL 集成 • Oracle Server 集成
PostgreSQL	• PostgreSQL 集成
SAP	• SAP HANA 集成 • SAP MaxDB 集成 • SAP R/3 集成
Sybase	• Sybase IQ 集成 • Sybase Server 集成
虚拟化	• 适用于 Microsoft Hyper-V 的虚拟环境集成 • 适用于 VMware 的虚拟环境集成 • 适用于 H3C CAS 的虚拟环境集成
零宕机时间备份	• Microsoft Exchange Server ZDB 集成 • 基于 Microsoft SharePoint Server VSS 的解决方案 - ZDB • Microsoft SQL Server ZDB 集成 • Oracle Server ZDB 集成 • SAP R/3 ZDB 集成 • 适用于 VMware 的虚拟环境 ZDB 集成

Amazon EC2 集成

Data Protector 提供了基于脚本的解决方案，以使用 EC2 备份和恢复 包执行 Amazon Elastic Compute Cloud (EC2) 快照的备份和还原。您可以将此包与 Data Protector 2020.08 及更高版本一起使用。

本主题介绍了执行 EC2 快照的备份和还原的步骤:

1. 设置所需的 EC2 实例。
2. 下载并配置 EC2 备份脚本。
3. 备份 EC2 快照。
4. 还原 EC2 快照。

设置所需的 EC2 实例

按照以下步骤在 AWS 中将 Linux EC2 实例设置为备份主机和 Windows EC2 实例，以托管用于管理 Linux 实例的 Data Protector GUI:

1. 设置 Linux EC2 实例。确保服务器上的 Python 版本为 3.4.2 或更高版本。
   a. 创建适当大小的装载点或文件夹以存储快照信息。例如 EC2Backup 。
   b. 安装 AWSCLI:
      curl "https://s3.amazonaws.com/aws-cli/awscli-bundle.zip" -o "awscli-bundle.zip"
      unzip awscli-bundle.zip
      ./awscli-bundle/install -b /usr/local
2. 检查 aws 命令的版本和状态，确保您的 Python 版本正确。
   aws --version
3. 确保在 shell 中定义了 aws 和 python 命令的路径。
4. 在 AWS 中为您的区域配置配置文件:
   i. 为配置和凭据文件创建 AWS 路径。
      mkdir ~/.aws
   ii. 创建名为“凭据” 的文件并提供相关配置文件的访问权和密钥。

      [root@testip.aws]# cat credentials

      [User1]
      aws_access_key_id=XXXXXXXXXXXXXXXXXXXXXYEHA
      aws_secret_access_key=XXxxxXxxxxXXxxxxxxxXXXXXXxxxxxxxxxxxxxxxxxbq

      [User2]
      aws_access_key_id=XXXXXXXXXXXXXXXXXXXXXDPQ
      aws_secret_access_key=XXxxxXxxxxXXxxxxxxxXXXXXXxxxxxxxxxxxxxxxxnyR
      [root@testip.aws]#

   iii. 配置您的区域。
      [root@testip .aws]# aws configure --profile User1
      AWS Access Key ID [****************YEHA]:
      AWS Secret Access Key [****************vJbq]:
      Default region name [None]: ap-south-1
      Default output format [None]: text
      [root@testip.aws]# aws configure --profile User2
      AWS Access Key ID [****************ADPQ]:
      AWS Secret Access Key [****************4nyR]:
      Default region name [None]: us-west-2
      Default output format [None]: text
   iv. 验证配置文件内容。
      [root@testip.aws]# cat config
      [profile User1]
      output = text
      region = ap-south-1
      [profile User2]
      output = text
      region = us-west-2
      [root@testip.aws]#
   v. 使用以下命令在 Linux 客户机上安装 jq 。
      $ sudo wget -O jq https://github.com/stedolan/jq/releases/download/jq-1.6/jq-linux64
      $ sudo chmod +x ./jq
      $ sudo cp jq /usr/bin
5. 在此实例上安装 Data Protector Cell Manager 包，并照常完成所有必需的配置步骤。如果已经将其他主机配置为充当 Cell Manager，则不需要此步骤。
6. 在 Cell Manager 所在的 AWS 区域中设置 Windows EC2 实例。将此 Windows EC2 实例配置为 Linux Cell Manager 的 GUI。如果已配置其他主机来托管 Data Protector GUI，则无需执行此步骤。

下载并配置 EC2 脚本

1. 从 Micro Focus Marketplace 下载 EC2 备份和恢复 包。该包包括以下内容:
   - EC2_snapshot_backup.sh
   - EC2_post_backup_cleanup.sh
   - EC2_snapshot_restore.sh
2. 登录 EC2 快照备份主机，并将下载的脚本解压缩到以下位置:
   /opt/omni/lbin

3. 设置脚本的文件许可:
   cd /opt/omni/lbin | chmod 755 EC2*
4. 配置脚本。在 vi 或任何文件编辑器中打开每个脚本，并基于带有 # change/check 标记的环境指定变量值。

备份 EC2 快照

创建设备

按照以下步骤在 Data Protector 中创建 AWS S3 设备以存储备份:

1. 打开 DP GUI 并转到“设备和介质”上下文。
2. 右键单击“设备”，然后单击“添加设备”。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”作为“设备类型”，然后将“接口类型”设置为“云 (Amazon S3 API 兼容目标)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“S3 目标类型”。
   - 如果要创建指向 Amazon S3 的设备，请选择“AWS S3”。
   - 如果要创建指向内部部署目标的设备 (Amazon S3 API 兼容)，请选择“Ceph/Scality”。
7. 指定网关。
   - **AWS S3**: 选择散列存储可用的“S3区域”，或要创建散列存储的区域。
   - **Ceph/Scality**: 对于内部部署目标，输入网关 URL。
8. 指定“访问密钥 ID”和“密码访问密钥”信息。
9. 单击“选择/创建散列存储”以获取已创建的所有散列存储列表并显示它们。此时将显示“选择散列存储”窗口。

   选择现有散列存储或新建散列存储以上载数据。

10. 单击“添加”以添加网关。
11. 单击“检查”以验证网关是否已连接到云 (Amazon S3/Ceph/Scality)。如果连接成功，则状态显示为“正常”。
12. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

创建备份规范

要创建备份规范，请完成以下步骤:

1. 在 Data Protector UI 中，选择“备份”上下文。
2. 在“范围窗格”中，展开“备份规范”，右键单击“文件系统”，然后单击“添加备份”。
3. 如果您的 EC2 备份主机不同于 Cell Manager，请选择客户机，然后选择您在设置 Linux EC2 实例步骤 (EC2Backup) 中创建的装载点或文件夹。
4. 单击“下一步” 并选择创建的用于存储 EC2 备份的 S3 设备。
5. 在“选项”选项卡中，转到“文件系统选项”，然后单击“高级”。
6. 将 **pre-exec** 脚本指定为 **EC2_snapshot_backup**，将 **Post-exec** 脚本指定为 **EC2_post_backup_cleanup**。从“在客户机上” 下拉列表中选择客户机。

   > 注意: 确保提供正确的脚本名称并选择正确的客户机。

7. 设置“保护”，单击“下一步”，然后选择“保存并计划”。指定备份规范名称，然后按照调度程序计划备份。
   创建备份规范后，它会在左窗格的“文件系统”类别下列出。它会在计划的时间自动运行备份。如果要手动启动备份，请右键单击备份规范，然后单击“启动备份”。

还原 EC2 快照

按照以下步骤还原所需的 EC2 快照:

1. 在 Data Protector UI 中，选择“还原”上下文。
2. 右键单击“文件系统” 下的所需对象，然后单击“属性”。 选择要还原的快照 ID。
3. 转到“选项” 选项卡。指定还原脚本名称 (EC2_snapshot_restore.sh)，然后单击“还原”。
4. 验证实例状态，并测试从时间点备份还原的数据。

业务价值仪表板集成

业务价值仪表板 (BVD) 可以如实地呈现您的数据。使用 BVD 可以创建灵活的自定义仪表板，从而以详实且吸引人的方式对 OMi 和其他来源的信息进行可视化。您可以随时随地从任何设备访问 BVD 仪表板。您可以加入自己的图形、添加颜色来标识状态以及接收实时更新，从而随时了解受 IT 环境驱动的价值。有关 BVD 与其他产品集成的详细信息，请参阅 https://docs.microfocus.com/itom/Business_Value_Dashboard:latest/Home 下提供的最新 BVD 文档。

集成 BVD

要将 Data Protector 与 BVD 集成，请执行以下步骤：

1. 从 ITOM Marketplace 下载 BVD 脚本 zip 包。如果您有任何问题，请联系客户支持。
   - 将 zip 内容提取并保存到本地文件夹。
2. 下载以下 perl 模块并将其放在 Data Protector perl 库下。在 Windows 上，默认路径为 C:\Program Files\OmniBack\lib\perl ；在 Linux 上，为 /opt/omni/lib/perl 。
   - WWW::Mechanize，网址为 http://cpansearch.perl.org/src/PETDANCE/WWW-Mechanize-1.60/lib/WWW/Mechanize.pm
   - Math::Round，网址为 http://cpansearch.perl.org/src/GROMMEL/Math-Round-0.07/Round.pm
   - HTML::Form，网址为 http://cpansearch.perl.org/src/GAAS/HTML-Form-6.03/lib/HTML/Form.pm
   - REST:Client.pm，网址为 https://github.com/hggh/librest-client-perl/blob/master/lib/REST/Client.pm
3. 从包中复制 Crypt 文件夹，并将其放在 Data Protector 的 Perl 库目录下。如果目标服务器是 Linux 计算机，请在 /opt/omni/lib64 目录下创建软链接，如下所示:
   ln -s libomnissl.so.1.0.0 libssl.so.1.0.0
   ln -s libomnicrypto.so.1.0.0 libcrypto.so.1.0.0
4. 将 plink.exe 下载到本地目录。
   plink.exe 是 putty 后端的开源命令行接口。如果您的环境同时包含 Windows 和 UNIX/Linux Cell Manager 客户机，请使用 Windows 客户机上的 plink.exe 创建与 UNIX/Linux 客户机的 SSH 连接。
   使用 plink.exe 的保存目录更新 PATH 环境变量
5. 启动 BVD 仪表板。请参阅登录 BVD。
6. 上载 Data Protector 仪表板。请参阅将仪表板上载到 BVD。
7. 在 zip 内容所提取到的文件夹下，更改 DP.pl 文件中的以下变量值:
   - $bvd_dir - BVD 脚本的保存位置
   - $bvd_url - BVD 服务器的路径
   - $bvd_api_key - BVD 服务器的 API 密钥
   - $bvd_machine_IP - BVD 服务器的 IP 地址
   - $user - BVD 用户名
   - $pwd - BVD 用户密码
8. 。在 $bvd_dir 路径下，更新以下脚本中的 $bvd_dir 变量值:
   - Windows：GetDPOverview.ps1 和 GetCellCount.ps1
   - UNIX：GetDPOverview.sh 和 GetCellCount.sh
9. 使用基于您环境的值更新 $bvd_dir/DP 文件夹下的 sitelist 文件:
   - 对于 Windows Cell Manager，添加以下内容: *<sitenameA>*:*<FQDN>*:*<Username>*:*<Password>*:Windows
   - 对于 Linux Cell Manager，添加以下内容: *<sitenameA>*:*<hostname>*:*<Username>*:*<Password>*
10. 您可以配置无密码访问。
    - 使用 PowerShell 向运行脚本的用户授予对要查询的其他 Windows 主机的访问权限。
    - 将 plink.exe 与已保存的 putty 会话一起使用，并使用与另一个名为 Pageant.exe 的程序一起保存的密钥。
    - 将用户的公钥添加到目标系统的 authorized_keys 文件中。
    - 设置无密码访问后，相应地修改 GetCellCount.sh 和 GetCellCount.ps1 脚本
11. 运行以下脚本:
    - Windows： GetDPOverview.ps1
    - UNIX： GetDPOverview.sh
12. 如果您的环境中同时包含 Windows 和 UNIX/Linux Cell Manager，请在 Windows 主机上运行 GetDPOverview.ps1 。如果您的环境仅包含 UNIX/Linux Cell Manager，则在 UNIX/Linux 主机上运行 GetDPOverview.sh 。您可以将 cron 作业或调度程序作业设置为按指定间隔运行此脚本，以持续更新仪表板。
13. 如果脚本上载到 BVD 的预配置数据不符合您的要求，请参阅将自有数据发送到仪表板。

您可以随时启动 BVD 仪表板来检查 Data Protector 中最新更新的值。

登录 BVD

1. 确保在计划为 BVD 创建仪表板的系统上已安装 Visio。
2. 登录 BVD:
   - 访问 BVD，URL 如下: http://*<BVD_server>*:*<port>*/login/
     其中：
     - *<BVD_server>* 是 BVD 服务器的完全限定域名 (FQDN)
     - *<port>* 是配置期间为 BVD 接收方分配的端口。默认值：12224 (HTTP) 或 12225 (HTTPS)
       输入您的登录名和密码。
   - *推荐*。打开“个人用户设置”>“我的帐户”菜单并指定一个新密码。
3. 在 BVD 中，打开“管理”>“系统设置”，然后复制“API 密钥”。
   - 此密钥标识您的 BVD 实例，必须包含在数据发送方所提交的数据中。
   - “系统设置”页仅供具有管理员权限的用户使用。
   - 此密钥为可选项，仅在设置脚本包时使用一次。
4. 导航或浏览到所需的仪表板。

将自有数据发送到仪表板

创建 BVD 仪表板之前，请考虑要发送和显示的数据。BVD 应该以 JavaScript 对象表示法 (JSON) 格式将您的数据作为 HTTP post 请求接收。建议您的 JSON 输入包含由名称-值对构成的平面数据。如果必须发送嵌套数据，BVD 会自动展平数据。此外，您也可以采用数组形式发送 JSON

数据。这样，您便可以在单个 Web 服务调用中发送多个数据对象。

URL 应如下所示: http(s)://<BVD 服务器>:<端口>/api/submit/<API 密钥>/dims/<*dims*>

其中：

1. <*BVD_server*> 是 BVD 服务器的完全限定域名 (FQDN)
2. <*port*> 是配置期间为 BVD 接收方所分配的端口。默认值：12224 (HTTP) 或 12225 (HTTPS)。
3. <*API_key*> 标识您的 BVD 实例。您可以在“管理”>“系统设置”中找到 API 密钥。
4. <*dims*>是 JSON 名称-值对中的名称。选择并组合用于唯一标识数据的 dims。

将仪表板上载到 BVD

1. 在 BVD 中，打开“管理”>“管理仪表板”并单击“+ 添加”，选择 $bvd_dir 路径中的 **DataProtector.svg** 文件，然后单击“上载仪表板”将其导入。BVD 仪表板编辑器将打开，并显示已上载的仪表板。BVD 提供多个仪表板自定义选项。例如，您可以从 $bvd_dir 路径导入 **AMSCM.svg** 文件，并将其链接到 DataProtector.svg.Optional 中的 AMS 标签: 有关进一步自定义或创建您自己的仪表板的信息，请参阅在 Visio 中设计自有仪表板。
2. 您可以更改仪表板本身的属性 (例如，与仪表板关联的 SVG 文件、标题或背景颜色)。
   - 要编辑某个小部件的属性，请单击该小部件。单击“数据通道”字段时，将打开一个下拉列表，其中显示 BVD 已接收的所有数据流。
   - 选择数据通道作为 omi、mdb、Live、BACKUP_OVERVIEW、SPARKLINE。
   - 在“数据字段”中选择以下内容:
     1. TOTAL_CLIENTS
     2. TODAY_DATE
     3. TOTAL_DATASIZE
     4. TOTAL_RUNNINGOBJECTS (总对象计数)
     5. TOTAL_PASSED
     6. TOTAL_FAILED
     7. TOTAL_PENDING
     8. PASSED (以百分比表示)
     9. FAILED (以百分比表示)
     10. PENDING (以百分比表示)
   - 根据需要调整其他所有属性，然后单击“保存”。
3. 默认情况下，新导入的仪表板会显示在“仪表板”菜单中。要显示或隐藏仪表板，请单击“在菜单中显示/隐藏”。
4. 要查看仪表板，请在“仪表板”菜单中将其选中。通过数据渠道发送数据时，查看仪表板的更新情况。

在 Visio 中设计自有仪表板

1. 在 Visio 中新建一个绘图。将 BVD 形状拖放到绘图中，然后根据需要进行排列和修改。建议不要在 Visio 本身中更改 BVD 形状的形状数据。可通过 BVD 调整已上载的仪表板中的小部件，这样操作更方便、更快捷 (“管理”>“管理仪表板”)。
2. 将绘图另存为 SVG 文件，同时确保选择以下 Visio 设置:
   - **另存类型:** 可扩展矢量图像 (*.svg)
   - **选择:** 将 Visio 数据包括在文件中
3. 按 **Ctrl+A** 可以选择绘图中的所有内容。这可确保导出整个绘图，而不仅仅是当前选定的元素。另外，如果您已安装 BVD Visio 插件，可以单击“仪表板”功能区中的“导出仪表板”。

DB2 UDB 集成

This feature is available in the Premium Edition

Data Protector 与 IBM DB2 Universal Database Server (“DB2 服务器”) 集成，可以联机和脱机备份 DB2 数据库对象。

Data Protector 提供以下类型的交互式备份和安排的备份：

备份类型	描述
完整	备份完整的 DB2 对象。
增量	备份自上次完整备份以来的更改。
差量	备份自任何类型的上一次备份以来的更改。

基本备份单位是表空间。只能选择表空间或数据库 (DB2 对象) 进行备份。

还原数据库或表空间时，可以指定要执行的还原选项:

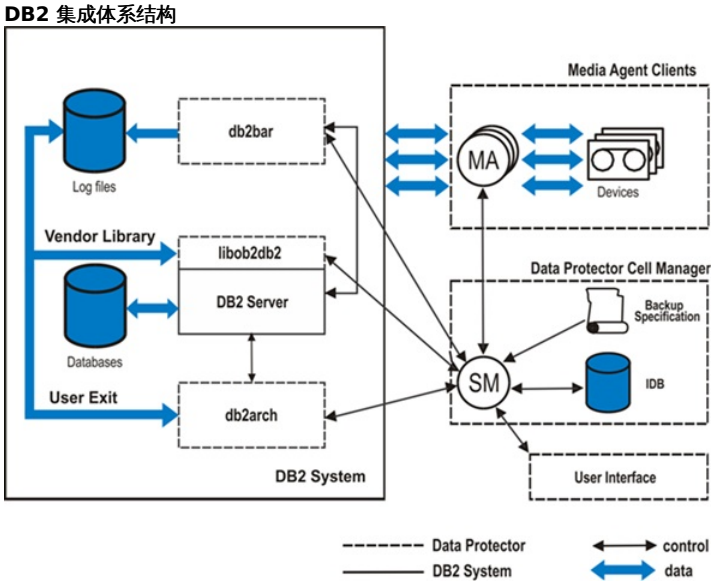
- 前滚恢复
- 版本恢复
- 还原到新数据库 (仅限数据库)
- 还原到另一个实例 (仅限数据库)
- 还原到另一个系统 (仅限数据库)
- 从增量或差量备份自动还原

脱机还原数据库，联机还原表空间。

集成概念

Data Protector 通过一组负责数据备份和还原的模块与 DB2 服务器集成。DB2 集成体系结构显示 Data Protector DB2 集成的体系结构。

DB2 集成体系结构



图例

图例	描述
SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
db2bar	Data Protector 模块，用于控制 DB2 服务器与 Data Protector 备份和还原之间的活动。
db2arch	当 DB2 日志存档方法 (logarchmeth1) 设置为“用户退出”时用于备份和还原 DB2 日志文件的程序
libob2db2	DB2 服务器调用的数据传输 (logarchmeth1 设置为“供应商”时的数据库备份和还原、日志存档/检索) 模块。
MA	Data Protector 常规介质代理。
备份规范	要备份的对象列表、备份设备和要使用的选项。
IDB	Data Protector 内部数据库。

DB2 服务器负责磁盘的读/写操作，而 Data Protector 则读取和写入设备并管理介质。

满足 DB2 UDB 的先决条件

以下是 DB2 UDB 集成的先决条件:

- 建议您将日志存档方法 (logarchmeth1) 设置为“供应商”，因为 IBM DB2 已从 DB2 版本 9.5 开始弃用“用户退出”选项。
- 如果现有数据库已将日志存档方法设置为“用户退出”并且要将其更改为“供应商”，则使用“用户退出”选项备份的日志的数据库恢复可通过使用以下步骤完成:
  a. 还原数据库 (不启用 Data Protector GUI 中的前滚恢复)。
  b. 使用活动日志目录中的“用户退出”程序还原备份的日志。
- 在使用自动前滚还原到 DB2 数据库之前，需在 omnirc 文件中设置环境变量:
  - 在 DB2 客户机上，在 omnirc 文件中设置以下环境变量:
    - OB2APPNAME = “source_Instance_name”
    - OB2BARHOSTNAME =”Source_client_name”
    - OB2APPDATABASE = “source_database_name”

    > **注意**这适用于使用“供应商”库的所有 DB2 日志备份，而对“用户退出”模式不是必需的。
    >
    > 在 omnirc 文件中，在前滚 DB2 数据库之后删除上述三种变量。这可确保在同一系统上运行的其他 DB2 实例在备份期间不受这些环境变量的影响。

  - 执行 DB2 前滚命令。
- 使用 DB2 版本 9.7 (Fix Pack 4) 及更高版本中的 omnirc 变量 OB2_DB2DEDUP 支持 DB2 重复数据删除优化。
- 确保已正确安装和配置 DB2 服务器。
- 确保已正确安装 Data Protector。

  要执行备份或还原的每个 DB2 服务器系统均必须安装 Data Protector DB2 Integration 和 Disk Agent 组件。

  在分区环境中，请确保在 DB2 数据库所在的所有物理节点上安装“DB2 集成”和“磁盘代理”组件。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 DB2 服务器系统与 Cell Manager 是否正常通信，请在 DB2 服务器系统上配置并运行 Data Protector 文件系统备份和还原。

群集感知客户机

如果您使用的是 Microsoft Windows Failover 群集，请将 omnirc 变量 OB2BARHOSTNAME 设置为群集节点和 Cell Manager 中的虚拟服务器名称。

OB2BARHOSTNAME =< virtual_server_name >

> **注意**OB2BARHOSTNAME 变量区分大小写。例如，"domain.com" 将解释为与 "DOMAIN.com" 不同的主机名，这会导致产生不同的备份对象。

- 确保 DB2 实例处于联机状态。
- 要启用 DB2 对象的联机备份，请按备份部分中所述设置 DB2 Logarchmeth1 (在分区环境中，在对象所驻留的每个节点上)。然后，重新启动数据库，使新参数生效并执行完整脱机数据库备份。
- 要启用 DB2 对象的增量或差量备份，请将 DB2 *trackmod* 参数设置为 ON:
  1. 运行：

     db2 update db cfg for db_name USING TRACKMOD ON

     在分区环境中，在 DB2 对象所在的每个节点上运行该命令。
  2. 重新启动数据库。
  3. 通过运行以下命令对非 Data Protector 介质执行完整脱机数据库备份:

     backup db db_name
- 要启用一个或多个 DB2 表空间 (不是整个数据库) 的脱机备份，请将 DB2 *logretain* 参数设置为 ON。

安装 IBM DB2 UDB 客户机

This feature is available in the Premium Edition

假设 DB2 服务器已启动并正在运行。为了能够备份 DB2 数据库，您需要在安装过程中选择 DB2 集成和磁盘代理组件。在物理分区的环境中，在数据库所驻留的每个物理节点 (系统) 上安装 DB2 集成和磁盘代理组件。

注意以 root 用户身份登录，以执行安装。

配置 DB2 UDB 集成

This feature is available in the Premium Edition

您需要配置 DB2 用户以及要备份或还原到的每个 DB2 实例。

分区环境

在物理分区的环境中，分别在每个物理节点上配置集成。

确保将 MaxBSession 全局选项设置为分区数据库节点数的至少两倍。

配置 DB2 用户

确保 DB2 用户具有执行 DB2 备份和还原的相应权限（SYSADM 、 SYSCTRL 或 SYSMAINT）。

将用户 root (仅限 UNIX) 和 DB2 用户添加到 Data Protector 和 DB2 admin 用户组。

在配置和还原过程中提供此用户。Data Protector 需要此用户来启动 Data Protector Inet Service (Windows) 或进程 (UNIX)。

配置 DB2 实例

向 Data Protector 提供 DB2 实例配置参数:

- DB2 用户
- DB2 用户密码
- DB2 实例主目录 (仅在分区环境中)

然后，Data Protector 在 Cell Manager 上创建 DB2 实例配置文件，并验证与实例的连接。

这些参数用于连接到 DB2 服务器系统以执行备份、还原和其他操作，例如列出备份对象。

要配置 DB2 实例，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“DB2 集成”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在客户机中，选择 DB2 服务器系统。

   在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，键入 DB2 实例名称。

   有关“用户和组/域”选项的信息，请按 **F1**。

   单击**确定**。
5. 单击“下一步”。此时将显示“配置 DB2”对话框。
6. 键入 DB2 用户的名称及其密码。必须按配置 DB2 用户中所述配置此用户。

   在分区环境中，选择“DB2 EEE”并指定 DB2 实例主目录的路径名。
7. 即会配置 DB2 实例。退出 GUI 或继续在步骤 6 创建备份规范。

使用 Data Protector CLI

请执行以下命令：

util_db2 -CONFIG DB2_instance username password [DB2 _instance_home]

参数描述

DB2_instance
username
password
DB2_instance_home

消息 *RETVAL*0 表示配置成功。

备份 DB2 UDB 集成

This feature is available in the Premium Edition

Data Protector DB2 集成提供三种备份类型和两种备份模式。

备份类型

备份类型	描述
完整	备份完整的 DB2 对象。
增量	备份自上次完整备份以来的更改。
差量	备份自任何类型的上一次备份以来的更改。

备份模式

备份模式	描述
联机	数据库处于联机状态。
脱机	数据库无法使用。

要配置 DB2 备份，请执行以下操作:

1. 使用 DB2 Database Backup 模板创建 DB2 对象的备份规范。
2. 要备份存档日志，请使用 Archived_Logs_Backup 模板为存档日志创建备份规范。指定一个与备份 DB2 对象所用设备不同的设备。否则，无法备份存档日志，因为设备被 DB2 对象的联机备份会话锁定。

   您可以使用“用户退出”选项或“供应商”选项备份存档日志。

   在创建备份规范之前，根据您选择的存档日志处理，执行以下任一命令:

   - **“用户退出”选项**: db2 update db cfg for <db_name> using LOGARCHMETH1 USEREXIT
   - **“供应商库”选项**: db2 update db cfg for <db_name> using LOGARCHMETH1 VENDOR:C:\Progra~1\OmniBack\lib\libob2db2.dll

> **重要提示:** 建议您将日志存档方法 (logarchmeth1) 设置为“供应商”，因为 IBM DB2 已从 DB2 版本 9.5 开始弃用“用户退出”选项。

> **重要说明**每次显示新的脱机重做日志时 (例如，在 DB2 对象的联机备份完成之后)，将自动备份存档日志。因此，在创建存档日志备份规范之前，请不要启动 DB2 对象的联机备份。
>
> 在创建新的存档日志备份规范之前，需删除所有旧备份规范，其中包括备份映像中的日志文件。

默认情况下，Data Protector 不包括备份映像中的日志文件。要在备份映像中包括最新的日志文件，请在 DB2 服务器系统上将 omnirc 变量 OB2_DB2INCLDLOGS 设置为 1 。

在还原会话期间，包括的日志将还原到 Data Protector 临时文件夹，并用于前滚恢复。

请注意，如果要执行恢复到已包括日志未涵盖的时间点，则仍需存档日志。

物理分区的环境

在物理分区的环境中，为 DB2 数据库对象创建一个备份规范，为 DB2 对象所在的每个物理节点 (系统) 创建一个存档日志。

确保在所有物理节点上选择相同的 DB2 数据库对象进行备份。

由于需要两个设备来备份单个系统中的 DB2 对象和存档日志，因此所需的设备 (驱动器) 总数是物理节点数的两倍。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“DB2 集成”，然后单击“添加备份”。
3. 选择模板，然后单击“确定”。

备份模板

备份模板	描述
DB2 Database Backup	用于仅备份 DB2 数据库对象。
Archived_Logs_Backup	用于仅备份存档日志。可以保存此类备份规范，但不能启动或计划。 “用户退出”或“供应商库”程序每次启动存档日志的备份时，都会使用它

4. 在“客户机”中，选择 DB2 服务器系统；在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，选择要备份的 DB2 实例，然后单击“下一步”。

   有关“用户和组/域”选项的信息，请按 **F1**。

5. 如果未将 DB2 实例配置为与 Data Protector 一起使用，则会显示“配置 DB2”对话框。按照配置 DB2 实例中所述进行配置。
6. 选择要备份的 DB2 对象，然后单击“下一步”。基本备份单位是表空间。只能选择表空间和数据库进行备份。

   如果仅选择 DB2 临时表空间，则备份将失败。要备份 DB2 临时表空间，请选择整个数据库。

   > **重要说明**在物理分区环境中，请仅选择一个数据库或同一数据库的几个表空间。

   单击“下一步”。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后依次单击“属性”和“下一步”。
8. 设置备份选项，然后单击“下一步”。
9. 要对特定 DB2 对象执行脱机备份，请右键单击该对象，然后单击“属性”。在“对象属性”对话框中，选择“脱机备份”，然后单击“确定”。
10. 单击“另存为”以保存备份规范，指定名称和备份规范组。您可以单击“保存并计划”选项进行保存，然后对备份规范进行计划 (可选)。

    > **提示**对物理分区的 DB2 对象的备份规范使用一致的名称。例如 MyObject1 、 MyObject2 等等。

    > **提示**在使用之前预览备份规范的备份会话。

DB2 备份选项

备份选项	描述
pre-exec 和 post-exec	在备份每个选定的 DB2 对象之前 (pre-exec) 之后 (post-exec)，先指定 DB2 服务器系统上由 db2bar 启动的命令。不要使用双引号。 仅键入命令的名称，而非路径名。命令必须位于以下目录中： *Windows 系统：* Data Protector\bin *HP-UX 系统：* /opt/omni/lbin *其他 UNIX 系统：* /usr/omni/bin
并行性	指定用于从节点备份数据库的数据流的数量。 在分区环境中， Parallelism 必须与设备并发相等。 默认值：1.

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

预览备份会话

预览备份会话以对其进行测试。使用 Data Protector GUI 或 CLI。

预览将在 DB2 服务器系统上的 *Data Protector*\tmp 目录中创建文件 *backup_specification_name_TEST_FILE*。测试之后将其删除。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“DB2 服务器”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

   预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

请执行以下命令：

```
omnib -db2_list backup_specification_name -test_bar
```

预览期间会发生什么?

启动 db2bar 命令，这会启动 Data Protector testbar2 命令以测试:

- Data Protector 单元中的通信
- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中

然后，检查 DB2 实例是否存在选定的 DB2 对象以及它们是否处于适当的备份状态。

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份十分有用。

可以使用 Data Protector GUI 或 CLI 启动 DB2 对象的备份。

> **注意**Data Protector 当前不支持使用 DB2 CLI 启动备份。您只能使用 Data Protector GUI 或 CLI 来完成这些步骤。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“DB2 集成”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 选择“备份类型”和“网络负载”。单击**确定**。

   成功备份显示消息“会话已成功完成”，并提供备份大小，即完整备份和增量/差量备份的大小之和。

使用 Data Protector CLI

请执行以下命令：

```
omnib -db2_list backup_specification_name [-barmode db2_mode] [options] [-preview]
```

示例

要使用备份规范 MyObjects 执行完整的 DB2 备份并将数据保护设置为 10 周，请执行以下操作:

```
omnib -db2_list MyObjects -barmode -full -protect weeks 10
```

开始备份物理分区的 DB2 对象

1. 对驻留在具有编目节点的系统上的部分 DB2 对象运行备份规范。使用 Data Protector GUI 或 CLI。
2. 以任何顺序对其他部分的 DB2 对象运行备份规范。

   只有对象驻留在编目节点上时，运行备份规范的顺序才十分重要。

提示对于第一个备份规范，添加一个 post-exec 脚本，该脚本将自动运行其他备份规范。

检查配置

在为 DB2 实例创建至少一个备份规范之后，可以检查 DB2 实例的配置。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，展开“备份规范”，然后展开“DB2 集成”。单击 DB2 实例的备份规范。
3. 在结果区域中，右键单击 DB2 实例，然后单击“检查配置”。

使用 Data Protector CLI 执行以下命令：util_db2.exe -CHKCONF DB2_instance

还原 DB2 UDB 集成

使用 Data Protector GUI 或 CLI 还原 DB2 对象。

> **注意**Data Protector 当前不支持使用 DB2 CLI 还原 DB2 对象。您只能使用 Data Protector GUI 或 CLI 来完成这些步骤。

> **重要说明**数据库将脱机还原。表空间将联机还原。只有未还原的表空间可供使用。只能从完整数据库备份还原已删除的表空间。

使用 Data Protector GUI 还原

1. 在上下文列表中，选择**还原**。
2. 在“范围窗格”中，展开“DB2 集成”，展开其中已备份要还原数据的客户机，然后单击要还原的 DB2 实例。
3. 在“源”页面中，指定是要还原数据库/表空间还是存档日志，然后浏览并选择所需的 DB2 对象。

   > **重要说明**在物理分区环境中，请仅选择一个数据库或同一数据库的几个表空间。

   默认情况下，将还原最新备份版本。要从特定备份版本还原 DB2 对象，请右键单击该对象，单击“属性”，然后在“属性”的“DB2_object”对话框中指定备份版本。

   要将一个数据库还原到新数据库，请右键单击该数据库，单击**属性**，然后单击**选项**选项卡。选择“还原到新数据库”，然后指定新数据库的名称。
4. 在“选项”页中，设置 DB2 还原选项。

   > **注意**对于前滚恢复，使用最新的日志文件备份版本。要使用较旧版本的日志文件执行前滚恢复，请先还原所需的日志文件，然后在清除“前滚”选项的情况下还原数据库/表空间。在分区环境中，连接到编目节点。最后，使用 DB2 工具执行前滚恢复。
5. 在“设备”页中，选择要用于还原的设备。

   单击**还原**。
6. 在“开始还原会话”对话框中，单击**下一步**。
7. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
8. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

DB2 还原选项

还原选项	描述
恢复到客户机	要还原到的客户机。默认情况下，DB2 对象还原到源客户机。此选项仅在还原整个数据库时有效。
用户名 用户组 密码	目标 DB2 实例的 DB2 用户、组和密码。
恢复到实例	要还原到的 DB2 实例。默认情况下，DB2 对象还原到源 DB2 实例。必须按照配置 Informix 实例中所述将实例配置为与 Data Protector 一起使用。

前滚	选择此选项以执行前滚恢复。在特定时间将数据库/表空间还原到其状态。在前滚恢复期间，恢复数据库/表空间和归档的日志，然后将归档日志中记录的更改应用于数据库/表空间。日志文件的最新备份版本用于此目的。如果日志文件包括在备份中且 omnirc 变量 OB2_DB2INCLDLOGS 设置为 1，则包括的日志将还原到 Data Protector 临时文件夹。通过选择“前滚到日志结尾”或“前滚到日期”来指定前滚恢复。指定“前滚到日期”时，请使用协调世界时 (UTC)。 系统目录的前滚恢复只能执行到日志的结尾。无法同时从相同会话恢复相同数据库的其他表空间。 要在物理分区的环境中执行前滚恢复，请还原清除了“前滚”的所有部分，连接到编目节点，然后使用 DB2 命令行处理器启动前滚恢复。 要执行版本恢复，请清除此选项。将数据库/表空间恢复到其备份时的状态。对于版本恢复，需要完整脱机数据库备份。从清除了“前滚”的联机备份还原时，数据库进入前滚挂起状态，并且变为不可用。要使它可用，请使用 DB2 命令行处理器或命令中心启动前滚恢复 (在分区环境中，必须从编目节点启动前滚恢复)。
还原路径	日志文件要还原到的目录。仅在使用 Vendor Library 选项存档日志时，才使用此选项。

使用 Data Protector CLI 还原

请执行以下命令：

omnir -db2 -barhost source_client [-destination target_client] -instance target_instance -dbname source_db [-session BackupID] [-newdbname new_db] [-frominstance source_instance] -tsname table_space [-session BackupID] -logfile log_file [-logdir log_path] [-rollforward [-time YYYY-MM-DD.hh.mm.ss]]

参数描述

参数	描述
source_client	要备份 DB2 对象的 DB2 服务器系统。在群集环境中，指虚拟服务器的名称。
target_client	目标 DB2 服务器系统 (仅当未还原到源客户机时)。
source_instance	已备份其 DB2 对象的 DB2 实例。
target_instance	目标 DB2 实例。
source_db	要还原的数据库。
new_db	目标数据库 (仅在不是源数据库时指定)。
table_space	要还原的表空间。
log_file	要还原的日志文件。
BackupID	指定要从中还原备份数据的会话，例如 2011/10/09–2。 备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。 镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是对象*复制*会话的会话 ID。 如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有通过设置介质分配优先级列表，才能使用 Data Protector GUI。
log_path	日志文件要还原到的目录。仅当 logarchmeth1 设置为“供应商”的情况下存档日志时，才使用此选项。

示例

要从 DB2 服务器系统 degas 上的实例 DB2Inst 还原 DB2 数据库 TEMP，并将其前滚到 2011 年 1 月 10 日上午 9:15，请执行以下操作:

omnir -db2 -barhost degas -instance DB2Inst -dbname TEMP -rollforward time: 2011-01-10.09.15.00

还原到新数据库或其他 DB2 实例

要将数据库还原到源 DB2 实例或其他实例中的新数据库，请执行以下操作:

1. a. 查找源数据库的容器:
   - 要列出驻留在特定节点上的特定数据库的表空间，请连接到该节点，然后连接到数据库，并运行以下命令:

     db2 list tablespaces
   - 要列出特定表空间的容器，请运行以下命令:

     db2 list tablespace containers for table_space_number

通过添加重定向到 DB2 配置文件的选项，为非系统表空间定义新的表空间容器。针对每对表空间容器执行以下命令:

> 必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。
>
> 设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

```
util_cmd -putopt DB2 target_instance "old_container" "new_container" -sublist Redirection/source_db
```

目标实例的 DB2 用户必须具有新容器的读写权限。

b. 如果使用自动存储数据库 (其中可以创建表空间且其容器和空间管理特征完全由 DB2 数据库管理器确定)，请定义新的存储路径。为此，请针对每个存储路径执行以下命令:

```
util_cmd -putopt DB2 target_instance "index_number" "new_storage_path" -sublist Autostore/source_db
```

参数说明:

target_instance

目标实例。

source_db

备份的数据库。

2. 在物理分区的环境中，在每个系统上重复查找源数据库的容器。
3. 将源数据库还原到新数据库，而不指定前滚恢复。使用 Data Protector GUI 或 CLI。

   在物理分区的环境中，首先使用编目节点还原驻留在系统上的数据库部分，然后按任意顺序还原其他部分。

   还原之后，新数据库进入前滚挂起状态。
4. 如果已从脱机备份还原，请使用 DB2 工具执行前滚恢复:
   - 在非分区的环境中，运行:

     ```
     db2 rollforward db db_name stop
     ```
   - 在分区的环境中，运行:

     ```
     db2 terminate

     export DB2NODE=catalog_node_number

     db2 rollforward db db_name stop
     ```

   如果已从联机备份还原，则使用“用户退出”选项利用 Data Protector GUI 还原已存档日志，然后使用 DB2 工具执行前滚恢复:

   a. 登录到源实例。如果已使用存档日志处理的“用户退出”方法，请执行下面两个步骤。否则，如果使用“供应商库”选项，请转到步骤 e。

   b. 确保您有权使用 Data Protector GUI 写入存档日志目录并还原存档日志。

      存档日志将还原到备份它们的同一目录。

   c. 将源数据库的存档日志和重做日志复制到新数据库的相应日志路径目录中 (分区环境中的目标实例的每个节点)。

      如果目标日志文件目录中存在 SQLLPATH.TAG 文件，请将其删除以避免可能的数据库不一致。

   d. 如果要还原到另一个实例，请将复制的日志的所有权授予目标实例的 DB2 用户，然后登录到目标实例。

   e. 使用 DB2 工具执行前滚恢复:
      - 在非分区的环境中，运行:

        ```
        db2 rollforward db db_name [to time | to end of logs] [and complete]
        ```
      - 在分区的环境中，运行:

        ```
        db2 terminate

        export DB2NODE=catalog_node_number

        db2 rollforward db db_name [to time | to end of logs] [and complete]
        ```

   f. 在使用自动前滚还原到 DB2 数据库之前，需在 omnirc 文件中设置环境变量:
      - 在 DB2 客户机上，在 omnirc 文件中设置以下环境变量:
        - OB2APPNAME = “source_Instance_name”
        - OB2BARHOSTNAME =”Source_client_name”
        - OB2APPDATABASE = “source_database_name”

> **注意**这适用于使用“供应商”库的所有 DB2 日志备份，而对“用户退出”模式不是必需的。
>
> 在 omnirc 文件中，在前滚 DB2 数据库之后删除上述三种变量。这可确保在同一系统上运行的其他 DB2 实例在备份期间不受这些环境变量的影响。

- 执行 DB2 前滚命令。

以下示例来自非分区环境。

示例 1

要将数据库 db2db_old 从联机备份还原到数据库 db2db_new（两个数据库均驻留在实例 db2inst 中），db2db_old 的日志文件位于 /db2_db/db2inst/NODE0000/SQL00003/SQLLOGDIR 目录中，"/tmp/db2cont1" 是表空间之一的容器:

1. 使用 Data Protector CLI 为表空间定义新容器 "/tmp/db2cont2"：

   util_cmd -putopt DB2 db2inst "/tmp/db2cont1" \ "tmp/db2cont2" -sublist Redirection/db2db_old

2. 使用 Data Protector CLI 将数据库 db2db_old 还原到数据库 db2db_new：

   omnir -db2 -barhost source_client -instance db2inst -dbname db2db_old -newdbname db2db_new

   如果使用“用户退出”选项进行日志备份，请执行步骤 3 和 4。

3. 使用 Data Protector GUI 还原前滚恢复所需的所有存档日志。
4. 将源数据库的存档日志和重做日志复制到新数据库的相应日志路径目录中。
5. 使用 DB2 CLI 执行前滚恢复到日志的结尾:

   db2 rollforward db db2db_new to end of logs

6. 在使用自动前滚还原到 DB2 数据库之前，需在 omnirc 文件中设置环境变量:
   - 在 DB2 客户机上，在 omnirc 文件中设置以下环境变量:
     - OB2APPNAME = “source_Instance_name”
     - OB2BARHOSTNAME =”Source_client_name”
     - OB2APPDATABASE = “source_database_name”

   > **注意**这适用于使用“供应商”库的所有 DB2 日志备份，而对“用户退出”模式不是必需的。
   >
   > 在 omnirc 文件中，在前滚 DB2 数据库之后删除上述三种变量。这可确保在同一系统上运行的其他 DB2 实例在备份期间不受这些环境变量的影响。

   - 执行 DB2 前滚命令。

示例 2

要将实例 inst1 中的数据库 db2db 还原到实例 inst2 中的数据库 db2db，请执行以下操作:

1. 使用 Data Protector CLI 为表空间定义新容器 /tmp/db2cont2：

   util_cmd -putopt DB2 inst2 "/tmp/db2cont1" "/tmp/db2cont2" -sublist Redirection/db2db

2. 使用 Data Protector CLI 将数据库 db2db 还原到实例 inst2：

   omnir -db2 -barhost source_client [-destination *target_client*] -instance inst2 -dbname db2db -frominstance inst1

示例 3

要将自动存储数据库 db2db_old（具有两个关联的存储路径）从联机备份还原到数据库 db2db_new：

1. 使用 Data Protector CLI 检查路径是否存在并指定新的存储路径:

   util_cmd -putopt DB2 inst2 "1" "c:\db2\db2db_new\1" -sublist Autostore/db2db_old

   util_cmd -putopt DB2 inst2 "1" "c:\db2\db2db_new\2" -sublist Autostore/db2db_old

2. 使用 Data Protector CLI 或 GUI 将数据库 db2db_old 还原到数据库 db2db_new。
3. **仅限“用户退出”选项:** 使用 Data Protector GUI 还原前滚恢复所需的所有存档日志。
4. **仅限“用户退出”选项:** 将源数据库的存档日志和重做日志复制到新数据库的相应日志目录中。
5. 使用 DB2 CLI 执行前滚恢复到日志的结尾。
6. 在使用自动前滚还原到 DB2 数据库之前，需在 omnirc 文件中设置环境变量:

- 在 DB2 客户机上，在 omnirc 文件中设置以下环境变量:
  - OB2APPNAME = “source_Instance_name”
  - OB2BARHOSTNAME =”Source_client_name”
  - OB2APPDATABASE = “source_database_name”

> **注意**这适用于使用“供应商”库的所有 DB2 日志备份，而对“用户退出”模式不是必需的。
>
> 在 omnirc 文件中，在前滚 DB2 数据库之后删除上述三种变量。这可确保在同一系统上运行的其他 DB2 实例在备份期间不受这些环境变量的影响。

- 执行 DB2 前滚命令。

> **注意**还原到另一个系统上的另一个实例时，请使用 db2 list tables for all 命令以列出表。

在分区环境中还原

您可以将分区的 DB2 对象还原到原始数据库或新数据库 (在另一个 DB2 实例上)。

以下限制适用：

- 仅当分区环境只有一个节点 (单个分区) 时，才能将对象从非分区环境还原到分区环境 (反之亦然)。
- 在物理分区的环境中，无法实现自动恢复。
- 在物理分区的环境中，将忽略前滚参数，前滚必须使用 DB 工具手动完成。

还原到原始数据库

损坏的数据库

要还原损坏的数据库，请执行以下操作:

1. 连接到属于损坏数据库的编目节点的节点。
2. 创建一个具有相同名称的新数据库。
3. 按照还原到新数据库或其他 DB2 实例中所述继续执行还原。

物理分区的环境 要还原物理分区的 DB2 对象 (驻留在多个系统上)，请执行以下操作:

1. 使用编目节点还原驻留在系统上的 DB2 对象的一部分，而不指定前滚恢复。使用 Data Protector GUI 或 CLI。
2. 以任何顺序将 DB2 对象的所有其他部分还原到相应的系统，而不指定前滚恢复。
3. 使用 DB2 工具连接到编目节点并执行前滚恢复:

   ```
   db2 terminate

   export DB2NODE=catalog_node_number

   db2 rollforward db db_name [[stop]][to time|to end of logs] [and complete]]
   ```

> **注意**只有对象驻留在编目节点上时，还原部分 DB2 对象的顺序才十分重要。

逻辑分区的环境

要还原逻辑分区的 DB2 对象 (仅驻留在一个系统上)，请执行以下操作:

- 对于版本恢复:
  1. 还原对象，而不指定前滚恢复。使用 Data Protector GUI 或 CLI。
  2. 连接到编目节点并执行前滚恢复:

     ```
     db2 terminate

     export DB2NODE=catalog_node_number

     db2 rollforward db db_name stop
     ```

- 对于前滚恢复，请还原该对象，并指定前滚。使用 Data Protector GUI 或 CLI。

还原到新数据库或其他实例

要将数据库还原到原始 DB2 实例中的新数据库，请参阅还原到新数据库或其他 DB2 实例。

要将数据库还原到另一个 DB2 实例中的新数据库，请执行以下操作:

1. 登录到目标实例。
2. 确保实例具有与源实例相同的节点结构 (节点数、节点组)。
3. 连接到与源数据库的编目节点具有相同节点号的节点:

   ```
   EXPORT DB2NODE=catalog_node_of_the_source_database
   ```

4. 创建一个与源数据库同名的数据库:

   ```
   db2 create db source_db
   ```

5. 按照还原到新数据库或其他 DB2 实例中所述继续执行还原

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

您还可以使用监视器上下文监视安装有 User Interface 组件的任何 Data Protector 客户机的会话。

> **注意**前滚恢复期间显示的消息中的所有 DB2 时间戳都是按协调世界时 (UCT) 格式由 DB2 设计的。

删减 DB2

数据库管理器在恢复历史记录文件中为事件 (例如备份操作、还原操作、表空间创建等等) 创建条目。您可能要从恢复历史记录文件中删除或删减不再相关的条目，因为不再需要关联的恢复对象来恢复数据库。

在以下实例期间，数据库管理器会自动更新并删减恢复历史记录文件条目:

- 成功完成数据库完整备份或表空间操作之后。
- 成功完成数据库还原操作之后，不需要前滚操作。
- 成功完成数据库前滚操作之后。

在自动删减期间，数据库管理器执行以下操作:

1. 更新恢复历史记录文件条目的状态。
2. 删减过期的恢复历史记录文件条目。
3. 调用 Data Protector DB2 集成以在过期的 DB2 备份对象上将保护设置为“无”。

数据库管理器以下列方式更新恢复历史记录文件条目:

- 不再需要的所有活动数据库备份映像都将标记为已过期。
- 标记为非活动的所有数据库备份映像以及在获取数据库备份之前获取的映像也会标记为已过期。
- 如果已还原活动数据库备份映像，并且它不是历史记录文件中记录的最新数据库，则同一日志序列中可用的任何后续数据库备份映像都将标记为非活动。
- 如果已还原非活动数据库备份映像，则当前日志序列中可用的任何非活动数据库备份将再次标记为活动。
- 与当前日志序列不对应的任何数据库或表空间备份映像 (也称为当前日志链) 都标记为非活动状态。
- 如果在还原之后表空间级备份映像变为非活动状态，则应用当前日志序列无法访问数据库的当前状态。
- 任何具有 do_not_delete 状态的条目都不会被删减，并且不会删除其关联的日志文件、备份映像和加载副本映像。
- 升级数据库时，历史记录文件中的所有联机数据库备份条目和所有联机或脱机表空间备份条目都将标记为已过期，因此自动重建时不会选择这些条目作为重建所需的映像。加载副本映像和日志存档条目也将标记为已过期，因为这些类型的条目不能用于恢复目的。

以下数据库配置参数控制数据库管理器删减的条目:

- **num_db_backups**

  指定要为数据库保留的数据库备份数。

- **rec_his_retentn**

  指定可以保留有关备份的历史信息的天数。

- **auto_del_rec_obj**

  指定数据库管理器是否必须删除与已删减的恢复历史记录文件条目关联的日志文件、备份映像和加载副本映像。

您需要设置以下配置参数以配置数据库管理器，从而自动管理恢复历史记录文件:

- num_db_backups
- rec_his_retentn
- auto_del_rec_obj

注意当 auto_del_rec_obj 设置为“开启”且成功的数据库备份条目数多于使用 num_dp_backups 配置参数生成的条目数时，数据库管理器将自动删减早于 rec_his_retentn 的恢复历史记录文件条目。

Microsoft Exchange 和 Granular Recovery Extension

This feature is available in the Premium Edition

本主题介绍适用于 Microsoft Exchange Server 2010 和 Microsoft Exchange Server 2013 (下文均称为 **Microsoft Exchange Server**，除非指出不同之处) 的 Data Protector Granular Recovery Extension，包括以下子主题:

适用于 Microsoft Exchange 的 GRE 简介

This feature is available in the Premium Edition

适用于 Microsoft Exchange Server 的 Granular Recovery Extension（扩展）不提供任何备份解决方案。可以使用 Data Protector Microsoft Exchange Server 2010 集成备份 Microsoft Exchange Server 2010 邮箱数据库和公用文件夹数据库或 Microsoft Exchange Server 2013 邮箱数据库 (“数据库”)。可以使用扩展还原 Microsoft Exchange Server 邮箱数据库文件，以及恢复单个 Microsoft Exchange Server 项目或整个邮箱。

因此，使用扩展，您可以恢复各个邮箱项目（例如电子邮件文件夹、日历、联系人或便笺），而无需恢复整个 Microsoft Exchange Server 邮箱或整个邮箱数据库。

Granular Recovery Extension 文档集

- **电子 PDF 格式**

  适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 章节提供特定于此扩展的信息:

  - 有关 Microsoft Exchange Server 规范的详细信息，请参见 Microsoft Exchange Server 官方文档。

- **帮助**

  为完善本节 (以电子 PDF 格式提供) 中提供的信息，适用于 Microsoft Exchange Server 的 Granular Recovery Extension 提供了集成到 Microsoft 管理控制台 (MMC) 的上下文相关帮助 (F1)。该帮助介绍了 Granular Recovery Extension 图形用户界面 (GUI) 中提供的页面和选项。可以通过按 F1 或单击操作窗格中的问号 (?) 或“帮助”来访问该帮助。

备份

适用于 Microsoft Exchange Server 的 Granular Recovery Extension 不提供任何备份解决方案。可以使用 Data Protector Microsoft Exchange Server 2010 集成备份 Microsoft Exchange Server 数据库。

- Data Protector Microsoft Exchange Server 2010 集成
- Data Protector Microsoft 卷影复制服务集成

还原和恢复

扩展可带来以下好处：

- **恢复粒度**

  可还原的最小 Microsoft Exchange Server 对象是数据库。还原后，您可以浏览各个 Microsoft Exchange Server 邮箱项目（例如电子邮件文件夹、日历、联系人或便笺）。因此，可以选择恢复整个数据库，也可以选择仅恢复所需的邮箱项目。

- **多个还原请求**

  可以同时接收多个还原请求。

- **恢复多个邮箱**

  可以同时恢复多个邮箱。

- **恢复到不同位置**

  可以将 Microsoft Exchange Server 项目恢复到以下位置：

  - 邮箱中的原始位置
  - 不同位置：
    - 不同邮箱
    - 个人文件夹文件 (.pst)

      可以使用个人文件夹文件 (.pst) 将 Microsoft Exchange Server 项目恢复到位于未安装扩展组件的不同 Microsoft Exchange 邮箱服务器上的 Microsoft Office Outlook 客户机。

    - 未安装扩展组件的不同邮箱服务器节点

- **易于搜索**

  可以通过指定电子邮件主题、作者、日期、附件名称字词或电子邮件正文字词来过滤 Microsoft Exchange Server 项目。可以在启动恢复过程之前搜索 Microsoft Exchange Server 项目。这样可以预览将恢复的所有 Microsoft Exchange Server 项目。

- **扩展的安全操作**

  要还原并恢复 Microsoft Exchange Server 项目，必须由 Data Protector 备份管理员为您 (作为 Microsoft Exchange Server 管理员) 分配“启动还原”用户权限。

有关详细信息，请参阅。

- **Microsoft 管理控制台 (MMC) 管理单元**

  扩展的图形用户界面 (GUI) 是与 Exchange 管理控制台 (EMC) 集成的 Microsoft 管理控制台 (MMC) 管理单元。可以在控制台树中 EMC 入口点（Microsoft Exchange 图标）的上方找到扩展的入口点。

  通过该集成，您可以轻松地在管理 Exchange 任务和执行 Granular Recovery Extension 任务（例如请求还原和启动恢复会话等）之间切换。

先决条件

- 将以下对象安装到所选的 Microsoft Exchange Server 系统：
  - Data Protector“MS Exchange Server 2010+ 集成” 组件。
  - Data Protector“MS Exchange Server 2010+ 集成” 组件。
  - 所有必需的非 Data Protector 组件。
- 将 TCP/IP 端口 60000（默认）在所选 Microsoft Exchange Server 系统上保持空闲。

Microsoft Exchange Server 软件

安装以下各项：

- Microsoft Exchange Server

  确保已正确安装和配置 Microsoft Exchange Server 环境。

  有关安装、配置和使用 Microsoft Exchange Server 的信息，请参见 Microsoft Exchange Server 文档。

- Microsoft 管理控制台 (MMC) 3.0 或更高版本
- .NET Framework 3.5.1 或更高版本
- Internet 信息服务 (IIS) 6.0 或更高版本

Data Protector 软件

安装以下 Data Protector 组件：

- Data Protector MS Exchange Server 2010+ 集成组件
- 所有 Microsoft Exchange Server 系统上的 Data Protector MS Exchange Server 2010+ 集成组件

确保按照《Data Protector 安装指南》和《Data Protector 集成指南》中所述已安装和配置 Data Protector 备份解决方案。

其他非 Data Protector 软件和服务

- 安装 Windows PowerShell 1.0 或更高版本（Windows Management Framework Core 包）
- 不支持除英语以外的 PowerShell 本地化（Windows OS 必须使用英语本地化）。
- 将 TCP/IP 端口 60000（默认）在 Granular Recovery Web 服务上保持空闲。
- 将防火墙配置为允许新端口。

Data Protector Granular Recovery Extension 注意事项

- 不能同时使用 Granular Recovery Extension GUI 或 GUI 和命令行界面 (CLI) 的两个或更多实例。
- 在 GRE 用户界面已打开时使用管理工具（例如 Exchange 管理控制台）在 Granular Recovery Extension (GRE) 外部执行的任何 Microsoft Exchange Server 操作不会反映在 GRE 用户界面中。
- 从相同备份版本还原同一个备份对象（邮箱数据库）的多个请求只会处理一次。
- 如果选择 Data Protector Granular Recovery Extension 节点，操作窗格中会显示“导出列表...”按钮。该按钮创建控制台树中显示的所有内容的列表: 缓存管理、状态 (导入会话/恢复会话) 和设置 Microsoft Exchange。可以使用以下格式导出列表：文本、Unicode 文本、逗号分隔值 (CSV) 和 Unicode CSV。默认情况下，此功能由 Microsoft 管理控制台 (MMC) 提供。
- 可以对同一个已还原的数据库执行多个恢复请求。
- 在 GRE 向导中，可以指定搜索条件来缩小可选择进行恢复的项目的列表。在“邮箱搜索条件”页面中输入一些值并在特定的邮箱文件夹中选择一个或多个项目进行恢复之后，如果该文件夹的子文件夹中的任何项目满足相同的搜索条件，也会恢复这些项目。
- “搜索结果”页面只会显示三个文件夹级别，这不会影响还原过程。如果在第三级别上选择一个项目，也会还原其子项目。
- 执行还原之前，请确保目标文件夹为空。

> **提示**可以在“从备份导入”向导的“还原设置”页面中指定新的还原文件夹，扩展会创建新文件夹。

- 在“从备份导入”向导的“邮箱选择”页面中，以非 ASCII 字符开头的邮箱用户名会分组到 -- 下。
- 不支持在路径中使用非 ASCII 字符。键入还原路径时，请避免使用非 ASCII 字符。否则，还原可能会失败。
- 如果邮箱服务器上的目标位置中已存在恢复数据库，粒度恢复缓存会保留所有版本而不会删除它们。
- 可以向同一个目标位置执行多个还原请求。
- 可以在一个邮箱服务器上创建多个恢复数据库。
- 恢复数据库的数量受临时还原位置中可用的磁盘空间限制。
- 即使恢复会话完成后已还原的数据库文件仍位于磁盘上，粒度恢复缓存也只会为每个 Microsoft Exchange 邮箱服务器保留一个已装载的恢复数据库 (RDB)。

  在一个 Microsoft Exchange 邮箱服务器上，仅存储一个恢复数据库。

  例如，在 DAG 环境中，每个邮箱节点可以包含一个恢复数据库，但只有一个服务器上可以有已装载的恢复数据库。

Data Protector 注意事项

- Granular Recovery Extension 无法从使用 Data Protector Microsoft 卷影复制服务 (VSS) 集成创建的备份映像还原或恢复项目。
- Granular Recovery Extension 不支持即时恢复 (IR)。

Microsoft Exchange Server 注意事项

- 将数据恢复到 PST 文件的选项仅适用于使用 Microsoft Exchange Server 2010 SP1 或更高版本服务包的 Microsoft Exchange Server 2010 环境。
- 无法搜索已移动的或已删除的邮箱数据库（这是 Microsoft Exchange Server 的已知问题）。但是，可以在移动邮箱后恢复该邮箱。

  仅当保留期未到期时，已删除的邮箱才会显示在“从备份导入”向导中的“从备份导入 — 邮箱选择”上。保留期已到期并且已删除的邮箱在“从备份导入”向导中不再可用之后，必须重新导入包含所需邮箱的邮箱数据库。
- 在 Microsoft Exchange Server 2013 环境中，由于 Microsoft Exchange Server 的限制，New-MailboxRestoreRequest 、 Search-Mailbox 和 New-SearchMailbox cmdlet 操作的组合会导致出现无法避免的存储空间因素和性能因素。
- 请确保独立配置或 DAG 配置（GRE 支持的 Microsoft Exchange Server 配置）中的活动数据库具有源邮箱大小两倍的存储空间用于在恢复期间创建临时邮箱。
- 请确保要将恢复项目存储到的目标邮箱具有足够的存储空间用于存储已恢复的项目。
- Microsoft Exchange Server 2013 要求在将数据库还原到的邮箱服务器上重新启动“Microsoft Exchange 信息存储服务”以提高数据库性能。虽然不执行该操作不会导致无法访问还原数据库，但 Microsoft 建议执行服务的重新启动。因此，成功执行数据库还原之后，请手动重新启动“Microsoft Exchange 信息存储服务”。
- 确保目标 Exchange 邮箱服务器上有足够的可用磁盘空间。
- Granular Recovery Extension 无法从使用 Data Protector Microsoft 卷影复制服务 (VSS) 集成创建的备份映像还原或恢复项目。
- Data Protector Granular Recovery Extension 不支持即时恢复 (IR)。
- 确保已在“粒度恢复缓存管理”中还原（导入）邮箱数据库文件。
- 确保已装载要从中恢复各个 Microsoft Exchange Server 项目的恢复数据库。
- 确保要卸除的恢复数据库已装载。
- 只能保持装载一个恢复数据库。因此，如果要从不同的备份版本或不同的邮箱数据库恢复单个项目或整个邮箱，必须先卸除已呈现给 Microsoft Exchange Server 的邮箱数据库，该数据库显示在“粒度恢复缓存管理”中。
- 确保要从磁盘中删除的恢复数据库已还原。
- 已还原的邮箱数据库将在“粒度恢复缓存管理”中保留 30 天（默认值）。保留期到期之后，将自动删除数据库。
- 确保邮箱数据库在粒度恢复缓存中可用。
- 使用命令 --Config 并提供“用户名”、“密码”和“域”，以配置用于远程执行 Exchange Management cmdlet 操作的用户帐户。使用 CLI 命令执行任何粒度恢复操作之前，必须先配置远程 powershell。
- 启用调试。
- 确保已安装最新的 Data Protector 官方修补程序。

限制

以下限制适用：

- 在还原到现有文件夹期间，GRE 恢复发生在根级别而不是子文件夹下。

安装适用于 **Microsoft Exchange** 的 **GRE**

This feature is available in the Premium Edition

适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 用于恢复各个 Microsoft Exchange Server 邮箱项目。根据 Microsoft Exchange Server 环境的配置，您可能需要在单个或多个 Microsoft Exchange Server 系统上安装相应的 Data Protector 组件。

在 Granular Recovery Extension 软件包的安装过程中，将重新启动 IIS（Internet 信息服务）。请对 Granular Recovery Extension 软件包安装进行相应规划，以便能够事先处理其他依赖 IIS 的应用程序。

配置适用于 Microsoft Exchange 的 GRE

This feature is available in the Premium Edition

本部分介绍需要执行的配置步骤。

满足 Granular Recovery Extension 的 Data Protector 配置要求

配置 Granular Recovery Web 服务端口

Granular Recovery Web 服务使用 TCP/IP 60000 端口号建立通信。如果其他服务正在使用该端口号，请将 Granular Recovery Web 服务配置为使用备用端口号：

1. 在不启动扩展的情况下，搜索以下 Windows 注册表项: HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Plugins\exchgre 。
2. 编辑项 Client port 并输入新端口号。
3. 通过运行以下命令更新 IIS 配置，以将新的端口值用于 Granular Recovery Web 服务：

   IIsWeb /create Web Service web site pathwebsite name/b new port number

   其中：

   “Web 服务网站路径”是 Granular Recovery Web 服务网站的根路径。默认路径 C:\inetpub\wwwroot 。

   “网站名称”是由 Granular Recovery Web 服务托管的网站。

   “新端口号”是 Granular Recovery Web 服务用于建立通信的新端口号。

   例如：

   IIsWeb /create c:\inetpub\wwwroot "HP MS Exchange GRE" /b 8000

为 Granular Recovery Extension 配置用户帐户

配置具有以下用户权限和特权的 Granular Recovery Extension (GRE) 用户帐户：

Data Protector 用户权限

确保您已获得以下 Data Protector 用户权限：

1. 打开 Data Protector GUI (**Data Protector Manager**)。
2. 创建新的用户组以供扩展使用，例如 GRE_Microsoft_Exchange_Server 。

   有关添加用户组的详细信息，请参阅《Data Protector 帮助》索引: “添加, 用户组”。
3. 为 GRE_Microsoft_Exchange_Server 用户组分配以下 Data Protector 用户权限:

   监控、**中止**、**装载请求**、**启动还原**、**还原到其他客户机**和**查看私有对象**。
4. 每次执行 Granular Recovery Extension 的新安装时，请向 GRE MS Exchange 用户组添加 Data Protector 用户。指定以下常规用户属性：

   名称: SYSTEM、“域或 UNIX 组:”NT AUTHORITY、“客户机系统:””ComputerName”(指定包含安装了 Granular Recovery Extension 的节点的计算机的名称)。

   有关详细的步骤，请参阅《Data Protector 帮助》索引: “添加, 用户”。

其他必要特权

为 GRE 用户帐户分配以下权限：

- 创建 Windows 注册表项
- 设置 Windows 注册表项值

执行 Exchange Management cmdlet 操作的特权

要创建远程运行空间以用于远程执行 Exchange Management cmdlet 操作，请配置具有特定 Exchange Management 角色的用户凭据。这些操作在 Microsoft Exchange Server 备份和还原操作的过程中执行，要成功运行扩展，必须执行这些操作。

配置具有以下 Exchange 特权的 GRE 用户帐户：

- 分配了某些内置管理角色的特定 Exchange Management 内置角色组的成员：
  - “组织管理”角色组
  - “发现管理”角色组
  - Mailbox Import Export 管理角色

    作为“组织管理”角色组的成员，默认情况下不为您分配此管理角色。要成功将 Exchange 邮箱项目恢复到原始邮箱中的原始位置或恢复到个人文件夹文件（.pst），请为您的 GRE 用户帐户分配此角色。

    > **注意**要恢复到 .pst 文件，您需要创建网络共享文件夹并向“Exchange 受信任子系统”组授予读/写权限。

- 安装了扩展的 Microsoft Exchange Server 系统的管理员组成员

在“远程 Powershell 配置”对话框中指定的用户凭据存储在安装了扩展的本地 Microsoft Exchange Server 系统上 Windows 注册表中的 HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Plugins\exchgre 目录下。

> **重要说明**只能存储单个用户的用户凭据（用户名、密码和域名）。每次输入新的用户凭据时，将覆盖现有凭据。加密密码存储在安装了扩展的 Microsoft Exchange Server 系统上。

以下是有关如何从 Exchange PowerShell cmdlet 界面将“邮箱导入导出”管理角色直接分配给用户帐户的工作示例。将 -User 选项值替换为用于 Exchange GRE 还原的用户名。

```
New-ManagementRoleAssignment -Name "Exchange-GRE Import Export" -User "GRE user account" -Role "Mailbox Import Export"
```

有关 Exchange Management cmdlet 操作和如何分配 Exchange Management 内置管理角色的详细信息，请参见 Microsoft Exchange Server 文档。

备份适用于 **Microsoft Exchange** 的 **GRE**

This feature is available in the Premium Edition

适用于 Microsoft Exchange Server 的 Granular Recovery Extension 不提供任何备份解决方案。可以使用 Data Protector Microsoft Exchange Server 2010 集成备份 Microsoft Exchange Server 数据库。

支持以下备份类型: 完整、增量、复制和差异。

不支持以下基于磁盘的备份：

- Microsoft 卷影复制服务 (VSS) 零宕机时间备份 (ZDB) 到磁盘
- VSS ZDB 到磁盘 + 磁带
- VSS ZDB 即时恢复可传输备份

注意恢复过程与 Data Protector 备份类型无关。

还原和恢复适用于 Microsoft Exchange 的 GRE

This feature is available in the Premium Edition

要先还原再恢复 Microsoft Exchange Server 项目，请遵循以下基本步骤：

1. **导入**
   a. **还原**

      Data Protector Granular Recovery Extension 使用 Data Protector Microsoft Exchange Server 2010+ 集成来还原 Microsoft Exchange Server 邮箱数据库。

      临时还原位置

      首先 Microsoft Exchange Server 数据库文件会保存到临时还原位置。将数据库文件 (.edb)、检查点文件 (.chk)、预留事务日志文件 (.jrs) 和事务日志文件 (.log) 还原到 Microsoft Exchange Server 系统上指定的临时还原位置。

      将在临时位置中创建恢复数据库 (RDB)。

      还原的文件位于选择作为还原目标系统的 Microsoft Exchange Server 系统上。默认位置为 C:\Restore ，但您可以指定其他还原位置。

      从备份映像成功还原邮箱数据库之后，还原的数据库在粒度恢复缓存中可用。

   b. **装载**

      将粒度恢复缓存中的还原的数据库装载到 Microsoft Exchange Server。浏览并恢复项目之前，必须先装载还原的数据库文件。

2. **恢复**

   浏览恢复数据库中的 Microsoft Exchange Server 项目，然后将这些项目恢复到原始邮箱数据库或任何其他位置。

3. **卸除**

   只能保持装载一个恢复数据库，因此，当不再需要从恢复数据库恢复项目时：

   - 从 Microsoft Exchange Server 卸除恢复数据库。

   卸除恢复数据库后，恢复数据库仍在“粒度恢复缓存管理”中，但其状态为已卸除。此时，如果需要用于其他恢复会话，您仍可以重新装载它们。

删除

恢复数据库将在缓存中保留 30 天（默认值），或者保留直至所设置的保留时间到期。

保留时间到期之后，系统会自动从 Granular Recovery Extension 缓存中卸除并删除数据库，但还原的数据库文件仍存在于临时还原位置中。

- （可选）更改保留期。
- （可选）在保留期到期之前手动从缓存中删除不再需要的恢复数据库。
- 还原的数据库文件仍保留在临时还原位置中，您可以通过手动删除临时还原位置中的文件来彻底删除它们。

打开 Data Protector Granular Recovery Extension GUI

要打开扩展，请执行以下操作：

1. 登录到安装了 Granular Recovery Extension 的 Microsoft Exchange Server 系统。
2. 单击“开始”按钮，然后单击 Data Protector Exchange GRE 图标以打开扩展的图形用户界面 (GUI)。

   将启动适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension。

项目	描述
1	控制台树
2	“结果”窗格
3	“工作”窗格
4	“操作”窗格

注意: 在 Microsoft Exchange Server 环境中，Exchange Management 任务通过 Exchange 管理中心 (EAC) 进行管理。EAC 具有自己的基于 Web 的图形用户界面，无法通过扩展的 Microsoft 管理控制台 (MMC) 管理单元 GUI 访问它。

3. 在控制台树中，单击**缓存管理**图标。

   此时将显示空的“粒度恢复缓存管理”页面。

   执行任何粒度恢复操作之前，必须先配置远程 powershell。

   要导入 Microsoft Exchange Server 数据库，请遵循导入邮箱数据库的过程。

远程 powershell 配置

配置用于远程执行 Exchange Management cmdlet 操作的用户帐户。

如果没有指定用于远程执行 Exchange Management cmdlet 操作的有效用户凭据，将显示“远程 Powershell 配置”对话框。输入所需的用户凭据，然后单击**确定**。

导入邮箱数据库

浏览并恢复项目之前，必须先导入数据库：

1. 在控制台树中，单击**缓存管理**图标。结果窗格中会显示**粒度恢复缓存管理**页面。
2. 在“缓存管理”节点下的操作窗格中，单击**从备份导入**。此时将显示“从备份导入”向导。
3. 在“简介”页面中，选择备份源：
   - 要仅导入特定邮箱，请选择**邮箱选择**，然后单击**下一步**。此时将显示“邮箱选择”页面。

     提示当邮箱数据库未知时，**邮箱选择**页面特别有用。

     a. 指定邮箱用户名，然后单击**下一步**。

     b. 此时将显示“备份版本选择”页面。选择要还原的备份数据，然后单击**下一步**。
   - 要导入整个数据库和数据库中包含的所有邮箱，请选择**数据库选择**，然后单击**下一步**。

     注意如果由于任何原因，要恢复的邮箱在“邮箱选择”页面中不可见，可以使用“数据库选择”页面选择数据库进行还原。

     a. 此时将显示“数据库选择”页面。选择要还原的数据库，然后单击**下一步**。

     b. 此时将显示“备份版本选择”页面。选择要还原的备份版本，然后单击**下一步**。
4. 此时将显示“还原设置”页面。确认或调整“数据库名称”、“服务器名称”和“还原位置”的值。

   执行还原之前，请确保目标文件夹为空。

   提示可以在“从备份导入”向导的“还原设置”页面中指定新的还原文件夹，扩展会创建新文件夹。

5. （可选）如果在“还原设置”页面中指定的服务器上的“粒度恢复缓存管理”中已存在恢复数据库，则可以卸除恢复数据库。选择选项，然后单击**完成**。
6. 要监控还原会话，请在控制台树中单击**状态（导入会话/恢复会话）**。此时将显示“粒度恢复状态（导入会话/恢复会话）”页面。
7. 要停止还原会话，请单击**中止会话**。

装载数据库

导入邮箱数据库之后（还原过程完成后），手动装载数据库。

要手动装载邮箱数据库，请执行以下操作：

1. 在控制台树中，选择“缓存管理”节点。
2. 在结果窗格中，选择要装载的数据库。

3. 在“数据库”节点下的操作窗格中，单击**装载恢复数据库**。

装载数据库后，工作窗格中会显示邮箱显示名称和大小以及上次登录时使用的用户名。

启动恢复

要恢复各个 Microsoft Exchange Server 项目，请执行以下操作：

> **注意**作为邮箱搜索和恢复过程的一部分，动态创建临时邮箱，名称以 **DP_** 开头。临时邮箱的用户显示在 Active Directory (AD) 中。完成恢复操作之后，将删除临时邮箱，而这又会将用户从 AD 中删除。如果即使在完成恢复操作之后仍未删除临时邮箱，请使用 Exchange 管理控制台或 Exchange Management Shell 等 Exchange 管理软件手动删除它们。

1. 在控制台树中，选择“缓存管理”节点。在结果窗格中，选择要从中恢复的恢复数据库。
2. 在“数据库”下的操作窗格中，单击**启动恢复**。

   > **提示**任何操作按钮（例如**启动恢复**）的快捷访问方式是在“粒度恢复缓存管理”中右键单击数据库。

3. 在“邮箱选择”页面中，选择用于恢复的邮箱。（可选）要还原整个邮箱文件夹，请选择**还原整个邮箱**选项。

   单击“下一步”。此时将显示“邮箱搜索条件”页面。
4. 按主题、作者、收件人、附件字词、个人文件夹或电子邮件内容过滤电子邮件，然后单击**下一步**。
5. 在“搜索结果”页面中，从邮箱中选择文件夹。项目会显示在表中。

   选择要恢复的项目，然后单击**下一步**。此时将显示“恢复设置”页面。

   > **提示**按住 **Ctrl** 或 **Shift** 键可选择多个项目。

   > **提示**如果未选择“保留最新邮件”，则会覆盖项目。

6. 指定目标恢复位置：现有的 Exchange Server 邮箱，或者要在恢复期间创建的 PST 文件的名称。

   > **提示**将项目恢复到邮箱的现有文件夹时，只会显示您创建的文件夹。不能将特殊文件夹（例如“收件箱”、“草稿”、“已发送邮件”、“已删除邮件”、“垃圾邮件”、“发件箱”、“RSS 源”、“同步问题”、“会话历史记录”、“任务”、“日历”和“联系人”）设置为目标，因此不会显示这些文件夹。单击“恢复到现有文件夹”或“恢复到不同邮箱”的“浏览”按钮不会显示特殊文件夹。只有“恢复到原始位置”可以将项目恢复到特殊文件夹。

   PST 文件文件夹必须可从 Exchange Server 系统访问。

   要使用远程系统或当前服务器，请按以下格式 (UNC) 输入网络共享文件夹的路径：

   \\SystemName\FolderShareName\Filename.pst

   > **注意**确保执行恢复的本地系统用户帐户对网络共享文件夹具有读取和写入权限集，以便创建 PST 文件。如果文件夹位于远程服务器系统上，则不需要在远程系统上安装 Data Protector MS Exchange Granular Recovery Extension 组件。

   单击**完成**以开始恢复操作，然后关闭向导。

卸除数据库

还原过程完成后，将在“粒度恢复缓存管理”中装载所选数据库。已装载的数据库会显示在结果窗格中。

要从“粒度恢复缓存管理”卸除不再需要的数据库，请执行以下操作：

1. 在控制台树中，选择“缓存管理”节点。此时将显示“粒度恢复缓存管理”页面。
2. 在结果窗格中，选择数据库。在“数据库”节点下的操作窗格中，单击**卸除恢复数据库**。
3. 此时将显示确认对话框。单击**是**。将卸除数据库，并且邮箱信息不再显示在工作窗格中。

删除数据库

要手动从“粒度恢复缓存管理”和磁盘上的临时还原位置删除不再需要的数据库，请执行以下操作：

1. 在控制台树中，选择“缓存管理”节点。此时将显示“粒度恢复缓存管理”页面。
2. 在结果窗格中，选择数据库。在“数据库”节点下的操作窗格中，单击**删除恢复数据库**。
3. 此时将显示确认对话框。单击**是**。该数据库将从临时还原位置中删除。

更改设置

还原会话完成后，数据库文件（.edb）、检查点文件（.chk）、预留事务日志文件（.jrs）和事务日志文件（.log）会复制到临时还原位置 c:\restore 。

要更改扩展的默认设置，请执行以下操作：

1. 在控制台树中，单击**设置**图标。结果窗格中会显示**粒度恢复设置**页面。
2. 临时还原位置设置为 c:\restore（默认）。要更改临时还原位置，请键入或浏览新目录以指定新路径。
3. 要设置在“粒度恢复状态”页面中显示的已完成会话（还原会话和恢复会话）的数量，请指定历史会话的最大数量。
4. 要启用 Granular Recovery Extension 调试，请选择**启用调试日志**。要更改调试文件的默认位置，请键入新位置，或者单击**浏览**以指定新位置，然后单击**保存**。

更改保留期

邮箱数据库的保留期为 30 天。在到期日期已过之后，系统会自动从缓存中删除这些数据库。要更改默认值，请执行以下操作：

1. 在结果窗格中，选择数据库。
2. 在“数据库”节点下的操作窗格中，单击**更改保留期**。此时将显示“更改保留期”对话框。
3. 在“新保留期”下拉列表中，在日历中选择新日期。

命令行参考

This feature is available in the Premium Edition

适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 提供命令行界面，您可以使用该界面来代替 GUI。

> **注意**如果没有指定用于远程执行 Exchange Management cmdlet 操作的有效用户凭据，命令将显示错误消息。

命令 ExchangeGre.CLI.exe 位于扩展的安装目录中:

C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin

语法

ExchangeGre.CLI.exe --Version | --Help

ExchangeGre.CLI.exe --List { --Cache [--EntriesCount *Number* | --Verbose]| --HistorySessions | --Mailboxes [--RecoveryDatabase *RecoveryDatabaseName*] | --BackupVersions { MailboxDB *DatabaseName* | Mailbox *MailboxName*} | --AllBackupDatabases }

ExchangeGre.CLI.exe --Remove { --Sessions *SessionID* [*SessionID*...]| --AllSessions | --RecoveryDatabase *DatabaseName* --Server *ComputerName*}

ExchangeGre.CLI.exe { --MountDB | --DismountDB } --RecoveryDatabase *RecoveryDatabase* --MailboxDB *Database* --Server *ComputerName*

ExchangeGre.CLI.exe --SetRP --RecoveryDatabase *RecoveryDatabaseName* --Server ComputerName--Period *NewDate*

ExchangeGre.CLI.exe --Details --Session *SessionID*

ExchangeGre.CLI.exe --Search { --Mailbox *MailboxName* | --Cache --Mailbox *MailboxName* --MailboxDB *DatabaseName*}

ExchangeGre.CLI.exe --ListOptions | --GetOption *OptionName* | --SetOption *OptionName* --Value *Value*

ExchangeGre.CLI.exe --StartSession --Restore --DismountRDB [true | false] --MailboxDB *DatabaseName* --BackupID *BackupVersion* --Server *ComputerName* --TargetLocation *TargetFolderPath*

ExchangeGre.CLI.exe --StartSession --Recovery --SrcMailbox *SourceMailboxName* --RecoveryDatabase *RecoveryDatabaseName* --MailboxDB *DatabaseName* { --RecoverWholeMailbox | --Filter [*FILTER_OPTIONS*]} --RecoveryTargetType [*ORG_MAILBOX* | *DIFF_MAILBOX* | *PST*]

ORG_MAILBOX

OrgLocation --KeepLatestMsg [true | false] *[RECOVERY_OPTIONS]*

DIFF_MAILBOX

DiffMailbox [*RECOVERY_OPTIONS*] --TargetMailbox *MailboxName*

PST

pst --PSTFileName *PSTFileNameWithPath*

RECOVERY_OPTIONS

--DiffLocation { --CreateNewFolder {NewFolderName | Default} | --ExistingFolder *FolderName*}

FILTER_OPTIONS

Subject="Term" | Contents="Term" | Attachments="Term" | Senders="SenderName" | Recipients="RecipientName" | Folders="FolderName" | StartDate="Date" | EndDate="Date"

描述

ExchangeGre.CLI.exe 是适用于 Microsoft Exchange Server 的 Granular Recovery Extension 的命令行界面。可以使用该界面来执行查询，还可以使用该界面来还原、装载、恢复和卸除数据库以及恢复单个项目和设置不同的恢复选项。

> **注意**不能同时使用命令行界面和图形用户界面。

选项

可用选项

选项
--Version
--Help
--HistorySessions | --Mailboxes [--RecoveryDatabase *RecoveryDatabaseName*] | --BackupVersions [--MailboxDB *MailboxDatabaseID* | --Mailbox *MailboxName*] | --AllBackupDatabases }
--Details --Session *SessionID*
--GetOption OptionName | --SetOption OptionName --Value Number
--AllSessions | --RecoveryDatabase *DatabaseName* --Server *ComputerName*}
--Dismount } --RecoveryDatabase RecoveryDatabaseName
--Cache --Mailbox *MailboxName* --MailboxDB *DatabaseName*}
false] --MailboxDB DatabaseName --BackupID BackupVersion --Server ComputerName --TargetLocation TargetFolderPath
--Filter [FILTER_OPTIONS]} --RecoveryTargetType [*ORG_MAILBOX* | *DIFF_MAILBOX* | *PST*]

示例

> **注意**为简单起见，下面的示例中省略了 ExchangeGre.CLI.exe 。

更改 Granular Recovery Extension 设置

要列出 Granular Recovery Extension 的可用选项，请指定：

--ListOptions

要获取选项“EnableDebugLogging”的值，请指定：

--GetOption EnableDebugLogging

要将选项“EnableDebugLogging”的值设置为“1”，请指定：

--SetOption EnableDebugLogging --Value 1

从 Data Protector 备份还原邮箱数据库

要列出备份数据库，请指定：

--List --AllBackupDatabases

要从 ID 为 2011/09/08-5 的 Data Protector 备份会话将邮箱数据库导入到临时还原位置 c:\restore ，请指定:

Microsoft Exchange 2010 Server:

```
--StartSession --Restore --DismountRDB false --MailboxDB DatabaseName --BackupID 2011/09/08-5 --Server computer.company.com --
TargetLocation "c:\Restore"
```

列出邮箱数据库信息

要列出邮箱数据库信息（例如数据库名称、恢复数据库 ID、服务器名称、装载状态、备份版本及其在粒度恢复缓存中所有数据库条目的大小，请指定：

```
--List --Cache
```

要列出有关恢复会话的更多特定详细信息（例如邮箱数据库名称、服务器名称、已还原的数据库文件的位置、数据库 ID、装载状态、备份版本、数据库大小和保留期），请指定：

```
--List --Cache --Verbose
```

要列出粒度恢复缓存中 20 个数据库条目的邮箱数据库信息，请指定：

```
--List --Cache --EntriesCount 20
```

要列出有关已完成的恢复会话的详细信息（例如会话 ID、会话名称、类型、会话的开始日期和时间以及结束日期和时间、装载状态），请指定：

```
--List --HistorySessions
```

要列出属于已备份的 Exchange 邮箱数据库一部分的所有邮箱，请指定：

```
--List --Mailboxes
```

要列出属于 Exchange 数据库“RDB_ExchangeGRE_dpexchange5_2011-11-15_1”粒度恢复缓存一部分的所有邮箱，请指定：

```
--List --Mailboxes --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1
```

要列出 Exchange 邮箱数据库“Mailbox Database 0474359329”的所有备份版本，请指定：

```
--List --BackupVersions --mailboxDB "Mailbox Database 0474359329"
```

要列出包含邮箱“Administrator”的已备份 Exchange 邮箱数据库的所有备份版本，请指定：

```
--List --BackupVersions --Mailbox Administrator
```

要列出已备份的 Exchange 邮箱数据库，请指定：

```
--List --AllBackupDatabases
```

要显示有关已完成的还原会话“ExchangeGRE_dpexchange5_2011-11-09_4”的详细信息，请指定：

```
--Details --Session ExchangeGRE_dpexchange5_2011-11-09_4
```

更改保留期

要将服务器“dpexchange5.company.com”上的恢复数据库“ExchangeGRE_dpexchange5_2011-11-09_4”的保留期更改为在 2012 年 1 月 15 日结束，请指定：

```
--SetRP --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --Server dpexchange5.company.com --Period 2012/01/15
```

装载邮箱数据库

要装载数据库，请指定：

```
--MountDB --RecoveryDatabase RecoveryDatabaseName --MailboxDB DatabaseName --Server computer.company.com
```

要将已还原的邮箱数据库“Mailbox Database 0474359329”装载到服务器“dpexchange5.company.com”上的恢复数据库“RDB_ExchangeGRE_dpexchange5_2011-11-15_1”，请指定：

```
--MountDB --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Server dpexchange5.company.com
```

要从粒度恢复缓存卸除邮箱数据库并在临时还原位置中保留文件，请执行以下操作：

```
--DismountDB --RecoveryDatabase RecoveryDatabaseName --MailboxDB DatabaseName --Server computer.company.com
```

要从 Exchange 服务器“dpexchange5.company.com”上的恢复数据库

“RDB_ExchangeGRE_dpexchange5_2011-11-15_1”卸除已装载的 Exchange 数据库“Mailbox Database 0474359329”，请指定：

```
--DismountDB --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Server dpexchange5.company.com
```

搜索邮箱

要在备份中搜索邮箱“john”，请指定：

```
--Search --Mailbox john
```

要在粒度恢复缓存中已装载的还原的数据库“Mailbox Database 0474359329”中搜索邮箱“john”，请指定：

```
--Search --cache --Mailbox john --MailboxDB "Mailbox Database 0474359329"
```

将项目恢复到原始位置

在下面的恢复示例中，将从装载到恢复数据库“RDB_ExchangeGRE_dpexchange5_2011-11-15_1”的邮箱数据库“Mailbox Database 0474359329”执行恢复。

要将邮箱数据库还原到临时还原位置，请执行以下操作：

```
--StartSession --Restore --DismountRDB true --MailboxDB DataBaseName --BackupID ID --Server computer.company.com --TargetLocation C:/restore
```

要将整个邮箱恢复到原始位置并将旧的电子邮件替换为最新版本，请指定：

```
--StartSession --Recovery --SrcMailbox mailbox_name --RecoveryDatabase DBName --MailboxDB mailbox_name --RecoveryWholemailbox --RecoveryTargetType orgMailbox --OrgLocation --KeepLatestMsg true
```

要将用户邮箱“Administrator”中的文件夹“inbox”恢复到原始位置但不覆盖新邮件，请指定：

```
--StartSession --Recovery --SrcMailbox Administrator --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Filter Folders=inbox --RecoveryTargetType orgMailbox --OrgLocation --KeepLatestMsg true
```

要仅将用户邮箱“john”中的文件夹“inbox”中主题为“market analysis”的电子邮件恢复到原始位置但不覆盖新邮件，请指定：

```
--StartSession --Recovery --SrcMailbox john --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Filter subject="market analysis"|folders="inbox" --RecoveryTargetType orgMailbox --OrgLocation --KeepLatestMsg true
```

将项目恢复到其他位置

要将整个邮箱恢复到新位置（例如新邮箱），请指定：

--StartSession --Recovery --SrcMailbox mailbox_name --RecoveryDatabase RecoveryDatabaseName --MailboxDB mailbox_name --RecoveryWholemailbox --RecoveryTargetType

要将整个用户邮箱“Administrator”恢复到邮箱“john”中的新文件夹“recovered mailbox”，请指定：

--StartSession --Recovery --SrcMailbox Administrator --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Filter Folders=inbox --RecoveryTargetType diffMailbox --DiffLocation --CreateNewFolder "recovered mailbox" --TargetMailbox john

要仅将用户邮箱“john”中的文件夹“inbox”中主题为“market analysis”的电子邮件恢复到不同的默认位置但不覆盖新邮件，请指定：

--StartSession --Recovery --SrcMailbox john --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Filter subject="market analysis"|folders="inbox" --RecoveryTargetType orgMailbox --OrgLocation --KeepLatestMsg true --DiffLocation --CreateNewFolder default

要仅将用户邮箱“john”中的文件夹“inbox”中主题为“market analysis”的电子邮件恢复到不同的（现有）文件夹“recovered data items”但不覆盖新邮件，请指定：

--StartSession --Recovery --SrcMailbox john --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --Filter subject="market analysis"|folders="inbox" --RecoveryTargetType orgMailbox --OrgLocation --KeepLatestMsg true --DiffLocation --ExistingFolder "recovered data items"

要将整个邮箱恢复到 .pst 文件，请指定:

--StartSession --Recovery --SrcMailbox mailbox_name --RecoveryDatabase RecoveryDatabaseName --RecoveryDatabase MailboxDB mailbox_name --RecoveryWholemailbox --RecoveryTargetType pst

要将整个用户邮箱“john”恢复到文件“C:\recovered\john.pst”，请指定：

--StartSession --Recovery --SrcMailbox john --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --MailboxDB "Mailbox Database 0474359329" --RecoverWholeMailbox --RecoveryTargetType pst --PSTfilename "C:\\recovered\\john.pst"

删除会话

要从粒度恢复缓存中删除 ID 为 2011/09/08-5 的已完成恢复会话，请指定：

--Remove --Session 2011/09/08-5

要从粒度恢复缓存中删除所有恢复会话，请指定：

--Remove --AllSessions

删除恢复数据库

要从服务器“dpexchange5.company.com”上的磁盘中删除邮箱数据库“RDB_ExchangeGRE_dpexchange5_2011-11-15_1”，请指定：

--Remove --RecoveryDatabase RDB_ExchangeGRE_dpexchange5_2011-11-15_1 --Server dpexchange5.company.com

Microsoft SharePoint Server 和 Granular Recovery Extension

本主题描述用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension，包括以下子主题:

有关受支持的 Microsoft SharePoint Server 版本的信息，请参阅支持矩阵。

适用于 **Microsoft SharePoint Server** 的 **GRE** 简介

This feature is available in the Premium Edition

本文档中提供的部分信息在适用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension 添加到基本 Microsoft SharePoint Server 帮助的自定义“帮助” 集合中也可用。该集合包含与 Granular Recovery Extension 相关的主题。您可以通过在管理中心网站的 Granular Recovery Extension 上下文中单击“帮助”图标来访问这些主题。

备份

使用以下某个备份解决方案备份 Microsoft SharePoint Server 数据：

- Data Protector Microsoft SharePoint Server 集成
- 基于 Data Protector Microsoft SharePoint Server VSS 的解决方案
- Data Protector Microsoft SQL Server 集成
- Data Protector Microsoft 卷影复制服务集成

恢复

Data Protector Granular Recovery Extension 的优点如下:

- 恢复粒度

  使用备份解决方案可还原的最小对象是 Microsoft SQL Server 数据库（**内容数据库**），其中可能包含多个网站的数据。相反，使用 Data Protector Granular Recovery Extension 可恢复的最小对象是单个网站项，例如: 日历项、日历、任务项、团队讨论项、文档、共享文档、文件夹、列表、库、声明、表单、报告模板、对象的元数据以及文档工作流状态。

- 集成到 Microsoft SharePoint Server 管理中心

  Granular Recovery Extension 完全集成到 Microsoft SharePoint Server 管理中心中。这使网站集管理员能够独立执行单个项目的恢复或将备份管理员的干预降至最低。

- 恢复多个网站

  意外的网站删除操作将不再成为一个问题，即使无法使用回收站功能恢复网站也是如此。Granular Recovery Extension 可以恢复包含多个子网站的整个网站。

- 易于搜索

  Granular Recovery Extension 高级和快速搜索可帮助您找到需要恢复的项。此搜索系统检查对象的元数据，从而使您可按文档类型、作者、日期等等过滤搜索。对象显示在对象树浏览器中。

- 恢复到不同位置

  通过 Granular Recovery Extension 可将对象恢复到不同的目标，例如，可将对象恢复到不同的网站、场及文件系统。

安装适用于 **Microsoft SharePoint Server** 的 **GRE**

This feature is available in the Premium Edition

为了恢复各个 Microsoft SharePoint Server 对象，请在 Microsoft SharePoint Server Central Administration 系统上安装 Data Protector Granular Recovery Extension for Microsoft SharePoint Server 。

相关主题

- 有关安装 Data Protector Granular Recovery Extension for Microsoft SharePoint Server 的信息，请参阅安装 Microsoft SharePoint Server 客户机。

配置适用于 Microsoft SharePoint Server 的 GRE

本节介绍为了避免恢复对象失败而必须遵循的配置步骤。

验证恢复 Web 应用程序的配置

1. 打开“管理中心”网页，然后单击**应用程序管理**选项卡。
2. 在“安全” >“常规安全” 下，单击“指定身份验证提供程序” ，然后单击“默认值”。
3. 确保“恢复 Web 应用程序”的设置与“管理中心应用程序”的默认设置相同。

配置 Data Protector 用户权限

1. 启动 Data Protector GUI (**Data Protector Manager**)。
2. 在“上下文”列表中，选择**用户**。
3. 确保向运行 Windows SharePoint Services Timer 服务的用户帐户分配 Data Protector“启动还原” 和“查看私有对象” 的用户权限。

> **注意**在创建已配置私有访问类型和备份对象所有者的备份规范后，“查看私有对象”用户权限很有用。这是执行过备份的帐户或**所有权**备份选项中指定的帐户。如果此用户帐户与运行 Windows SharePoint Services Timer 服务的用户帐户不同，则无法在“恢复缓存管理”中访问私有备份对象。

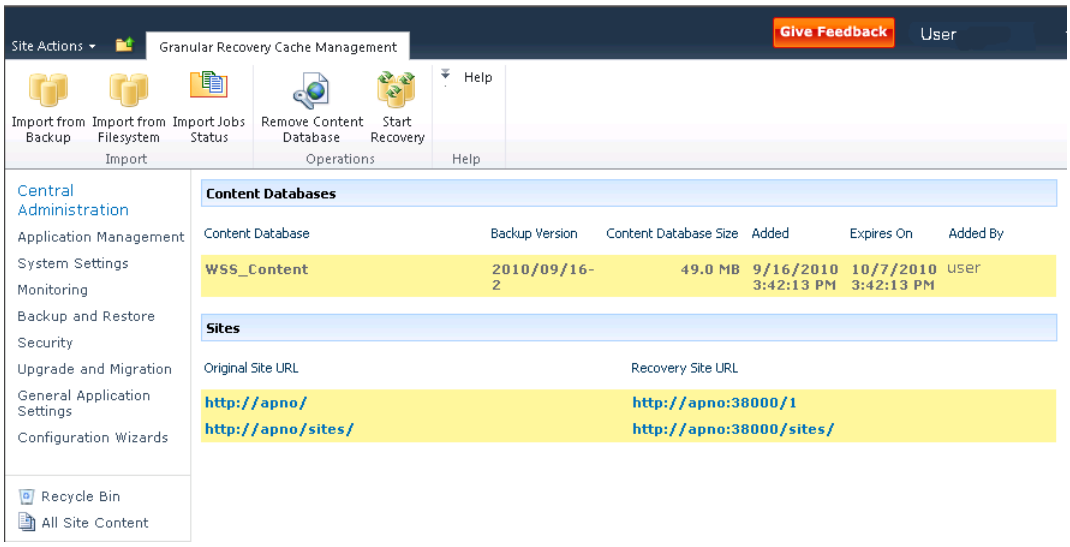
配置 Data Protector 备份规范

- 创建 VSS 可传输备份时，确保未选择“跟踪复本以用于即时恢复”选项。
- 要防止 Data Protector 备份“Granular Recovery 缓存管理”中的内容数据库 (也就是说防止 Data Protector 两次备份相同内容数据库)，请根据配置进行以下操作:
  - 如果 Microsoft SharePoint Server 和 Data Protector Granular Recovery Extension 使用的 Microsoft SQL Server 实例相同，则:

    创建备份规范时，请选择单独的内容数据库，而不要选择客户端、Microsoft SQL Server 实例或 Microsoft 卷影副本写入程序。

    由 Data Protector Granular Recovery 还原的内容数据库称为 *OriginalName_DataProtectorSessionID*。

    选择内容数据库

    > **注意**如果已选择具有单独内容数据库的备份规范，则在场管理员每次添加新内容数据库时，您都需要在备份规范中加入新添加的内容数据库。

  - 如果将一个单独的 Microsoft SQL Server 实例用于粒度恢复目的，则将此系统指定为“从备份导入”过程的目标 Microsoft SQL Server。

    确保从备份规范中排除此系统。

验证 Internet Information Services 应用程序池的配置

“恢复 Web 应用程序”和“SharePoint 管理中心”应用程序池都使用相同的 Microsoft SharePoint Server 用户帐户。

为了将项目恢复到文件系统，请验证是否已向这些应用程序池中指定的用户授予了足够的权限。确保让此用户完全控制文件系统。

要验证在“恢复 Web 应用程序”或“SharePoint 管理中心”应用程序池中配置的用户帐户，请执行以下操作:

1. 连接到 Microsoft SharePoint Server 管理中心系统。
2. 在“开始”菜单中，单击“控制面板”>“系统和安全”>“管理工具”，双击“Internet 信息服务 (IIS) 管理器”。
3. 打开“应用程序池”页面。
4. 右键单击一个应用程序池，然后单击**高级设置**。
5. 在“进程模型”下，验证 Microsoft SharePoint Server 用户帐户的“身份”。

备份适用于 GRE 的 Microsoft SharePoint Server 数据

按照 Data Protector 备份解决方案文档中所述备份 Microsoft SharePoint Server 数据。请参阅集成。

注意: 适用于 Microsoft SharePoint Server 的 Granular Recovery Extension 使用相同过程恢复不同的对象。恢复过程与备份类型无关。

注意事项

- 建议通过 VSS 可传输备份还原大于 10 GB 的内容数据库。
- 如果已使用“ZDB 至磁盘 + 磁带”配置了 VSS 可传送备份，则适用于 Microsoft SharePoint Server 的 Granular Recovery Extension 将从用于还原的磁盘中选择内容数据库版本。这种备份类型不需要额外的磁盘空间，并且适合较大的内容数据库。完成还原会话所需的时间也较少。

使用 GRE 恢复 Microsoft SharePoint Server 数据

每个网站都将其数据存储在一个 Microsoft SQL Server 数据库（**内容数据库**）中。要恢复站点项目，请执行以下操作:

1. 导入
   a. 还原**:** 将内容数据库从备份文件还原到 Microsoft SQL Server 系统中的临时位置。
   b. 装载**:** 向 Microsoft SharePoint Server 提供还原的内容数据库（**恢复内容数据库**）。这将创建一个临时网站（**恢复网站**）。
2. 恢复**:**
   将网站项从恢复网站传输到原始网站或选定的其他位置。
3. 卸除**:**
   从 Microsoft SharePoint Server 卸除恢复内容数据库。还可以从磁盘删除数据库。

启动 Data Protector Granular Recovery Extension GUI

1. 使用 Microsoft SharePoint Server **场管理员**用户帐户登录到 Microsoft SharePoint Server 管理中心系统。
2. 连接到“管理中心”网页。
3. 查找 **Data Protector Granular Recovery Extension**。
4. 单击**粒度恢复缓存管理**。此时将显示“恢复缓存管理”页面。

   Granular Recovery Cache 显示当前哪些恢复内容数据库装入到 Microsoft SharePoint Server。最初，Granular Recovery Cache 为空。有关该功能的高级说明，请参阅以下内容:

   a. 从备份导入

      使用 Data Protector 备份解决方案备份内容数据库之后，可使用“从备份导入”将数据库还原到临时位置，以及将数据库装载到 Microsoft SharePoint Server。

   b. 从文件系统导入

      如果已将内容数据库还原到文件系统，可使用**从文件系统导入**将内容数据库装载到 Microsoft SharePoint Server。

   c. 导入作业状态

      通过此功能可监视导入作业（从备份或从文件系统导入内容数据库）状态。

   d. 删除内容数据库

      此功能从 Microsoft SharePoint Server 卸除恢复内容数据库（从 Granular Recovery 缓存中删除内容数据库），然后从磁盘删除数据库文件。

   e. 启动恢复

      浏览和恢复存储在恢复内容数据库中的对象。原始网站中也为网站集管理员提供了此选项。单击设置图标，然后单击“网站设置”。在“网站设置”页面上，找到“Micro Focus Data Protector Granular Recovery Extension”，然后单击“粒度恢复”。

   f. 原始网站 **URL**

      指向原始网站的链接。

   g. 恢复网站 **URL**

      指向恢复网站的链接。

从备份导入内容数据库

在导入内容数据库之前，请检查以下内容:

先决条件

- 在目标 Microsoft SQL Server 系统上，需要有足够的磁盘空间容纳要导入的内容数据库。

注意事项

- 如果网站已存在于恢复缓存管理中，并且对同一个网站执行“从文件系统导入”会话，则 URL 更改如下：
  - http://computer.company.com:38000/OriginalNameSequenceNumber
  - http://computer.company.com:25884/SequenceNumber

    （根网站）
- 如果原始网站不存在于恢复缓存管理中，则网站 URL 不会更改。
- 如果不存在根网站，则“恢复缓存管理”将在还原会话过程中使用空字符串，并且根网站的 URL 将更改为：

  http://computer.company.com:25884/SequenceNumber
- 如果网站 URL 超过 260 个字符，则无法导入两个备份版本。
- 如果目标路径超过 260 个字符，则无法执行恢复。您必须选择其他位置。

要导入内容数据库，请执行以下操作:

1. 在“恢复缓存管理”页面中，单击**从备份导入**。随后将显示“网站集选择 (Site Collection Selection)”页面。选择要恢复的网站的内容数据库，然后单击**继续**。

2. 在“备份版本选择”页面中，选择要还原的内容数据库版本，然后单击**继续**。
3. 将显示“内容数据库恢复”页面: 在 **SQL Server** 下拉列表中，选择目标 Microsoft SQL Server 实例。可以通过指定新路径更改默认还原位置。默认为 C:\Restore 。

> **注意**如果在群集中配置 Microsoft SQL Server，请确保还原位置位于 Microsoft SQL Server 群集共享磁盘上。

4. 单击**导入内容数据库**。
5. （可选）要监视作业状态，请单击**继续**。此时将显示“Granular Recovery 导入作业状态 (Granular Recovery Import Job Status)”页面：
6. 单击**恢复缓存管理**以返回该页面。

   此时内容数据库即装入 Microsoft SharePoint Server。

> **注意:** 内容数据库装载到 Microsoft SharePoint Server 后，即向网站集管理员分配“执行内容恢复”任务。

从文件系统导入内容数据库

先决条件

- 必须将内容数据库还原到文件系统。
- 必须向运行 SharePoint Timer Service 的用户帐户授予对内容数据库的完全控制权限。

注意事项

- 无法从网络共享导入 Microsoft SQL Server Database Primary Data Files 和所有事务日志文件。
- 如果网站已存在于恢复缓存管理中，并且对同一个网站执行“从文件系统导入”会话，则 URL 更改如下：
  - http://computer.company.com:38000/OriginalNameSequenceNumber
  - http://computer.company.com:25884/SequenceNumber

    （根网站）
- 如果原始网站不存在于恢复缓存管理中，则网站 URL 不会更改。
- 如果不存在根网站，则“恢复缓存管理”将在还原会话过程中使用空字符串，并且根网站的 URL 将更改为：

  http://computer.company.com:25884/SequenceNumber

要导入内容数据库，请执行以下操作**:**

1. 在“恢复缓存管理”页面上，单击**从文件系统导入**。
2. 在“输入内容数据库数据”页面上，指定 Microsoft SQL Server 数据库主数据文件 AbsolutePath.mdf 和所有事务日志文件 AbsolutePath.ldf 的位置。单击“添加”，然后单击“继续”。
3. 在 **SQL Server** 下拉列表中，选择目标 Microsoft SQL Server 实例。
   随后将自动填充内容数据库名称和版本。或者，您也可编辑数据库的名称和版本以更好地满足您的需要。
4. 单击**导入内容数据库**。
5. （可选）要监视作业状态，请单击**继续**。
   此时将显示“Granular Recovery 导入作业状态 (Granular Recovery Import Job Status)”页面：
6. 单击**恢复缓存管理**以返回该页面。
   此时内容数据库即装入 Microsoft SharePoint Server。

> **注意:**内容数据库装载到 Microsoft SharePoint Server 后，即向网站集管理员分配“执行内容恢复”任务。请参阅执行内容恢复任务。

执行内容恢复任务

先决条件

- 将内容数据库装载到 Microsoft SharePoint Server。请参阅从备份导入内容数据库和从文件系统导入内容数据库。
- 您必须是要恢复的网站的**网站集管理员**。有关如何将用户添加到网站集管理员组的详细信息，请参见 Microsoft SharePoint 文档。

要执行“执行内容恢复”任务，请执行以下操作:

1. 单击“执行内容恢复”任务中的链接。将显示“浏览并选择对象”页。
2. 按照提示操作。

恢复网站项目

先决条件

- 在所有前端 Web 服务器系统上，都需要有足够的磁盘空间容纳要恢复的网站项目。默认位置为 C:\Recovery 。要更改默认路径，请参阅更改 Data Protector Granular Recovery Extension 设置。
- 您必须是要恢复的网站的**网站集管理员**。有关如何将用户添加到网站集管理员组的详细信息，请参见 Microsoft SharePoint 文档。
- 必须将恢复内容数据库装载到 Microsoft SharePoint Server。
- 如果原始站点已不存在，则请不通过模板创建与原始站点语言相同的站点集合。使用**覆盖现有**恢复模式。您必须是要在“恢复缓存管理”中恢复的网站的**场管理员**。如果所恢复的网站中有子网站，则快速链接、顶部导航栏将重新安置在列表末尾。
- 确保网站 URL 长度不超过 260 个字符：

  如果使用**如果存在则重命名**恢复模式，则 URL 路径的长度不应超过 255 个字符。

注意事项

- 如果目标上已存在要恢复的数据，则根据恢复模式需注意以下各项：
  - **如果存在则重命名**: 以不同名称 *OriginalName* _DPGRE_ *Timestamp* 恢复文件和文件夹项目。

    例如，假定在 2012 年 11 月 17 日 10:59:35 开始恢复文件 wizard.txt 。系统将以名称 wizard_DPGRE_20121117-105935.txt 恢复该文件。

    将不会恢复其他项目（例如表单模板、文档和任务项目），也不会将其重命名到原始位置。

    不能在恢复过程中重命名列表项。
  - **保留现有**: 不恢复项目，现有项在目标位置保持不变。
  - **覆盖现有**: 以原始名称恢复项目，替换现有项目。例如，以备份数据中的 Microsoft SharePoint Server 项目（文档库）覆盖现有的这些项目。不覆盖的只有列表和网站。
- 如果目标中不存在要恢复的数据，则用原始名称恢复这些数据。
- 如果将列表项（声明、联系人、链接、日历或任务）恢复到其他位置，或恢复到其他场两次，则根据恢复模式：
  - **覆盖现有**: 以相同的名称和不同的 ID 复制列表项目。删除同名的项目。
  - **如果存在则重命名**: 重命名列表项目，即使这些类型的项目不支持重命名也是如此。
- 如果以**覆盖现有**恢复模式恢复包含附件和回复的讨论项目或包含答复的调查，则会覆盖项目，但不会恢复附件、回复或答复。要避免数据丢失，请在启动恢复会话之前，删除附件、答复或回应。
- 可以同时执行多个恢复会话，但选择相同项目进行恢复的情况除外。
- 多个场管理员和网站集管理员可以同时浏览对象。
- 要恢复文档工作流状态，请确保您在目标网站上创建了模板和关联。仅当恢复到原始位置以及原始项目存在时，才能恢复工作流状态。
  - 无法恢复工作流历史记录。
- 不恢复项目的唯一用户权限。恢复的项目继承要向其恢复项目的目标容器类型的权限。
- 要恢复网站集或子网站，需要手动创建目标网站集或子网站。目标必须使用与要恢复的网站集或子网站相同的模板，并且必须使用**覆盖现有**恢复模式。

支持的项目

可以使用 Data Protector Granular Recovery Extension 恢复以下受支持的 Microsoft SharePoint Server 项目:

- 库：
  - 文档库
  - Wiki 页库
  - 报告库
  - 资产库
  - 图像库
  - 转换管理库
- 通信：
  - 公告
  - 联系人
  - 讨论板
- 跟踪：
  - 链接
  - 日历
  - 任务
  - 项目任务
  - 问题跟踪
  - 调查

- 自定义列表
- 用户信息列表
- 页面与网站：
  - 第
  - 网站
  - 发布页面
  - 博客模板网站：发布、注释、类别
  - 会议模板网站：会议、日程、与会者、决定、会议目标、文本框、必带物品、主页库

> **注意**支持对 SharePoint 列表（这些列表使用大于 10000 的自定义 ID 值进行自定义）执行粒度恢复。但是，粒度恢复能否成功取决于列表的自定义程度。

要恢复站点项目，请执行以下操作:

1. 在“恢复缓存管理”页上，选择要恢复的内容数据库和网站。请注意，一个内容数据库可能包含多个网站的数据。

   > **提示**要从多个网站恢复项目，请在按住 **Ctrl** 的同时在“网站 (Sites)”下选择特定网站，然后单击**开始恢复 (Start Recovery)**。还可以在按住 **Shift** 的同时在“网站 (Sites)”下选择一组网站，然后单击**开始恢复 (Start Recovery)**。

   > **注意**此外，可通过以下方式启动恢复会话：
   >
   > - 连接到原始网站。
   >
   >   单击“设置”图标 >“网站设置”，然后单击“网站设置”页上“Micro Focus Data Protector Granular Recovery Extension”下面的“粒度恢复” 。
   > - 通过执行网站任务。请参阅执行内容恢复任务。

2. 在“浏览并选择对象”页面上，选择要恢复的网站项。

   > **注意:** 可通过单击项目名称预览所有项。

   > **提示:**
   > - 要选择多个列表视图项目，请在按住 **Ctrl** 的同时选择特定项目。或者，也可以在按住 **Shift** 的同时选择一组项目。
   > - 可以使用**高级搜索**筛选项目。例如，在**结果类型**中，选择 **Microsoft Office Word 文档**。在**添加属性限制**中，选择一个属性，然后单击**搜索**。
   >   要选择多个列表视图项目，请在按住 **Ctrl** 的同时选择特定项目。或者，也可以在按住 **Shift** 的同时选择一组项目。

   单击**继续**。

3. 在“恢复对象 (Recovery Objects)”页面上显示所选的网站项。

   > **注意:恢复模式**下拉列表提供以下选项：
   >
   > - **如果存在则重命名**: 以新名称 *OriginalName*_DPGRE_*Timestamp* 恢复文件和文件夹等项目。
   > - **保留现有**: 不恢复项目，现有项在目标位置保持不变。
   > - **覆盖现有**: 恢复的项目替换现有项目。

   > **提示**恢复周期性事件（例如“日历”中的每周小组会议）时，请在选择**覆盖现有**恢复模式之前确保删除所有周期性事件。

临时路径选项指定 Microsoft SharePoint Server 系统上用于执行恢复操作的位置。

注意至下拉列表指定恢复的目标位置：

- **原始位置**: 项目将恢复到原始网站中的原始位置。此选项不适用于使用 Rename If Exists 恢复网站或子网站。
- **其他位置**: 项目将恢复到不同网站或原始网站中的不同位置。如果原始网站不再存在，则使用此位置。
- **其他场**: 项目将恢复到不同的目标场。
- **文件系统**: 项目将恢复到文件系统中的某个目录。仅对文件和文件夹提供此选项。

- 如果选择**其他位置**，则显示“恢复到其他位置”对话框。

  在“网站 (Site)”下拉列表中，选择目标网站。

  如果选择**适用于相同类型的所有项目**选项，则相同类型的项目（例如日历项目）将恢复到相同位置。

  单击**确定**。

  提示“恢复到其他位置 (Recovery to other location)”对话框中列出的网站是您对其拥有足够权限的网站。例如，如果您是网站集管理员，则需要向您授予“读取配置数据库”权限。

- 如果选择**其他场**，则显示“恢复到其他场”对话框。

  指定目标场和要使用的 Windows 域用户帐户。

  如果选择**适用于相同类型的所有项目**选项，则相同类型的项目（例如日历项目）将恢复到相同的场。

  单击**连接**。

- 如果选择**文件系统**，则显示“恢复到文件系统”对话框。

  在**路径**中，指定目标目录。

  指定网络共享作为目标时，请确保：

  - 向启动恢复会话的用户授予读取、写入和更改权限。
  - 向网络共享授予所有必要权限。授予为用户帐户 (在“Web 恢复应用程序”和“SharePoint 管理中心 v4”应用程序池中配置该用户帐户) 指定的相同权限。有关详细信息，请参阅验证 Internet Information Services 应用程序池的配置。
  - 可从运行 Microsoft SharePoint Foundation Web 应用程序的系统中访问共享，其中已启动恢复会话。

  指定文件夹作为目标时，请确保:

  - 可从运行 Microsoft SharePoint Foundation Web 应用程序的系统中访问该文件夹。
  - 向启动恢复会话的用户授予读取、写入和更改权限。

如果选择**适用于所有文件和文件夹**选项，则所有文件和文件夹将恢复到相同目录。

单击**确定**。

4. 单击**启动恢复**。

恢复完成后，即可在指定目标找到所恢复的项目。

从缓存删除内容数据库

内容数据库在三周内可用，此后它们将自动从缓存中删除。要手动从恢复缓存中删除内容数据库，请执行以下操作：

1. 在“恢复缓存管理”页面上，选择要删除的内容数据库，然后单击**从恢复缓存删除**。随后将显示“从恢复缓存删除”页。
2. 要将内容数据库文件保留在磁盘上，请清除**从磁盘删除文件**选项。单击**删除**。

监视粒度恢复导入作业

完成以下步骤：

1. 连接到“管理中心”网页。
2. 找到 **Data Protector Granular Recovery Extension**，然后单击“Granular Recovery 导入作业状态”。随后将显示“Granular

Recovery 导入作业状态”页。

3. 启动内容数据库导入会话后，Data Protector Granular Recovery Extension 即开始监视导入作业的进度。

   根据需要，在完成恢复作业并且不再需要作业状态之后，单击**清除历史记录**。

   要停止正在执行的操作，请单击**中止**。

更改 Data Protector Granular Recovery Extension 设置

在粒度还原会话期间，内容数据库首先还原到选定 Microsoft SQL Server 系统上的一个临时位置 (默认位置为: C:\Restore)。

恢复网站项目之前，会将其复制到 Microsoft SharePoint Server 系统上的一个临时位置 (默认位置为: C:\Recovery)。

完成以下步骤：

1. 要更改这些默认位置，请连接到“管理中心”网页。
2. 在“Granular Recovery 设置”页面上，输入新的还原位置或临时恢复位置，然后单击**确定**。

命令行参考

This feature is available in the Premium Edition

根据 SharePoint Server 的版本，使用位于以下位置的 HP.SharePoint.GranularRecovery.CLI.exe 命令行工具:

- 对于 **Microsoft SharePoint Server 2010:**
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN
- 对于 **Microsoft SharePoint Server 2013** 及更高版本**:**
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN

要显示对选项及其用法的说明，请运行以下命令:
HP.SharePoint.GranularRecovery.CLI.exe --help 。

示例

注意: HP.SharePoint.GranularRecovery.CLI.exe 在以下示例中省略 (为了简单起见)。

从 Data Protector 备份还原内容数据库

- 要列出名为 WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193 的内容数据库的所有备份版本，请指定:

  --ListBackupVersions --ContentDB=WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193

监视作业进度

- 要列出内容数据库中已启动的所有作业，请指定：

  --ListJobs

- 要通过将备份版本 " 2010/04/20-4 " 中的内容数据库导入到默认还原位置 C:\Restore 来启动还原作业，请指定:

  --StartImportJob

  --ContentDB WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193

  --BackupID "2010/04/20-4" –-Server computer

  –-Instance OFFICESERVERS --TargetLocation C:\Restore

  注意在已使用默认实例安装 Microsoft SQL Server 的情况下，要成功导入内容数据库，请将 OFFICESERVERS 替换为以下项之一:

  - 实例名称
  - DEFAULT
  - MSSQLSERVER

  您也可以将实例名称留空以确保 Data Protector 使用其正确名称。

- 假定您要通过将文件系统中的内容数据库导入到 Microsoft SharePoint Server 的默认还原位置 C:\Restore 来启动还原作业。

  如果 Microsoft SQL Server 数据库主数据文件为 WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193.mdf ，SQL Server 事务日志文件为 WSS_Content054a5bfa-f23c-49b8-8f78-e0b3ce00b193_log.LDF ，请指定:

  --StartImportJob

  --ContentDB WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193

  --BackupID "2010/04/20-4" –-Server computer

  –-Instance OFFICESERVERS

  –-Files="C:\Restore\WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce

  00b193.mdf";"C:\Restore\WSS_Content054a5bfa-f23c-49b8-8f78-e0b

  3ce00b193_log.LDF"

--TargetLocation C:\Restore

验证目标位置磁盘空间大小

- 要检查默认还原位置 C:\Restore 中的可用磁盘空间，请指定:

  --QueryServerInfo --Server computer --Instance OFFICESERVERS --TargetLocation C:\Restore

  此命令还可列出树结构中所有内容数据库文件的位置。

列出内容数据库

- 要列出恢复缓存中的所有内容数据库（包括备份版本），请指定：

  --ListCache --All

- 要列出内容数据库的详细信息，请指定：

  --ListCache --Verbose

删除还原作业

- 要删除所有还原作业状态，请指定：

  --DeleteAllJobs Confirm

- 要删除特定还原作业，请指定：

  --DeleteJob= *作业 ID*

将网站项恢复到原始网站

- 假定要恢复已从网站 http://computer.company.com:25884/sites/AnikyB 备份的网站项目 /Shared Documents/Document.txt 。假定恢复网站为 http://computer.company.com:38000/sites/AnikyB 。要将项目恢复至原始位置，请指定：

  --Recover

  --Source http://computer.company.com:38000/sites/AnikyB

  --Destination http://computer.company.com:25884/sites/AnikyB

  --TempLocation="C:\Recovery"

  --Items "/Shared Documents/Document.txt"

  恢复会话将完成并显示以下消息：

  ```
  恢复结束，对象状态: 对象: [/Shared Documents/Document.txt] 目标: [/Shared Documents/Document_MOSSGR_24032010-024302.txt] 状态: 已完成 状态详细信息: [recovered to [http://computer.company.com: 25884/sites/AnikyB//Shared Documents]]
  ```

将网站项恢复到其他位置

- 要将网站项目 "/Shared Documents/Document.txt" 恢复到“我的文档”，请指定:

  --Recover

  --Source http://computer.company.com:38000/sites/AnikyB

  --Destination http://computer.company.com:25884/sites/AnikyB

  --TempLocation="C:\Recovery"

  --Items "/Shared Documents/Document.txt:/My Documents"

从缓存删除内容数据库

- 要从缓存删除某个数据库，请指定：

  --RemoveFromCache --ContentDB DatabaseName--BackupIDBackupID

- 要从缓存删除所有内容数据库，请指定：

  --RemoveFromCache --All

从磁盘删除内容数据库

- 要在从缓存中删除内容数据库后从磁盘删除内容数据库，请指定：

  --RemoveFromCache --ContentDB DatabaseName --DeleteFiles

设置内容数据库自动删除

内容数据库将保存 21 天（默认保留期），之后将从缓存中删除。

- 要显示在将内容数据库从缓存中删除前其保持可用的时间（天数），请指定：

--GetOption RecoveryDatabaseAutoCleanupDays

- 要设置将内容数据库从缓存中自动删除前其保持可用的时间，请指定：

  --SetOption RecoveryDatabaseAutoCleanupDays --Value number_of_days

从内容数据库导出项目

- 要从内容数据库导出一个项目，请指定：

  --Export --Source source --Location path

  --Item item

- 要从内容数据库导出多个项目，请指定：

  --Export --Source source --Location path

  --Items item1item2item3

> **注意**无法导出工作流。

列出导出的项目

- 要列出导出的项目，请指定：

  --ListExport --Location

从内容数据库导入项目

- 要从内容数据库导入一个项目，请指定：

  --Import --Destination destination --Location path

  --Item item

- 要从内容数据库导入多个项目，请指定：

  --Import --Destination destination --Location path

  --Items item1item2item3

> **注意**无法导入工作流。

显示 Microsoft SharePoint 场信息

- 要显示场的详细信息，如名称、显示名称、地址、类型名称、角色、版本、状态和此场中运行的所有服务，请指定：

  --FarmInfo

显示内容数据库信息

- 要显示内容数据库信息（例如：办公服务器、共享服务、SharePoint 配置、共享服务搜索、恢复 Web 应用程序、共享服务内容、共享管理内容、内容数据库名称），请指定：

  --DatabaseInfo

显示网站列表

- 要显示 Web 应用程序名称、网站 URL、内容数据库名称以及此内容数据库中的所有网站，请指定：

  --ListSites

浏览网站

- 要浏览“我的网站”结构和项目（例如：表单、列表、模板库、母版页样式库、个人文档、共享文档、共享图片、网站模板库、用户信息列表和 Web 部件库），请指定：

  --BrowseSite --Site http://ivanka/personal/anikyb

显示 Granular Recovery Extension 版本

- 要显示 Granular Recovery Extension 版本，请指定：

  --Version

VMware 和 Granular Recovery Extension

本节介绍适用于 VMware vSphere 的 Data Protector Granular Recovery Extension (GRE)。

包括以下主题:

适用于 VMware 的 GRE 简介

Data Protector Granular Recovery Extension (GRE) 使用 Data Protector 虚拟环境集成来还原数据；此扩展只是一款恢复解决方案。

本主题提供有关 Data Protector GRE 的以下信息:

- GRE 功能
- 恢复流程

可以使用 HTML5 GRE Web 插件用户界面访问 GRE 插件。

GRE 功能

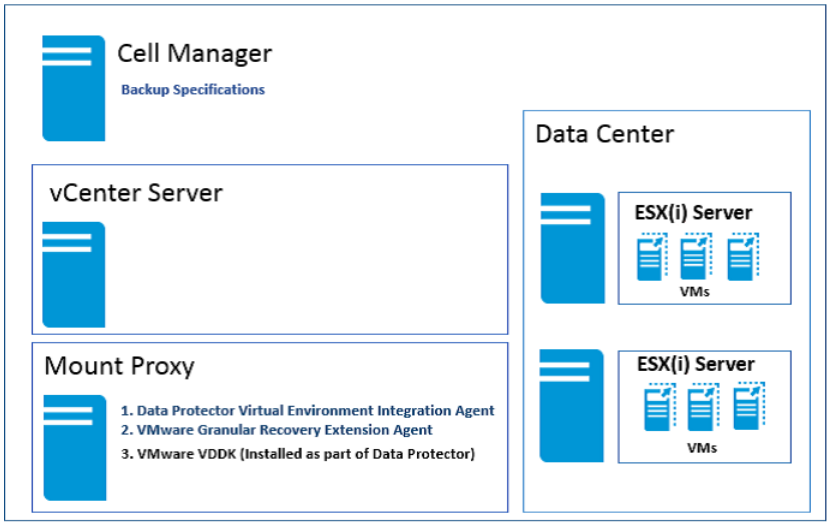
- **还原和恢复:** 适用于 VMware vSphere 的 Data Protector GRE 可将 VMDK 还原到临时的还原位置 (装载代理系统)，然后从已还原的 VMDK 恢复各个 VMware 虚拟机文件。此功能在 HTML5 GRE Web 插件中可用作非缓存还原和恢复。
- **呈现和恢复**: 适用于 VMware vSphere 的 Data Protector GRE 不会将 VMDK 文件还原到临时位置 (装载代理) 以恢复各个文件。相反，它会在临时位置（装载代理）呈现 VMDK 以恢复各个文件。可以从 VMDK 执行文件恢复，而无需将 VMDK 文件还原到临时位置（装载代理）。适用于 VMware vSphere 的 GRE 可直接将 VMDK 装载到装载代理主机，并使用户能够浏览磁盘以及选择要恢复的文件。因此，对于呈现，不必还原任何特定备份的磁盘（或整个链）以恢复文件。此功能在 HTML5 GRE Web 插件中可用作缓存恢复。

> **注意**无论是备份到智能缓存设备、StoreOnce Catalyst、重复数据删除存储和数据域设备，还是从驻留在 3PAR 存储上的阵列快照执行备份，均称为“缓存备份”，其他备份则称为“非缓存备份”。

恢复流程

Data Protector HTML5 GRE Web 插件可让用户从虚拟机磁盘执行文件恢复。使用该插件执行文件恢复操作之前，必须配置 Data Protector GRE 环境。下图描述了标准 GRE 环境。

Data Protector 组件显示为蓝色，VMware 组件显示为黑色。



满足先决条件

- 确保在 vCenter 中配置了 HTML5 GRE Web 插件的 IP 地址。
- 在链接模式配置中，并非在所有 vCenter 上都应注册 HTML5 VMware GRE 插件。
- 必须有“用户配置”用户权限才能添加用户。
- 启用调试。
- 确保已安装最新的 Data Protector 补丁。

注意事项

- 适用于 VMware vSphere 的 Granular Recovery Extension 不支持跨平台恢复。不支持从 Windows 虚拟机将 Windows 虚拟机文件恢复到 Linux 虚拟机，也不支持其他恢复方法。但是，通过安装 FUSE，可以使用 Linux 代理恢复 Windows 虚拟机。请注意，此方案不会保留 ACL。

  支持将 Windows 虚拟机磁盘还原到不同的装载代理系统平台。

- 请考虑具有两个或更多 vCenter 且每个 vCenter 属于不同 Data Protector 单元配置的 VMware vSphere HTML5 Web Client。如果每

个 Data Protector 单元的用户列表中包含同一个用户但具有不同的权限集，该用户将从 Data Protector 单元获取特权，并且所选 vCenter 的 VMware GRE 代理首先开始在该单元上运行。
- 如果 vSphere vCenter 中的虚拟机名称在完整备份之后已更改，则无法从增量备份和差异备份恢复虚拟机。
- 如果两个操作员通过 VMware vSphere HTML5 Web Client 使用同一个用户帐户以远程方式连接并同时浏览虚拟机磁盘的其中一个分区，则在装载第一个分区之后，将卸除第二个分区。不支持并行装载分区。
- *仅 StoreOnce Catalyst 和数据域设备*: 扩展将显示整个还原链。浏览文件时，所显示的对象包含整个还原链：对象的完整备份和任意数量的相关增量备份。
- 浏览包含许多文件和子文件夹的文件夹时，您可能会遇到性能不佳的问题。
- 要在目标虚拟机和装载代理系统上保留所有权和权限位 UID/GUID，必须同时映射两者。网络共享服务器必须配置正确才受支持。
- 不支持来宾虚拟机上的非分区磁盘。
- 只能对分区类型 ID 设置为 8E 的 LVM 卷执行 GRE 操作。此外，具有 LVM 分区的磁盘需要 kpartx。
- 如果无法从装载代理访问 ESX Server，则您需要修改主机文件并添加 ESX 主机名和 IP 地址或解析 ESX Server 的主机名。

注意需要在添加卷组之前对磁盘进行分区。只能考虑 `fdisk –l` 中报告的分区。

注意Granular Recovery Extension 界面不支持 Windows Internet Explorer 8。
有关受支持环境的列表，请参阅最新支持矩阵。

3PAR 存储系统

- 要从 3PAR 副本执行 GRE 操作，装载 ESX Server 和生产 ESX Server 必须存在于同一个 3PAR 区域中。
- 通过在 Cell Manager 上执行以下命令，配置具有一个复本且用于 Cell Manager 中的 GRE 的 3PAR 阵列: omnidbzdb --diskarray 3PAR --ompasswd --add <3PAR array CIM server name/ip> --user <CIM server login name> --passwd <CIM server password>
- 要使用 Linux 装载代理为 Windows 来宾操作系统执行 GRE 操作，备份会话必须具有已备份的操作系统磁盘，且必须选择同一个磁盘用于创建新请求和要浏览的磁盘。
- 如果无法从装载代理访问 ESX Server，则您需要修改主机文件并添加 ESX 主机名和 IP 地址或解析 ESX Server 的主机名。

限制

适用于 VMware vSphere 的 Data Protector Granular Recovery Extension (GRE) 具有某些限制。

恢复

- 要在 Linux 装载代理上对 Windows Server 2012 和 Windows Server 2012 R2 执行 GRE，请使用 SLES 上的 NTFS-3G（适用于 Linux 的 NTFS 驱动程序）版本 2011。要下载 NTFS-3G 驱动程序，请访问以下链接：
  https://www.rpmfind.net/linux/rpm2html/search.php?query=ntfs-3g
- 在 Linux 上，备份计算机和装载代理必须是两台不同的计算机。
- 不能执行以下操作：
  - 恢复空文件夹。
  - 从 Windows 2012 复原文件系统 (ReFS) 执行文件恢复。
  - 恢复具有较长路径名称的文件。

注意对于在装载代理上装载的磁盘，必须确保装载点和所选磁盘中的文件路径不超过 260 个字符。

- 如果目标计算机没有足够的磁盘空间，则在恢复详细信息中列出跳过的和失败的文件。
- 在恢复期间在 Linux 目标虚拟机或 Linux 装载代理系统上保留 POSIX ACL。
- 重新启动 GRE 装载代理主机时，为 LVM 磁盘的请求 (至少被浏览了一次) 创建的装载点将变得无效。因此，必须重新创建这些请求才能执行 GRE 操作。
- 对于 HTML5 GRE Web 插件，不支持从动态磁盘执行 GRE。
- 从 Data Protector 9.03 和更低版本对驻留在数据存储 (使用多个 3PAR LUN 创建) 上的 VM 执行的 3PAR ZDB 备份不支持粒度恢复。
- 在 Linux 上浏览逻辑卷取决于文件系统版本 (内核版本)；旧版内核无法装载最新文件系统。因此，装载代理操作系统的版本不得低于备份计算机的操作系统。

还原并保留所有权、ACL、文件属性和备用数据流

下面的表列出了文件属性和保留条件。

Windows 虚拟机/Windows 装载代理

文件属性	文件	目录
所有权	是	否
ACL	是	否
文件属性	是。由于操作系统限制，部分文件属性不会保留，例如隐藏文件属性和加密文件。	否

备用数据流	是。	否

注意从 Data Protector 2020.08 起，可以通过在装载代理主机上将 omnirc 变量 OB2_USE_VMDK_MOUNTER 设置为 1 来恢复备用数据流。

Linux 虚拟机/Linux 装载代理

文件属性	文件	目录
所有权	是。将保留不具有 root:root 所有权的文件。 不会保留具有 root:root 所有权的文件，因为所有权将变为 nobody:nobody .所有权设置取决于在目标 Linux 系统中设置的 NFS 设置 /etc/exports 。	否。所有权将变为 root:root .
ACL	否	否
文件属性 e:Extent format 设置为默认值。	否	否
权限	是	否

注意如果 GRE 操作未保留所有权、ACL、文件属性和备用数据流，则已还原的对象将使用虚拟机操作系统凭据 (在 GRE 页面中提到) 作为其属性。

3PAR 存储系统

- 只有在轮换/呈现副本之后才能执行缓存 GRE。
- 如果备份为“磁盘 + 磁带”，则只有在轮换副本之后才会考虑使用辅助存储执行 GRE。

智能缓存设备

- 只能从智能缓存设备上的增量/差异备份执行非缓存恢复。缓存 GRE 操作不支持增量或差异备份。
- 不支持对网络共享（CIFS 或 NFS 共享）执行到智能缓存设备的 VMware 备份。要从驻留在网络共享上的智能缓存设备执行缓存呈现操作，智能缓存设备应列为装载点而非共享。
- 不支持到智能缓存设备的 AES 加密 VMware 备份。

StoreOnce Catalyst 和数据域提升设备

- 如果使用 Linux 装载代理恢复 Windows 来宾虚拟机，则不会恢复所有权、ACL、文件属性和备用数据流。
- GRE 操作不支持在不同设备上执行完整备份和增量备份。
- 到 StoreOnce Catalyst 设备的非 CBT 备份将显示为非缓存。
- 如果在重新启动装载代理主机时有任何 GRE 请求处于活动状态，则在 StoreOnce 设备上最多将在 4 小时内无法访问该请求。
- 如果使用软件压缩或 AES 加密来执行到 StoreOnce Catalyst 或数据域提升设备的备份，则不支持缓存 GRE。
- 如果在版本 9.07 中通过单一会话复制将使用 Data Protector 9.04 或更低版本备份的数据传输到 StoreOnce Catalyst，则不支持缓存 GRE。

注意如果要将 Data Protector 9.05 或 9.06 版本的备份迁移到 StoreOnce Catalyst 以使用缓存 GRE 功能，则建议您通过单独的会话执行对象操作。如果同时选择多个会话，则无法确保数据一致性。

安装 VMware 客户机

需要在 VMware 系统上安装的 Data Protector 组件会因您要使用的还原和恢复解决方案而异。

适用于 VMware vSphere 的 Data Protector GRE

Data Protector Granular Recovery Extension (GRE) 使用 Data Protector 虚拟环境集成来还原数据；此扩展只是一款恢复解决方案。GRE 环境（包括装载代理）和 vCenter Server 必须满足特定的要求，然后才能安装这两种 GRE 插件。

注意: 无法将 Data Protector 组件安装在具有 GRE 的 vCenter Server 上。

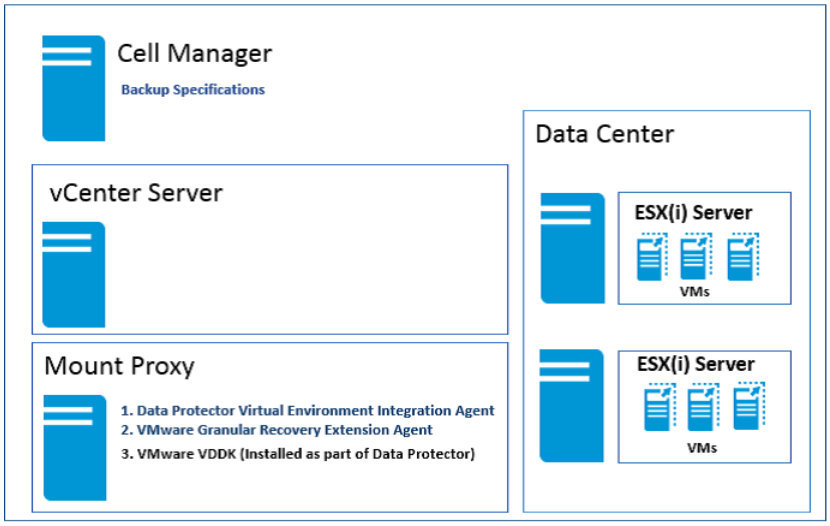
GRE 插件可通过 HTML5 GRE Web 插件用户界面进行访问。本节提供创建此环境所必需的信息。

GRE 环境

在下图中

- Data Protector 组件用蓝色表示。
- VMware 组件用黑色表示。

安装 Data Protector Granular Recovery Extension



装载代理系统

适用于 VMware vSphere 的 Data Protector Granular Recovery Extension 需要一个装载代理系统，此系统在 VMware vCenter Server 系统上用作原始位置与目标位置之间的临时还原或恢复位置。任何受支持的系统（也称为虚拟机）均可用作装载代理系统。

虚拟机磁盘未立即装载。当您以 VMware vCenter 用户身份在 vCenter 环境中使用集成的扩展开始浏览这些文件时，装载会话将启动。装载代理系统需要为已还原的数据提供足够的磁盘空间。此外，您还可以通过附加额外的磁盘或添加其他装载代理系统按需调整磁盘空间。建议将专用的系统配置为装载代理系统。

系统要求 装载代理系统必须满足以下系统要求:

- ***Linux 系统：***
  - FUSE 2.7.3 或更高版本*
  - cifs-utils 包（用于在 Linux 装载代理系统上装载 Windows 虚拟机磁盘）
  - ntfs-3g 包 (用于在 Linux 装载代理系统上装载 Windows 虚拟机磁盘)
  - NFS 服务
  - 具有 LVM 分区的磁盘需要 kpartx
  - Samba 服务器，在恢复期间，Data Protector 使用 Samba 服务器创建共享。确保 Samba 共享具有读写权限。如果已在 Linux 系统中部署增强安全机制的 Linux (SELinux) 内核安全模块，请执行 `# setsebool -P samba_export_all_rw on` 命令来启用对 Samba 共享的读写权限。
  - 使用以下命令将介质代理主机的用户添加到 Samba 密码数据库：`smbpasswd –a <user>` 。可以使用以下命令验证用户是否已添加到密码数据库： `pdbedit -w -L`。
  - 应配置 Windows 防火墙。
- 确保安装以下操作系统组件和实用程序：
  - 对于 SUSE Linux Enterprise Server (SLES)，请使用 FUSE 2.7.2
  - 对于 SUSE Linux Enterprise Server 12 (SLES 12)，请使用 FUSE 2.9.3

装载代理系统上所需的 Data Protector 组件

安装 Data Protector 客户机。然后，继续在装载代理系统上远程安装以下 Data Protector 组件：

- Virtual Environment Integration
- VMware Granular Recovery Extension Agent

您需在安装期间选择组件。如果远程安装失败，请在本地系统上安装扩展。但是，对于补丁更新，必须远程安装 GRE 代理。默认情况下，没有为 RHEL 7.0 和 SLES 12 创建 Linux 循环设备。确保装载代理系统上具有足够的 Linux 循环设备。由于要装载大量磁盘才能使整个逻辑卷组可用，因此需要足够的循环设备。

注意如果已添加或删除任意 Data Protector 组件或 VMware VDDK，请在安装 VMware Granular Recovery Extension 代理之前重新启动系统。

注意
在装载代理系统上安装 VMware Granular Recovery Extension 代理组件期间，系统可能会在安装会话输出中通知用户，指出必须重新启动目标主机才能完成安装。

注意您打算作为备份主机使用的客户机不必安装 VMware Consolidated Backup (VCB) 软件。

VMware vCenter Server（VirtualCenter 服务器）

适用于 VMware vSphere 的 Data Protector Granular Recovery Extension (GRE) 已集成至 VMware vCenter Server 中。您可使用 HTML5 VMware vSphere Web Client 访问虚拟机。Data Protector 选项卡将添加到 VMware vSphere Web 客户机界面中。

注意VMware vSphere Web Client 版本 6.5 u2 或更高版本支持 GRE 的 HTML5 GRE Web 插件。

安装适用于 VMware vSphere Web 客户机的 Data Protector GRE

完成以下步骤以安装适用于 VMware vSphere Web 客户机的 GRE。

环境：Data Protector 版本 (9.02 或更高版本)、vCenter (6.5 u2 或更高版本) 和 HTML5 GRE Web 插件。

步骤 1：安装 Cell Manager。Cell Manager 可以位于 Windows 和 Linux 系统中。

步骤 2：安装相应安装服务器: 默认情况下，会在安装 Cell Manager 过程中添加安装服务器。

- 如果已在 Windows 中随 Cell Manager 安装了 Windows 安装服务器 (默认选项)，则可跳过此步骤，并继续安装装载代理。
- 如果已在 Linux 上安装 Cell Manager，则需要设置 Windows 安装服务器并将其导入到 Linux 上的 Cell Manager 中。

步骤 3：安装装载代理。

- 可在 Windows 和/或 Linux 系统中完成。
- 建议在 Cell Manager 以外的其他专用计算机上安装装载代理。
- 必须在已安装以下组件的装载代理计算机上安装 Data Protector 客户机：
- *# Virtual Environment Integration
    1. VMware Granular Recovery Extension Agent。

步骤 4：安装 vCenter Server。

- vCenter 可以位于 Windows 或 Linux 环境中。
- 不需要 Data Protector 客户机。

步骤 5：在 vCenter Server 上安装 HTML5 GRE Web 插件。

1. 要将 vCenter 计算机作为 vCenter 客户机导入到 Data Protector Cell Manager 中，请执行以下操作。
    1. 右键单击**客户机**，并选择**导入客户机**。
    2. 输入 vCenter 的主机名并选择类型 **VMware vCenter**。单击“下一步”。
    3. 输入 vCenter 的凭据（用于登录 vCenter Web 客户机的相同凭据）。选中“HTML5 GRE Web 插件”复选框并单击“完成”。

注意您可以分别使用 omnicc -import_vcenter 和 omnicc -export_host 命令注册和取消注册 HTML5 GRE Web 插件。

> **注意**您可以将多个 vCenter 导入 Data Protector Cell Manager 中。

升级

请遵循以下步骤：

1. 要从 Data Protector 取消注册 HTML5 GRE Web 插件，请取消选中“HTML5 GRE Web 插件”复选框并单击“应用”。确保从 HTML5 GRE Web 插件主机列表删除所有 Cell Manager。
2. 要注册 HTML5 GRE Web 插件，请选中“HTML5 GRE Web 插件”复选框并单击“应用”。

> **注意**确保 Cell Manager 和所有代理服务器都已升级。

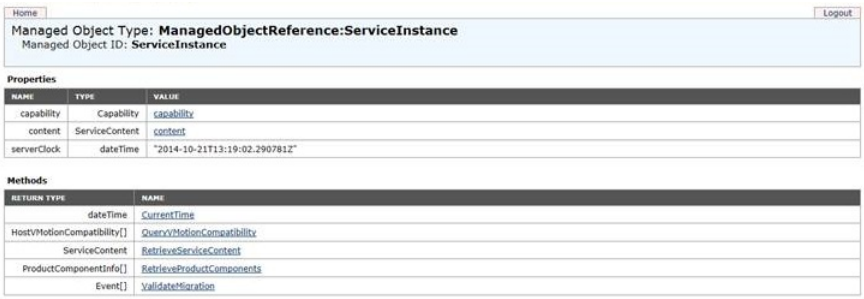
卸载 HTML5 GRE Web 插件

如果在启动这些插件时遇到任何问题，则完成以下步骤并根据您的环境重新启动之前提供的升级过程。

要卸载 HTML5 GRE Web 插件，请取消选中 VMware vCenter 客户机的“登录”选项卡中的“Advanced GRE Web 插件”复选框，然后单击“应用”。

如果您已卸载一个或多个 Cell Manager，而没有取消注册 HTML5 GRE Web 插件，则会在 VMware vSphere Web 客户机中看到“Data Protector”选项卡，但无法与其建立连接。您必须手动取消注册 HTML5 GRE Web 插件。要手动取消注册 VMware vSphere 托管对象引用，请完成以下步骤以删除在 vCenter 中注册的一个或多个 Cell Manager:

1. 转至 VMware vSphere 托管对象引用 URL，https://<vcenter>/mob


Home

Logout

Managed Object Type: **ManagedObjectReference:ServiceInstance**
Managed Object ID: **ServiceInstance**

Properties

NAME	TYPE	VALUE
capability	Capability	capability
content	ServiceContent	content
serverClock	dateTime	"2014-10-21T13:19:02.290781Z"

Methods

RETURN TYPE	NAME
dateTime	CurrentTime
HostVMotionCompatibility[]	QueryVMotionCompatibility
ServiceContent	RetrieveServiceContent
ProductComponentInfo[]	RetrieveProductComponents
Event[]	ValidateMigration

2. 单击**内容**，然后单击 **ExtensionManager**。
3. 将密钥 **com.MicroFocus.DataProtector.VMwareGREAng.WebClient** 复制到剪贴板。
4. 单击 **UnregisterExtension** 并将复制的密钥粘贴到 **VALUE**。
5. 单击“调用方法”。

安装适用于 VMware 的 GRE

Data Protector Granular Recovery Extension 要求安装并配置以下系统：

- Data Protector 单元和以下客户机：
  - VMware vCenter Server 系统 (版本 6.5 u2 或更高版本)
  - 装载代理系统

Data Protector 过滤侦听程序服务将侦听来自 VMware 的数据请求，然后从 StoreOnce Catalyst 设备获取所请求的数据。过滤侦听程序服务还支持从数据域系统设备读取数据。当正在打开 GRE 或实时迁移会话正在进行时，不得启动或停止该服务。

使用 Windows 备份主机时，确保 Data Protector INET 服务和“Data Protector 过滤侦听程序服务” 正在使用相同的用户凭据运行。有关满足 GRE 环境要求以及安装 Granular Recovery Extension 和所需的 Data Protector 组件的详细说明，请参见“安装”的“VMware 客户机”一节。

有关以远程或本地方式安装以下任意组件或所有组件的详细说明，请参阅“相关主题”一节中的相关主题。

- Data Protector Cell Manager - 请参阅《安装 Data Protector Cell Manager 和安装服务器》一节。
- Data Protector 客户机 - 请参阅《安装 Data Protector 集成客户机》一节。

重要说明升级方案: 如果要将 Data Protector 升级到最新版本，请确保在 Data Protector 升级过程完成之后完成以下步骤:

1. 删除现有的 GRE Web 插件。
2. 再次注册插件。

相关主题

安装 Cell Manager 和安装服务器

安装 Data Protector 集成客户机

配置适用于 VMware 的 GRE

本主题介绍需要执行的配置步骤。

满足 Granular Recovery Extension 的 Data Protector 配置要求

本节提供有关以下任务的信息：

- 配置 GRE 用户组和用户
- 配置 GRE 管理员
- 为 vSphere 配置系统
- 配置防病毒例外

为 VMware vSphere 用户组和用户配置 GRE

本节提供以下详细信息：

- 为 VMware vSphere 用户组添加 GRE
- 将用户添加到 VMware vSphere 用户组的 GRE
- 将 Inet 用户帐户添加到管理员组

为 VMware vSphere 用户组添加 GRE

> **注意**
>
> - 要使用 GRE Web 插件，需要执行本节中介绍的步骤。用户必须属于 Data Protector 管理员组才能对特定虚拟机执行 GRE。否则，Data Protector 会限制用户执行 GRE 操作。此外，用户在相应的 vCenter Server 上必须具有执行 GRE 操作的足够权限或特权。否则，Data Protector 不会限制用户，相反，用户将从 vCenter Server 收到错误消息。
> - 执行 GRE 操作需要 **webusername**。您可以通过在 GUI 中访问用户属性 (转到“上下文”列表 > 选择用户 > 单击“属性”) 或通过执行 omniusers -list 命令获取 **webusername**。

完成以下步骤，使用 Data Protector GUI (Data Protector Manager) 为 GRE VMware 创建 Data Protector 组:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，右键单击**用户**。
3. 单击**添加用户组**以打开向导。
4. 在“常规”下，键入新组的**名称**和**说明**。
5. 单击“下一步”。
6. 设置该组的“启动还原”用户权限。
7. 单击**完成**退出向导。

   新的 GRE VMware 用户组即被添加到 Data Protector。

将用户添加到 VMware vSphere 组的 GRE

> **注意**要使用 GRE Web 插件，需要执行本节中介绍的步骤。

要将用户添加到 GRE VMware 组，请执行以下操作：

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要向其添加用户的用户组。
4. 单击**添加/删除用户**打开向导。
5. 在“添加/删除用户”对话框中，输入特定用户属性。

   输入**名称**和**组/域**时，确保输入有关网络上现有用户的信息。

   要确保 GRE VMware 管理员有权访问扩展的管理入口点，请指定以下信息：

类型: Windows

名称: username

组/域: GRE VMware user group, VCENTER

客户机: vCenterSystemName

必须将 GRE VMware 管理员添加到 vSphere 权限选项卡。将用户角色设置为管理员。

6. 单击箭头按钮 **>>** 将用户添加到用户列表。
7. 单击**完成**退出向导。

用户随即会添加到 GRE VMware 管理员组，并获得“启动还原”用户权限。

> **提示**要删除用户，请在用户列表中选择用户，并单击 **<<**。

将 Inet 用户帐户添加到 Data Protector 管理员组

要确保 VMware Granular Recovery Extension Agent 和 VMware Granular Extension Web Plug-In 扩展组件正常运行，您需要将 Inet 用户帐户添加到以下系统上的 Data Protector Admin 用户组:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要向其添加用户的**管理员**用户组。
4. 单击**添加/删除用户**打开向导。
5. 在“添加/删除用户”对话框中，输入以下用户属性：

   装载代理系统：

   类型: Windows 或 Linux

   名称: SYSTEM 或 root

   组/域: NT AUTHORITY 或 root

   > **注意**确保指定网络上的现有用户帐户。

   客户机: MountProxySystemName

   设置 vCenter Server 系统属性。

   vCenter Server 系统：

   类型: Windows

   名称: 用来运行 VMware vCenter Server 的帐户 (默认为 SYSTEM)。

   组/域: 用来运行 VMware vCenter Server 的帐户组/域 (默认为 NT AUTHORITY)。

   客户机: VCenterSystemName 。
6. 单击箭头按钮 **>>** 将用户添加到用户列表。
7. 单击**完成**退出向导。

   用户帐户即被添加到 Data Protector admin 用户组，并具有分配给该组的用户权限。

> **注意**Data Protector Inet 使用 Data Protector Local 系统帐户 (在 Windows 操作系统中) 中所用的 SYSTEM, NT AUTHORITY。

使用 Data Protector 配置 GRE 管理员

要使 GRE 管理员能够自由访问扩展及其任务，请使用 Data Protector GUI (**Data Protector Manager**) 继续执行以下步骤:

1. 在“上下文”列表中，选择**用户**。
2. 右键单击 GRE VMware 用户组。
3. 单击**属性**，然后单击**用户权限**选项卡。
4. 确保为 Data Protector 用户帐户分配了 Data Protector“启动还原”用户权限。

> **注意**指定的用户权限会分配给用户组以及属于该组的所有用户。建议创建特定的 VMware GRE vSphere 用户组以向其添加扩展的管理员。

为 VMware vSphere 配置系统

配置 Windows/Linux 防火墙例外

本节提供为 VMware Granular Recovery Extension Agent 组件设置或添加防火墙例外的说明。

要确保装载代理系统组件和 vCenter Server 上的扩展之间的通信，请执行以下操作：

1. 检查 Windows/Linux 防火墙例外列表。
2. 请确保 VMware Granular Recovery Extension Agent（vmwaregre-agent.exe）在装载代理系统上位于 Windows/Linux 防火墙例外列表中。

配置防病毒例外

如果您在装载代理主机上安装了防病毒软件 (例如 McAfee 或 Trend Micro)，请通过为以下文件夹 (包括子文件夹) 的所有进程添加排除项来配置防病毒例外:

- C:\Program Files\OmniBack\
- C:\ProgramData\OmniBack\tmp\

对于访问保护，请为以下项添加排除项:

- 虚拟机保护: 所有规则
- 将以下进程添加到排除列表:
  - C:\Program Files\OmniBack\bin\vepa_bar.exe
  - C:\Program Files\OmniBack\bin\vepa_util.exe
  - C:\Program Files\OmniBack\bin\vmwaregre-agent.exe

> **注意**如果您使用 **Trend Micro Internet Security**，则关闭“病毒和间谍软件控制”不足以执行 GRE。您必须:
>
> - 完全退出 **Trend Micro Internet Security**。
>
> 或
>
> - 在 **Trend Micro Internet Security** 中添加上述例外。

要配置 Sophos 防病毒例外，必须为以下文件夹 (包括子文件夹) 的所有进程添加排除项:

- C:\ProgramData\OmniBack\tmp\VMWareGRE\<vCentreHostname>\restore

备份适用于 VMware 的 GRE

适用于 VMware vSphere 的 Data Protector GRE 依赖适用于 VMware vSphere 的 Data Protector 虚拟环境集成组件来备份 VMDK。使用备份解决方案备份 VMware vSphere 数据。扩展支持完整备份、增量备份和差异备份。仅来自 StoreOnce Catalyst、Data Domain 设备、3PAR 阵列和重复数据删除存储设备的缓存恢复操作会支持增量和差异备份。

注意

- 适用于 VMware vSphere 的 GRE 使用相同的过程来恢复所有 VMware vSphere 数据。该过程与备份类型无关。建议设置专用的装载代理系统。扩展需要为虚拟机磁盘的临时还原位置分配可扩展的磁盘空间（可扩大的磁盘空间）以用于非缓存恢复。
- 非 CBT 备份显示为非缓存。

要利用适用于 VMware vSphere 的 GRE 的 GRE Web 插件中的缓存恢复功能，请使用下列设备之一进行 VMware vSphere VMDK 备份:

备份到智能缓存设备

智能缓存设备是基于磁盘的设备，可在 Windows 和 Linux 上进行配置。管理员可以使用 Data Protector GUI 将 vCenter 配置中的虚拟机备份到智能缓存设备。

注意智能缓存设备仅可用作 VMware 虚拟环境集成备份的目标。每个智能缓存设备仅支持使用一个目录作为装载点。

当智能缓存设备将磁盘呈现到装载代理主机时，将执行缓存恢复操作。智能缓存设备以本机格式保存虚拟机磁盘，当请求呈现操作时，这些磁盘将可供 GRE 代理使用。通过以本机格式管理磁盘并启用简单呈现，可避免还原，从而节省时间和空间。

注意无论是备份到磁盘设备，还是从驻留在 3PAR 存储上的阵列快照执行备份，均称为“缓存备份”，其他备份则称为“非缓存备份”。

从 3PAR 阵列执行备份

可以从驻留在 3PAR 阵列存储上的阵列快照对虚拟机中的数据执行缓存恢复。可以通过使用“ZDB 到磁盘”、“ZDB 到磁带”和“ZDB 到磁盘 + 磁带”选项对虚拟机执行零宕机时间备份 (ZDB) 来执行此操作。使用**快照备份**方法保护的虚拟机可用于执行恢复操作。

3PAR 存储系统支持对虚拟机使用的磁盘卷进行快照复制。此唯一方法利用适用于 VMware vSphere 的 GRE 中提供的 GRE Web 插件的缓存恢复功能。通过此方法执行的备份使用现有的 ZDB 功能。适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成支持使用 3PAR 存储系统进行设置、且通过 vCenter Server（vCenter 环境）进行管理的 ESX 和/或 ESXi Server 系统环境。

备份到 StoreOnce Catalyst 和数据域设备

StoreOnce Catalyst 设备是“备份到磁盘”(B2D) 设备。要利用适用于 VMware vSphere 的 GRE 中的缓存恢复功能而不暂存还原，必须使用 StoreOnce Catalyst 设备进行备份。管理员可以使用 Data Protector GUI 将 vCenter 配置中的虚拟机备份到 StoreOnce Catalyst 设备。

数据域设备是“备份到磁盘”(B2D) 设备。要利用适用于 VMware vSphere 的 GRE 中的缓存恢复功能而不暂存还原，必须使用数据域设备进行备份。管理员可以使用 Data Protector GUI 将 vCenter 配置中的 VM 备份到数据域设备。

注意

- 使用 Data Protector 版本 9.07 和更高版本对数据域设备执行的备份将显示为缓存会话。
- 数据域系统 (OS 版本 6.1) 的阈值限制为每个进程 64 个连接。此限制影响 GRE 操作支持的增量会话数。如果达到此阈值限制，将显示一条消息。要继续执行 GRE 操作，请通过关闭当前处于活动状态的 GRE 请求释放连接。

StoreOnce 和数据域设备缓存恢复操作支持完整备份、增量备份和差异备份。执行 GRE 时，在版本 9.07 之前对 StoreOnce 和数据域设备执行的所有备份将列为非缓存。

备份到 Data Protector 重复数据删除存储设备

重复数据删除存储设备是“备份到磁盘”(B2D) 设备。要利用适用于 VMware vSphere 的 GRE 中的缓存恢复功能而不暂存还原，必须使用重复数据删除存储设备进行备份。管理员可以使用 Data Protector GUI 将 vCenter 配置中的 VM 备份到重复数据删除存储设备。

注意事项

下表根据 GRE 期间设备的配置方式 (FC 地址或 IP 地址) 列出了注意事项:

行为	备份/还原	GRE
使用 IP 地址配置的设备	如果选择使用 "FC" 的选项，请检查 FC 地址并使用 FC 进行连接。	在 GRE 设备连接期间，Data Protector 会检查是否使用 IP 地址配置设备。如果使用 IP 地址，请获取 FC 地址，并使用 FC 地址连接设备。如果连接失败，则回退到 IP 地址。
	如果成功则使用 FC 连接，否则如果选择“允许回退”，则回退到 IP。使用 IP 地址连接。	在 GRE 设备连接期间，Data Protector 会检查是否使用 IP 地址配置设备。如果使用 IP 地址，请获取 FC 地址，并使用 FC 地址连接设备。如果连接失败，则回退到 IP 地址。
使用 FC 地址配置的设备	仅使用 FC 地址。 如果使用 FC 连接失败，则会话失败。没有选项可用于查找连接 StoreOnce Catalyst 或数据域设备的 IP 地址。	仅使用 FC 地址。 如果使用 FC 连接失败，则会话失败。没有选项可用于查找连接 StoreOnce Catalyst 或数据域设备的 IP 地址。

使用 HTML5 GRE Web 插件进行恢复

VMware HTML5 GRE Web 插件提供了从虚拟机磁盘执行恢复的界面。

使用 HTML5 GRE Web 插件，您可以执行以下任务:

访问 HTML5 GRE Web 插件

完成以下步骤，从 VMware vSphere HTML5 Web 客户机访问 HTML5 GRE Web 插件:

1. 打开 VMware vSphere HTML5 Web 客户机。您可以指定任何已导入 Data Protector Cell Manager 的 vCenter URL。指定 vCenter 用户的凭据，并单击“登录”。

   此时将显示 VMware vSphere HTML5 Web 客户机主页，默认情况下已选择“主页”选项卡。

2. 选择“主机和群集”或“VM 和模板”，并展开虚拟机节点，以选择所需的虚拟机。

3. 单击“配置”>“更多”>“粒度恢复”。

   > **注意**如果在访问 VMware vSphere HTML5 Web Client 应用程序之后收到安全警报通知，则说明系统中并没有安装 vSphere 证书。单击**是**打开扩展。

   将打开 HTML5 GRE Web 插件。

4. 在“粒度恢复”页上，从“Cell Manager”下拉列表中选择一个 Cell Manager。

   如果您是第一次在当前 vSphere 会话中连接到特定 Cell Manager，系统将提示您进行身份验证。

5. 指定“用户名”和“密码”，然后单击“登录”。

   在当前 vSphere 会话中再次连接到同一 Cell Manager 时，无需进行身份验证。

   身份验证成功之后，将启用“装载代理”下拉列表。

6. 从“装载代理”下拉列表中选择装载代理服务器。

   “装载代理”下拉列表包含可用于选定 Cell Manager 的所有装载代理服务器。

   您选择的装载代理不必与备份期间使用的备份主机相同。

7. 单击“提交”。选定的装载代理服务器将与特定的 Cell Manager 关联，并用于初始配置。

配置 GRE 设置

您可以在“设置”页上配置以下设置:

- 保留时间选项
- 启用记录
- 装载代理信息 (系统用作还原虚拟机磁盘的目标位置)

修改保留时间

要修改保留时间选项，请按照下列步骤操作:

1. 在“粒度恢复”页上，单击“设置”  。
2. 在**保留时间选项**下，输入以下文本框的保留期：
   - **操作后删除非缓存磁盘 (天)**
   - **操作后删除缓存磁盘 (天)**
   - > **注意**非缓存备份的默认保留期为 7 天（最多可以设置为 7 天）。缓存备份的默认保留期为 1 天（最多可以设置为 7 天）。

启用调试

如果在使用此扩展时遇到问题，日志文件中的信息可帮助您确定问题。单击“是”以启用日志记录。

日志文件位于默认的 Data Protector 日志文件目录和默认的临时文件目录中。

配置装载代理

要配置、添加或修改用作还原虚拟机磁盘的目标位置的装载代理系统，请执行以下操作：

1. 从“Windows 主机”或“Linux 主机”下拉列表中，选择所需的 Windows 或 Linux 装载代理系统。

   > **注意**可以配置多个装载代理和还原路径。

2. 在 Windows 和/或 Linux“还原路径”文本框中，键入装载代理系统中的位置路径，然后按 **Enter**。您可以根据需要添加多个恢复路径。使用以下格式：
   - DriveLetter:\Folder\Subfolder （Windows 装载代理系统）
   - /Directory/Subdirectory （Linux 装载代理系统）

   可以单击 **x** 来删除所需的还原路径。如果还原路径是装载代理系统的唯一路径，则无法删除该路径。
3. 单击**保存**。

查看请求列表

“请求”页是 HTML5 GRE Web 插件的登录页。在此页中，您可查看请求列表，以及执行诸如浏览、查看会话报告或创建请求之类的操作。

您还可以基于顶部的“备份类型”和“状态”过滤器来过滤请求列表。

要查看请求列表，请在“粒度恢复”页面上单击“请求”。此时将显示恢复请求列表。对于每个请求，将显示以下信息 -“ID”、“状态”、“提交日期”、“类型”和“备份时间”。此外，每个请求都可以使用“操作”和“会话报告”选项。“操作”列显示“浏览”或“中止”按钮，具体取决于请求的状态。

请求可以具有下列状态之一:

- 已缓存
- 正在缓存
- 缓存失败
- 已中止
- 已恢复
- 正在恢复
- 恢复失败
- 还原
- 正在挂起

要查看请求的可用选项，请选择请求。根据请求的状态，“操作”和“会话报告”列中将提供适当的按钮或操作:

状态	可用选项
正在缓存	中止 会话报告
已缓存	会话报告、浏览
缓存失败	会话报告
正在恢复	中止
已恢复	会话报告
恢复失败	会话报告
正在挂起	会话报告
已中止	会话报告
还原	会话报告

根据您的请求，可以执行以下操作:

- 单击“浏览”，浏览创建请求时选择的磁盘。可以浏览磁盘中的分区，并选择要恢复的文件或文件夹。但是，无法同时浏览多个磁盘。在给定的时间点，仅可浏览一个磁盘。此时将显示“恢复文件”页。
- 单击“中止”，停止正在进行的还原或恢复。
- 单击“会话报告”，显示选定 GRE 请求最近执行的操作的日志消息。
- 单击“请求”，为缓存操作或非缓存操作创建请求。

创建请求

> **注意**在继续为非缓存备份创建请求之前，请从“GRE 设置”页中配置装载代理。但是，不必为缓存备份配置装载代理。

1. 在“请求”页面上，单击“请求”。“请求”页面列出了所选 VM 的所有可用备份。您可以使用“备份自”(全部、过去 30 天、过去 90 天、过去 6 个月、去年) 和“备份类型”(全部、缓存备份、非缓存备份) 过滤器下的可用选项来过滤结果。
2. 选择所需的备份，然后单击“下一步”。
   a. 从**虚拟磁盘**部分中，选择要还原/呈现的一个或多个虚拟磁盘。
   b. 在“磁盘保留时间 (天)”文本框中，输入保留期 (以天为单位)。此期限从还原或呈现操作开始计算。超过保留期后，虚拟磁盘不可用。

      > **注意**非缓存备份的默认保留期为 7 天（最多可以设置为 7 天）。缓存备份的默认保留期为 1 天（最多可以设置为 7 天）。

   c. 从 **ESX 主机**下拉列表中，选择所需的 ESX 主机。对于 3PAR 缓存会话，默认情况下选择生产 ESX。
   d. 从“装载代理”下拉列表中，选择所需的装载代理。
   e. 从**还原路径**下拉列表中，选择所需的还原路径。只有非缓存备份才需要还原路径。
3. 单击**完成**。此时将显示“请求”页，您可监视请求的状态。
4. 单击“刷新”，更新备份列表。

> **注意**重新启动 GRE 装载代理主机时，至少浏览一次的请求将变为无效。因此，必须重新创建这些请求才能执行 GRE 操作。

> **注意**如果要删除为 StoreOnce Catalyst 或数据域设备创建的请求，请运行以下命令强制清理 StoreOnce Catalyst 或数据域请求 ID:
> vmwaregre-agent.exe -force_cleanup <request_id> -vcenter <hostname> ，其中，
>
> - request_id : 需要清理的 StoreOnce Catalyst 或数据域设备请求 ID
> - hostname : 在其上面发出请求的 vCenter 主机的名称

恢复文件

要验证导出的目录的列表，可以在 Linux 装载代理主机上运行以下命令：

```
showmount -e
```

要从虚拟机磁盘中恢复文件，请执行以下操作：

1. 转到“请求”页面。选择缓存的请求，然后单击“浏览”。此时将显示“恢复文件”页。VM 的文件结构显示在“浏览文件”部分中。
2. 在“浏览文件”部分下，选择包含要恢复的文件的虚拟机磁盘。

   > **注意**对于缓存的 3PAR 会话，选择虚拟机磁盘将装载备份复本、装载数据存储并注册虚拟机，导致显示以下消息:
   >
   > Request submitted successfully and is in progress. Please try browsing after some time.
   >
   > 当进程仍在进行时选择虚拟机磁盘会导致显示以下消息:
   >
   > Request is still in progress. Please try browsing after some time.

   您可以通过在搜索框中键入名称或关键字，使用“搜索” 选项来轻松找到要恢复的文件或文件夹。只有当展开文件夹时，搜索选项才启用。

   浏览操作使您一次可展开一个磁盘和一个分区，这是因为系统仅支持恢复一个磁盘和一个分区。

   请执行以下操作：

1. 单击磁盘名称，展开所需的分区。如果选择 Linux 分区，则从可用的逻辑卷列表中选择逻辑卷。

   注意
   - 如果在磁盘/分区中选择了文件或文件夹，并尝试浏览另一个磁盘/分区，则较早的磁盘/分区将折叠，并且其中的选择将无效。
   - 不支持在分区中使用“搜索” 选项。

2. 选择要从磁盘的选定分区中恢复的文件。

3. 在“恢复选项”下，从“目标 VM”下拉列表中选择虚拟机，并在“用户名”和“密码”文本框中输入其凭据。**目标 VM** 将列出所选 vCenter 下的所有正在运行的 VM。
   您还可以通过单击“在装载代理上恢复”复选框 来选择恢复到装载代理。如果选中，将禁用“目标 VM 详细信息”下的“目标 VM”、“用户名” 和“密码” 字段 ，因为这些凭据不需要恢复到装载代理。

   注意确保在目标 Linux VM 上完成以下步骤：
   1. 解决目标 VM 的任何主机名或 IP 冲突。
   2. NFS 服务必须已配置并正在运行。

4. 在**位置**文本框中，输入目标恢复位置路径。
   - 对于 Windows 系统中的位置，请使用格式 DriveLetter:\Folder\Subfolder 。
   - 对于 Linux 系统中的位置，请使用格式 /Directory/Subdirectory 。

   注意对于共享目录，请输入不含主机名的路径。例如，对于 NFS 共享主机名，请使用： /shared_dir/subdir 。文件将恢复到 shared_dir/subdir/<target location specified> 。此外，请确保已正确设置 Samba 和 NFS 共享。NFS 共享必须导出为伪 root 共享。例如，在目标虚拟机上，配置要导出的共享时，在 /etc/exports 中使用以下选项：

   rw,fsid=0, crossmnt, no_root_squash, no_subtree_check

   目标虚拟机将被装载在装载代理主机上。装载后，文件将复制到装载目录。

   系统将自动创建路径中缺少的任何目录。例如，如果指定 /shared_dir/subdir1/subdir2 ，则当 subdir1/subdir2 子目录不存在时，系统将自动在 /shared_dir 内创建它们。

5. 如果目标系统上已存在该文件，则选择以下恢复选项之一：
   - **覆盖**：删除原始文件，并保存最新的文件。
   - **重命名**: 保留原始文件，并使用唯一的编号 (由 Data Protector 生成) 保存恢复的文件。
   - **跳过**：保留原始文件。

6. 选择**保留目录结构**，保留目标系统上源虚拟机磁盘的原始目录结构。

7. 单击**完成**。此时将显示确认消息和“请求”页，在此页中，您可监视恢复。

标识 GRE Web 插件版本

要确定 VMware Granular Recovery Extension 代理和插件版本，请在“Granular Recovery”页面上单击“关于”。

Informix Server 集成

This feature is available in the Premium Edition

Data Protector 与 Informix Dynamic Server (Informix Server) 集成，可以联机备份 dbobject。备份期间，数据库服务器 (Informix 实例) 处于联机状态且已正常使用。

Data Protector 提供以下类型的交互式备份和安排的备份：Informix Server 备份类型:

备份类型	描述
完整	完整备份 (级别 0)。
增量 1	增量备份 (级别 1)。备份自上次完整备份以来的更改。
2 级增量备份	增量备份 (级别 2)。备份自上次 1 级增量备份以来的更改。

Data Protector 提供两种类型的还原:

Informix Server 还原类型

还原类型	描述
完整数据库还原	从任何备份还原。ON-Bar 同时还原 dbobject 并重播逻辑日志一次。
整个系统还原	从整个系统备份还原。无论是否还原逻辑日志，ON-Bar 都会按顺序还原整个系统。如果不需要还原日志进行灾难恢复，或者还原到其他客户机时，整个系统还原适用于小型系统。

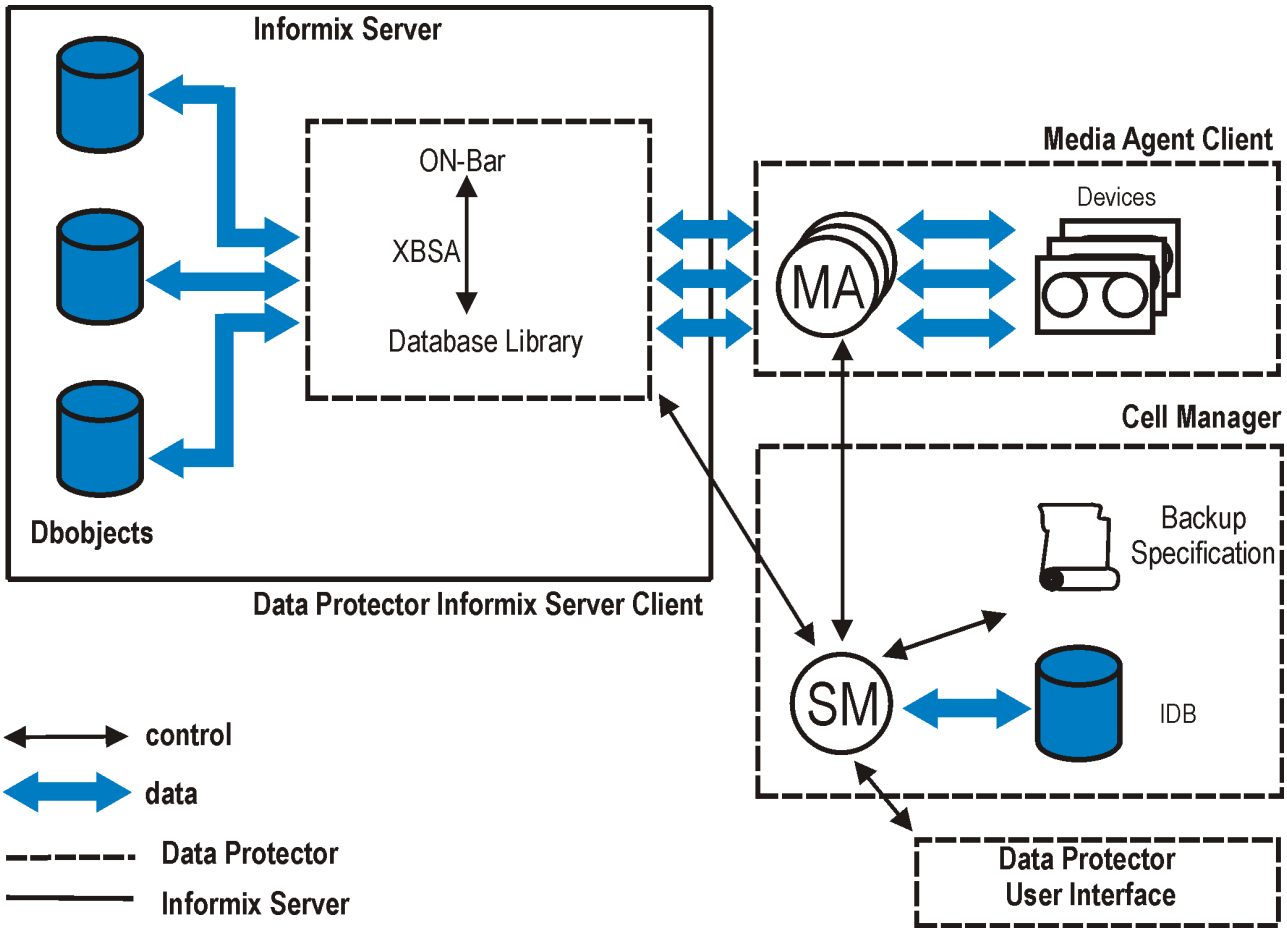
还可以使用 onbar 命令备份并还原 dbobject。

本节提供特定于 Data Protector Informix Server 集成的信息。

集成概念

Data Protector 通过基于名为 Data Protector **BAR** (备份和还原) 的公共带库的 Data Protector 数据库例程库与 Informix Server 集成。Data Protector 数据库通道通过“XBSA 接口”在 Data Protector 会话管理器与 Informix Server“ON-Bar 实用程序”之间进行通信。Data Protector Informix Server 集成体系结构显示 Data Protector Informix Server 集成的体系结构。

Data Protector Informix Server 集成体系结构



Informix Server 集成体系结构 - 图例和说明

图例	描述
SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
ON-Bar	ON-Bar 通过 Data Protector 和 Informix Server 命令行执行备份和还原请求。
XBSA	X/Open Backup Services 应用程序编程接口，ON-Bar 和 Data Protector 通过该接口交换控制和数据。
数据库例程库	用于在 Informix 实例和 Data Protector 之间传输数据的一组 Data Protector 可执行文件。
MA	Data Protector 常规介质代理。
备份规范	要备份的对象列表、备份设备和要使用的选项。
IDB	Data Protector 内部数据库。

始终通过 Informix Server ON-Bar 实用程序在 Informix Server 上执行备份。ON-Bar 将备份和还原请求传送给 Informix 实例。

Informix 实例负责磁盘的读/写操作，而 Data Protector 则读取和写入设备并管理介质。

满足 Informix Server 集成的先决条件

以下是 Informix Server 集成的先决条件:

- 确保已正确安装和配置 Informix Server。
- 确保已正确安装 Data Protector。

  要执行备份或还原的每个 Informix Server 系统均必须安装 Data Protector Informix 集成组件。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 Informix Server 系统与 Cell Manager 是否正常通信，请在 Informix Server 系统上配置并运行 Data Protector 文件系统备份和还原。
- *Windows 系统：*
  - 在 Windows 操作系统上，为具有相应 Informix Server 权限的用户配置 Data Protector Inet 服务用户模拟，以便运行备份和还原。

群集感知客户机

仅在一个群集节点上配置 Informix 实例，因为配置文件驻留在 Cell Manager 上。

如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称，如下所示:

Windows 系统： set OB2BARHOSTNAME=virtual_server_name

UNIX 系统： export OB2BARHOSTNAME=virtual_server_name

- 确保 Informix 实例处于联机状态。
- 确保您具有足够的逻辑日志空间来创建备份。

  如果所有逻辑日志文件中的可用空间量小于单个日志文件的一半，则 Informix Server 不会创建备份。
- 在完整备份之前，打印或保存 ONCONFIG 文件、紧急引导文件以及 UNIX 上的 sqlhosts 文件。
- 验证数据一致性。
- 在还原根 dbspace 或执行整个系统还原之前，请关闭 Informix 实例 (冷还原)。以用户 informix 登录 Informix Server 系统并执行:

  Windows 系统： INFORMIXDIR\bin\onmode -ky

  UNIX 系统： INFORMIXDIR/bin/onmode -ky

  > **注意**Informix 实例脱机后，您无法仅对非关键 (用户) dbspace 进行还原。还必须选择根 dbspace 进行还原。

- 要仅还原非关键 dbspace，请确保 Informix 实例处于联机状态或处于静止模式 (热还原)，且要还原的非关键 dbspace 处于脱机状态。

  要检查 dbspace 是否处于脱机状态，请执行:

  Windows 系统： INFORMIXDIR\bin\onstat -d

  UNIX 系统： INFORMIXDIR/bin/onstat -d
- 要还原 dbobject，请先查找所需的介质以及上次完整备份会话的会话 ID。使用 Data Protector GUI 或 CLI。

还原到另一台 Informix 服务器 要将数据还原到 Informix Server 系统而不是执行备份的系统，请执行以下操作:

1. 在要还原到的客户机 (目标客户机) 上安装 Data Protector Informix 集成软件组件。
2. 在目标客户机上创建用户 informix 。
3. 通过在目标客户机上使用 Informix Server ON-Monitor 实用程序，创建 Informix 实例，该实例与原始 Informix 实例具有相同的数据库名称和相同的服务器编号。

   要获取数据库名称和服务器编号，请以用户 informix 身份登录原始服务器，然后执行以下操作:

   a. 要获取数据库名称，请在 onstat –c 输出中查找 DBSERVERNAME 的值。

      在 UNIX 系统上，您可以通过执行以下命令来完成此操作: onstat -c | grep DBSERVERNAME

   b. 要获取服务器编号数据库名称，请在 onstat –c 输出中查找 SERVERNUM 的值。

      在 UNIX 系统上，您可以通过执行以下命令来完成此操作: onstat -c | grep SERVERNUM
4. 确保 Informix 实例处于联机状态。
5. 按照配置 Informix 实例中所述配置 Informix 实例。
6. 使 Informix 实例处于脱机状态。
7. 将以下原始 Informix Server 配置文件复制到目标客户机:
   - ONCONFIG
   - 紧急引导文件
   - oncfg_DBSERVERNAME.SERVERNUM
8. 在 UNIX 系统上，还将 sqlhosts 文件复制到目标客户机。将复制的 sqlhosts 文件中的源客户机主机名更改为目标客户机主机名。
9. 在 UNIX 系统上，将 sqlhosts 文件中的 *service_name* 条目与目标客户机上唯一的端口号 (例如，1535/tcp) 一起添加到 etc/services 文件中，以允许实例正常启动运行。
10. 从目标客户机的原始数据库重新创建数据库文件，然后更改文件的权限和所有权以匹配原始数据库文件。
11. 按照 Data Protector Informix Server 集成中所述，启动 dbobject 的整个系统还原。

使用其他设备进行还原

您可以使用与备份不同的设备执行还原。**使用 Data Protector GUI**

使用 Data Protector CLI 或 Informix Server 命令

如果要使用 Data Protector CLI 或 Informix Server 命令进行还原，请在文件中指定新设备:

Windows 系统： Data_Protector_program_data\Config\Server\cell\restoredev

UNIX 系统： /etc/opt/omni/server/cell/restoredev

使用以下格式: " DEV 1 " " DEV 2 "，其中 DEV 1 为原始设备， DEV 2 为新设备。

> **重要说明**使用后删除此文件。

在 Windows 系统上，对此文件使用 Unicode 格式。

以下限制适用:

- 在 Windows 系统上，不能冷还原非关键的数据库空间。

安装 Informix Server 客户机

This feature is available in the Premium Edition

假设 Informix Server 已启动并正在运行。

要备份 Informix Server 数据库，需要在安装期间选择以下 Data Protector 组件：

- Informix Integration - 为了能够备份 Informix Server 数据库
- Disk Agent - 出于两个原因而安装磁带客户机：
  - 运行 Informix Server 的文件系统备份。请在配置 Data Protector Informix Server 集成“之前”执行该备份，并解决与 Informix Server 和 Data Protector 有关的所有问题。
  - 对“无法”使用 ON-Bar 进行备份的重要 Informix Server 数据 (例如，ONCONFIG 文件、sqlhosts 文件、ON-Bar 紧急引导文件、oncfg_INFORMIXSERVER.SERVERNUM 和配置文件等) 运行文件系统备份。

IBM HACMP Cluster

如果 Informix Server 安装在 IBM HACMP 群集环境中，请在所有群集节点上安装 Informix 集成组件。

配置 Informix Server 集成

This feature is available in the Premium Edition

您需要配置 Informix Server 用户以及要备份或还原的每个 Informix 实例。

配置 Informix Server 用户

在 UNIX 上，将 Informix Server 管理员添加到 Data Protector admin 或 operator 用户组。此用户在 informix 组中通常为 informix 或 root。要确定它，请检查 Informix Server onbar_d 文件的所有者。本节假定 Informix Server 用户在 informix 组中为 informix。

配置 Informix 实例

您需要为 Data Protector 提供 Informix 实例的配置参数:

- Informix 实例的名称。
- Informix Server 主目录的路径名。
- *Windows 系统：*Windows 注册表中带有 sqlhosts 条目的系统的名称。

  *UNIX 系统：*sqlhosts 文件的路径名。
- Informix 实例 ONCONFIG 文件的名称。

然后，Data Protector 在 Cell Manager 上创建 Informix 实例配置文件，并验证与实例的连接。要配置 Informix 实例，请使用 Data Protector GUI 或 CLI。**使用 Data Protector GUI**

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Informix Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在客户机中，选择“Informix Server 系统”。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，输入 Informix 实例名称。

   在“用户和组/域”选项中，指定要在其下运行备份会话的帐户。

   请确保此用户已加入 Data Protector admin 或 operator 用户组，并且具有 Informix Server 备份权限。此用户成为备份所有者。

   - *UNIX 系统：*在“用户名”和“组/域名”中键入 informix。
   - *Windows 系统：*在“用户名”和“组/域名”中，键入用户名和域 (例如，用户名 Administrator，域 DP)。必须为 Data Protector Inet 服务用户模拟设置此帐户。

   单击“下一步”。
5. 在 Informix Server 主目录中，指定 Informix Server 主目录的路径名。

   在 sqlhosts 文件的完整路径名中，输入以下内容:

   *Windows 系统：*Windows 注册表中带有 sqlhosts 条目的系统的名称。使用 UNC 表示法，例如：\\computer_name。

   *UNIX 系统：*sqlhosts 文件的路径名。

   在“ONCONFIG 文件的名称”中，输入位于以下目录中的 Informix 实例 ONCONFIG 文件的名称:

   Windows 系统： INFORMIXDIR\etc

   UNIX 系统： INFORMIXDIR/etc

   单击**确定**。
6. 如果发生错误，请单击“详细信息”。
7. 即会配置 Informix 实例。退出 GUI 或继续在选择要备份的 dbobject。中创建备份规范。

使用 Data Protector CLI 以用户 informix 登录 Informix Server 系统。从以下目录中: *Windows 系统：* Data_Protector_home\bin *HP-UX 和 Solaris 系统：* /opt/omni/lbin *其他 UNIX 系统：* /usr/omni/bin 执行以下命令：Windows 系统: perl -I..\lib\perl util_informix.pl -CONFIG INFORMIXSERVER INFORMIXDIR sqlhosts ONCONFIG *UNIX 系统：* util_informix.pl -CONFIG INFORMIXSERVER INFORMIXDIR sqlhosts ONCONFIG

参数描述

INFORMIXSERVER	Informix 实例的名称。
INFORMIXDIR	Informix Server 主目录的路径名。

sqlhosts	**Windows 系统：**Windows 注册表中带有 sqlhosts 条目的系统的名称。使用 UNC 表示法，例如： \\computer_name. **UNIX 系统：**的路径 sqlhosts file.
ONCONFIG	Informix 实例 ONCONFIG 文件的名称。

消息 *RETVAL*0 表示配置成功。

处理错误

如果发生错误，错误编号将以 *RETVAL*error_number 的形式显示。

要获取错误说明，请执行以下操作:

*Windows 系统：*在 Cell Manager 上，请参阅文件 Data_Protector_home\help\enu\Trouble.txt 。

*HP-UX 和 Solaris 系统：*执行：

```
/opt/omni/lbin/omnigetmsg 12 error_number
```

*其他 UNIX 系统：*执行：

```
/usr/omni/bin/omnigetmsg 12 error_number
```

备份 Informix Server 集成

This feature is available in the Premium Edition

集成提供以下类型的联机数据库备份:

Informix Server 备份类型

备份类型	描述
完整	完整备份 (级别 0)。
增量 1	增量备份 (级别 1)。备份自上次完整备份以来的更改。
2 级增量备份	增量备份 (级别 2)。备份自上次 1 级增量备份以来的更改。

ON-Bar 备份“除”以下内容之外的所有 dbobject，您“必须”使用文件系统备份进行备份:

哪些内容需要备份为文件系统

对象	位置
ONCONFIG 文件	***Windows 系统：***
oncfg_*SERVERNAME.SERVERNUM* 文件	*INFORMIXDIR* \etc
紧急引导文件，一个名为 ixbar.*server_id* 的 Informix Server 配置文件，其中 *server_id* 是 SERVERNUM 配置参数的值。	***UNIX 系统：***
UNIX 系统： sqlhosts 文件	*INFORMIXDIR* /etc 注意 这不适用于 Informix 版本 11.7 和 12.1。
blobspace 中的简单大对象数据	磁盘或光盘

重要说明备份这些对象所需的频率取决于其更改频率。但是，至少每天备份紧急引导文件，并始终在关键的 dbspace 备份之后备份。

哪些数据无需备份?

ON-Bar 不会备份以下项目，因为它会在还原过程中自动重新创建此类项目:

- 分配给 Informix 实例但尚未分配给 tblspace 范围的 dbspace 页面。
- 镜像块 (如果可访问相应的主数据块)。
- 临时 dbspace。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Informix Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在客户机中，选择“Informix Server 系统”。在群集环境中，选择虚拟服务器。

在“应用程序数据库”中，选择要备份的 Informix 实例。

在“用户和组/域”选项中，指定要在其下运行备份会话的帐户。

请确保此用户已加入 Data Protector admin 或 operator 用户组，并且具有 Informix Server 备份权限。此用户成为备份所有者。

- *UNIX 系统：*在“用户名”和“组/域名”中键入 informix 。
- *Windows 系统：*在“用户名”和“组/域名”中，键入用户名和域 (例如，用户名 Administrator ，域 DP)。必须为 Data Protector Inet 服务用户模拟设置此帐户。

单击“下一步”。

5. 如果尚未将 Informix 实例配置为与 Data Protector 一起使用，则会显示“配置 Informix”对话框。按照配置 Informix 实例中所述进行配置。
6. 选择要备份的 db 对象。

   对于 Informix 版本 11.7 和 12.1，如果已创建另一个数据库，则必须相应地选择系统数据库对象 rootdbs 、 physdbs 、 plog 、 llog 和 log dbs 。如果没有为还原会话一起选择这些对象，则会话失败。

   单击“下一步”。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。在“并发”选项卡中，指定并行备份流的数量和要使用的介质池。

   > **注意**除了整个系统备份以外，ON-Bar 还会同时备份和还原 dbobject，并为每个对象创建一个新进程。进程数受 Informix Server BAR_MAX_BACKUP 配置参数的限制。将 Informix 配置参数 BAR_MAX_BACKUP 设置为 Data Protector 并发。

   要指定可以备份到设备的资源类型，请单击“Informix”选项卡，选择所需的资源类型，然后单击“确定”。

   确保所选设备涵盖为备份指定的所有资源类型，且在启动备份时未锁定。理想情况下，请将每个资源备份到单独的设备。

   > **重要说明**对于逻辑日志备份，始终使用单独的设备，并确保 ONCONFIG 文件中的 LTAPEDEV 参数未设置为 /dev/null 或。

Informix Server 资源类型

资源类型	描述
B	Blobspace
CD	关键 dbspace (根 dbspace 或包含物理日志或逻辑日志文件的 dbspace)
L	逻辑日志
MR	Master root dbspace
ND	非关键 dbspace
R	根 dbspace
CF	关键文件 **注意**对于 Informix 版本 11.7 和 12.1，必须选择此资源。

提示选择另一组设备 (涵盖为备份指定的所有资源类型)，使它们能够在主组中的某些设备出现故障时接管相应任务。选择“负载均衡”选项，并将 Min 和 Max 参数设置为主设备数。

单击“下一步”。

8. 设置备份选项

   单击“下一步”。

9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份会话进行调度。

提示在使用之前预览备份规范的备份会话。

Informix Server 备份选项

选项		描述
备份类型	**存储空间备份** (默认)	在存储空间备份中，则 onbar 命令并行备份选定的存储空间和逻辑日志。从存储空间备份还原时，还必须还原逻辑日志，才能使数据一致。 存储空间备份与对大型数据库的整体系统备份相比速度更快。
	整体系统备份	在整个系统备份中，则备份 onbar 命令中所有 Informix 实例的 dbobject。ON-Bar 无法同时备份这些 dbobject；而是按顺序备份它们。整体系统备份对于灾难恢复或还原到其他客户机很有用。从整体系统备份还原时，必须要还原逻辑日志即可使数据一致。
Pre-exec **Post-exec**		指定在备份之前 (pre-exec) 或之后 (post-exec) 将由 Informix Server 系统上的 ob2onbar.pl 启动的命令。不要使用双引号、空格或特殊字符。仅提供命令的名称，该命令必须位于以下目录中: ***Windows 系统：*** *Data_Protector_home*\bin ***HP-UX、Solaris、Linux 系统:*** /opt/omni/lbin ***其他 UNIX 系统：*** /usr/omni/bin 如果已选择逻辑日志进行备份，最好添加 onmode -l 作为 pre-exec 命令以确保始终有日志文件要备份。如果没有要备份的日志文件，则备份失败。 如果 onmode -l 命令返回非零值，则 Data Protector 将此解释为错误，并且不启动备份会话。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Informix Server”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行以下命令：

```
omnib -informix_list backup_specification_name -test_bar
```

预览期间会发生什么?

1. Informix Server onbar 命令通过 -F 选项启动，该选项指定伪备份。这将测试是否已正确配置 Informix 实例进行备份。
2. Data Protector 测试配置的 Data Protector 部分。测试以下内容:
   - Informix 实例与 Data Protector 之间的通信
   - 备份规范的语法
   - 如果正确指定设备
   - 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

在开始备份会话之前，请执行以下操作:

1. 设置以下环境变量:
   1. *ONCONFIG*
      1. INFORMIXSQLHOSTS
      2. INFORMIXDIR
      3. INFORMIXSERVER
   2. *PATH* (将 $INFORMIXDIR/bin 添加到 *PATH*)
2. 相应地设置 *ONCONFIG* 文件中的 tapedev 和 ltapedev 变量。如果 tapedev 和 ltapedev 变量均不存在，则使用 informix 所有权创建文件，并至少创建 660 个权限。在 *ONCONFIG* 文件中设置这些路径。

备份方法

以下列任何方式启动 dbobject 的备份:

- 使用 Data Protector GUI。请参阅使用 Data Protector GUI。
- 使用 Data Protector CLI。请参阅使用 Data Protector CLI。
- 使用 Informix Server onbar 命令。请参阅使用 Informix Server 命令。
- *UNIX 系统：*使用 Informix Server log_full.sh 脚本。请参阅在 UNIX 上使用 Informix Server log_full.sh。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Informix Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 选择“备份类型”和“网络负载”。单击**确定**。

   备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

请执行以下命令：

```
omnib -informix_list backup_specification_name [-barmode InformixMode] [List_options]
```

其中， InformixMode 为下列项之一:

```
full|inf_incr1|inf_incr2
```

> **注意**Data Protector 术语 full、 inf_incr1 和 inf_incr2 备份分别等同于 Informix Server 术语 level-0、level-1 和 level-2 备份。

有关 List_options ，请参阅 omnib 手册页。

示例

要使用 Informix Server 备份规范 InformixWhole 启动完整备份，请执行以下操作:

```
omnib -informix_list InformixWhole -barmode full
```

要使用 Informix Server 备份规范 InformixIncr 启动增量备份 (级别 1)，请执行以下操作:

```
omnib -informix_list InformixIncr -barmode inf_incr1
```

使用 Informix Server 命令

使用 Informix Server onbar 命令从相关 Informix 实例所在的 Informix Server 系统启动 dbobject 的备份。

备份之前:

- 以用户 informix 登录 Informix Server 系统。
- 设置以下变量:

  Data Protector 和 Informix Server 变量

变量	描述
ONCONFIG	Informix 实例 ONCONFIG 文件的名称。
INFORMIXSQLHOSTS	*Windows 系统：*存在 Windows 注册表中的 sqlhosts 条目的系统。 *UNIX 系统：* sqlhosts 文件的路径名，例如 /applications/informix/etc/sqlhosts 。
INFORMIXDIR	Informix Server 主目录的路径名。
INFORMIXSERVER	Informix 实例的名称。
OB2APPNAME	Informix 实例的名称。
OB2BARLIST	对于“备份”，要用于备份的备份规范的名称。 对于“还原”，用于抢救逻辑日志的备份规范的名称。

- 确保 Informix 实例处于联机或静止模式。启动备份之后，在备份完成之前不要更改模式；更改模式会终止备份。仅备份联机 dbspace 和 blobspace。要列出联机 dbobject，请执行以下操作:

  Windows 系统： INFORMIXDIR\bin\onstat -d

  UNIX 系统： INFORMIXDIR/bin/onstat -d

  备份模式

备份模式	描述
联机	如果在备份期间必须可以访问 Informix 实例，请使用联机模式。联机备份可能会影响性能。
静止	使用静止模式消除备份中的部分事务。如果需要连续访问 Informix 实例，则静止备份可能不实用。

- 在创建完整备份之后，保留 ONCONFIG 文件、紧急引导文件以及 UNIX (也称为 sqlhosts 文件) 的副本。您需要此信息来还原 dbobject。

要备份 dbspace 的列表，请执行以下操作:

```
onbar -b dbspace_list
```

例如，要备份 dbspace dbspace1 和 dbspace3 ，请执行以下操作:

```
onbar -b dbspace1, dbspace3
```

在 UNIX 上使用 Informix Server log_full.sh

在 UNIX 上，当 Informix Server 在 Informix Server 上发出日志满事件警报时， log_full.sh 用于启动逻辑日志文件的备份。

要从 log_full.sh 脚本启用 Informix Server 备份，请执行以下操作:

1. 在 Informix 实例 ONCONFIG 文件中添加以下行:

   ALARMPROGRAM INFORMIXDIR/etc/log_full.sh 。

2. 如果 Informix Server 系统上未安装 Data Protector 用户界面，请创建 Informix Server 备份规范以仅备份逻辑日志，并编辑 INFORMIXDIR/etc/log_full.sh 。

   在文件的开头添加以下内容:

   export OB2BARLIST=backup_specification_name

   export OB2APPNAME=INFORMIXSERVER

3. 如果在 Informix Server 系统上已安装 Data Protector 用户界面，则创建 Informix Server 备份规范以仅备份逻辑日志。

手动和连续逻辑日志备份 要备份已满并准备备份的逻辑日志文件，请启动:

- 手动逻辑日志备份，用于备份所有完整逻辑日志文件并停在当前逻辑日志文件中。
- 连续逻辑日志备份，用于在每个逻辑日志文件变满时自动备份它们。如果无需监视逻辑日志文件，请使用此备份。

默认情况下，设置 ALARMPROGRAM 配置参数，以便 ON-Bar 执行连续备份。

> **重要说明**如果使用连续备份，请确保设备始终可用于逻辑日志备份过程。

要执行手动逻辑日志备份，请按照 Data Protector 和 Informix Server 变量中所述设置 OB2APPNAME 和 OB2BARLIST 环境变量，然后执行以下操作:

```
onbar -l
```

检查配置

在为 Informix 实例创建至少一个备份规范之后，可以检查 Informix 实例的配置。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Informix Server”。单击备份规范以显示要检查的 Informix 实例。
3. 右键单击“Informix 实例”，然后单击“检查配置”。

使用 Data Protector CLI

以用户 informix 登录 Informix Server 系统。从以下目录中:

Windows 系统： Data_Protector_home\bin

HP-UX 和 Solaris 系统： /opt/omni/lbin

其他 UNIX 系统： /usr/omni/bin

执行:

Windows 系统：

```
perl -I..\lib\perl util_informix.pl -CHKCONF INFORMIXSERVER
```

UNIX 系统：

```
util_informix.pl -CHKCONF INFORMIXSERVER
```

其中 INFORMIXSERVER 是 Informix 实例的名称。

成功的配置检查将显示消息 *RETVAL*0 。

如果发生错误，错误编号将以 *RETVAL*error_number 的形式显示。

还原 Informix Server 集成

This feature is available in the Premium Edition

Data Protector Informix Server 集成提供两种类型的还原:

Informix Server 还原类型:

还原类型	描述
完整数据库还原	从任何备份还原。ON-Bar 同时还原 dbobject 并重播逻辑日志一次。
整个系统还原	从整个系统备份还原。无论是否还原逻辑日志，ON-Bar 都会按顺序还原整个系统。如果不需要还原日志进行灾难恢复，或者还原到其他客户机时，整个系统还原适用于小型系统。

还原方法

以下列任一方式还原 dbobject:

- 使用 Data Protector GUI。请参阅使用 Data Protector GUI 还原。
- 使用 Data Protector CLI。请参阅使用 Data Protector CLI 还原。
- 使用 Informix Server onbar 命令。请参阅 使用 Informix Server 命令还原。

使用 Data Protector GUI

在“内部数据库”上下文中，展开“对象”或“会话”。要查看报告的详细信息，请右键单击该会话，并单击“属性”。

使用 Data Protector CLI

本地化数据库名称: 如果备份对象的名称包含来自不同 Unicode 语言组的字符 (例如，如果使用日语和拉丁字符)，则必须将 Data Protector 实用程序的输出重定向为使用 UTF-8 编码:

- 将环境变量 OB2_CLI_UTF8 设置为 1。
- 将终端上使用的编码设置为 UTF-8。

如果使用本地化数据库，且系统的区域设置使用相同的 Unicode 语言组，则无需进行任何更改。

1. 获取 Informix Server 备份对象的列表:

   omnidb -informix

2. 获取特定对象的备份会话列表，其中包括会话 ID:

   omnidb -informix object_name

   重要说明对于对象副本，请使用对象备份 ID (与对象备份会话 ID 相同)。不要使用对象副本会话 ID。

   要获取对象备份 ID 的信息，请执行以下操作:

   omnidb -session session_id -detail

3. 获取还原所需的介质列表:

   omnidb -session session_id -media

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“Informix Server”，展开其中已备份要还原数据的客户机，然后单击要还原的 Informix 实例。
3. 在“源”页中，选择要还原的对象。要还原整个数据库或整个系统，请选择“还原完整数据库”。

   > 对于 Informix 版本 11.7 和 12.1，如果已创建另一个数据库，则必须相应地选择系统数据库对象 rootdbs、 physdbs、 plog、 llog 和 logdbs。

4. 在“选项”页中，设置特定于 Informix Server 的还原选项。
5. 在“设备”页中，选择要用于还原的设备。
6. 如果执行整个系统还原，且 Informix 实例处于联机模式，请执行以下命令使 Informix 实例处于脱机状态:

   ```
   onmode -ky
   ```

   单击**还原**。
7. 在“开始还原会话”对话框中，单击**下一步**。
8. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
9. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。
10. 如果已执行整个系统还原，请执行以下命令使 Informix 实例处于联机状态:

    ```
    onmode -m
    ```

Informix Server 还原选项

选项	描述
备份规范	用于在还原之前抢救仍在磁盘上的逻辑日志文件的备份规范。最好指定用于备份逻辑日志的备份规范。
用户名	*UNIX 系统：* Informix Server 备份所有者的用户名。 onbar 在指定用户的帐户下启动。
用户组	*UNIX 系统：* Informix Server 备份所有者的用户组。
恢复到客户机	要还原到的客户机。默认情况下，将还原到原始备份客户机。此选项仅对整个系统还原有效。
按日志编号还原	(此选项在“源”页中选择了“还原完整数据库”时才可用)。使用此选项可将数据还原到特定的日志编号。如果存在进一步日志，则 ON-Bar 不恢复它们。此选项调用 onbar -r -n last_log_number。
按日期还原	(此选项在“源”页中选择了“还原完整数据库”时才可用)。使用此选项可将数据还原到特定时间点。此选项调用 onbar -r -t time。
还原最新版本	选择此选项可还原最新备份版本。
整个数据库还原	(此选项在“源”页中选择了“还原完整数据库”时才可用)。选择此选项可执行整个系统还原。仅在从整个系统备份恢复时才使用此选项。如果存在整个系统备份，则 Data Protector 不自动进行检测。 Data Protector 将搜索最后一个完整系统备份，并从中还原。此选项调用 onbar -r -w。

> **重要说明**还原后，请确保在执行下一次还原之前已执行完整备份。

使用 Data Protector CLI 进行还原

在开始还原过程之前，按照“Data Protector 和 Informix Server 变量”(第 32 页) 备份 Informix Server 集成中所述，设置 OB2BARLIST 环境变量。例如：

```
set OB2BARLIST=dbspace5
```

运行以下命令：

```
omnir -informix -barhost ClientName -barcmnd ob2onbar.pl -user User:Group -appname INFORMIXSERVER -bararg OnBarRestoreArguments [INFORMIX_OPTIONS]
```

ClientName	Informix Server 系统的名称。在群集环境中，指虚拟服务器的名称。
INFORMIXSERVER	Informix 实例的名称。
User, Group	**UNIX 系统**：用户名及其用户组名称。
OnBarRestoreArguments	ON-Bar 还原参数。将每个参数放在双引号中。
INFORMIX_OPTIONS	常规还原选项的子集。

重要说明还原后，请确保在执行下一次还原之前已执行完整备份。

示例

要使用 bar 参数 -r rootdbs 在 UNIX 系统 computer 上还原 Informix 实例 informix_instance1 ，请执行以下操作:

```
omnir -informix -barhost computer -barcmnd ob2onbar.pl -user informix:informix -appname informix_instance1 -bararg "-r rootdbs"
```

使用 Informix Server 命令还原

还原前:

- 以用户 informix 登录 Informix Server 系统。
- 按照 Data Protector 和 Informix Server 变量中所述，设置 Data Protector 和 Informix Server 变量。
- 如果发生磁盘故障，请通过执行以下命令来抢救仍在磁盘上的逻辑日志文件:

  ```
  onbar -l -s
  ```

以下是用于还原的 onbar 命令语法的示例。

重要说明还原后，请确保在执行下一次还原之前已执行完整备份。

还原 dbspace、blobspace 和 逻辑日志

1. 如果要还原的 Informix 实例处于联机模式，请将其脱机:

   ```
   onmode -ky
   ```

2. 还原 dbspaces 、 blobspaces 和相应的逻辑日志:

   完成数据库还原: onbar -r

   整个系统还原: onbar -r -w

3. 还原后，将 Informix 实例联机:

```
onmode -m
```

仅还原 dbspace 和 blobspace

要在没有逻辑日志的情况下还原 dbspaces 和 blobspaces，请执行:

```
onbar -r -p
```

还原特定的 dbspace 或 blobspace

要还原特定的 dbspace (例如 dbspace_1)，请执行:

```
onbar -r dbspace_1
```

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

您还可以使用监视器上下文监视安装有 User Interface 组件的任何 Data Protector 客户机的会话。

当 ON-Bar 遇到错误或需要警告的情况时，它会将消息写入 Informix Server ON-Bar 消息文件。此文件的完整路径名在 BAR_ACT_LOG 配置参数中指定。

要成功中止备份或还原会话，请将 ON-Bar BAR_RETRY 配置参数设置为 0 。此参数指定在第一次尝试失败后 ON-Bar 重试备份或还原的次数。

Lotus Notes/Domino Server 集成

This feature is available in the Premium Edition

Data Protector 与 Lotus Notes/Domino Server 集成可联机备份数据库和事务日志。在备份期间，可主动使用数据库。

Data Protector 备份所有类型的数据库: 存储数据库、模板和邮箱 (NSF、NTF 和 BOX 文件)。可以备份和还原单个数据库或整个服务器 (Lotus Notes/Domino Server 下的所有数据库)。

还可以：

- 在“存档”日志记录有效时备份存档的事务日志。
- 当前事务日志。

Data Protector 提供以下类型的交互式备份和安排的备份：

Lotus Notes/Domino Server 备份类型

备份类型	描述
完整	备份所有选定的 Lotus Notes/Domino Server 数据库。 如果选择了存档日志，还会备份尚未备份的存档日志，其中包括目前在用的日志。
增量型	备份至少符合下列两项条件中一项的选定 Lotus Notes/Domino Server 数据库： • 自上次备份以来对数据库所做更改的大小超过**日志更改量 (KB)** 选项所设置的大小。 • 用于数据库的 Lotus Notes/Domino Server DBIID 已更改。 不会备份不符合至少一项条件的数据库。 如果选择了存档日志，还会备份尚未备份的存档日志。

Data Protector 提供以下还原选项：

- 还原但不恢复。
- 还原 Lotus Notes/Domino Server 数据库的特定备份版本，并可以应用从事务日志进行备份以来做出的更改。
- 将 Lotus Notes/Domino Server 数据库恢复到一个特定的时间点或最新的一致状态。
- 将数据库还原到原始备份位置以外的 Lotus Notes/Domino Server 位置。
- 恢复时自动还原存档的事务日志。

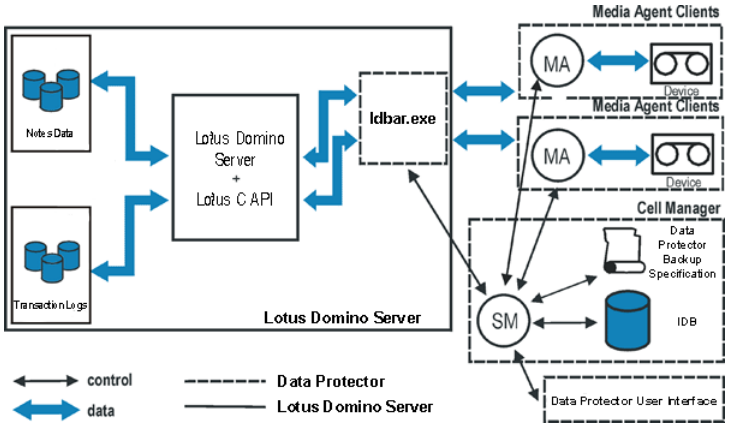
即使 Lotus Notes/Domino Server 正在运行时也可以还原数据库，并且对当前正在使用的其他数据库没有影响。要允许使用联机备份中的日志进行恢复，必须设置 Lotus Notes/Domino Server 才能使用“存档”事务日志记录。

本节提供特定于 Data Protector Lotus Notes/Domino Server 集成的信息。

集成概念

Data Protector Lotus Notes/Domino Server 集成通过使用 Lotus C API 提供 Lotus Notes/Domino Server 的联机备份、还原和恢复。Data Protector Lotus Notes/Domino Server 集成架构显示集成的体系结构。

Data Protector Lotus Notes/Domino Server 集成体系结构



图例

图例	描述
SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
ldbar.exe	集成的中心组件安装在 Lotus Notes/Domino Server 系统上，控制在 Lotus Notes/Domino Server 与 Data Protector 备份和还原过程之间的活动。
Lotus C API	由 Lotus 定义的接口，通过它可以在 Data Protector 与 Lotus Notes/Domino Server 之间传输数据。
Notes 数据	一组 Lotus Notes/Domino Server 数据库，用户可以在其中创建、更新、存储和跟踪各种格式的文档。
MA	Data Protector 常规介质代理。
备份规范	要备份的对象列表、备份设备和要使用的选项。
IDB	Data Protector 内部数据库。

Lotus Notes/Domino Server 数据库通过并行流进行备份，每个流都传输多个数据库。流数量等于所有使用设备的并发总和。并发在备份规范中定义。

满足 Lotus Notes/Domino Server 集成的先决条件

以下是 Lotus Notes/Domino Server 集成的先决条件:

- 确保已正确安装和配置 Lotus Notes/Domino Server。

  Lotus Domino 群集: 配置 Lotus Domino 群集时，请决定是否需要用于群集的专用 LAN。主要好处是可在使用群集复制和服务器探测时分离由群集创建的网络流量，从而在主 LAN 上留下更多带宽。如果预计会有大量群集复制活动，请创建专用 LAN。为此，请在每个群集服务器中安装一个额外的网络接口卡，并通过专用集线器或交换机连接这些卡。

- 确保已正确安装 Data Protector。

  要执行备份或还原的每个 Lotus Notes/Domino Server 系统均必须安装 Data Protector Lotus 集成组件。

- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 Lotus Notes/Domino Server 系统与 Cell Manager 是否正常通信，请在 Lotus Notes/Domino Server 系统上配置并运行 Data Protector 文件系统备份和还原。

  Windows 系统 :

  - 在 Windows 操作系统上，为具有相应 Lotus Notes/Domino Server 权限的用户配置 Data Protector Inet 服务用户模拟，以便运行备份和还原。

  要允许从联机备份中恢复，必须设置 Lotus Notes/Domino Server 才能使用事务日志记录。通过这种方式，事务会存储到事务日志目录，并可用于在数据库恢复期间应用或撤消数据库事务。

  您可以对事务日志执行每日完整备份，而不是完整数据库备份。

  启用事务日志记录后，系统将自动记录所有数据库。启用事务日志记录后，日志目录中可能会出现多个 S0000000.TXN 文件。

事务日志记录样式

日志记录样式	描述
线性 (循环) 日志记录	默认模式。Lotus Notes/Domino Server 不断重用相同的日志文件，该文件以指定大小定义，因此在事务日志填满后，会覆盖旧事务日志。您只能恢复存储在事务日志中的事务。无法恢复存档事务日志。
存档日志记录	Lotus Notes/Domino Server 在备份之前不会重用日志扩展区。对于因系统出现故障时数据库打开而没有刷新到磁盘的数据库事物，系统可使用事务日志以应用或撤消它们。

重要说明要在增备份量备份中的日志文件，必须将事务日志记录设置为“存档”日志记录。

- **Lotus Domino 群集:**以与普通 Domino 数据库相同的方式，从 Domino server 备份复本数据库。

与操作系统群集不同，Domino 群集不涉及虚拟服务器或虚拟 IP 地址。因此，在创建 Data Protector 备份规范时，请为备份的源数据库选择通用物理主机名。

安装 Lotus Notes/Domino Server 客户机

This feature is available in the Premium Edition

假设 Lotus Notes/Domino Server 已启动并正在运行。为了能够备份 Lotus Notes/Domino Server 数据库，您需要在安装过程中选择 Lotus 集成和磁盘代理组件。为了能够将 Data Protector 备份文件系统数据用于以下目的，您需要“磁盘代理” 组件:

- 备份*无法*使用 Lotus 集成代理备份的重要数据。它们是所谓的非数据库文件，需要备份这些文件 (notes.ini 、 desktop.dsk 和所有 *.id 文件) 才能为 Lotus Notes/Domino Server 提供完整的数据保护解决方案。
- 测试文件系统备份，以解决通信和其他与应用程序及 Data Protector 有关的问题。

Lotus Domino Cluster

在将用于备份的 Domino 服务器上安装 Lotus 集成和磁盘代理组件，并且如果计划将 Domino 数据库还原到包含这些数据库的复本的其他 Domino 服务器上，请同时在这些 Domino 服务器上安装这两个组件。

配置 Lotus Notes/Domino Server 集成

This feature is available in the Premium Edition

您需要配置 Lotus Notes/Domino Server 用户以及要备份或还原的每个 Lotus Notes/Domino Server。

启用事务日志记录

在 Lotus Notes/Domino Server 系统上，使用 Lotus Domino 管理员。此外，使用 Web 管理员或者编辑 notes.ini 文件。

在群集环境中，启用所有群集节点上的事务日志记录。

要启用事务日志记录并设置“存档”日志记录，请执行以下操作:

1. 启动 Lotus Domino 管理员。
2. 登录 Lotus Notes/Domino Server 并选择“配置”选项卡。
3. 展开“服务器”，选择“所有服务器文档”，然后选择所需的 Lotus Notes / Domino Server。
4. 选择“事务日志”选项卡并设置合适的值。
5. 保存设置并重新启动 Lotus Notes/Domino Server，使所做的更改生效。

配置 Lotus Notes/Domino Server 用户

在 UNIX 上，将 Lotus Notes/Domino Server 管理员添加到 Data Protector admin 或 operator 用户组。您需要在备份规范中指定此用户。默认情况下，该用户在 notes 组中为 notes。

此外，将 Lotus Notes/Domino Server 系统上的操作系统 root 用户添加到 Data Protector admin 或 operator 用户组。

配置 Lotus Notes/Domino Server 系统

使用 Data Protector GUI

1. 在上下文列表中，单击“备份”。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Lotus Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在客户机中，选择“Lotus Notes/Domino Server 系统”。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，选择要备份的 Lotus Notes/Domino Server 的名称。

   有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 在“配置 Lotus”对话框中，指定 Lotus Notes/Domino Server 系统上 notes.ini 文件的路径名。

   检查并根据需要更新其他自动确定的选项。

   单击**确定**。

   如果发生错误，请单击“详细信息”。
6. 此时已完成集成配置。退出 GUI 或继续在步骤 6 创建备份规范。

使用 Data Protector CLI

在 Lotus Notes/Domino Server 系统上，执行:

Windows 系统：

```
Data_Protector_home\bin\util_notes.exe -CONFIG -SERVER:SRV_NAME -INI:notes.ini_file
```

Solaris 系统：

/opt/omni/lbin/util_notes.exe -CONFIG -SERVER:SRV_NAME -INI:notes.ini_file [-HOMEDIR:Lotus_home_directory] [-DATADIR:Domino_data_directory] [-EXECDIR:Domino_executables_directory]

AIX 系统：

/usr/omni/bin/util_notes.exe -CONFIG -SERVER:SRV_NAME -INI:notes.ini_file [-HOMEDIR:Lotus_home_directory] [-DATADIR:Domino_data_directory] [-EXECDIR:Domino_executables_directory]

参数描述

SRV_NAME	Lotus Notes/Domino Server 名称。
notes.ini_file	Lotus Notes/Domino Server notes.ini 文件的路径名。
Lotus_home_directory	Lotus Notes/Domino Server 主目录的路径名。
Domino_data_directory	Lotus Notes/Domino Server 数据目录的路径名。
Domino_executables_directory	Lotus Notes/Domino Server 可执行文件目录的路径名。

注意*UNIX 系统：*如果未指定 –HOMEDIR 、 –DATADIR 和 –EXECDIR 选项，则会自动从 notes.ini 文件中读取值。

消息 *RETVAL*0 表示配置成功。

示例

Windows 系统：

Data_Protector_home\bin\util_notes.exe -CONFIG –SERVER:BLUE –INI:d:\Lotus\Domino\BLUE\notes.ini

Solaris 系统：

/opt/omni/lbin/util_notes.exe -CONFIG -SERVER:BLUE -INI:/opt/lotus/notesdata/notes.ini -HOMEDIR:/opt/lotus -DATADIR:/opt/lotus/notesdata -EXECDIR:/opt/lotus/notes/latest/hppa

备份 Lotus Notes/Domino Server 集成

This feature is available in the Premium Edition

集成提供以下类型的备份:

Lotus Notes/Domino Server 备份类型

备份类型	描述
完整	备份所有选定的 Lotus Notes/Domino Server 数据库。 如果选择了存档日志，还会备份尚未备份的存档日志，其中包括目前在用的日志。
增量	备份至少符合下列两项条件中一项的选定 Lotus Notes/Domino Server 数据库： • 自上次备份以来对数据库所做更改的大小超过**日志更改量 (KB)** 选项所设置的大小。 • 用于数据库的 Lotus Notes/Domino Server DBIID 已更改。 不会备份不符合至少一项条件的数据库。 如果选择了存档日志，还会备份尚未备份的存档日志。

Lotus Notes/Domino Server 数据库包含以下文件:

- Notes 存储工具文件 (**NSF** 文件)
- Notes 模板工具文件 (**NTF** 文件) - 用于创建新 NSF 数据库的模板
- 邮箱文件 (**BOX** 文件) - 邮件路由器使用的文件
- 事务日志文件，名为 `SXXXXXXX.TXN` ，其中 `XXXXXXX` 是一个 7 位数字，该数字随每个新事务文件自动递增

  在备份后，Lotus Notes/Domino Server 自动回收存档的事务日志。

重要说明频繁备份存档日志。备份后，Lotus Notes/Domino Server 会在需要时使用新的日志条目将其覆盖。否则，将创建新的日志文件，这会占用额外的磁盘空间。因为存档日志记录样式对于日志文件的数量没有任何大小限制，因此可能导致磁盘空间不足。

要删除所有备份的存档日志，请重新启动 Lotus Notes/Domino Server 实例。建议不要手动删除存档日志。

提示要加速 Lotus Notes/Domino Server 备份，请从备份规范中排除 NTF 文件。创建单独的备份规范以备份 NTF 文件。这些文件不需要频繁备份，因为它们不会更改。

您“必须”使用文件系统来备份以下非数据库文件:

- notes.ini
- desktop.dsk
- 所有 *.id 文件

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击“备份”。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Lotus Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在客户机中，选择“Lotus Notes/Domino Server 系统”。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，选择要备份的 Lotus Notes/Domino Server。

   有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 如果未将 Lotus Notes/Domino Server 配置为与 Data Protector 一起使用，则会显示“配置 Lotus”对话框。按照配置 Lotus Notes/Domino Server 系统中所述配置集成。
6. 选择要备份的 Lotus Notes/Domino Server。

   单击“下一步”。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。

   单击“下一步”。
8. 设置备份选项。

   单击“下一步”。
9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

> **提示**在使用之前预览备份规范的备份会话。

Lotus Notes/Domino Server 备份选项

备份选项	描述
日志容量更改 (KB)	适用于增量备份。如果至少满足以下两个条件中的一个条件，则备份会跳过数据库： • 要备份的数据库的日志容量小于由该选项指定的值。 • 用于数据库的 Lotus Notes/Domino Server DBIID 未更改。 如果数据库超过指定日志容量，或者用于数据库的 Lotus Notes/Domino Server DBIID 未更改，则会备份数据库。
pre-exec、post-exec	指定在备份之前 (pre-exec) 或之后 (post-exec) 将由 Lotus Notes/Domino Server 系统上的 ldbar.exe 启动的命令。命令必须位于以下目录中： *Windows 系统：* Data_Protector_home\bin *Solaris 系统：* /opt/omni/lbin *AIX 系统：* /usr/omni/bin 在备份规范中，仅提供文件名。

备份缓冲区大小	备份期间用于读取和写入数据的缓冲区的大小。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 **Data Protector GUI**

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“内部数据库”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

   预览成功后将显示消息“会话已成功完成”。

使用 **Data Protector CLI**

可以在 Lotus Notes/Domino Server 系统上或已安装 Data Protector 用户界面的同一 Data Protector 单元中的任何 Data Protector 客户机系统上执行测试。

请执行以下命令：

```
omnib -lotus_list backup_specification_name -test_bar
```

预览期间会发生什么?

该命令测试配置的 Data Protector 部分。测试以下内容:

- Lotus Notes/Domino Server 与 Data Protector 之间的通信。
- 备份规范的语法。
- 如果正确指定设备。
- 如果必要的介质位于设备中。

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份十分有用。

您可以使用以下命令启动备份:

- Data Protector GUI。
- Data Protector CLI。请参阅 omnib 手册页。

使用 **Data Protector GUI**

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“内部数据库”。右键单击要使用的备份规范，然后单击“启动备份”。

3. 选择“备份类型”和“网络负载”。单击**确定**。

   备份会话成功后将显示消息“会话已成功完成”。

性能调整

通过微调以下备份设备参数，可以明显缩短“备份”所需的时间:

- 并发
- 块大小

并发性对备份性能的影响远大于块大小。测试表明，当使用较低的并发值和中等块大小 (256 kB) 时，可以获得更好的结果。最佳值仍取决于您的环境。

通过尽可能将“并行性”选项设置得高一些，可以进一步提高“还原”性能。因此，Data Protector 将自动创建最合适的流数。

检查配置

在至少为 Lotus Notes / Domino Server 创建一个备份规范后，可以使用 Data Protector GUI 检查 Lotus Notes/Domino Server 的配置。如果使用 Data Protector CLI，则不需要备份规范。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“内部数据库”。单击“备份规范”以显示要检查的服务器。
3. 右键单击该对象，并单击“检查配置”。

使用 Data Protector CLI

在 Lotus Notes/Domino Server 系统上，从以下目录中:

Windows 系统： Data_Protector_home\bin

Solaris 系统： /opt/omni/lbin

AIX 系统： /usr/omni/bin

执行:

```
util_notes.exe -CHKCONF -SERVER:SRV_NAME
```

Data Protector 检查指定目录和文件的路径。

消息 *RETVAL*0* 表示配置成功。

处理错误

如果发生错误，错误编号将以 *RETVAL*error_number* 的形式显示。

要查看错误描述:

Windows 系统：*在 Cell Manager 上，请参阅文件* Data_Protector_home\help\enu\Trouble.txt

*Solaris 系统：*执行：

```
/opt/omni/lbin/omnigetmsg 12 error_number
```

*AIX 系统：*执行：

/usr/omni/bin/omnigetmsg 12 error_number

还原 Lotus Notes/Domino Server 集成

This feature is available in the Premium Edition

您可以将数据库直接还原到 Lotus Notes/Domino Server 系统。还原数据库时，数据库将脱机、还原，然后联机。如果需要，还可还原事务日志。如果已选择恢复，则在恢复过程中会自动执行对存档日志的还原。

如果未访问数据库，则可以在服务器联机时还原数据库还原。新还原的 Lotus Notes/Domino Server 数据库处于非活动状态。如果您访问它，它将自动联机，但不会执行使用备份日志的恢复。要获取数据库的上一个可能的一致状态，或者执行到特定时间点的恢复，请使用“恢复”选项。

您可以将数据库还原到:

- 它在备份时的原始位置。

  选择此选项可替换损坏或已删除的数据库。
- 不同位置。

  选择此选项可保持原始数据库的完整性。

无法恢复到其他客户机系统。

要还原 Lotus Notes/Domino Server 数据库，请使用 Data Protector GUI 或 CLI。

查找要还原的信息

您可以找到有关在 Data Protector IDB 中使用的备份会话和介质的详细信息。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在“内部数据库”上下文中，展开“对象”或“会话”。要查看报告的详细信息，请右键单击该会话，并单击“属性”。

提示要查看备份对象中包含哪些文件，请单击“消息”选项卡。在不同会话中创建的同名备份对象 (例如， ARIEL:Databases:1 [Lotus]) 可能包含不同的文件。

使用 Data Protector CLI

1. 获取在特定会话中创建的 Lotus Notes/Domino Server 对象的列表:

   ```
   omnidb -session session_id
   ```
2. 查看特定会话的特定 Lotus Notes/Domino Server 对象中包含哪些 Lotus Notes/Domino Server 数据库:

   ```
   omnidb -lotus client:Lotus_instance::stream_id -session session_id -catalog
   ```

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“Lotus Server”，展开从中备份数据的客户机，然后选择要还原的实例。
3. 在“源”页面中，选择要还原的对象。

注意“源”页面中会列出所有已备份的数据库。从特定备份会话还原多个数据库时，请确保数据库在选定备份会话中备份。如果不是，则在还原时出现警告“未在数据库中找到对象”。从不同的备份会话进行还原需要单独的还原会话。唯一的例外是未指定备份会话时。在这种情况下，Lotus 集成代理将查找要还原的每个数据库的最新备份版本。

您可以在“选项”页中选择备份版本 (Lotus Notes/Domino 服务器还原选项)。单击“浏览”以选择其他备份版本。

4. 在“目标”页中，设置目标选项。

   重要说明如果还原到的位置已驻留正在被还原的具有相同文件名的数据库，则该数据库将脱机并删除。

5. 在“选项”属性页中，设置还原选项。
6. 在“设备”页中，选择用于还原的设备。

   单击**还原**。
7. 在“开始还原会话”对话框中，单击**下一步**。
8. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
9. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

有关详细信息，请参阅 omnir 手册页。

仅限本地化数据库: 如果已备份对象的名称包含无法使用当前语言组 (在 Windows 上) 或代码页 (在 UNIX 上) 显示的字符:

- 将环境变量 OB2_CLI_UTF8 设置为 1 。
- *Windows 系统：*将终端使用的编码设置为 UTF-8。

如果未设置，则 Data Protector CLI 命令 (例如 omnidb) 返回的备份对象的名称，在将参数提供给其他 Data Protector 命令 (例如 omnir) 时可能无法使用。

还原选项

指定特定于 Data Protector Lotus Notes/Domino Server 集成的目标和还原选项。如果目标系统是 UNIX 系统，也请指定特定于 UNIX 的选项。

目标选项

目标选项	描述
恢复到客户机	默认情况下，Lotus Notes/Domino Server 数据库还原到从中备份它们的同一客户机。要还原到另一个客户机，请从下拉列表中选择新客户机，或在文本框中键入其名称。客户机必须是 Data Protector 单元的一部分，并且安装了 Lotus Notes/Domino Server 集成。
恢复到实例	默认情况下，Lotus Notes/Domino Server 数据库还原到从中备份它们的同一 Lotus Notes/Domino Server 实例。要还原到另一个实例，请从下拉列表中选择新实例，或在文本框中键入其名称。必须配置该实例才能与此集成一起使用。
还原到原始位置	默认情况下，数据库还原到从中备份它们的同一目录（在原始系统上或在选择的某些其他系统上）。
还原到新位置	使用此选项可以将数据还原到另一个目录。指定要将数据还原到的 Lotus Notes/Domino Server 数据目录的相对路径。

示例

Lotus Notes/Domino Server 数据目录位于:

Windows 系统： C:\Lotus\Domino\BLUE\

UNIX 系统： /opt/lotus/notesdata/BLUE/

要将数据库还原到目录，请执行以下操作:

Windows 系统： C:\Lotus\Domino\BLUE\restore_dir\

UNIX 系统： /opt/lotus/notesdata/BLUE/restore_dir/

选择“还原到新位置”并输入 type restore_dir 。还原数据库的文件名与备份时的文件名相同。

还原选项

还原选项	用户名	*UNIX 系统：*Lotus Notes/Domino Server 备份所有者的用户名，例如 notes 。
	用户组	*UNIX 系统：*Lotus Notes/Domino Server 备份所有者的用户组，例如 notes 。
	备份版本	默认情况下，从数据库的最后一个完整备份执行还原。单击浏览可以选择除最后一个备份之外的备份版本。
	并行性	指定应使用多少并行流还原数据。默认值：1.
恢复类型选项	恢复（最后可能一致的状态）	选择此选项可以将数据库恢复到最后一个可能一致的状态。如果在恢复期间需要，这还包括存档的事务日志的还原。
	时间点恢复	应将数据库状态恢复到的时间点。单击**浏览**可以指定希望的日期和时间。只有在指定的日期和时间之前写入的事务才应用于数据库。
	不要恢复	默认选项。选择此选项可以还原数据库，而不从备份日志恢复它们。在备份之后执行的事务不会反映在还原的数据库中。
生成新 ReplicaID		此选项仅适用于恢复类型为“恢复 (最后可能的一致状态)”的情况。如果选择了此选项，则会向每个还原的存储数据库（NSF 数据库）都分配一个新复本 ID。 默认：未选择。

在 Lotus Domino 群集环境中还原

以下是还原 Domino 数据库时要考虑的典型情况。

无需恢复即可还原复本数据库

在这种情况下，复本数据库将还原到备份时的状态。存档日志的内容将被忽略，因此不会执行恢复到可能的最新状态。

即使在将已还原复本数据库从已还原目标 Domino 群集服务器复制到包含复制数据库的 Domino 群集服务器时使用“推送”复制样式，包含复制数据库的 Lotus Domino 群集服务器也会保留其最新状态。

如果使用“推送”或“推送/拉取”复制样式来复制还原的复本数据库，则已还原的复本数据库与复制的数据库一样恢复到最新状态。还原之后收集的状态将会丢失。

如果还原的复本数据未复制且恢复到上一个一致状态，则永远不得使用“推送”或“推送/拉取”复制样式从还原的 Domino 群集服务器中复制它。

使用恢复还原到可能的最新状态

在这种情况下，通过应用目标系统的存档日志，数据库将还原并恢复到可能的最新状态。如果另一个 Lotus Domino 群集服务器包含已还原数据库的复本，则此复本将已处于最新状态。

如果还原目标 Lotus Domino 群集服务器的存档日志不允许恢复到最新状态，请对从还原的目标 Domino 群集服务器到包含复本的其他 Domino 群集服务器使用“推送”或“推送/拉取”复制样式，以便复制已还原数据库并将其恢复到最新状态。

时间点恢复

在这种情况下，无论最新存档日志包含什么，数据库都将还原到选定备份时间的时间点状态。

如果另一个 Lotus Domino 群集服务器包含已还原数据库的复本，该复本数据库的状态比已还原数据库更新，则即使在从还原的目标 Domino 群集服务器复制到包含复本数据库的其他 Domino 群集服务器时使用“推送”复制样式，复本数据库也将保留其最新状态。

如果使用“推送”或“推送/拉取”复制样式将时间点恢复的数据库从已还原目标 Domino 群集服务器复制到包含复本数据库的其他 Domino 群集服务器，则时间点恢复数据库与复制的数据库一样恢复到最新状态。在时间点恢复之后收集的状态将会丢失。

如果不对时间点恢复的数据库进行复制并恢复到上一个一致状态，则永远不得使用“推送”或“推送/拉取”复制样式从还原的 Domino 群集服务器中复制它。您还可以按如下方式实现此目的:

1. 在还原之前，从其他 Domino 群集服务器删除已复制数据库的所有复本数据库。
2. 按照以上描述还原已复制数据库。
3. 在 Domino 群集服务器上，通过在其中删除 (在 步骤 1 中) 复本的数据库，创建已复制数据库的新复本。

这样，复本将包含已还原的时间点状态，而不是最新状态。

还原到新位置

在这种情况下，数据库将还原到的新位置的 ID 与原始复制数据库及其复本相同。新数据库被视为复本数据库。还原状态取决于您在“选项”>“恢复类型”中选择的还原/恢复的类型。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

Microsoft 365 Exchange 在线集成

本主题概述了可用于备份和还原用户邮箱的 Data Protector Microsoft 365 (M365) Exchange Online 集成。

> **重要说明:**从 11.01 版本开始，Data Protector 支持云工作负载，为 Microsoft Exchange Online、Microsoft SharePoint Online、Microsoft OneDrive 和 Microsoft Teams 提供备份和还原解决方案。适用于云工作负载的 Data Protector 支持废弃用于备份用户邮箱的现有 Microsoft 365 Exchange Online 集成解决方案。有关详细信息，请参阅适用于云工作负载的 Data Protector 简介。
>
> 有了这个产品:
>
> - 不再支持用于备份用户邮箱的现有 Microsoft 365 Exchange Online 集成解决方案。
> - 仍然可以还原使用现有 Microsoft 365 Exchange Online 集成解决方案进行的旧用户邮箱备份。
>
> 使用适用于云工作负载的 Data Protector 进行任何新备份或还原这些备份。

Data Protector Microsoft 365 Exchange Online 集成会备份和还原以下 Microsoft 365 邮箱邮件:

- 来自各个邮箱的电子邮件
- 日历约会和活动
- 联系人
- 共享日历
- 邮箱设置

Data Protector 会提供 Microsoft 365 邮箱的完整和增量备份。安装 Microsoft 365 集成组件后，可以在“主页”上下文中查看以下 UI 选项:

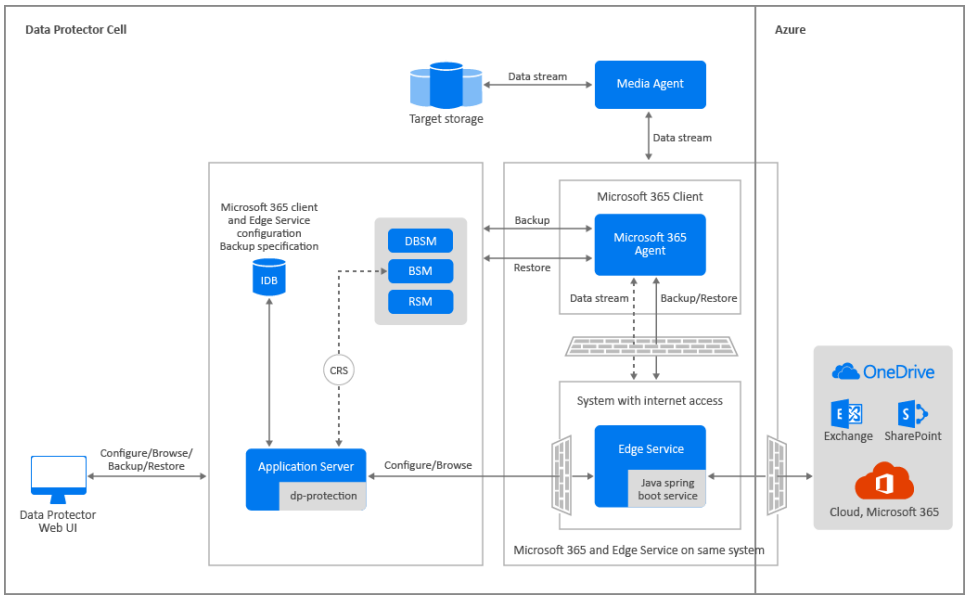
- 备份
- 还原
- 边缘服务 (“仪表板”>“客户机”>“边缘服务”)
- M365 设置 (“设置” >“M365”)

集成概念

Data Protector 使用 Microsoft 365 集成代理与 Microsoft 365 集成。Microsoft 365 集成组件在 Microsoft 365 客户机上安装 Microsoft 365 集成代理和边缘服务。

Microsoft 365 集成体系结构

下图说明了 Data Protector Microsoft 365 集成的体系结构。



Data Protector 使用 Microsoft 365 集成代理与 Microsoft 365 集成。Microsoft 365 集成组件在 Microsoft 365 客户机上安装 Microsoft 365 集成代理和边缘服务。

Azure 应用程序

Microsoft 365 使用 Azure Active Directory (AD) 进行用户身份和访问管理。Azure 应用程序是 Azure AD 使用的数字身份，用于代表外部用户、组织、应用程序或设备。为了使软件或应用程序与 Azure AD 通信，必须在 Azure 门户上注册 Azure 应用程序，才能为该应用程序创建身份配置，以允许其与 Azure AD 集成。有关 Azure 应用程序的详细信息，请参考 Microsoft 文档上的可用文档。

有关添加和注册 Azure 应用程序的信息，请参阅添加或注册 Azure 应用程序。

用户权限

下表列出了执行 Microsoft 365 邮箱的备份和还原操作所需的用户权限:

操作	所需权限
备份	以下权限之一: • 启动备份 • 启动备份规范 • 保存备份规范 • 作为 root 备份
还原	以下权限之一: • 开始还原 • 作为 admin 恢复 • 作为 root 还原

备份并行性

Microsoft 365 集成支持并行运行多个备份或还原会话。默认情况下，可以并行运行的最大备份或还原会话数为 10。不过，您可以根据需要修改此值。如果多个备份或还原会话并行运行，则可能导致诸如会话突然结束之类的问题。在这种情况下，您可以减少并发会话数或关闭多线程。使用 omnirc 文件中的选项可以修改并发会话数和启用或禁用多线程。

Microsoft 365 omnirc 选项

要自定义 Microsoft 365 代理的操作，可以在 Cell Manager 和代理系统上设置以下 omnirc 选项。

Omnirc 变量	默认值	描述
OB2_REST_CLIENT_SESSION_TIMEOUT	300 秒	Microsoft 365 代理等待边缘服务响应的超时。
OB2_O365_REST_RETRY_COUNT	5	REST API 调用失败后 Microsoft 365 代理重试与边缘服务联系的次数。
OB2_O365_REST_RETRY_INTERVAL	30000 毫秒	REST API 调用失败后 Microsoft 365 代理重试与边缘服务联系的时间。
OB2_O365AGENT_THREADED_BACKUP	TRUE	使用此选项可关闭 Microsoft 365 Exchange 备份和还原中的多线程。
OB2_O365AGENT_THREADS	10	此变量用于设置可并行运行的邮箱备份或还原会话的最大数量。

注意事项和限制

本节列出了 Data Protector Microsoft 365 集成、备份和还原中的注意事项和限制。

边缘服务

通过运行 setup.exe 或使用卸载向导修改边缘服务客户机时，不会显示“边缘服务代理配置” 页面。修改客户机后，必须在 edgeservice.properties 和 proxy.conf 文件中手动更新代理详细信息。

备份

- 不支持以下各项的备份和还原:
  - 公用文件夹和公用文件夹邮箱
  - 邮件提示
  - 生日日历
- 支持仅备份默认的根联系人文件夹。
- 不支持创建备份规范的副本。
- 支持仅备份和还原默认“日历”文件夹下存在的日历。
- 支持仅备份和还原默认“联系人”文件夹下存在的联系人。
- 不支持 Microsoft 365 备份的备份后对象验证。

Azure 应用程序

- 不支持编辑 Azure 应用程序。如果要修改 Azure 应用程序，则必须根据要求删除该应用程序并新建一个应用程序。
- 在“添加 Azure 应用程序” 和“注册 Azure 应用程序” 页上，“Cell Manager 租户名称” 字段仅支持英文名称。

还原

- 不支持在同一还原会话中从多个组织还原用户邮箱。
- 还原后，将不维护日历层次结构。

安装 Microsoft 365 客户机

要使用 Data Protector Microsoft 365 集成，必须在安装过程中选择“Microsoft 365 集成”组件。此组件在 Microsoft 365 客户机上安装 Microsoft 365 集成代理和边缘服务。Data Protector 通过边缘服务和 Data Protector Microsoft 365 集成代理与 Microsoft 365 租户集成。

安装 Microsoft 365 集成组件的推荐硬件配置是 16 GB RAM 和 4 个 CPU 内核。

> 注意: Windows 2016 及更高版本支持 Microsoft 365 集成组件安装。不支持远程安装。

按照以下步骤安装 Microsoft 365 集成组件:

1. 复制下载的安装包，然后将文件解压缩到本地目录。
2. 运行 setup.exe 文件。按照安装向导操作，并仔细阅读许可协议。单击“下一步”继续。
3. 在“安装类型”页面上，选择“客户机”，然后单击“下一步”。
4. 输入 Cell Manager 的名称。
5. 如果 Cell Manager 使用默认 5565 之外的端口，则更改端口号。通过单击“检查响应”可测试 Cell Manager 是否活动并使用所选端口。

   如果在安装期间指定了 Cell Manager，则作为安装的一部分，将在客户机中配置 Cell Manager 证书，但不会执行导入。

   单击“下一步”。
6. 选择“Microsoft 365 集成” 组件，然后单击“下一步”。
7. 在“边缘服务信息” 页面上，指定边缘服务登录用户的“用户名” 和“密码”。该用户帐户必须是管理员组的一部分。此外，指定将运行边缘服务的“端口”。
8. 单击“下一步”。将显示“边缘服务代理配置” 页面。
9. *可选*。在“边缘服务代理配置” 页上，选中“使用 Internet 代理” 复选框并指定以下详细信息:
   - 代理地址
   - 端口
   - 代理协议
   - 用户名
   - 密码

   如果您不想配置 Internet 代理，请取消选中“使用 Internet 代理” 复选框。
10. *可选*。选择“代理例外”，然后指定“要排除的域”。如果要排除多个域，请使用管道字符 (|) 分隔域。
    您在“边缘服务代理配置” 页面上指定的代理详细信息存储在 proxy.conf 和 edgeservice.properties 文件中。这些配置文件可从以下位置获取:
    ProgramData\OmniBack\Config\client\modules\edgeservice
    如果要在安装后更新代理设置，则可以编辑这些文件并进行所需的更改。
11. 单击“下一步” 继续。单击“完成” 完成安装。

导入 Microsoft 365 客户端

如果边缘服务与 Cell Manager 不在同一主机上，请按照下列步骤操作:

1. 通过在 Cell Manager 和 Microsoft 365 客户机之间建立安全的通信来导入 Microsoft 365 客户机。
    1. 在 Cell Manager 中运行以下命令:
       omnicc -secure_comm -configure_peer msoffice365client.mydomain.net
    2. 在 Microsoft 365 客户机上运行以下命令:
       omnicc -secure_comm -configure_peer cellmanager.mydomain.net
    3. 在 Cell Manager 中运行以下命令:
       omnicc -import_host msoffice365client.mydomain.net
2. 在 Cell Manager 上为 Microsoft 365 客户机添加边缘服务登录用户。运行以下命令。这是在边缘服务的安装过程中指定的用户。
   示例**:** omniusers -add -type w -usergroup admin -name "edgeservicelogonuser" -client "m365client.mydomain.net" -group "m365client" -pass <password>

配置 Microsoft 365 集成

先决条件

- 确保您拥有一个具有活跃订阅的 Azure 帐户。
- 在 Azure Active Directory 中为您的组织配置一个或多个发布者域。
- 确保完成 Microsoft 365 客户机、Cell Manager 和 NTP 服务器之间的时间同步。

配置集成

1. 更新代理设置
2. 配置边缘服务
3. 导入边缘服务
4. 添加或注册 Azure 应用程序

更新代理设置

> 重要说明:
>
> - 仅当安装过程中未提及边缘服务详细信息或者要在安装后修改详细信息时，才需要执行以下步骤。
> - 要在 proxy.conf 和 edgeservice.properties 文件中配置多个 nonProxyHost，请使用管道符号 (|) 作为主机的分隔符。

1. 更新 proxy.conf 文件中的 proxy 和 nonProxyHosts 详细信息。 proxy.conf 文件可从以下位置获得:
   <ProgramData>\OmniBack\Config\client\modules\edgeservice\proxy.conf
2. 运行以下命令以更新服务注册表:
   "<Data_Protector_Home>\OmniBack\bin\edgeservice\install_dp_edge_service.bat" update_service
3. 使用 proxy 和 nonProxyHosts 详细信息手动更新 edgeservice.properties 文件。 edgeservice.properties 文件可从以下位置获得:
   <ProgramData>\OmniBack\Config\client\modules\edgeservice\edgeservice.properties

配置边缘服务

在 Microsoft 365 客户机上执行以下步骤以配置边缘服务:

1. 检查 Windows Management Framework (WMF) 和 Microsoft .NET Framework 版本:
   - WMF 版本必须为 5.1。在 PowerShell 提示中运行以下命令以检查 WMF 版本:

     ```
     $PSVersionTable.PSVersion
     ```

   - Microsoft .NET Framework 必须为 4.5 版或更高版本。
2. 运行以下 Perl 脚本以创建边缘服务所需的密钥库和信任库证书:

   ```
   <Data_Protector_Home>\bin\perl <Data_Protector_Home>\bin\esgencert.pl
   ```

   > 注意: Perl 脚本必须以边缘服务登录用户身份运行。如果边缘服务登录用户属于管理员组但不是管理员用户，则通过以管理员身份打开命令提示符来运行上述脚本 (单击“开始” 按钮，键入 cmd，右键单击“命令提示符”图块，然后单击“以管理员身份运行”)。

   在脚本执行期间，显示以下消息:

   ```
   Executing esgencert.pl will remove exising edgeservice SSL certificates and create new certificates. After SSL certificates creation, script will re start edgeservice. Do you want to proceed?
   ```

   输入 **Y** 继续，或输入 **N** 取消脚本执行。

导入边缘服务

按照以下步骤导入边缘服务:

1. 转到“主页” 上下文，然后单击“客户机” 。
2. 从“边缘服务” 下拉列表中，选择“导入” 。
3. 在“边缘服务配置” 页面上，指定以下内容:
   - 主机名: 安装边缘服务的计算机的主机名。
   - 端口: 运行边缘服务的端口。
4. 单击“导入” 。

如果要删除边缘服务，请选择服务器，然后从“边缘服务” 下拉列表中选择“导出” 。

导出边缘服务

从单元中导出 Microsoft 365 客户机时，不会导出边缘服务。它继续列在“仪表板” 页上的“客户机” 部分中。按照以下步骤手动导出边缘服务:

1. 转到“主页” 上下文，然后单击“客户机” 。

2. 从“边缘服务” 下拉列表中，选择“导出” 。

添加或注册 Azure 应用程序

Microsoft 365 使用 Azure Active Directory (AD) 进行用户身份和访问管理。要与 Azure AD 通信，必须执行以下操作:

1. 向 Azure AD 注册应用程序以便为您的应用程序创建身份配置，以使其能够与 Azure AD 集成。
2. 在 Data Protector (DP) 中添加应用程序。

有关 Azure 应用程序的详细信息，请访问 https://docs.microsoft.com/。

Azure AD 管理 Microsoft 365 实例与 Data Protector Microsoft 365 集成代理之间的连接。您可以使用现有的 Azure 应用程序，也可以注册新的应用程序。DP 为您提供以下用于管理 Azure 应用程序的选项:

- 添加 **Azure** 应用程序: 使用此选项可将 Azure 应用程序添加到 DP。您可以添加现有应用程序，或者注册新应用程序，然后将该应用程序添加到 DP。有关注册 Azure 应用程序的详细步骤，请参阅注册 Azure 应用程序。
- 注册 **Azure** 应用程序: 使用此选项可在 Azure AD 中注册新的 Azure 应用程序。

> 注意: 如果要通过 DP 注册 Azure 应用程序，请确保已禁用 Azure AD 中的多因素身份验证。如果您不想禁用多因素身份验证，请通过 Azure 门户注册应用程序，然后使用上述“添加 Azure 应用程序” 选项。

Azure 应用程序通过 Microsoft Graph API 调用访问 Microsoft 365 数据。Azure 应用程序需要一组权限才能访问 Microsoft Graph 中的数据。使用“注册 Azure 应用程序” 选项注册 Azure 应用程序时，该应用程序是通过以下 Microsoft Graph 权限创建的:

Microsoft 365 的权限

权限名称		类型	描述
Microsoft Graph	Application.ReadWrite.All	应用程序	允许应用程序代表登录用户创建、读取、更新和删除应用程序。
	Calendars.ReadWrite	应用程序	允许应用程序创建、读取、更新和删除用户日历中的事件。
	Contacts.ReadWrite	应用程序	允许应用程序创建、读取、更新和删除用户联系人。
	Directory.Read.All	应用程序	允许应用程序读取组织目录中的数据，例如用户、组和应用程序。
	Mail.ReadWrite	应用程序	允许该应用程序创建、阅读、更新和删除用户邮箱中的电子邮件。此权限不包括发送电子邮件的权限。
	MailboxSettings.ReadWrite	应用程序	允许应用程序创建、读取、更新和删除用户的邮箱设置。不包括直接发送电子邮件的权限，但允许应用程序创建可以转发或重定向消息的规则。
	Reports.Read.All	应用程序	允许应用程序在无需登录用户的情况下读取与 Microsoft 365 和 Azure Active Directory 相关的所有服务使用情况报告。
Exchange	full_access_as_app	应用程序	允许应用程序使用对所有邮箱具有完全访问权限的 Exchange Web 服务。

添加多租户 Azure 应用程序

已向其注册了多个租户的 Azure 应用程序称为多租户应用程序。DP 不支持注册多租户 Azure 应用程序。但是，如果您的组织已经在 Azure AD 中注册了多租户应用程序，则可以在 DP 中添加该应用程序以从所有关联的租户执行用户邮箱的备份和还原。在将多租户应用程序添加到 DP 之前，请确保将上述 Microsoft 365 的权限表中列出的所有权限都添加到该应用程序中。在多租户应用程序上添加或删除权限需要所有租户的管理员同意，该管理员有权访问多租户应用程序。

注册 Azure 应用程序

可以使用 DP GUI 或通过 Azure Active Directory 门户注册 Azure 应用程序。

要使用 DP GUI 在 Azure AD 中注册新的 Azure 应用程序，请按照下列步骤操作:

1. 打开“主页” 上下文，然后单击“设置” 。
2. 选择“Microsoft 365” ，然后单击“注册” 。
3. 在“注册 Azure 应用程序” 页上，指定以下内容:
   - **Cell Manager** 租户名称: 您选择的用于标识租户的名称。
   - **Azure** 管理员用户名和 **Azure** 管理员密码: 您在 Azure AD 中的管理帐户的用户名和密码。
   - 客户机密钥有效期: 客户机密钥有效的持续时间 (以月为单位)。边缘服务会在到期日期之前自动更新客户机密钥并删除旧的客户机密码。对于使用 DP 2021.02 注册的应用程序，您必须在第一次通过 Azure 门户更新密钥后手动删除旧客户机密钥。对于后续更新，旧的客户机密钥将自动删除。
     在客户机密钥自动续订期间，如果应用程序是使用 DP 2021.02 注册的，则“客户机密钥有效期”将设置为六个月。如果应用程序是使用更高版本的 DP 注册的，则该应用程序的“客户机密钥有效期”保持不变。

除了这些字段之外，此页面还显示 Azure 应用程序的“权限”设置。

4. 单击“提交”。

要通过 Azure Active Directory 门户在 Azure AD 中注册新的 Azure 应用程序，请按照下列步骤操作:

1. 登录 Azure Active Directory 门户。
2. 注册新的 Azure 应用程序，并添加“Microsoft 365 的权限”表中列出的权限。

有关注册 Azure 应用程序和添加权限的详细步骤，请参阅 Azure 文档。

添加 Azure 应用程序

按照以下步骤将现有 Azure 应用程序添加到 DP:

1. 打开“主页”上下文，然后单击“设置”。
2. 选择“Microsoft 365”，然后单击“添加”。
3. 在“添加 Azure 应用程序”页上，指定以下内容:
   - **Cell Manager** 租户名称: 您选择的用于标识租户的名称。
   - “Azure 应用程序 (客户机) ID”和“Azure 应用程序 (客户机) 密钥”: 在 Azure AD 上生成的客户机 ID 和客户机密钥。有关详细信息，请参阅 Azure Active Directory 文档。
   - **Azure** 发布者域: 向其注册 Azure 应用程序的发布者域。

> 注意: 如果要添加多租户应用程序，请重复此步骤为每个租户创建一个单独的条目。多租户应用程序的每个条目必须具有相同的“Azure 应用程序 (客户机) ID”和“Azure 应用程序 (客户机) 密钥”以及唯一的“Cell Manager 租户名称”和“Azure 发布者域”。
> 例如，如果要添加具有两个租户 (Azure 发布者域) *backuprecovery1.onmicrosoft.com* 和 *backuprecovery2.onmicrosoft.com* 的 Azure 应用程序，您必须创建两个具有唯一“Cell Manager 租户名称”和“Azure 发布者域”(backuprecovery1.onmicrosoft.com 和 backuprecovery2.onmicrosoft .com) 的条目。两个条目都必须具有相同的“Azure 应用程序 (客户机) ID”和“Azure 应用程序 (客户机) 密钥”。

4. 单击“提交”。

查看 Azure 应用程序

“列出 Azure 应用程序”屏幕提供了在 DP 中配置的 Azure 应用程序的列表。要查看应用程序的列表，请转到“主页”上下文，单击“设置”，然后单击“Microsoft 365”。“列出 Azure 应用程序”页显示以下信息:

- **Cell Manager** 租户名称: 指定在 Cell Manager 中添加应用程序的租户的名称。
- 创建者: 指定用于创建应用程序的管理帐户的用户名。
- 操作: 指定是添加还是注册应用程序。
- 到期: 指定应用程序的到期日期。
- **Azure** 发布者域: 指定在其下创建应用程序的 Azure 发布者域。
- 状态: 指定应用程序的当前状态。可用选项为“有效”和“无效”。
- 删除: 允许您删除应用程序。

编辑 Azure 应用程序

可以编辑 Azure 应用程序以修改以下内容:

- 客户机密钥
- Azure 发布者域:
- 权限
- 客户机密钥有效期

> 注意: 无法通过 DP 修改添加的 Azure 应用程序 (未通过 DP 注册的应用程序) 的客户机密钥有效期。在 Azure 中续订客户机密钥时，必须通过编辑 Azure 应用程序以在 DP 中手动更新它。

按照以下步骤编辑 Azure 应用程序:

1. 打开“主页”上下文。
2. 单击“设置”，然后单击“Microsoft 365”。
3. 在“列出 Azure 应用程序”页上，选择应用程序，然后单击“编辑”。此时将显示“编辑 Azure 应用程序”页面。
4. 指定新的“Azure 应用程序 (客户机) 密钥”。通过 DP 注册的 Azure 应用程序的客户机密钥会在有效期前自动续订。但是，您也可以手动续订客户机密钥。对于未通过 DP 注册的应用程序，在 Azure 中更新时必须更新客户机密钥。
5. *此步骤仅适用于通过 DP 注册的 Azure 应用程序。*更新客户机密钥有效期:
   a. 单击“更新”。此时将显示“Azure 客户机密钥续订”页面。
   b. 指定“Azure 管理员用户名”和“Azure 管理员密码”。
   c. *可选。*选择“客户机密钥有效期”(以月为单位)。
   d. 单击“更新”。“客户机密钥有效期”字段显示更新后的客户机密钥有效期。
6. *可选。*修改“Azure 发布者域”:
7. 使用“权限”下拉列表为 Azure 应用程序添加或删除权限。
8. 单击“更新”保存更改。

删除 Azure 应用程序

按照以下步骤删除 Azure 应用程序:

1. 打开“主页” 上下文。
2. 单击“设置”，然后单击“Microsoft 365”。
3. 在“列出 Azure 应用程序” 页上，选择应用程序，然后单击  “删除” 。

> 注意: 如果删除通过 DP GUI 注册的 Azure 应用程序，该应用程序也会从 Azure 中删除。但是，如果删除通过 Azure 门户注册的应用程序，则该应用程序将从 DP 中删除，但不会从 Azure 中删除。

4. 单击“是” 进行确认。

备份 Microsoft 365 邮箱

从 11.01 版本开始，Data Protector 支持云工作负载以备份和还原许多平台和应用程序，包括用户邮箱。适用于云工作负载的 Data Protector 支持废弃用于备份用户邮箱的现有 Microsoft 365 Exchange Online 集成解决方案。有关此支持的详细信息，请参阅适用于云工作负载的 Data Protector 简介。

.

还原 Microsoft 365 邮箱

本主题概述了“主页” 上下文中的“还原” 选项，并介绍了在 Microsoft 365 实例中还原邮箱的步骤。

> 注意: 从 11.01 版本开始，Data Protector 支持云工作负载，为 Microsoft Exchange Online、Microsoft SharePoint Online、Microsoft OneDrive 和 Microsoft Teams 提供备份和还原解决方案。适用于云工作负载的 Data Protector 支持废弃用于备份用户邮箱的现有 Microsoft 365 Exchange Online 集成解决方案。有关详细信息，请参阅适用于云工作负载的 Data Protector 简介。
>
> - 仍然可以还原使用现有 Microsoft 365 Exchange Online 集成解决方案进行的旧用户邮箱备份。
> - 只有使用适用于云工作负载的 Data Protector 的还原功能，才能还原使用 适用于云工作负载的 Data Protector 进行的新备份。

还原概述

“还原” 页用于还原已备份的 Microsoft 365 邮箱。要访问“还原” 页，请在 Data Protector GUI 上选择“主页” 上下文，然后单击“还原” 。

> 注意: 您无法通过“还原” 页来还原使用 Data Protector 2021.02 进行的 Microsoft 365 备份。请使用 omnir 命令还原此类备份。

下表描述了“还原” 页上显示的各种控件:

控件	描述
搜索	使您可以根据显示名称、电子邮件 ID、名字或姓氏搜索邮箱。必须至少键入三个字符才能开始搜索。

筛选器	使您可以通过选择其他组织和日期范围来过滤邮箱列表。默认情况下，“还原” 页显示最近三个月为所有已配置组织备份的邮箱列表。要更改过滤条件，请单击“过滤” 并修改以下选项:
	• 组织: 该下拉列表包括具有备份的所有组织。您可以通过从下拉列表中选择组织来过滤邮箱。
	• 选择日期范围: 选择下列日期范围之一:
	  ◦ 最近 1 个月
	  ◦ 最近 2 个月
	  ◦ 最近 3 个月
	  ◦ 最近 6 个月
	另外，您可以通过选择“间隔” ，然后选择所需的“开始日期” 和“结束日期” 来指定其他持续时间。

还原	使您可以配置还原选项并开始还原。

使用 GUI 还原邮箱

要使用 Data Protector GUI 还原邮箱，请按以下步骤操作:

1. 打开 Data Protector GUI，选择“主页” 上下文。
2. 单击“还原” 。“邮箱” 页面显示指定保护期内成功的邮箱备份会话的列表。

   > 注意: “邮箱” 页面不显示使用 Data Protector 2021.02 进行的 Microsoft 365 备份。如果有此类备份可用，则会显示一条通知。您可以使用 omnir 命令来还原相应的备份。

3. 选择要还原的一个或多个邮箱。如果要还原特定邮箱文件夹，则必须选择单个邮箱。
   您可以根据显示名称、电子邮件 ID、名字或姓氏搜索邮箱。键入至少三个字母以开始搜索。搜索不支持正则表达式和通配符。默认情况下，将显示最近三个月为所有已配置组织备份的邮箱列表。如果要查看特定组织或不同日期范围的邮箱，请单击“过滤器” 。选择所需的过滤条件，然后单击“应用” 。
4. 单击“还原” 以配置还原选项。根据上一步中的选择，“选定的邮箱” 页面会显示选定邮箱的列表或选定邮箱的文件夹结构。默认情况下，将显示最新的备份会话，但您也可以选择另一个会话进行还原。要选择另一个会话，请单击“编辑” 。在“选择备份版本” 部分中，指定“备份类型” ，然后从“选择日期范围” 下拉列表中选择日期范围。“选择会话” 下拉列表将显示所有符合过滤条件的会话。从下拉列表中选择会话并单击“更新” 。
   选择要还原的所需文件夹或邮箱。对于文件夹级还原，您可以选择父文件夹中的特定子文件夹，但不能选择父文件夹然后排除其某些子文件夹。

   > 注意: 如果未选择任何文件夹，则还原所有文件夹。

5. 单击“下一步” 以选择还原选项。
6. 在“选项” 页面上，“输入还原位置” 字段以“Data Protector_Restore_M365_日期_时间”格式显示还原文件夹的名称。日期和时间基于 Cell Manager 的区域设置。如果需要，您可以修改还原文件夹的名称。修改还原文件夹名称时，请确保它 对于同一邮箱的多个还原会话是唯一的。
7. 在“选择 M365 代理” 字段中，选择要用于还原的 M365 代理。
8. *可选。*选中“覆盖” 复选框以覆盖规则、类别、设置、日历和联系人。例如，如果在运行备份后修改规则，则还原邮箱后该规则将被覆盖。“覆盖” 设置适用于所有选择供还原的邮箱。

> 注意:
> - 如果运行备份后更改了日历事件的重现，然后通过启用“覆盖” 选项执行还原操作，则该重现不会还原为原始 (备份前) 状态。例如，如果运行备份后将非重现事件更改为重现事件，然后通过选择“覆盖” 选项还原邮箱，则该事件仍在还原的邮箱中显示为重现事件。
> - Microsoft 365 代理不删除联系人照片，导致出现以下情况:
>   - 如果运行备份后将联系人照片添加到联系人，然后通过启用“覆盖” 选项执行还原操作，则该联系人照片不会在已还原的邮箱中删除。在这种情况下，您可以在还原后手动删除联系人照片。
>   - 如果在完整备份期间联系人有联系人照片，然后在后续增量备份之前删除该照片，则启用“覆盖” 选项的增量会话还原不会删除该照片。

9. 从“选择 Azure 应用程序” 下拉列表中，选择要与 Microsoft 365 通信的 Azure 应用程序。仅当配置多个 Azure 应用程序时，才会显示此字段。如果仅配置一个 Azure 应用程序，则自动选择该应用程序进行还原。
10. 单击 还原。所选邮箱将还原到指定的还原位置。

> 注意:
> - 隐藏文件夹将与邮箱中的其他文件夹一起备份和还原。因此，运行还原操作后，您可能会在还原的邮箱中看到一些隐藏文件夹，这些文件夹在原始邮箱中不可见。
> - 有时，还原后您可能会看到重复的实体。发生这种情况是由于还原过程中 Exchange Web 服务 (EWS) 连接超时。

使用 CLI 还原邮箱

要使用命令行界面还原邮箱，请运行 omnir 命令。

示例: 要从 Azure 应用程序 "app1" 下还原文件夹 "MyTempfolder" 中的备份会话 2020/06/23-2 中创建的数据还原位于名为 "test.onmicrosoft.com" 的发布者域中的邮箱 ("Mailbox1" 和 "Mailbox2") 内容，请运行以下命令:

```
omnir -m365 -m365-environment exchange -barhost ExampleHost.net -mailbox Mailbox1@test.onmicrosoft.com -session 2020/06/23-2 -azureapp app1 -mailbox Mailbox2@test.onmicrosoft.com -session 123 -restorelocation "MyTempfolder" -debug 1-500 Debug.txt
```

监视 Microsoft 365 备份和还原会话

如果一个或多个备份或还原会话正在进行，则顶部窗格中显示 “会话” 图标和活动会话数。

> 注意: 仅当存在活动的备份或还原会话时，才会显示“会话” 图标。

要查看有关会话的详细信息，请单击 “会话” 。将为每个活动的会话显示以下详细信息:

- 会话 ID
- 类型 (备份/还原)
- 应用程序类型
- 规范
- 大小
- 开始时间
- 持续时间
- 状态

单击“刷新” 刷新视图。

Microsoft 365 集成调试日志

如果在使用 Microsoft 365 集成时遇到问题，则以下日志文件中的信息可以帮助您确定该问题:

Web GUI 日志文件

“主页”上下文 >“设置”>“日志”

应用程序服务器日志

- <OMNIDATA>/log/AppServer/server.log
- <OMNIDATA>/log/AppServer/DPServer.log

边缘服务日志

<OMNIDATA>/log/edgeservice/edgeservice.log

Microsoft 365 代理日志

- <OMNIDATA>/log/m365.log
- <OMNIDATA>/tmp/ (available if debugs are enabled)

Microsoft Exchange Server 2010+ 集成

This feature is available in the Premium Edition

本主题解释如何配置和使用 Data Protector Microsoft Exchange Server 2010+ 集成 (其中 Data Protector 与 Microsoft Exchange Server 集成)，并描述了要备份和还原 Microsoft Exchange Server 邮箱数据库所需了解的概念和方法。

独立环境和数据库可用性组 (Database Availability Group，DAG) 环境均受支持。

具有零宕机时间备份的 Microsoft Exchange Server 支持的阵列:

- HPE 3PAR
- NetApp FAS
- Dell EMC Unity

零宕机时间备份的前提条件:

- Data Protector Microsoft Exchange Server 集成基于卷影复制服务 (**VSS**) 技术
  - HPE 3PAR: 安装 HPE 软件中心提供的 **3PAR VSS** 提供程序
  - NetApp FAS: 安装 **NetApp SmartDrive** 应用程序，该应用程序可在其支持站点中获得
  - Dell EMC Unity: 安装 **Unity VSS** 硬件提供程序，该提供程序可从 EMC 支持站点中获得

备份

在备份期间，可以动态地使用数据库 (“联机备份”)。在 DAG 环境中，可以备份活动和/或被动数据库副本。

可以在以下 Microsoft Exchange Server 备份类型中选择:

- 完整
- 复制
- 增量
- 差异

还原

在恢复期间，每个数据库均可以使用不同的恢复方法进行恢复。可用的恢复方法如下：

- 修复所有处于失败状态的被动副本
- 还原到最新状态
- 还原到某时间点
- 还原到新邮箱数据库
- 还原文件到临时位置

本节提供特定于 Microsoft Exchange Server 集成的信息。

集成概念

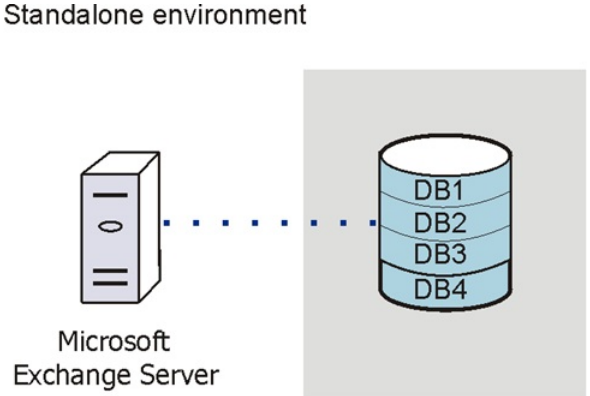
Data Protector 通过 Data Protector Microsoft Exchange Server 集成代理与 Microsoft Exchange Server 集成，在 Microsoft Exchange Server 环境下，Data Protector 会话管理器与客户机通过该集成代理进行通信。代理通过 Microsoft Exchange Management Shell 与 Microsoft Exchange Server 通信，且使用 VSS 技术备份数据。

支持的环境

Data Protector 支持 Microsoft Exchange Server 数据库可用性组环境 (“DAG 环境”) 以及具有独立 Microsoft Exchange Server 系统的环境 (“独立环境”)。

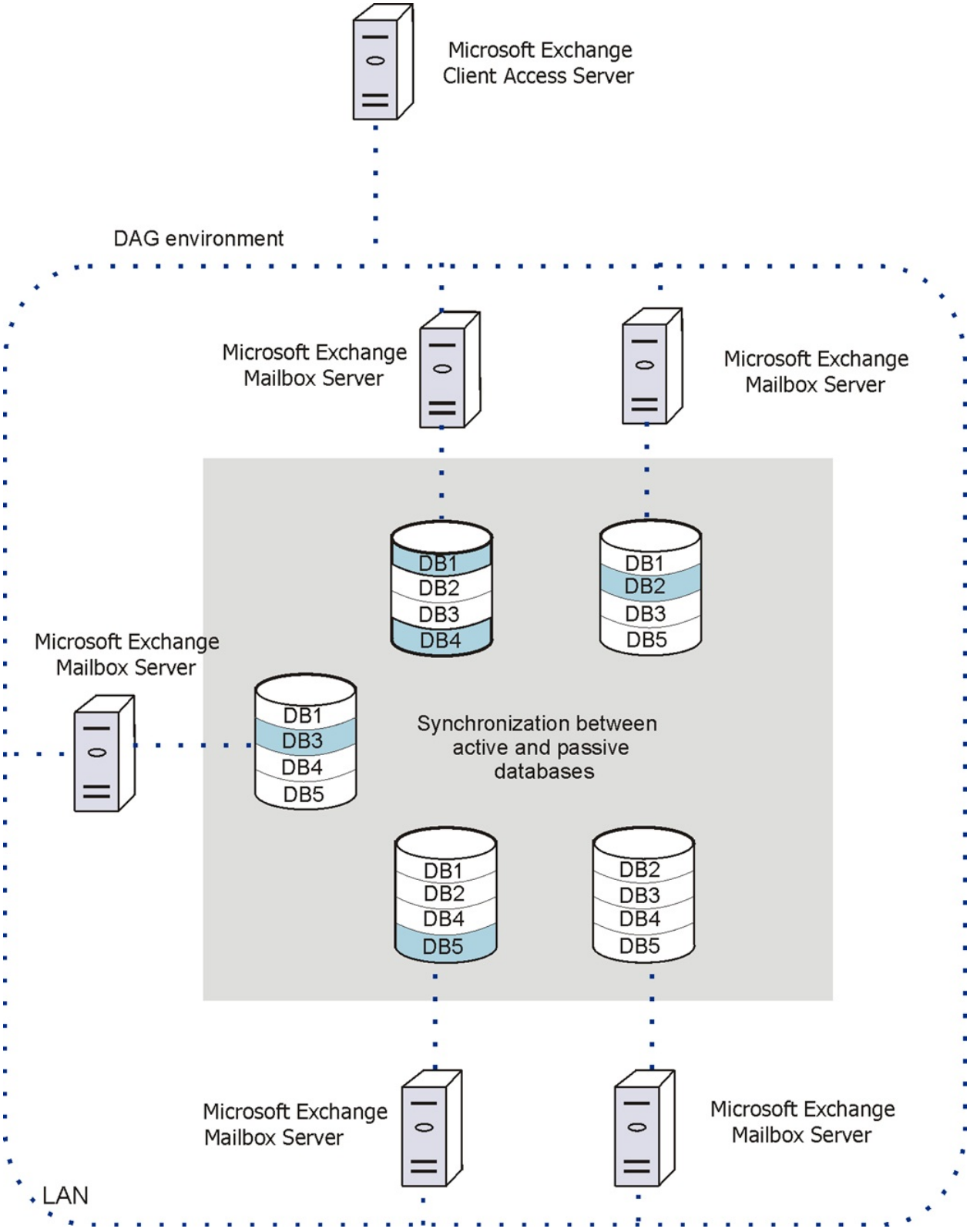
独立环境

在独立 Microsoft Exchange Server 环境中，每个 Microsoft Exchange Server 系统都独立存在。在一个会话中，只能备份一个 Microsoft Exchange Server 系统中的数据库。Data Protector 将备份和还原请求直接发送到 Microsoft Exchange Server 系统。



DAG 环境

在 DAG 环境中，Data Protector 使用 Microsoft Exchange Server 系统之一 (当前在环境中处于活动状态的系统) 与 DAG 进行通信。所有备份和还原请求均在此处发送。在一个会话中，可以备份属于同一 DAG 的不同 Microsoft Exchange Server 系统中的活动和/或被动数据库副本。



活动数据库以蓝色阴影显示。

如果数据库具有多个被动副本，可以使用以下备份策略之一指定要备份的特定被动副本:

- 最小主机数
- 最低激活首选项
- 最高激活首选项
- 最短重播延迟时间
- 最长重播延迟时间
- 最长截断延迟时间

也可以指定不备份其数据库副本的 Microsoft Exchange Server 系统。

DAG 环境中的 Microsoft Exchange Server 参数

参数	描述
激活首选号码	如果多个被动副本满足同一标准，则由激活首选号码确定激活哪个被动副本；激活首选号码最低的副本会被激活。
重播滞后时间	同步被动副本与活动副本时， ReplayLagTime 参数起作用。活动副本端的日志文件被填满后，该文件就会立即复制到被动副本端。默认情况下，新复制的日志还会应用于被动副本数据库文件。但是，如果被动副本 ReplayLagTime 参数设置为大于 0 的值，则会对日志应用延迟，从而创建滞后的数据库副本。最大值为 14 天。
截断滞后时间	TruncationLagTime 参数指定 Microsoft Exchange 复制服务在截断已应用于数据库文件的日志文件之前等待的时间。最大值为 14 天。

满足 Microsoft Exchange Server 的先决条件

以下是 Microsoft Exchange Server 集成的先决条件:

- 确保已正确安装和配置 Microsoft Exchange Server 环境。在服务器上安装 .NET Framework 3.5.1

  注意在 Windows Server 2012 及更高版本上，.NET Framework 3.5.1 是手动安装的，而非默认安装。
- 如果要运行增量备份和差异备份会话，请确保已禁用循环日志记录。
- 确保已正确安装 Data Protector。

  确保所有 Microsoft Exchange Server 系统上均已安装下列 Data Protector 组件:
  - MS Exchange Server 2010+ Integration
  - MS Volume Shadow Copy Integration
  - 适用于零宕机时间备份的 Data Protector 磁盘阵列集成代理
- 在 DAG 环境中，还必须将 DAG (分配给唯一 IP 或无 IP 的唯一名称) 导入到 Data Protector 单元中。
  - 将 DAG 作为虚拟主机 导入到 Data Protector。可使用 GUI 或 omnicc -import_host <DAG> -virtual 完成此操作。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 Microsoft Exchange Server 系统与 Cell Manager 是否正常通信，请在环境中的每个 Microsoft Exchange Server 客户机上配置并运行 Data Protector 文件系统备份和还原。
- 使用 Data Protector Microsoft 卷影复制服务集成备份的 Microsoft Exchange Server 数据库无法通过 Data Protector Microsoft Exchange Server 集成来还原，也无法使用其他方法还原。

以下限制适用:

- 不支持备份预览。
- 由于 Microsoft Exchange Server 版本之间不兼容，因此无法将属于特定 Exchange Server 版本的备份对象还原到安装了其他 Exchange Server 版本的 Data Protector 客户机上。

配置集成

用于备份和还原会话的 Windows 域用户帐户

通过 Data Protector Inet 服务启动备份和还原会话，默认情况下，这些会话使用 Windows 本地用户帐户 Local System 运行。因此，可以使用相同的用户帐户进行备份或恢复会话。

但是，您可以指定 Data Protector Inet 服务应使用不同的 Windows 域用户帐户来启动会话:

- 要以其他用户帐户执行备份会话，请在创建备份规范时指定“指定 OS 用户”选项。
- 要以其他用户帐户执行还原会话，请在“选项”页面（当执行标准还原时）或“高级”（当执行即时恢复时）页面中指定“用户名”和“组/域名”选项。

在指定其他 Windows 域用户帐户之前，请按如下方式配置用户帐户:

配置用户帐户

1. 授予用户适当的权限以备份和还原 Microsoft Exchange Server 数据库。
2. 将用户添加到 Data Protector admin 或 operator 用户组。
3. [可选] 将用户及其密码保存到计划启动集成代理的 Microsoft Exchange Server 系统上的 Windows 注册表。要保存用户帐户，请使用 Data Protector omniinetpasswd 命令。

> **注意**需要时 Data Protector Inet 服务将使用保存于 Windows 注册表中的用户帐户，进行 INET 模拟。

示例

要将域 CORP 中的用户 jane 保存到 Windows 注册表，请登录到 Microsoft Exchange Server 系统并执行以下命令：omniinetpasswd –add CORP\jane

配置用户帐户以创建远程运行空间

要创建远程运行空间以用于远程执行 Exchange Management cmdlet 操作，您需要分配了特定 Exchange Management 角色的用户凭据。这些操作在 Microsoft Exchange Server 的备份和还原操作期间执行。

使用以下 Exchange 特权配置用户帐户:

- “组织管理”角色组成员。
- “发现管理”角色组成员。
- 安装了集成的 Microsoft Exchange Server 系统的 Administrators 组成员。

创建备份规范时配置有效的 Exchange 域用户帐户。用户凭据保存在 Windows Cell Manager 上 %DP_SDATA_DIR%Config\Server\Integ\Config\E2010 或 Linux Cell Manager 上 /etc/opt/omni/server/integ/Config/E2010 中的配置文件中，该文件以 Exchange Server 或 DAG 的主机名命名。必要时，Data Protector 将使用用户凭据。

安装 Microsoft Exchange Server 客户机

This feature is available in the Premium Edition

需要在 Microsoft Exchange Server 系统上安装的 Data Protector 组件会因您要使用的备份和还原解决方案而异。

假设 Microsoft Exchange Server 环境已启动并正在运行。

要能够备份 Microsoft Exchange Server 2010 或 Microsoft Exchange Server 2013 数据库，请将以下 Data Protector 组件安装到所有 Microsoft Exchange Server 系统：

- MS Exchange Server 2010+ Integration
- MS Volume Shadow Copy Integration

  对于 VSS 可传输备份会话，必须在备份系统上安装 MS 卷影复制集成组件和相应的 Data Protector 磁盘阵列代理。
- 相应的 Data Protector 磁盘阵列代理（如果 Microsoft Exchange Server 数据位于磁盘阵列上）

在 DAG 环境中，DAG 虚拟系统（主机）还必须导入到 Data Protector 单元中。关于如何将客户机导入至 Data Protector 单元，请参阅《Data Protector 帮助》索引: “导入, 客户机系统”。

因为 Data Protector Microsoft Exchange Server 2010 集成以 VSS 技术为基础，在安装 MS Exchange Server 2010+ 集成组件时，Data Protector 将自动安装 MS 卷影复制集成组件。如果已经安装了 MS 卷影复制集成组件组件，则将对该组件进行升级。

如果从系统中删除 MS Exchange Server 2010+ 集成组件，MS 卷影复制集成组件不会自动删除。另请注意，不能从安装有 MS Exchange Server 2010+ 集成组件的系统中删除 MS 卷影复制集成组件。

备份 Microsoft Exchange Server 集成

备份 Microsoft Exchange Server 数据库时，将自动备份以下文件:

- 数据库文件 (.edb)
- 事务日志 (.log)
- 检查点文件 (.chk)

但是，根据您选择的 Microsoft Exchange Server 备份类型，并非始终备份所有文件。

Microsoft Exchange Server 备份类型

可以在以下 Microsoft Exchange Server 备份类型中选择:

完整	备份数据库文件 (.edb)、事务日志 (.log) 和检查点文件 (.chk)，然后截断事务日志。
复制	备份数据库文件 (.edb)、事务日志 (.log) 和检查点文件 (.chk)，而无需截断事务日志。
增量	备份自上次完整备份或增量备份以来所创建的事务日志 (.log)，然后截断事务日志。
差异	备份自上次完整备份以来已创建的事务日志 (.log)，而无需截断事务日志。

注意下列情况下，无法执行数据库的增量备份或差异备份:

- 尚未执行完整备份。
- 刚刚执行差异备份之后开始增量备份，或者反过来。
- 启用了 Microsoft Exchange Server 循环日志记录。

备份并行性

- 在备份会话期间，不同数据库的副本是并行备份的，但是，受限于 Microsoft Exchange Server VSS 写入程序，不会并行备份同一数据库的副本。
- 如果并行启动准备备份同一数据库的多个备份会话，只有首先锁定数据库的会话才能备份数据库，其他会话则不能。在 DAG 环境中，如果备份会话准备备份同一数据库的不同副本，情况也是如此，即只有首先锁定数据库 (即其所有副本) 的会话才能备份数据库副本，其他会话则不能。

  注意此行为可确保还原链的构成有效。例如，假设并行启动准备备份同一数据库的多个完整备份会话。如果所有会话都备份了数据库，则可能发生会话 ID 最新的会话并非最后完成数据库备份的情况。

备份考虑事项

在备份 Microsoft Exchange Server 数据库之前，请考虑以下事项:

备份策略

选择以下策略之一来备份数据：

- 完整
- 完整、增量、增量……
- 完整、差异、差异……
- 完整、副本、增量……副本、增量……

重要说明增量备份会话不能后跟差异备份会话，反之亦然。必须先运行完整备份会话。

主动副本与被动副本

主动副本和被动副本之间无太多区别，唯一区别是当前活动日志文件（位于主动副本一侧），该文件在填满（即达到 1 MB）之前不会复制到被动副本一侧。因此，如果备份被动副本，则当前活动日志文件中的事务将不包括在内。

滞后的数据库副本

备份滞后的数据库副本等同于备份非滞后的数据库副本。如果从滞后的数据库副本的备份中还原，则不仅会还原文件，还会将日志应用于数据库文

件，从而使数据库恢复到最新状态。但是，还原日志并将其应用于数据库文件非常耗时，因此会延长还原会话。另请注意，您需要足够的磁盘空间来还原所有必要的日志。

另一方面，通过从滞后数据库副本的备份还原，可以将数据库还原到进行备份之前的时间点。在不执行数据库恢复和装载的情况下还原数据库。然后删除不需要的日志，最后恢复并装载数据库。

并发备份会话

备份相同数据库的备份会话无法并行运行。

对象操作注意事项

对象复制和对象验证

复制或验证 Microsoft Exchange Server 对象时，需要选择在同一会话中创建的所有 Data Protector 备份对象。为了确保不是仅选择会话中的几个对象，Data Protector GUI 不会在“对象操作”上下文的“对象”范围中列出用于交互式对象复制或对象验证会话的 Microsoft Exchange Server 备份对象。

使用“会话”或“介质”范围替代。

创建备份规范

使用 Data Protector GUI (**Data Protector Manager**) 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS Exchange 2010+ Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。
4. 在“应用程序系统”中，选择要备份的 Microsoft Exchange Server 系统。在 DAG 环境中，选择 DAG 虚拟系统或 Microsoft Exchange Server 系统。

   > **注意**“应用程序系统”下拉列表包含安装了 Data Protector MS Exchange Server 2010+ 集成组件的所有客户机。在 DAG 环境中，该列表还包含 DAG 虚拟系统 (主机)。
   >
   > 备份会话在此处指定的客户机上启动。如果您选择 DAG 虚拟系统，则会在当前活动的 Microsoft Exchange Server 节点上启动集成代理。

   > **注意**在 Microsoft Exchange Server 环境中，要备份驻留在作为 DAG 环境一部分的 Microsoft Exchange Server 系统上的公用文件夹，请选择 Microsoft Exchange Server 系统而不是 DAG 虚拟系统 (主机)。如果您选择 DAG 虚拟系统，则只能备份属于 DAG 的数据库。Microsoft Exchange Server 公用文件夹数据库不是它的一部分。

   单击“下一步”。
5. 在“配置 MS Exchange 2010+ Server”对话框中，提供用于浏览、备份或恢复 Exchange Server 的域、用户名和密码。

   单击**确定**。
6. MS Exchange Server 即配置完成。退出 GUI 或继续在步骤 7 创建备份规范。
7. 如果选择的是 DAG 虚拟系统 (主机)，请指定“视图类型”以定义在下一页 (“源”页) 中应如何组织 Microsoft Exchange Server 数据库:

按角色	显示 DAG 中的所有数据库。
按客户机	显示 DAG 中的所有客户机，以及位于客户机上的所有数据库（主动或被动）。主动数据库结尾追加了标签 (主动)。被动数据库没有标签。

有关“用户和组/域”选项的信息，请按 **F1**。

> **注意**如果没有指定用于远程执行 Exchange Management cmdlet 操作的有效用户凭据，将显示 Microsoft Exchange Server 配置对话框。

8. 选择要备份的 Microsoft Exchange Server 数据库。

9. 如果选择了“按角色”视图类型，则以下内容适用于 DAG 环境。

   指定备份策略选项。

10. 选择用于备份的设备。

    要指定设备选项，请右键单击该设备，然后单击“属性”。在“并发”选项卡中指定并行备份流的数量，并指定要使用的介质池。

    单击“下一步”。

11. **设置备份选项。**

    单击“下一步”。

12. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

> **提示**请在实际使用之前先预览备份规范。

备份策略选项

选项	描述	
备份活动数据库	如果选中此选项，则会备份主动副本。	
备份被动副本	如果选中此选项，则会备份被动副本。如果数据库具有多个被动副本，请使用以下策略之一指定要备份的特定副本:	
	最小主机数（默认）	如果选中此选项，则备份中涉及最少的客户机数量。例如，如果要备份的数据库在相同的主机上各有一个被动副本，则从该客户机上将它们全部备份（不是从一个客户机备份一个数据库、从另一客户机备份另一数据库）。
	最低/最高激活首选参数	如果选中此选项，则会备份激活首选项编号最低/最高的数据库副本。
	最短/最长重播延迟时间	如果选中此选项，则会备份重播延迟时间最短/最长的数据库副本。
	最长截断延迟时间	如果选中此选项，则会备份截断延迟时间最长的数据库副本。
	有关详细信息，请参阅 Microsoft Exchange Server 文档。	
	如果无被动副本可用，则使用主动副本进行备份	在选中了“备份被动副本”时可用如果选中此选项，则在无被动副本可用时备份主动副本。
备份所有副本	仅当只选择一个数据库进行备份时可用。 此选项只应在 ZDB 环境中使用。否则，备份单个副本便已足够；可以从单个副本的备份还原数据库的不同副本。	
从备份中排除客户机	创建客户机列表。不会备份驻留在这些客户机上的数据库副本。	

特定于应用程序的备份选项

选项	描述

Pre-exec、**Post-exec**	指定备份之前（pre-exec）或之后（post-exec）要在 Microsoft Exchange Server 系统上运行的命令行。 命令行仅在启动备份会话的 Microsoft Exchange Server 系统上执行。 只键入命令的名称并确保命令位于同一系统上的默认 Data Protector 命令目录中。不要使用双引号。 *DAG 环境:* 如果在**应用程序系统**选项中选择 DAG 虚拟系统（主机），请确保命令位于当前活动的节点上。
执行一致性检查 [-exch_check [-exch_throttle Value] | -exch_checklogs]	如果选择此选项，Microsoft Exchange Server 会检查数据库备份数据的一致性。如果未选择此选项，会话会较早结束，但备份数据的一致性无法保证。 创建备份数据后，将对备份介质执行检查。如果发现数据损坏，数据将被弃用，并导致数据库备份失败。 默认：选择 如果选中“仅检查日志文件”选项，则仅检查日志文件的备份数据，这足以使 Microsoft Exchange Server 保证数据一致性。 默认：选择 默认情况下，一致性检查占用 I/O 较多，这可能会对磁盘性能产生负面影响。“限制检查 1 秒钟”选项会限制数据库文件 .edb 的一致性检查，以减少对磁盘性能的影响。指定在进行多少次输入/输出操作之后，应将检查停止一秒时间。 如果仅选中日志文件，则此选项不可用。 默认：未选择

修改备份规范

要修改备份规范，请在“备份”上下文的“范围窗格”中单击规范名称。

在“源”页面上，您可以更改用于远程执行 Exchange 管理 cmdlet 操作的 Exchange 域用户凭据。要更改凭据，请执行以下操作:

1. 右键单击选定的备份对象。
2. 单击“配置”。
3. 要验证您的配置，请单击“检查配置”。
4. 在其他选项卡上进行任何其他所需的更改。
5. 单击“应用” 应用更改。

> **注意**要在“源”页中显示所有数据库，请在“显示”选项中选择“全部”。在 DAG 环境中，这不仅会显示所有数据库，还会更新数据库的当前状态 (主动或被动)。
>
> 要仅显示选定用于备份或从备份中排除的数据库，请在“显示”选项中选择“选定”。如果未显示任何数据库，则表示未从备份规范中排除任何数据库，所有数据库都将进行备份。当有新的数据库添加到为备份选择的客户机上时，该数据库将自动被包括到备份规范中。

计划备份会话

您可以将备份会话计划为在特定时间自动启动或定期启动。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS Exchange 2010+ Server”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector User Interface 组件的客户机。
2. 请执行以下命令：

   omnib -e2010_list BackupSpecificationName -test_bar

预览期间会发生什么?

测试以下内容:

- 启动备份会话的 Microsoft Exchange Server 系统与 Cell Manager 之间的通信
- 应用“备份策略”选项和“客户机过滤”选项之后，每个选定数据库是否至少有一个副本可用于备份 (这适用于包含备份策略选项的备份规范)
- 选定数据库是否准备就绪，可进行备份 (即，它们不应被卸除、挂起或处于失败状态)

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

要启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS Exchange 2010+ Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用按配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector“用户界面”组件的客户机。
2. 请执行以下命令：

   omnib -e2010_list BackupSpecificationName [-barmode E2010Mode] [LIST_OPTIONS]

   其中， E2010Mode 为下列项之一:

   full|copy|incr|diff

   默认为 full 。

   示例

   要使用备份规范 MyDatabases 启动完整备份，请执行以下命令:

   omnib -e2010_list MyDatabases -barmode full

   要使用相同的备份规范启动差异备份，请执行以下命令:

   omnib -e2010_list MyDatabases -barmode diff

备份对象

对于每个数据库 (副本)，Data Protector 会创建以下备份对象:

- *数据库文件对象*
  - ClientName /Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/DBID/File [MSVSSW-APP]

    (独立数据库或主动副本)
  - ClientName /Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/DBID/File [MSVSSW-APP]

    (被动副本)
- *日志文件对象*
  - ClientName /Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/DBID/Logs [MSVSSW-APP]

(独立数据库或主动副本)

- ClientName /Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/DBID/Logs [MSVSSW-APP]

  (被动副本)

- *数据库对象*

  ClientName /DBID/DBName [E2010]

  数据库对象包含构造还原链所需的信息。

- *VSS 元数据对象*

  /BackupSession/Metadata [MSVSSW-APP]

有关对象是否备份成功的信息保存在 Data Protector IDB 中。

用于备份和还原会话的 Windows 域用户帐户

通过 Data Protector Inet 服务启动备份和还原会话，默认情况下，这些会话使用 Windows 本地用户帐户 SYSTEM 运行。因此，可以使用相同的用户帐户进行备份或恢复会话。

但是，您可以指定 Data Protector Inet 服务应使用不同的 Windows 域用户帐户来启动会话:

- 要以其他用户帐户执行备份会话，请在创建备份规范时指定“指定 OS 用户”选项。
- 要以其他用户帐户执行还原会话，请在“选项”页面或“高级”页面中指定“用户名”和“组/域名”选项。

还原 Microsoft Exchange Server 集成

This feature is available in the Premium Edition

可以通过执行标准还原会话来还原 Microsoft Exchange Server 数据。

重要说明还原某个数据库后，请对该数据库启动完整备份会话。否则，后续增量和差异备份会话将失败。

注意事项

- 使用 Data Protector Microsoft 卷影复制服务集成备份的 Microsoft Exchange Server 数据库无法通过 Data Protector Microsoft Exchange Server 2010 集成来还原，也无法使用其他方法还原。

还原方法

还原 Microsoft Exchange Server 数据库有多种原因。例如:

- 数据库已损坏。
- 活动和被动数据库副本之间的同步已中断，但您不想对被动副本进行种子重新设定，或者只是因为恢复操作不起作用。
- 需要将数据库还原到不同的时间点。
- 出于调查目的，需要还原数据库的备份数据。
- 需要将数据库的备份数据还原到恢复数据库，以便提取单个邮箱或邮箱文件。
- 需要将数据库的备份数据还原到拨号音数据库。

为了满足您的需求，Data Protector 提供了不同的还原方法。可以在以下选项中选择：

- **修复所有处于失败状态的被动副本**
- **还原到最新状态**
- **还原到某时间点**
- **还原到新邮箱数据库**
- **还原到临时位置**

您可以为同一会话中的不同数据库指定不同的还原方法。

注意前三个方法将备份数据还原到原始数据库，因此只有在原始数据库仍然存在时才可用。最后两种方法将备份数据还原到新位置。

修复所有处于失败状态的被动副本

只有属于 DAG 的数据库才可以使用此方法。当一些数据库的被动副本损坏而进入 Failed 或 FailedAndSuspended 状态时，可使用此方法。此方法使用上次备份会话 (和相应的还原链) 中创建的备份自动还原所有损坏的被动副本。数据恢复后，只要选择**恢复数据库复制**选项，副本便会与活动副本同步。

还原到最新状态

此方法用于将损坏的数据库及时还原到尽可能新的状态。Data Protector 使用上次备份会话（和相应的恢复链）中创建的备份恢复数据库。

在文件还原完毕后，所有的日志 (不只是从备份还原的日志，还包括任何现有的日志) 都会对数据库文件进行重放。

注意*DAG 环境:*

还原被动副本后，Microsoft Exchange Server 要根据 ReplayLagTime 参数设置确保已经对数据库文件进行了日志重放。

还原到某时间点

此方法用于将数据库还原到某个特定的时间点。

注意*标准还原:*

还原独立数据库或活动副本时，将重命名现有的 .log 和 .chk 文件 (在文件名后添加 .keep 扩展名)。在不执行数据库恢复的情况下还原文件时，此功能很有用。此功能可以对数据库文件应用其他日志；只需删除您也想要应用的日志文件的 .keep 扩展名，然后手动启动数据库恢复即可。通过这种方式，可以微调将数据库还原到的时间点。

还原被动副本时，将删除现有文件。

还原文件后，如果选择“执行数据库恢复”选项，则向数据库文件 (.edb) 重放日志。

注意*DAG 环境:*

- 还原被动副本后，Microsoft Exchange Server 要根据 ReplayLagTime 参数设置确保已经对数据库文件进行了日志重放。
- 对于不恢复的被动副本，一旦恢复会话完成，必须完整地重新设定种子。

还原到新邮箱数据库

此方法用于将数据还原到不同的数据库中，原因可能是原始数据库已不存在或需要将数据移往他处。

使用该选项，也可以将数据恢复到 Microsoft Exchange Server 恢复数据库。

还原文件到临时位置

使用此方法，可将数据库文件还原到所选位置。

- 当从差异或增量备份会话还原时，可以还原完整还原链或只还原所选会话中备份的文件 (.log)。
- 从完整备份会话还原数据时，可以选择只还原数据库文件 (.edb)。

还原目标

可将备份数据还原到:

- 现有数据库 (独立数据库、活动副本、被动副本)、
- 新的数据库、
- 临时位置。

还原到独立数据库

还原到原始独立数据库 (独立环境) 的过程如下:

1. 卸除数据库。
2. 还原备份数据。
3. (可选) 向数据库文件 .edb 重放新还原的日志 (如果执行“还原到最新状态”方法，还包括先前存在的日志) 并装载数据库。

要还原到原始独立数据库，请使用以下还原方法之一:

- **还原到最新状态**
- **还原到某时间点**

还原到活动副本

还原到活动副本 (DAG 环境) 的过程如下:

1. 卸除数据库。
2. 暂停所有复制。
3. 还原备份数据。
4. (可选) 向数据库文件 .edb 重放新还原的日志 (如果执行“还原到最新状态”方法，还包括先前存在的日志) 并装载数据库。

要还原到活动副本，请使用以下还原方法之一:

- **还原到最新状态**
- **还原到某时间点**

还原到被动副本

还原到被动副本 (DAG 环境) 的过程如下:

1. 暂停复制。

2. 还原备份数据。
3. (可选) 恢复对活动副本的复制。

要还原到被动副本，请使用以下还原方法之一:

- **还原所有处于失败状态的被动副本**
- **还原到最新状态**
- **还原到某时间点**

将数据还原到新数据库

还原到新数据库的过程如下:

1. 创建一个新的邮箱数据库。
2. 将备份数据还原到新数据库。

> **注意**如果还原到恢复数据库，则首先还原备份数据，然后创建恢复数据库。

要将数据还原到新邮箱数据库或恢复数据库，可使用“还原到新邮箱数据库”还原方法。

将文件还原到临时位置

可以将数据库文件 (.edb 和/或 .log 和/或 .chk) 还原到选择的客户机和目录。选择“将文件还原到临时位置”还原方法。

还原链

默认情况下，当您选择差异备份会话或增量备份会话进行还原时，Data Protector 不仅会还原在所选会话中备份的日志 (.log)，还会还原在先前会话 (“还原链”) 中备份的文件:

- 如果选择了差异备份会话，Data Protector 将还原:
  1. 在完整或复制备份会话中备份的 .edb 文件和 .log 文件。
  2. 在所选差异备份会话中备份的 .log 文件。
- 如果选择了增量备份会话，Data Protector 将还原:
  1. 在完整或复制备份会话中备份的 .edb 文件和 .log 文件。
  2. 在所有后续增量备份会话 (一直到所选增量备份会话) 中备份的 .log 文件。
- 如果选择了完整备份或复制备份会话，Data Protector 将还原在所选会话中备份的 .edb 文件和 .log 文件。

> - 如果使用“还原到最新状态”方法，则不会还原完整备份会话或复制备份会话中的 .log 文件。
> - 只有“还原到临时位置”方法可以只还原在所选增量或差异会话中备份的 .log 文件。

还原并行性

如果允许设备并发，则并行还原数据库副本，但以下情况除外:

- 如果数据库副本是从同一个客户机备份的，但现在还原到不同的客户机。
- 如果将同一个数据库副本的备份数据用作多个数据库副本的还原来源。

查找要还原的信息

可以从 Data Protector IDB 检索有关备份会话的信息 (例如有关备份类型和所用介质的信息，以及在备份期间报告的消息)。

要检索信息，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开“对象”或“会话”。

   如果展开“对象”，则会根据创建备份对象时所针对的 Microsoft Exchange Server 数据库对备份对象进行排序。

> **注意**备份对象名称包含数据库 GUID。要了解哪个 GUID 属于哪个数据库，请参阅数据库对象 /DB_GUID/DB_Name 。
>
> 例如，数据库 DB1 的数据库对象在 GUID 为 08bca794-c544-4e27-87e8-533fb81fd517 为:

/08bca794-c544-4e27-87e8-533fb81fd517/DB1

如果展开“会话”，则会根据创建备份对象的会话对备份对象进行排序。例如，在会话 2013/02/7–7 中创建的备份对象列在 2013/02/7–7 下方。

要查看某个备份对象的详细信息，请右键单击该备份对象，然后单击“属性”。

提示要查看在会话期间报告的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector User Interface 组件的任何 Microsoft Exchange Server 客户机。
2. 获取在备份会话中创建的 Microsoft Exchange Server 备份对象的列表:

   omnidb -session SessionID

3. 获取备份对象的详细信息:

   omnidb -e2010 BackupObjectName -session SessionID -catalog

   以下是备份对象名称的一个示例:

   devy.company.com:/08bca794-c544-4e27-87e8-533fb81fd517/DB1

还原过程

可以在同一个会话中还原多个 Microsoft Exchange Server 数据库，同时为每个数据库指定不同的还原方法。

要还原数据库，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“MS Exchange 2010+ Server”，展开 DAG 虚拟系统或独立的 Microsoft Exchange Server 系统，然后单击“MS Exchange 2010+ Server”。
3. 在“源”页面中，Data Protector 显示从选定的 DAG 或独立环境中备份的所有 Microsoft Exchange Server 数据库。

   选择要还原的 Microsoft Exchange Server 数据库。

   在选择数据库时，会自动显示“数据库属性”对话框。指定一种还原方法，然后单击“确定”。对于属于 DAG 的数据库，默认的还原方法为“修复状态为失败的所有被动副本”。对于独立数据库，默认方法为**恢复到最新状态**。

   要更改还原方法，请右键单击数据库并单击“属性”。
4. 在“选项”页面中，指定 Data Protector Microsoft Exchange Server 2010 集成还原选项。
5. 在“设备”页面中，选择要用于还原的设备。
6. 单击**还原**。
7. 在“启动还原会话”对话框中，单击“下一步”。
8. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
9. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 User Interface 组件的 Microsoft Exchange Server 客户机。
2. 执行以下命令：

```
omnir -e2010 -barhost ClientName [VSS_EXCHANGE_SPECIFIC_OPTIONS] Database [Database ...] [-user User:Domain] [GENERAL_OPTIONS] Database {-db_name SourceDatabaseName | -db_guid SourceDatabaseGUID } [-source SourceClientName] {-repair | -latest | -pit | -new | -temp} E2010_METHOD_OPTIONS E2010_REPAIR_METHOD_OPTIONS [–no_resume_replication] E2010_LATEST_METHOD_OPTIONS [-node TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount] E2010_PIT_METHOD_OPTIONS -session BackupID [-node
```

TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount]

E2010_NEW_METHOD_OPTIONS -session BackupID -client TargetClientName -location TargetDatabasePath -name TargetDatabaseName [-recoverydb] [–no_recover] [–no_mount] E2010_TEMP_METHOD_OPTIONS -session BackupID -client TargetClientName -location TargetDatabasePath [–no_chain] [–edb_only] [–no_recover]

注意备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，必须指定原始“备份”会话的会话 ID (即备份 ID)，而不是“对象复制”会话的会话 ID。

如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

示例 (还原方法 - 修复)

DAG 环境

要还原从虚拟系统名称为 dag0.company.com 的 DAG 中备份的数据库 DB1 的所有损坏被动副本，并确保在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source dag0.company.com -repair
```

示例 (还原方法 - 最新)

独立环境

要将位于客户机 exchange1.company.com 上的受损独立数据库 DB1 还原到可还原的最新时间点，并确保在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source exchange1.company.com –latest
```

DAG 环境

假设您要还原位于客户机 exchange1.company.com 上的数据库 DB1 的活动副本，以及位于客户机 exchange2.company.com 和 exchange3.company.com 上的数据库的被动副本。假设数据库 DB1 是虚拟系统名称为 dag0.company.com 的 DAG 的一部分，并且您希望在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)。请执行以下命令：

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source dag0.company.com –latest –node exchange1.company.com –node exchange2.company.com –node exchange3.company.com
```

示例 (还原方法 - pit)

独立环境

假设您要使用在会话 2013/5/14-1 中创建的备份数据来还原位于客户机 exchange1.company.com 上的受损独立数据库 DB1 。假设您希望在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)。请执行以下命令：

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 -pit –session 2013/5/14-1
```

注意未指定 –source 选项，在这种情况下，Data Protector 假定从使用 –barhost 选项指定的客户机备份数据库。

示例 (还原方法 - new)

DAG 环境

假设您想要将数据库 DB1 的备份还原到应在客户机 exchange2.company.com 上创建的恢复数据库，该数据库名为 Recovery1 ，文件在 C:\Recovery1Folder 目录中。假设数据库 DB1 从虚拟系统名称为 dag0.company.com 的 DAG 中的 2013/5/14-1 会话中创建。另外，还要确保在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source dag0.company.com –new –session 2013/5/14-1 –client exchange2.company.com -location C:\Recovery1Folder –name Recovery1 –recoverydb
```

示例 (还原方法 - temp)

独立环境

假设您想要还原位于客户机 exchange2.company.com 上的数据库 DB1 的事务日志。这些日志已在增量备份会话 2013/5/14-1 中备份。要不执行数据库恢复即将日志还原到客户机 exchange2.company.com 的 C:\DB1TransactionLogFolder 目录，并确保在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source exchange2.company.com –temp –session 2013/5/14-1 –client exchange2.company.com –location C:\DB1TransactionLogFolder -no_chain –no_recover
```

使用其他设备进行还原

您可以使用除备份时所用设备之外的设备进行还原。

还原选项

修复所有处于失败状态的被动副本

GUI/CLI 中的选项	描述
恢复数据库复制/ -no_resume_replication	在 DAG 环境中可用。在还原副本后，恢复活动副本和被动副本之间的复制。 请注意，CLI 选项 -no_resume_replication 具有相反的含义。如果指定此选项，则不会恢复复制。
目标节点	不可用。 自动选择状态为 Failed 或 FailedAndSuspended 的客户机 (即副本)。

还原到最新状态

GUI/CLI 中的选项	描述
为还原选择	指定是否应还原数据库。
执行数据库恢复/ -no_recover	在还原独立数据库 (独立环境) 或活动副本 (DAG 环境) 时可用。在还原完成之后将日志应用于数据库文件 (.edb)。 请注意，CLI 选项 -no_recover 具有相反的含义。如果指定此选项，则不执行数据库恢复。
装载数据库/ -no_mount	在还原独立数据库 (独立环境) 或活动副本 (DAG 环境) 时可用。在数据库恢复完成之后装载数据库。仅当选择“执行数据库恢复”时，此选项才可用。 请注意，CLI 选项 -no_mount 具有相反的含义。如果指定此选项，则不会装载数据库。
恢复数据库复制/ -no_resume_replication	在还原被动副本 (DAG 环境) 时可用。在还原副本后，恢复活动副本和被动副本之间的复制。 请注意，CLI 选项 -no_resume_replication 具有相反的含义。如果指定此选项，则不会恢复复制。

目标节点 -node | –all	仅在 DAG 环境中可用。指定要还原的客户机 (即数据库副本)。

还原到某时间点

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。
备份版本/ -session	指定要从中还原备份数据的会话。选择备份 ID。 如果选择差异备份会话，则会还原在所选差异备份会话中备份的 .log 文件。 如果选择增量备份会话，则会还原在所有后续增量备份会话 (一直到所选增量备份会话) 中备份的 .log 文件。
最后一个备份版本	显示上次进行数据库备份的会话。
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
装载数据库/ -no_mount	
恢复数据库复制/ -no_resume_replication	
目标节点/ -node | –all	请参阅还原到最新状态中的说明。将自动选择托管活动副本的节点 (客户机) 进行还原。

还原到新邮箱数据库

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。
目标客户机/ -client	指定要还原到的客户机。
还原到位置/ -location	指定要还原到的目录。
数据库名称/ -name	指定要用于新数据库的名称。如果已存在另一个具有相同名称的数据库，则还原将失败。
还原到恢复数据库/ -recoverydb	将数据还原到 Microsoft Exchange Server 恢复数据库。 虽然可以并行存在多个恢复数据库，但一次只能将一个恢复数据库装载到 Microsoft Exchange Server。

备份版本/ -session	请参阅还原到时间点中的说明。
最后一个备份版本	
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
装载数据库/ -no_mount	
目标节点	不可用。

还原文件到临时位置

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。
还原链	如果此选项设置为“仅还原此备份”，则仅还原在所选会话中备份的文件。 如果选择“完整还原 (完整、增量、差异备份)”选项，则会还原整个链。
目标客户机/ -client	请参阅还原到新邮箱数据库中的说明。
还原到位置/ -location	
备份版本/ -session	请参阅还原到时间点中的说明。
最后一个备份版本	
仅还原数据库文件/ -edb_only	仅还原数据库文件 (.edb)。不会还原日志 (.log) 和检查点文件 (.chk)。
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
目标节点	不可用。

常规还原选项

GUI/CLI 中的选项	描述
启动客户机/ -barhost	指定应启动集成代理 (e2010_bar.exe) 的客户机。如果选择 DAG 虚拟客户机（主机），则会在当前活动的节点上启动集成代理。要找出当前处于活动状态的节点，请参阅还原 Microsoft Exchange Server 2010+。 默认值：已指定用于备份会话的同一个客户机。如果已指定 DAG 虚拟客户机，则此时会选择此客户机。但是请注意，启动集成代理的物理节点可能与备份会话期间使用的物理节点不同；这取决于哪些节点当前处于活动状态。

用户名 **组/域名/** -user	指定要用于还原会话的 Windows 域用户帐户。确保按配置用户帐户中所述配置用户。 如果未指定这些选项，则会在运行 Data Protector Inet 服务的用户帐户下启动还原会话。
执行一致性检查/ [-exch_check [-exch_throttle Value] | -exch_checklogs]	如果选择此选项，Microsoft Exchange Server 会检查数据库备份数据的一致性。如果未选择此选项，会话会较早结束，但备份数据的一致性无法保证。 还原备份数据后，在源存储卷的目标位置进行检查。如果在备份时已执行一致性检查，则无须再次执行该检查。 默认：未选择 如果选择“仅检查日志文件”选项，则仅检查日志文件备份数据，这足以使 Microsoft Exchange Server 保证数据一致性。 默认：未选择 默认情况下，一致性检查占用 I/O 较多，这可能会对磁盘性能产生负面影响。“限制检查 1 秒钟”选项会限制数据库文件 .edb 的一致性检查，以减少对磁盘性能的影响。指定在进行多少次输入/输出操作之后，应将检查停止一秒时间。 如果仅选中日志文件，则此选项不可用。 默认：未选择

提示要找出当前处于活动状态的 Microsoft Exchange Server 节点，请连接其中一个节点并执行:

cluster group

示例

C:\Users\administrator.E2010BETA>cluster group 列出所有可用资源组的状态: 组 节点 状态 ---------- ---------- ------ 可用存储 spade 脱机 群集组 club 联机

当前活动节点的状态为联机。在本例中，此节点为 club 。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

Microsoft Exchange Server 2010+ ZDB 集成

This feature is available in the Premium Edition

本主题解释如何配置和使用 Data Protector Microsoft Exchange Server 2010+ ZDB 集成 (其中 Data Protector 与 Microsoft Exchange Server 集成)，并描述了要备份和还原 Microsoft Exchange Server 邮箱数据库所需了解的概念和方法。

独立环境和数据库可用性组 (Database Availability Group，DAG) 环境均受支持。

具有零宕机时间备份的 Microsoft Exchange Server 支持的阵列:

- HPE 3PAR
- NetApp FAS
- Dell EMC Unity

零宕机时间备份的前提条件:

- Data Protector Microsoft Exchange Server 集成基于卷影复制服务 (**VSS**) 技术
  - HPE 3PAR: 安装 HPE 软件中心提供的 **3PAR VSS** 提供程序
  - NetApp FAS: 安装 **NetApp SmartDrive** 应用程序，该应用程序可在其支持站点中获得
  - Dell EMC Unity: 安装 **Unity VSS** 硬件提供程序，该提供程序可从 EMC 支持站点中获得

备份

在备份期间，可以动态地使用数据库 (“联机备份”)。在 DAG 环境中，可以备份活动和/或被动数据库副本。

由于涉及 Microsoft Exchange Server、ZDB 磁盘阵列和 VSS，因此可以指定不同种类的备份类型:

- Microsoft Exchange Server 备份类型
- VSS 备份类型
- ZDB 备份类型

可以在以下 Microsoft Exchange Server 备份类型中选择:

- 完整
- 复制
- 增量
- 差异

可以从以下 ZDB 备份类型中选择:

- ZDB 到磁盘
- ZDB 到磁盘 + 磁带
- ZDB 到磁带

可以从以下 VSS 备份类型中选择:

- 本地或网络备份
- VSS 可传输

还原

可以使用标准恢复或即时恢复功能来恢复 Microsoft Exchange Server 数据库。

在恢复期间，每个数据库均可以使用不同的恢复方法进行恢复。可用的恢复方法如下：

- 修复所有处于失败状态的被动副本
- 还原到最新状态
- 还原到某时间点
- 还原到新邮箱数据库
- 还原文件到临时位置

本节提供特定于 Microsoft Exchange Server 集成的信息。

集成概念

Data Protector 通过 Data Protector Microsoft Exchange Server 集成代理与 Microsoft Exchange Server 集成，在 Microsoft Exchange Server 环境下，Data Protector 会话管理器与客户机通过该集成代理进行通信。代理通过 Microsoft Exchange Management Shell 与 Microsoft Exchange Server 通信，且使用 VSS 技术备份数据。

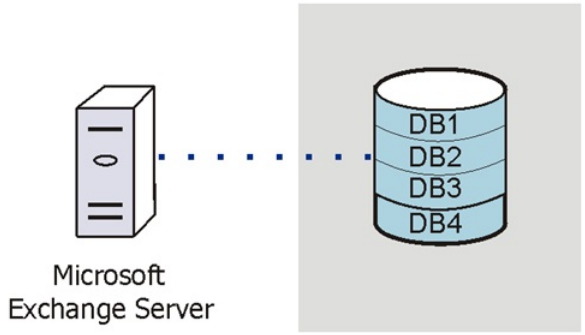
支持的环境

Data Protector 支持 Microsoft Exchange Server 数据库可用性组环境 (“DAG 环境”) 以及具有独立 Microsoft Exchange Server 系统的环境 (“独立环境”)。

独立环境

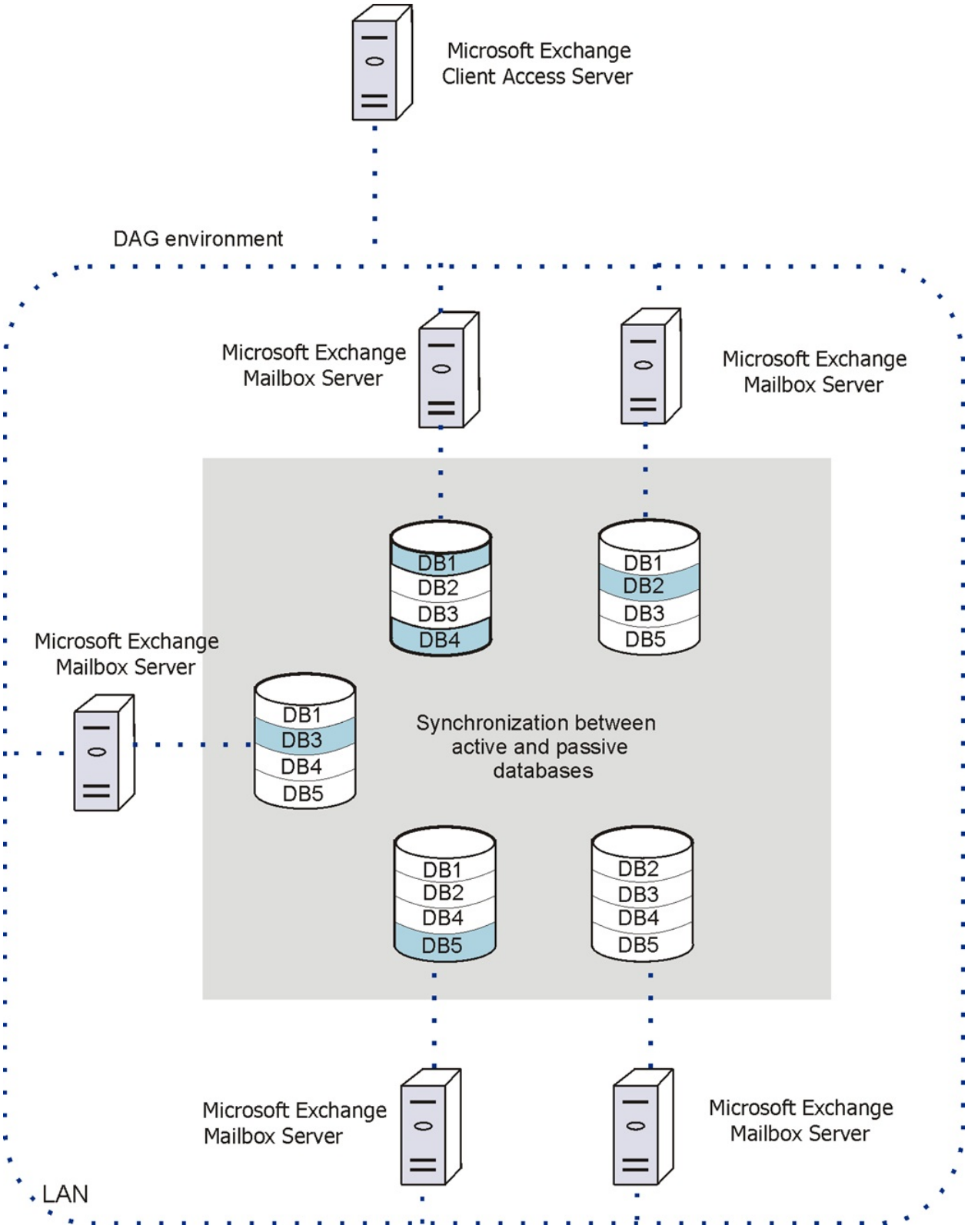
在独立 Microsoft Exchange Server 环境中，每个 Microsoft Exchange Server 系统都独立存在。在一个会话中，只能备份一个 Microsoft Exchange Server 系统中的数据库。Data Protector 将备份和还原请求直接发送到 Microsoft Exchange Server 系统。

Standalone environment



DAG 环境

在 DAG 环境中，Data Protector 使用 Microsoft Exchange Server 系统之一 (当前在环境中处于活动状态的系统) 与 DAG 进行通信。所有备份和还原请求均在此处发送。在一个会话中，可以备份属于同一 DAG 的不同 Microsoft Exchange Server 系统中的活动和/或被动数据库副本。



活动数据库以蓝色阴影显示。

如果数据库具有多个被动副本，可以使用以下备份策略之一指定要备份的特定被动副本:

- 最小主机数
- 最低激活首选项
- 最高激活首选项
- 最短重播延迟时间
- 最长重播延迟时间
- 最长截断延迟时间

也可以指定不备份其数据库副本的 Microsoft Exchange Server 系统。

DAG 环境中的 Microsoft Exchange Server 参数

参数	描述
激活首选号码	如果多个被动副本满足同一标准，则由激活首选号码确定激活哪个被动副本；激活首选号码最低的副本会被激活。
重播滞后时间	同步被动副本与活动副本时， ReplayLagTime 参数起作用。活动副本端的日志文件被填满后，该文件就会立即复制到被动副本端。默认情况下，新复制的日志还会应用于被动副本数据库文件。但是，如果被动副本 ReplayLagTime 参数设置为大于 0 的值，则会对日志应用延迟，从而创建滞后的数据库副本。最大值为 14 天。
截断滞后时间	TruncationLagTime 参数指定 Microsoft Exchange 复制服务在截断已应用于数据库文件的日志文件之前等待的时间。最大值为 14 天。

满足 Microsoft Exchange Server 的先决条件

以下是 Microsoft Exchange Server 集成的先决条件:

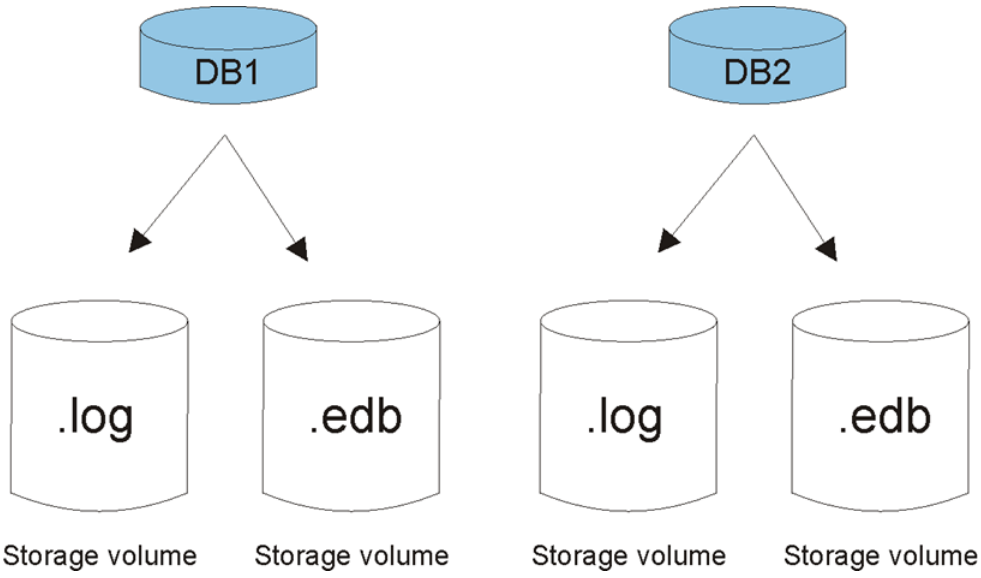
- 确保已正确安装和配置 Microsoft Exchange Server 环境。在服务器上安装 .NET Framework 3.5.1。

  请注意，在 Windows Server 2012 及更高版本上，.NET Framework 3.5.1 是手动安装的，而非默认安装。

- 如果要运行增量备份和差异备份会话，请确保已禁用循环日志记录。
- 确保已正确安装 Data Protector。

  确保所有 Microsoft Exchange Server 系统上均已安装下列 Data Protector 组件:

  - MS Exchange Server 2010+ Integration
  - MS Volume Shadow Copy Integration
  - 适用于零宕机时间备份的 Data Protector 磁盘阵列集成代理
    - 对于 VSS 可传输备份会话，必须在备份系统上安装 MS 卷影复制集成组件和相应的 Data Protector 磁盘阵列代理。
- 在 DAG 环境中，还必须将 DAG (分配给唯一 IP 或无 IP 的唯一名称) 导入到 Data Protector 单元中。
  - 将 DAG 作为虚拟主机 导入到 Data Protector。可使用 GUI 或 omnicc -import_host <DAG> -virtual 完成此操作。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 Microsoft Exchange Server 系统与 Cell Manager 是否正常通信，请在环境中的每个 Microsoft Exchange Server 客户机上配置并运行 Data Protector 文件系统备份和还原。
- 使用 Data Protector Microsoft 卷影复制服务集成备份的 Microsoft Exchange Server 数据库无法通过 Data Protector Microsoft Exchange Server 集成来还原，也无法使用其他方法还原。
- 如果计划运行即时恢复，建议将 Microsoft Exchange Server 数据库放置在单独的存储卷上。另外，将数据库的文件 (.edb 和 .log) 放置在不同的存储卷上。这种配置可以提供更好的还原粒度。确保不同 Microsoft Exchange Server 系统上的存储卷大小相同。否则，在复制备份即时恢复会话期间可能会出现问题。



以下限制适用:

- 不支持备份预览。
- 由于 Microsoft Exchange Server 版本之间不兼容，因此无法将属于特定 Exchange Server 版本的备份对象还原到安装了其他 Exchange Server 版本的 Data Protector 客户机上。

配置集成

用于备份和还原会话的 Windows 域用户帐户

通过 Data Protector Inet 服务启动备份和还原会话，默认情况下，这些会话使用 Windows 本地用户帐户 Local System 运行。因此，可以使用相同的用户帐户进行备份或恢复会话。

但是，您可以指定 Data Protector Inet 服务应使用不同的 Windows 域用户帐户来启动会话:

- 要以其他用户帐户执行备份会话，请在创建备份规范时指定“指定 OS 用户”选项。
- 要以其他用户帐户执行还原会话，请在“选项”页面（当执行标准还原时）或“高级”（当执行即时恢复时）页面中指定“用户名”和“组/域名”选项。

在指定其他 Windows 域用户帐户之前，请按如下方式配置用户帐户:

配置用户帐户

1. 授予用户适当的权限以备份和还原 Microsoft Exchange Server 数据库。
2. 将用户添加到 Data Protector admin 或 operator 用户组。
3. (可选) 将用户及其密码保存到计划启动集成代理的 Microsoft Exchange Server 系统上的 Windows 注册表。要保存用户帐户，请使用 Data Protector omniinetpasswd 命令。

   > **注意**需要时 Data Protector Inet 服务将使用保存于 Windows 注册表中的用户帐户，进行 INET 模拟。

   示例

   要将域 CORP 中的用户 jane 保存到 Windows 注册表，请登录到 Microsoft Exchange Server 系统并执行以下命令: omniinetpasswd –add CORP\jane

配置用户帐户以创建远程运行空间

要创建远程运行空间以用于远程执行 Exchange Management cmdlet 操作，您需要分配了特定 Exchange Management 角色的用户凭据。这些操作在 Microsoft Exchange Server 的备份和还原操作期间执行。

使用以下 Exchange 特权配置用户帐户:

- “组织管理”角色组成员。
- “发现管理”角色组成员。
- 安装了集成的 Microsoft Exchange Server 系统的 Administrators 组成员。

创建备份规范时配置有效的 Exchange 域用户帐户。用户凭据保存在 Windows Cell Manager 上 %DP_SDATA_DIR%Config\Server\Integ\Config\E2010 或 Linux Cell Manager 上 /etc/opt/omni/server/integ/Config/E2010 中的配置文件中，该文件以 Exchange Server 或 DAG 的主机名命名。必要时，Data Protector 将使用用户凭据。

安装 Microsoft Exchange ZDB 客户机

安装以下 Data Protector 软件组件：

- P9000 XP Agent – 在应用程序系统和备份系统上
- MS Exchange Integration – 仅在应用程序系统上

备份 Microsoft Exchange Server 集成

This feature is available in the Premium Edition

备份 Microsoft Exchange Server 数据库时，将自动备份以下文件:

- 数据库文件 (.edb)
- 事务日志 (.log)
- 检查点文件 (.chk)

但是，根据您选择的 Microsoft Exchange Server 备份类型，并非始终备份所有文件。

备份类型

由于涉及 Microsoft Exchange Server、ZDB 磁盘阵列和 VSS，因此可以指定不同种类的备份类型:

- Microsoft Exchange Server 备份类型
- ZDB/ZDB IR 备份类型
- VSS 备份类型

Microsoft Exchange Server 备份类型

可以在以下 Microsoft Exchange Server 备份类型中选择:

备份类型

完整	备份数据库文件 (.edb)、事务日志 (.log) 和检查点文件 (.chk)，然后截断事务日志。 *DAG 环境:* 如果为备份选择了多个数据库副本，Data Protector 会先对应用于数据库文件的日志最少的被动副本执行完整备份，然后再对所有其他副本执行复制备份，最后再备份主动副本。由于 Microsoft Exchange Server VSS 写入程序的限制，副本按顺序备份。
复制	备份数据库文件 (.edb)、事务日志 (.log) 和检查点文件 (.chk)，而无需截断事务日志。
增量	备份自上次完整备份或增量备份以来所创建的事务日志 (.log)，然后截断事务日志。 *DAG 环境:* 如果选择多个数据库副本进行备份，Data Protector 只会备份一个副本 (已选择其中一个被动副本) 中的事务日志。
差异	备份自上次完整备份以来已创建的事务日志 (.log)，而无需截断事务日志。

注意下列情况下，无法执行数据库的增量备份或差异备份:

- 尚未执行完整备份。
- 刚刚执行差异备份之后开始增量备份，或者反过来。
- 启用了 Microsoft Exchange Server 循环日志记录。

ZDB 备份类型

可以从以下 ZDB 备份类型中选择:

- ZDB 到磁盘
- ZDB 到磁盘 + 磁带
- ZDB 到磁带

注意Microsoft Exchange Server 增量和差异备份类型只能使用 ZDB 到磁带备份类型。

VSS 备份类型

可以从以下 VSS 备份类型中选择:

- 本地或网络备份
- VSS 可传输

备份并行性

- 在备份会话期间，不同数据库的副本是并行备份的，但是，受限于 Microsoft Exchange Server VSS 写入程序，不会并行备份同一数据库的副本。
- 如果并行启动准备备份同一数据库的多个备份会话，只有首先锁定数据库的会话才能备份数据库，其他会话则不能。在 DAG 环境中，如果备份会话准备备份同一数据库的不同副本，情况也是如此，即只有首先锁定数据库 (即其所有副本) 的会话才能备份数据库副本，其他会话则不能。

> **注意**此行为可确保还原链的构成有效。例如，假设并行启动准备备份同一数据库的多个完整备份会话。如果所有会话都备份了数据库，则可能发生会话 ID 最新的会话并非最后完成数据库备份的情况。

DAG 环境中的复本循环

通过 Data Protector Microsoft Exchange Server 2010 集成，可以在多系统环境 (DAG 环境) 中执行 ZDB 会话。这会为现有复本循环功能带来一些变化。

在独立环境中，复本循环功能的执行方式不变；它会限制 Data Protector IDB 数据库中保留用于即时恢复的备份数量。例如，如果“循环的复本数”选项设置为 1 ，则一次只有一个备份会话可用于即时恢复。如果您启动另一个备份会话 (使用相同的备份规范)，则会在创建新备份会话之前删除上一个备份会话中所创建的备份存储卷，并从“即时恢复”上下文中删除上一个会话。

在 DAG 环境中，可以在不同会话中备份来自不同系统的数据库。这就引入了变化。例如，您要备份在 node1.company.com 上处于主动状态的数据库 DB1 ，以及在 node2.company.com 上处于主动状态的数据库 DB2 。假设“循环的复本数”选项设置为 1 ，并且备份策略是始终备份主动副本。备份后，Data Protector VSSDB 数据库包含以下条目:

备份 1 (2013/10/05–1):

- 2013/10/05-1:node1.company.com (包含 DB1)
- 2013/10/05-1:node2.company.com (包含 DB2)

假设发生故障转移且数据库 DB1 在 node2.company.com 上变为主动状态。您启动另一个备份会话。现在，两个数据库都从 node2.company.com 进行备份。因此，VSSDB 数据库包含以下条目:

备份 2 (2013/10/05–2):

- 2013/10/05-1:node1.company.com (包含 DB1)
- 2013/10/05-2:node2.company.com (包含 DB1 和 DB2)

条目 2013/10/05-1:node2.company.com 不再位于 VSSDB 数据库中，因为由于复本循环功能它已退出循环 (相应的备份存储卷已被删除)。

> **注意**条目按系统循环，不按会话循环。因此，在同一会话中创建的多个条目可以在不同的时间点 (即，在不同会话中) 退出循环。

现在发生另一个故障转移，两个数据库在 node1.company.com 上都变为主动状态。您启动另一个会话，两个数据库都从 node1.company.com 进行备份。因此，VSSDB 数据库包含以下条目:

备份 3 (2013/10/05–3):

- 2013/10/05-3:node1.company.com (包含 DB1 和 DB2)
- 2013/10/05-2:node2.company.com (包含 DB1 和 DB2)

请注意，条目 2013/10/05-1:node1.company.com 也已退出循环。由于在会话 2013/10/05-1 中创建的两个部分都已退出循环，因此会话 2013/10/05-1 不能再用于即时恢复 (它已从“即时恢复”上下文中删除)。

如果您转到“即时恢复”上下文并在执行备份 2 后选择在备份 1 中创建的会话，则“源”页会错误地显示两个数据库均可还原。条目 2013/10/05-1:node2.company.com (包含 DB2) 在备份 2 中已退出循环。如果您选择 DB2 进行还原并启动即时恢复，则会话将失败。因此，请确保从 VSSDB 数据库中仍存在其必要条目的会话中还原数据库。

备份考虑事项

- *备份策略：*

选择以下策略之一来备份数据：

- 完整
- 完整、增量、增量……
- 完整、差异、差异……
- 完整、副本、增量……副本、增量……

重要说明增量备份会话不能后跟差异备份会话，反之亦然。必须先运行完整备份会话。

- *主动副本与被动副本：*

主动副本和被动副本之间无太多区别，唯一区别是当前活动日志文件（位于主动副本一侧），该文件在填满（即达到 1 MB）之前不会复制到被动副本一侧。因此，如果备份被动副本，则当前活动日志文件中的事务将不包括在内。

- *滞后的数据库副本：*

备份滞后的数据库副本等同于备份非滞后的数据库副本。如果从滞后的数据库副本的备份中还原，则不仅会还原文件，还会将日志应用于数据库文件，从而使数据库恢复到最新状态。但是，还原日志并将其应用于数据库文件非常耗时，因此会延长还原会话。另请注意，您需要足够的磁盘空间来还原所有必要的日志。

另一方面，通过从滞后数据库副本的备份还原，可以将数据库还原到进行备份之前的时间点。在不执行数据库恢复和装载的情况下还原数据库。然后删除不需要的日志，最后恢复并装载数据库。

- *公用文件夹：*

在 Microsoft Exchange Server 2010 环境中，不支持使用激活的复制来备份 Microsoft Exchange Server 公用文件夹。

- *并发备份会话:*

备份相同数据库的备份会话无法并行运行。

对象操作注意事项

- 对象复制和对象验证

  复制或验证 Microsoft Exchange Server 对象时，需要选择在同一会话中创建的所有 Data Protector 备份对象。为了确保不是仅选择会话中的几个对象，Data Protector GUI 不会在“对象操作”上下文的“对象”范围中列出用于交互式对象复制或对象验证会话的 Microsoft Exchange Server 备份对象。

  使用“会话”或“介质”范围替代。

创建备份规范

使用 Data Protector GUI (**Data Protector Manager**) 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS Exchange 2010+ Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，指定“备份类型” (VSS 备份类型)。有关详细信息，请按 **F1**。单击**确定**。
4. 在“应用程序系统”中，选择要备份的 Microsoft Exchange Server 系统。在 DAG 环境中，选择 DAG 虚拟系统或 Microsoft Exchange Server 系统。

   注意“应用程序系统”下拉列表包含安装了 Data Protector MS Exchange Server 2010+ 集成组件的所有客户机。在 DAG 环境中，该列表还包含 DAG 虚拟系统 (主机)。

   备份会话 (即集成代理 e2010_bar.exe) 将在此处指定的客户机上启动。如果您选择 DAG 虚拟系统，则会在当前活动的 Microsoft Exchange Server 节点上启动集成代理。

   注意在 Microsoft Exchange Server 环境中，要备份驻留在作为 DAG 环境一部分的 Microsoft Exchange Server 系统上的公用文件夹，请选择 Microsoft Exchange Server 系统而不是 DAG 虚拟系统 (主机)。如果您选择 DAG 虚拟系统，则只能备份属于 DAG 的数据库。Microsoft Exchange Server 公用文件夹数据库不是它的一部分。

   根据您选择的 VSS 备份类型，指定以下内容:

   - 如果选择的是“本地或网络备份”，则在“提供程序”中选择“使用硬件提供程序”。
   - 如果选择的是“VSS 可传输备份”，请指定“备份系统”。

指定特定于 ZDB 的选项。

有关详细信息，请按 **F1**。

> **注意**在 P9000 XP 磁盘阵列系列重新同步模式环境中，可为给定存储卷 (P-VOL) 创建的最大复本存储卷 (S-VOL) 数由硬件提供程序配置 (MU 范围) 限制 (最大为 3)。要启用增量和差异会话的执行，备份规范中的“循环的复本数”选项必须设置为小于 MU 范围的值。从而，保留一个复本存储卷用于增量和差异备份会话。
>
> **注意:** 要执行即时恢复，请在创建备份规范时选中“跟踪复本以用于即时恢复”(在“复本管理”下) 复选框。

对于 IR 备份，“复本类型”下拉列表具有两个选项:“差异 (快照)”和“Plex (克隆/镜像)”。单击“下一步”。

5. 在“配置 MS Exchange 2010+ Server”对话框中，提供用于浏览、备份或恢复 Exchange Server 的域、用户名和密码。

   单击**确定**。

6. MS Exchange Server 即配置完成。退出 GUI 或继续在步骤 7 创建备份规范。

7. 如果选择的是 DAG 虚拟系统 (主机)，请指定“视图类型”以定义在下一页 (“源”页) 中应如何组织 Microsoft Exchange Server 数据库:

按角色	显示 DAG 中的所有数据库。
按客户机	显示 DAG 中的所有客户机，以及位于客户机上的所有数据库（主动或被动）。主动数据库结尾追加了标签 (主动)。被动数据库没有标签。

有关“用户和组/域”选项的信息，请按 **F1**。

> **注意**如果没有指定用于远程执行 Exchange Management cmdlet 操作的有效用户凭据，将显示 Microsoft Exchange Server 配置对话框。

8. 选择要备份的 Microsoft Exchange Server 数据库。

   > **注意***DAG 环境:*
   >
   > 在一个会话中，可以备份下列项之一:
   >
   > - 多个数据库，但每个数据库仅备份一个副本
   > - 一个数据库，但可备份其多个副本

9. 如果选择了“按角色”视图类型，则以下内容适用于 DAG 环境。

   指定备份策略选项。

10. 选择用于备份的设备。

    要指定设备选项，请右键单击该设备，然后单击“属性”。在“并发”选项卡中指定并行备份流的数量，并指定要使用的介质池。

    单击“下一步”。

11. **设置备份选项。**

    单击“下一步”。

12. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

> **提示**请在实际使用之前先预览备份规范。

备份策略选项

选项	描述	
备份活动数据库	如果选中此选项，则会备份主动副本。	
备份被动副本	如果选中此选项，则会备份被动副本。如果数据库具有多个被动副本，请使用以下策略之一指定要备份的特定副本:	
	最小主机数 (默认)	如果选中此选项，则备份中涉及最少的客户机数量。例如，如果要备份的数据库在相同的主机上各有一个被动副本，则从该客户机上将它们全部备份（不是从一个客户机备份一个数据库、从另一客户机备份另一数据库）。
	最低/最高激活首选参数	如果选中此选项，则会备份激活首选项编号最低/最高的数据库副本。
	最短/最长重播延迟时间	如果选中此选项，则会备份重播延迟时间最短/最长的数据库副本。
	最长截断延迟时间	如果选中此选项，则会备份截断延迟时间最长的数据库副本。
	有关详细信息，请参阅 Microsoft Exchange Server 文档。	
	如果无被动副本可用，则使用主动副本进行备份	在选中了“备份被动副本”时可用如果选中此选项，则在无被动副本可用时备份主动副本。
备份所有副本	仅当只选择一个数据库进行备份时可用。 如果选中此选项，则会备份所有副本 (主动和被动)。当创建“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”备份 (即，可以用于即时恢复的备份) 时，此选项十分有用。如果备份了多个副本，则在即时恢复期间可以还原多个副本，因为每个副本都有自己用于还原的复本存储卷。 否则，在创建 ZDB-to-tape 备份时，备份单个副本便已足够；可以从单个副本的 ZDB-to-tape 备份还原数据库的不同副本。	
从备份中排除客户机	创建客户机列表。不会备份驻留在这些客户机上的数据库副本。	

特定于应用程序的备份选项

选项	描述
Pre-exec、**Post-exec**	指定备份之前 (pre-exec) 或之后 (post-exec) 要在 Microsoft Exchange Server 系统上运行的命令行。 命令行只能在启动了备份会话的 Microsoft Exchange Server 系统上执行 (在该系统上还启动了 Data Protector Microsoft Exchange Server 集成代理 e2010_bar.exe)。 只键入命令的名称并确保命令位于同一系统上的默认 Data Protector 命令目录中。不要使用双引号。 *DAG 环境:* 如果在**应用程序系统**选项中选择 DAG 虚拟系统（主机），请确保命令位于当前活动的节点上。

	如果选择此选项，Microsoft Exchange Server 会检查数据库备份数据的一致性。如果未选择此选项，会话会较早结束，但备份数据的一致性无法保证。 创建备份数据后，将对复本存储卷执行检查。如果发现数据损坏，复本存储卷将被弃用，并导致数据库备份失败。
执行一致性检查 [-exch_check [-exch_throttle Value] | -exch_checklogs]	默认：选择 如果选中“仅检查日志文件”选项，则仅检查日志文件的备份数据，这足以使 Microsoft Exchange Server 保证数据一致性。 默认：选择 默认情况下，一致性检查占用 I/O 较多，这可能会对磁盘性能产生负面影响。“限制检查 1 秒钟”选项会限制数据库文件 .edb 的一致性检查，以减少对磁盘性能的影响。指定在进行多少次输入/输出操作之后，应将检查停止一秒时间。 如果仅选中日志文件，则此选项不可用。 默认：未选择

修改备份规范

要修改备份规范，请在“备份”上下文的“范围窗格”中单击其名称。

在 Microsoft Exchange Server 2013 环境的“源”页中，通过右键单击所选备份对象并单击“配置”，可以更改用于远程执行 Exchange Management cmdlet 操作的 Exchange 域用户凭据。也可以通过单击“检查配置”来验证配置。

单击其他所需选项卡，然后应用更改。

> **注意**要在“源”页中显示所有数据库，请在“显示”选项中选择“全部”。在 DAG 环境中，这不仅会显示所有数据库，还会更新数据库的当前状态 (主动或被动)。
>
> 要仅显示选定用于备份或从备份中排除的数据库，请在“显示”选项中选择“选定”。如果未显示任何数据库，则表示未从备份规范中排除任何数据库，所有数据库都将进行备份。当有新的数据库添加到为备份选择的客户机上时，该数据库将自动被包括到备份规范中。

计划备份会话

您可以将备份会话计划为在特定时间自动启动或定期启动。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS Exchange 2010+ Server”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector User Interface 组件的客户机。
2. 请执行以下命令：

   ```
   omnib -e2010_list BackupSpecificationName -test_bar
   ```

预览期间会发生什么?

测试以下内容:

- 启动备份会话的 Microsoft Exchange Server 系统与 Cell Manager 之间的通信
- 应用“备份策略”选项和“客户机过滤”选项之后，每个选定数据库是否至少有一个副本可用于备份 (这适用于包含备份策略选项的备份规范)
- 选定数据库是否准备就绪，可进行备份 (即，它们不应被卸除、挂起或处于失败状态)

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

要启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS Exchange 2010+ Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用按配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector“用户界面”组件的客户机。
2. 请执行以下命令：

   omnib -e2010_list BackupSpecificationName [-barmode E2010Mode] [LIST_OPTIONS]

   其中， E2010Mode 为下列项之一:

   full|copy|incr|diff

   默认为 full 。

   示例

   要使用备份规范 MyDatabases 启动完整备份，请执行以下命令:

   omnib -e2010_list MyDatabases -barmode full

   要使用相同的备份规范启动差异备份，请执行以下命令:

   omnib -e2010_list MyDatabases -barmode diff

备份对象

对于每个数据库 (副本)，Data Protector 会创建以下备份对象:

- *数据库文件对象*
  - ClientName /Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/DBID/File [MSVSSW-APP]

    (独立数据库或主动副本)
  - ClientName /Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/DBID/File [MSVSSW-APP]

    (被动副本)
- *日志文件对象*
  - ClientName /Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/DBID/Logs [MSVSSW-APP]

    (独立数据库或主动副本)
  - ClientName /Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/DBID/Logs [MSVSSW-APP]

    (被动副本)
- *数据库对象*

  ClientName /DBID/DBName [E2010]

  数据库对象包含构造还原链所需的信息。
- *VSS 元数据对象*

  /BackupSession/Metadata [MSVSSW-APP]

有关对象是否备份成功的信息保存在 Data Protector IDB 中。

用于备份和还原会话的 Windows 域用户帐户

通过 Data Protector Inet 服务启动备份和还原会话，默认情况下，这些会话使用 Windows 本地用户帐户 SYSTEM 运行。因此，可以使用相同的用户帐户进行备份或恢复会话。

但是，您可以指定 Data Protector Inet 服务应使用不同的 Windows 域用户帐户来启动会话:

- 要以其他用户帐户执行备份会话，请在创建备份规范时指定“指定 OS 用户”选项。
- 要以其他用户帐户执行还原会话，请在“选项”页面或“高级”页面中指定“用户名”和“组/域名”选项。

还原 Microsoft Exchange Server 集成

This feature is available in the Premium Edition

可以使用标准还原或即时恢复会话来还原 Microsoft Exchange Server 数据。

重要说明还原某个数据库后，请对该数据库启动完整备份会话。否则，后续增量和差异备份会话将失败。

注意事项

- 使用 Data Protector Microsoft 卷影复制服务集成备份的 Microsoft Exchange Server 数据库无法通过 Data Protector Microsoft Exchange Server 2010 集成来还原，也无法使用其他方法还原。

还原方法

还原 Microsoft Exchange Server 数据库有多种原因。例如:

- 数据库已损坏。
- 活动和被动数据库副本之间的同步已中断，但您不想对被动副本进行种子重新设定，或者只是因为恢复操作不起作用。
- 需要将数据库还原到不同的时间点。
- 出于调查目的，需要还原数据库的备份数据。
- 需要将数据库的备份数据还原到恢复数据库，以便提取单个邮箱或邮箱文件。
- 需要将数据库的备份数据还原到拨号音数据库。

为了满足您的需求，Data Protector 提供了不同的还原方法。可以在以下选项中选择：

- **修复所有处于失败状态的被动副本**
- **还原到最新状态**
- **还原到某时间点**
- **还原到新邮箱数据库**
- **还原到临时位置**

您可以为同一会话中的不同数据库指定不同的还原方法。

注意前三个方法将备份数据还原到原始数据库，因此只有在原始数据库仍然存在时才可用。最后两种方法将备份数据还原到新位置。

修复所有处于失败状态的被动副本

只有属于 DAG 的数据库才可以使用此方法。当一些数据库的被动副本损坏而进入 Failed 或 FailedAndSuspended 状态时，可使用此方法。此方法使用上次备份会话 (和相应的还原链) 中创建的备份自动还原所有损坏的被动副本。数据恢复后，只要选择**恢复数据库复制**选项，副本便会与活动副本同步。

还原到最新状态

此方法用于将损坏的数据库及时还原到尽可能新的状态。Data Protector 使用上次备份会话（和相应的恢复链）中创建的备份恢复数据库。

在文件还原完毕后，所有的日志 (不只是从备份还原的日志，还包括任何现有的日志) 都会对数据库文件进行重放。

注意*DAG 环境:*

还原被动副本后，Microsoft Exchange Server 要根据 ReplayLagTime 参数设置确保已经对数据库文件进行了日志重放。

还原到某时间点

此方法用于将数据库还原到某个特定的时间点。

注意*标准还原:*

还原独立数据库或活动副本时，将重命名现有的 .log 和 .chk 文件 (在文件名后添加 .keep 扩展名)。在不执行数据库恢复的情况下还原文件时，此功能很有用。此功能可以对数据库文件应用其他日志；只需删除您也想要应用的日志文件的 .keep 扩展名，然后手动启动数据库恢复即可。通过这种方式，可以微调将数据库还原到的时间点。

还原被动副本时，将删除现有文件。

还原文件后，如果选择“执行数据库恢复”选项，则向数据库文件 (.edb) 重放日志。

注意*DAG 环境:*

- 还原被动副本后，Microsoft Exchange Server 要根据 ReplayLagTime 参数设置确保已经对数据库文件进行了日志重放。
- 对于不恢复的被动副本，一旦恢复会话完成，必须完整地重新设定种子。

还原到新邮箱数据库

此方法用于将数据还原到不同的数据库中，原因可能是原始数据库已不存在或需要将数据移往他处。

使用该选项，也可以将数据恢复到 Microsoft Exchange Server 恢复数据库。

注意*即时恢复：*

对于数据只能还原到原始存储卷的复本类型，此选项不可用。

还原文件到临时位置

使用此方法，可将数据库文件还原到所选位置。

- 当从差异或增量备份会话还原时，可以还原完整还原链或只还原所选会话中备份的文件 (.log)。
- 从完整备份会话还原数据时，可以选择只还原数据库文件 (.edb)。

注意*即时恢复：*

对于数据只能还原到原始存储卷的复本类型，此选项不可用。

还原目标

可将备份数据还原到:

- 现有数据库 (独立数据库、活动副本、被动副本)、
- 新的数据库、
- 临时位置。

还原到独立数据库

还原到原始独立数据库 (独立环境) 的过程如下:

1. 卸除数据库。
2. 还原备份数据。
3. (可选) 向数据库文件 .edb 重放新还原的日志 (如果执行“还原到最新状态”方法，还包括先前存在的日志) 并装载数据库。

要还原到原始独立数据库，请使用以下还原方法之一:

- **还原到最新状态**
- **还原到某时间点**

还原到活动副本

还原到活动副本 (DAG 环境) 的过程如下:

1. 卸除数据库。
2. 暂停所有复制。
3. 还原备份数据。
4. (可选) 向数据库文件 .edb 重放新还原的日志 (如果执行“还原到最新状态”方法，还包括先前存在的日志) 并装载数据库。

要还原到活动副本，请使用以下还原方法之一:

- **还原到最新状态**
- **还原到某时间点**

还原到被动副本

还原到被动副本 (DAG 环境) 的过程如下:

1. 暂停复制。
2. 还原备份数据。
3. (可选) 恢复对活动副本的复制。

要还原到被动副本，请使用以下还原方法之一:

- **还原所有处于失败状态的被动副本**
- **还原到最新状态**
- **还原到某时间点**

将数据还原到新数据库

还原到新数据库的过程如下:

1. 创建一个新的邮箱数据库。
2. 将备份数据还原到新数据库。

> **注意**如果还原到恢复数据库，则首先还原备份数据，然后创建恢复数据库。

要将数据还原到新邮箱数据库或恢复数据库，可使用“还原到新邮箱数据库”还原方法。

将文件还原到临时位置

可以将数据库文件 (.edb 和/或 .log 和/或 .chk) 还原到选择的客户机和目录。选择“将文件还原到临时位置”还原方法。

在 DAG 环境中即时恢复

在 DAG 环境中备份数据库时，可以决定是备份所有副本还是仅备份单个副本。如果在即时恢复期间备份了所有副本，则可以还原所有副本，因为每个副本都具有各自用于还原的复本存储卷。如果仅备份了单个副本，请注意以下事项:

- 在大多数情况下，只能从单个数据库副本的备份中还原一个数据库副本。某些复本类型与源 (“相关”复本类型) 直接相关，而其他复本则为“独立”，允许将数据还原到不同位置。对于后者，可以还原原始数据库副本或其他数据库副本。

  > **注意**以下复本类型是独立复本:
  >
  > - P9000 XP 磁盘阵列系列 (VSS 兼容模式下的拆分镜像复本类型)

  对于相关复本类型，Data Protector 会自动灰显“目标节点”选项中的客户机，这些客户机的数据库副本因无法还原而未备份。

- 可以从单个数据库副本的备份还原多个数据库副本的唯一复本类型是快照式克隆 (对于 Dell EMC Unity (VSA 版本 4.5 和 5.0) 以及 Netapp (9.x) 存储提供程序)。不过，还必须确保“使用 P6000 EVA SMI-S 进行还原”和“将复本数据复制到源卷”即时恢复选项均处于选中状态，在这种情况下，会按顺序将复本存储卷中的数据复制到多个位置，并依次各个还原数据库副本。

还原链

默认情况下，当您选择差异备份会话或增量备份会话进行还原时，Data Protector 不仅会还原在所选会话中备份的日志 (.log)，还会还原在先前会话 (“还原链”) 中备份的文件:

- 如果选择了差异备份会话，Data Protector 将还原:

1. 在完整或复制备份会话中备份的 .edb 文件和 .log 文件。
2. 在所选差异备份会话中备份的 .log 文件。

- 如果选择了增量备份会话，Data Protector 将还原:
  1. 在完整或复制备份会话中备份的 .edb 文件和 .log 文件。
  2. 在所有后续增量备份会话 (一直到所选增量备份会话) 中备份的 .log 文件。
- 如果选择了完整备份或复制备份会话，Data Protector 将还原在所选会话中备份的 .edb 文件和 .log 文件。

- 如果使用“还原到最新状态”方法，则不会还原完整备份会话或复制备份会话中的 .log 文件。
- 只有“还原到临时位置”方法可以只还原在所选增量或差异会话中备份的 .log 文件。

在即时恢复期间还原链

在即时恢复会话期间，首先选择使用:

- 完整 (ZDB 到磁盘或 ZDB 到磁盘 + 磁带) 会话还是
- 复制 (ZDB 到磁盘或 ZDB 到磁盘 + 磁带) 会话

进行即时恢复。然后，从数据库特定选项中，在“还原其他日志，直至”选项中选择后续增量或差异会话，指定是否还应还原其他日志。

在即时恢复会话中，Data Protector 将还原:

1. 在所选的完整或复制备份会话中备份的 .edb 文件和 .log 文件。
2. 在所选的差异备份会话 (一直到所选增量备份会话) 或所有后续增量备份会话中备份的 .log 文件。

还原并行性

如果允许设备并发，则并行还原数据库副本，但以下情况除外:

- 如果数据库副本是从同一个客户机备份的，但现在还原到不同的客户机。
- 如果将同一个数据库副本的备份数据用作多个数据库副本的还原来源。

查找要还原的信息

可以从 Data Protector IDB 检索有关备份会话的信息 (例如有关备份类型和所用介质的信息，以及在备份期间报告的消息)。

要检索信息，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开“对象”或“会话”。

   如果展开“对象”，则会根据创建备份对象时所针对的 Microsoft Exchange Server 数据库对备份对象进行排序。

   注意备份对象名称包含数据库 GUID。要了解哪个 GUID 属于哪个数据库，请参阅数据库对象 /DB_GUID/DB_Name 。

   例如，数据库 DB1 的数据库对象在 GUID 为 08bca794-c544-4e27-87e8-533fb81fd517 为:

   /08bca794-c544-4e27-87e8-533fb81fd517/DB1

   如果展开“会话”，则会根据创建备份对象的会话对备份对象进行排序。例如，在会话 2013/02/7–7 中创建的备份对象列在 2013/02/7–7 下方。

   要查看某个备份对象的详细信息，请右键单击该备份对象，然后单击“属性”。

   提示要查看在会话期间报告的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 Data Protector User Interface 组件的任何 Microsoft Exchange Server 客户机。

2. 获取在备份会话中创建的 Microsoft Exchange Server 备份对象的列表:

   omnidb -session SessionID

3. 获取备份对象的详细信息:

   omnidb -e2010 BackupObjectName -session SessionID -catalog

   以下是备份对象名称的一个示例:

   devy.company.com:/08bca794-c544-4e27-87e8-533fb81fd517/DB1

标准还原

标准还原是从 Data Protector 介质 (例如磁带) 上的备份数据进行还原。此类数据在“ZDB 到磁盘 + 磁带”和“ZDB 到磁带”会话中创建。

可以在同一个标准还原会话中还原多个 Microsoft Exchange Server 数据库，同时为每个数据库指定不同的还原方法。

要执行标准还原，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“MS Exchange 2010+ Server”，展开 DAG 虚拟系统或独立的 Microsoft Exchange Server 系统，然后单击“MS Exchange 2010+ Server”。
3. 在“源”页面中，Data Protector 显示从选定的 DAG 或独立环境中备份的所有 Microsoft Exchange Server 数据库。

   选择要还原的 Microsoft Exchange Server 数据库。

   在选择数据库时，会自动显示“数据库属性”对话框。指定一种还原方法，然后单击“确定”。对于属于 DAG 的数据库，默认的还原方法为“修复状态为失败的所有被动副本”。对于独立数据库，默认方法为**恢复到最新状态**。

   要更改还原方法，请右键单击数据库并单击“属性”。
4. 在“选项”页面中，指定 Data Protector Microsoft Exchange Server 2010 集成还原选项。
5. 在“设备”页面中，选择要用于还原的设备。
6. 单击**还原**。
7. 在“启动还原会话”对话框中，单击“下一步”。
8. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
9. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Cell Manager 或安装了 User Interface 组件的 Microsoft Exchange Server 客户机。
2. 执行以下命令：

```
omnir -e2010 -barhost ClientName [VSS_EXCHANGE_SPECIFIC_OPTIONS] Database [Database ...] [-user User:Domain] [GENERAL_OPTIONS] Database {-db_name SourceDatabaseName | -db_guid SourceDatabaseGUID } [-source SourceClientName] {-repair | -latest | -pit | -new | -temp} E2010_METHOD_OPTIONS E2010_REPAIR_METHOD_OPTIONS [–no_resume_replication] E2010_LATEST_METHOD_OPTIONS [-node TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount] E2010_PIT_METHOD_OPTIONS -session BackupID [-node TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount]
```

```
E2010_NEW_METHOD_OPTIONS -session BackupID -client TargetClientName -location TargetDatabasePath -name TargetDatabaseName [-recoverydb] [–no_recover] [–no_mount] E2010_TEMP_METHOD_OPTIONS -session BackupID -client TargetClientName -location TargetDatabasePath [–no_chain] [–edb_only] [–no_recover]
```

> **注意**备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。
>
> 镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，必须指定原始“备份”会话的会话 ID (即备份 ID)，而不是“对象复制”会话的会话 ID。
>
> 如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

示例 (还原方法 - 修复)

DAG 环境

要还原从虚拟系统名称为 dag0.company.com 的 DAG 中备份的数据库 DB1 的所有损坏被动副本，并确保在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source dag0.company.com -repair
```

示例 (还原方法 - 最新)

独立环境

要将位于客户机 exchange1.company.com 上的受损独立数据库 DB1 还原到可还原的最新时间点，并确保在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source exchange1.company.com –latest
```

DAG 环境

假设您要还原位于客户机 exchange1.company.com 上的数据库 DB1 的活动副本，以及位于客户机 exchange2.company.com 和 exchange3.company.com 上的数据库的被动副本。假设数据库 DB1 是虚拟系统名称为 dag0.company.com 的 DAG 的一部分，并且您希望在客户机 exchange2.company.com 上启动集成代理 (e2010_bar.exe)。请执行以下命令：

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source dag0.company.com –latest –node exchange1.company.com –node exchange2.company.com –node exchange3.company.com
```

示例 (还原方法 - pit)

独立环境

假设您要使用在会话 2013/5/14-1 中创建的备份数据来还原位于客户机 exchange1.company.com 上的受损独立数据库 DB1 。假设您希望在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)。请执行以下命令：

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 -pit –session 2013/5/14-1
```

注意未指定 –source 选项，在这种情况下，Data Protector 假定从使用 –barhost 选项指定的客户机备份数据库。

示例 (还原方法 - new)

DAG 环境

假设您想要将数据库 DB1 的备份还原到应在客户机 exchange2.company.com 上创建的恢复数据库，该数据库名为 Recovery1 ，文件在 C:\Recovery1Folder 目录中。假设数据库 DB1 从虚拟系统名称为 dag0.company.com 的 DAG 中的 2013/5/14-1 会话中创建。另外，还要确保在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source dag0.company.com –new –session 2013/5/14-1 –client exchange2.company.com -location C:\Recovery1Folder –name Recovery1 –recoverydb
```

示例 (还原方法 - temp)

独立环境

假设您想要还原位于客户机 exchange2.company.com 上的数据库 DB1 的事务日志。这些日志已在增量备份会话 2013/5/14-1 中备份。要不执行数据库恢复即将日志还原到客户机 exchange2.company.com 的 C:\DB1TransactionLogFolder 目录，并确保在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe)，请执行以下命令:

omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source exchange2.company.com –temp –session 2013/5/14-1 –client exchange2.company.com –location C:\DB1TransactionLogFolder -no_chain –no_recover

使用其他设备进行还原

您可以使用除备份时所用设备之外的设备进行还原。

即时恢复

为了能够执行即时恢复会话，需要使用存储在复本存储卷上的备份数据。此类备份数据在“ZDB 到磁盘”和“ZDB 到磁盘 + 磁带”会话中创建。

可以在同一个即时恢复会话中还原多个 Microsoft Exchange Server 数据库，同时为每个数据库指定不同的还原方法。

要启动即时恢复会话，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI 进行即时恢复

要执行即时恢复会话，请执行以下操作:

1. 在“上下文列表”中，单击“即时恢复”。
2. 展开“Exchange 2010+ Server”，然后选择要用于即时恢复的“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。会话根据所用的备份规范进行排序。
3. 在“源”页面中选择要还原的 Microsoft Exchange Server 数据库。

   在选择数据库时，会自动显示“数据库属性”对话框。指定一种还原方法，然后单击“确定”。对于属于 DAG 的数据库，默认的还原方法为“修复状态为失败的所有被动副本”。对于独立数据库，默认方法为**恢复到最新状态**。要更改还原方法，请右键单击数据库并单击“属性”。

   有关“配置检查模式”的详细信息，请按 **F1**。
4. 在“选项”页面中，指定特定于 ZDB 的选项。有关详细信息，请按 **F1**。
5. 在“高级”页面中，指定 Data Protector Microsoft Exchange Server 2010 集成即时恢复选项。

使用 Data Protector CLI 进行即时恢复

1. 使用按照配置用户帐户中所述进行配置的用户帐户，登录到 Data Protector Cell Manager 或 Microsoft Exchange Server 客户机。
2. 执行以下命令：

```
omnir -e2010 -barhost ClientName -instant_restore [VSS_INSTANT_RECOVERY_OPTIONS] [VSS_EXCHANGE_SPECIFIC_OPTIONS] Database [Database ...] [-user User:Domain] [GENERAL_OPTIONS] Database {-db_name SourceDatabaseName | -db_guid SourceDatabaseGUID} [-source SourceClientName] {-repair | -latest | -pit | -new | -temp} E2010_METHOD_OPTIONS E2010_REPAIR_METHOD_OPTIONS [–no_resume_replication]
```

```
E2010_LATEST_METHOD_OPTIONS [-node TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount] [E2010_IR_SPECIFIC_OPTIONS] E2010_PIT_METHOD_OPTIONS -session SessionID [-node TargetNode ... | -all] [–no_resume_replication] [–no_recover] [–no_mount] [E2010_IR_SPECIFIC_OPTIONS] E2010_NEW_METHOD_OPTIONS -session SessionID -client TargetClientName -location TargetDatabasePath -name TargetDatabaseName [-recoverydb] [–no_recover] [–no_mount] [E2010_IR_SPECIFIC_OPTIONS] E2010_TEMP_METHOD_OPTIONS -session SessionID -client TargetClientName -location TargetDatabasePath [–no_chain] [–edb_only] [–no_recover] [E2010_IR_SPECIFIC_OPTIONS] E2010_IR_SPECIFIC_OPTIONS [-from_session SessionID]
```

示例 (还原方法 - 最新)

独立环境

假设您想要还原位于客户机 exchange1.company.com 上的受损独立数据库 DB1 。要确保在客户机 exchange1.company.com 上启动集成代理 (e2010_bar.exe) ，并确保将数据库还原到最新状态，请执行以下命令:

```
omnir -e2010 -barhost exchange1.company.com –instant_restore –copy_back –db_name DB1 -latest
```

示例 (还原方法 - temp)

DAG 环境

假设您想要还原 DAG 虚拟系统 (主机) 名称为 dag0.company.com 的 DAG 中的数据库 DB1 。此数据库在会话 2013/5/14-1 中备份。要将该数据库还原到客户机 exchange1.company.com 上的临时位置，即目录 C:\BackupDatabase ，并确保在客户机 exchange1.company.com 上启动集成

代理 (e2010_bar.exe)，请执行以下命令:

omnir -e2010 -barhost exchange1.company.com –instant_restore –copy_back –db_name DB1 –source dag0.company.com –temp –session 2013/5/14-1 –client exchange1.company.com –location C:\BackupDatabase

还原选项

修复所有处于失败状态的被动副本

GUI/CLI 中的选项	描述
恢复数据库复制/ -no_resume_replication	在 DAG 环境中可用。在还原副本后，恢复活动副本和被动副本之间的复制。 请注意，CLI 选项 -no_resume_replication 具有相反的含义。如果指定此选项，则不会恢复复制。
还原其他日志，直至 -session	这是特定于即时恢复的选项。 不可用。
目标节点	不可用。 自动选择状态为 Failed 或 FailedAndSuspended 的客户机 (即副本)。

还原到最新状态

GUI/CLI 中的选项	描述
为还原选择	指定是否应还原数据库。
还原其他日志，直至 -session	这是特定于即时恢复的选项。 不可用。
执行数据库恢复/ -no_recover	在还原独立数据库 (独立环境) 或活动副本 (DAG 环境) 时可用。在还原完成之后将日志应用于数据库文件 (.edb)。 请注意，CLI 选项 -no_recover 具有相反的含义。如果指定此选项，则不执行数据库恢复。
装载数据库/ -no_mount	在还原独立数据库 (独立环境) 或活动副本 (DAG 环境) 时可用。在数据库恢复完成之后装载数据库。仅当选择“执行数据库恢复”时，此选项才可用。 请注意，CLI 选项 -no_mount 具有相反的含义。如果指定此选项，则不会装载数据库。
恢复数据库复制/ -no_resume_replication	在还原被动副本 (DAG 环境) 时可用。在还原副本后，恢复活动副本和被动副本之间的复制。 请注意，CLI 选项 -no_resume_replication 具有相反的含义。如果指定此选项，则不会恢复复制。
目标节点 -node | –all	仅在 DAG 环境中可用。指定要还原的客户机 (即数据库副本)。

还原到某时间点

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。

备份版本/ -session	这是特定于标准还原的选项。 此选项指定要从中还原备份数据的会话。选择备份 ID。 如果选择差异备份会话，则会还原在所选差异备份会话中备份的 .log 文件。 如果选择增量备份会话，则会还原在所有后续增量备份会话 (一直到所选增量备份会话) 中备份的 .log 文件。
最后一个备份版本	这是特定于标准还原的选项。 此选项显示上次进行数据库备份的会话。
还原其他日志，直至 -session	这是特定于即时恢复的选项。 如果选择差异备份会话，则会还原在所选差异备份会话中备份的 .log 文件。 如果选择增量备份会话，则会还原在所有后续增量备份会话 (一直到所选增量备份会话) 中备份的 .log 文件。
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
装载数据库/ -no_mount	
恢复数据库复制/ -no_resume_replication	
目标节点/ -node | –all	请参阅还原到最新状态中的说明。将自动选择托管活动副本的节点 (客户机) 进行还原。

还原到新邮箱数据库

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。
还原其他日志，直至 -session	这是特定于即时恢复的选项。 请参阅还原到时间点中的说明。
目标客户机/ -client	指定要还原到的客户机。
还原到位置/ -location	指定要还原到的目录 (标准还原) 或将复本存储卷装载到的目录 (即时恢复)。
数据库名称/ -name	指定要用于新数据库的名称。如果已存在另一个具有相同名称的数据库，则还原将失败。

还原到恢复数据库/ -recoverydb	将数据还原到 Microsoft Exchange Server 恢复数据库。 虽然可以并行存在多个恢复数据库，但一次只能将一个恢复数据库装载到 Microsoft Exchange Server。
备份版本/ -session	请参阅还原到时间点中的说明。
最后一个备份版本	
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
装载数据库/ -no_mount	
目标节点	不可用。

还原文件到临时位置

GUI/CLI 中的选项	描述
为还原选择	请参阅还原到最新状态中的说明。
还原其他日志，直至 -session	这是特定于即时恢复的选项。 请参阅还原到时间点中的说明。
还原链	如果此选项设置为“仅还原此备份”，则仅还原在所选会话中备份的文件。 如果选择“完整还原 (完整、增量、差异备份)”选项，则会还原整个链。
目标客户机/ -client	请参阅还原到新邮箱数据库中的说明。
还原到位置/ -location	
备份版本/ -session	请参阅还原到时间点中的说明。
最后一个备份版本	
仅还原数据库文件/ -edb_only	仅还原数据库文件 (.edb)。不会还原日志 (.log) 和检查点文件 (.chk)。
执行数据库恢复/ -no_recover	请参阅还原到最新状态中的说明。
目标节点	不可用。

常规还原选项

GUI/CLI 中的选项	描述

启动客户机/ -barhost	指定应启动集成代理（e2010_bar.exe）的客户机。如果选择 DAG 虚拟客户机（主机），则会在当前活动的节点上启动集成代理。要找出当前处于活动状态的节点，请参阅还原 Microsoft Exchange Server 2010+。 默认值：已指定用于备份会话的同一个客户机。如果已指定 DAG 虚拟客户机，则此时会选择此客户机。但是请注意，启动集成代理的物理节点可能与备份会话期间使用的物理节点不同；这取决于哪些节点当前处于活动状态。
用户名 **组/域名/** -user	指定要用于还原会话的 Windows 域用户帐户。确保按配置用户帐户中所述配置用户。 如果未指定这些选项，则会在运行 Data Protector Inet 服务的用户帐户下启动还原会话。
执行一致性检查/ [-exch_check [-exch_throttle Value] | -exch_checklogs]	如果选择此选项，Microsoft Exchange Server 会检查数据库备份数据的一致性。如果未选择此选项，会话会较早结束，但备份数据的一致性无法保证。 还原备份数据后，在源存储卷的目标位置进行检查。如果在备份时已执行一致性检查，则无须再次执行该检查。 默认：未选择 如果选择“仅检查日志文件”选项，则仅检查日志文件备份数据，这足以使 Microsoft Exchange Server 保证数据一致性。 默认：未选择 默认情况下，一致性检查占用 I/O 较多，这可能会对磁盘性能产生负面影响。“限制检查 1 秒钟”选项会限制数据库文件 .edb 的一致性检查，以减少对磁盘性能的影响。指定在进行多少次输入/输出操作之后，应将检查停止一秒时间。 如果仅选中日志文件，则此选项不可用。 默认：未选择

提示要找出当前处于活动状态的 Microsoft Exchange Server 节点，请连接其中一个节点并执行:

cluster group

示例

C:\Users\administrator.E2010BETA>cluster group 列出所有可用资源组的状态: 组 节点 状态 ------------------- --------------- ------ 可用存储 spade 脱机 群集组 club 联机

当前活动节点的状态为联机。在本例中，此节点为 club 。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

Microsoft SharePoint Server 集成

This feature is available in the Premium Edition

本主题介绍了如何配置和使用 Data Protector Microsoft Office SharePoint Server 与 Microsoft SharePoint Server 的集成 (以下称为“Microsoft SharePoint Server 集成”)。其中说明了备份和还原以下 Microsoft SharePoint Server 对象 (“对象”) 所需了解的概念和方法:

- 配置数据库
- 集中管理的内容数据库
- Web 应用程序

有关受支持的 Microsoft SharePoint Server 版本的信息，请参阅支持矩阵。

注意Microsoft SharePoint Server 集成不支持备份和还原 Microsoft SharePoint Server 搜索组件、SharePoint Service 应用程序 (**SSA**) 和 SharePoint Foundation 帮助搜索。

注意Microsoft SharePoint Server 集成不支持备份和还原 Microsoft SharePoint Server 单点登录数据库。

支持任意大小的场 (从单一系统到多个系统)。

备份

Data Protector 与 Microsoft SharePoint Server 集成以联机备份对象。在备份期间，可以正常使用 Microsoft SharePoint Server 和 Microsoft SQL Server 实例 (“联机备份”)。

可以运行以下类型的交互式和计划备份:

- 完整
- 差异
- 增量

还原

在还原期间，可以将每个对象还原：

- 到最新状态或特定时间点
- 到原始位置或新位置

尤其是：

- 可以将 Web 应用程序还原:
  - 为其他名称
  - 到其他 URL
- 可以将内容数据库 (Web 应用程序数据库、SSP 数据库、SSO 数据库) 还原:
  - 到其他 Microsoft SQL Server 客户机
  - 到其他 Microsoft SQL Server 实例
  - 为其他名称
  - 到其他目录
- 可以将 SSP 站点还原：
  - 为其他名称
  - 至不同的 Web 应用程序 URL
  - 至不同的“我的站点 Web 应用程序 URL”
- 可以将 SSP 索引文件还原：
  - 到其他 Microsoft SharePoint Server 客户机
  - 到其他目录

本主题包含 Microsoft SharePoint Server 集成的特定信息。

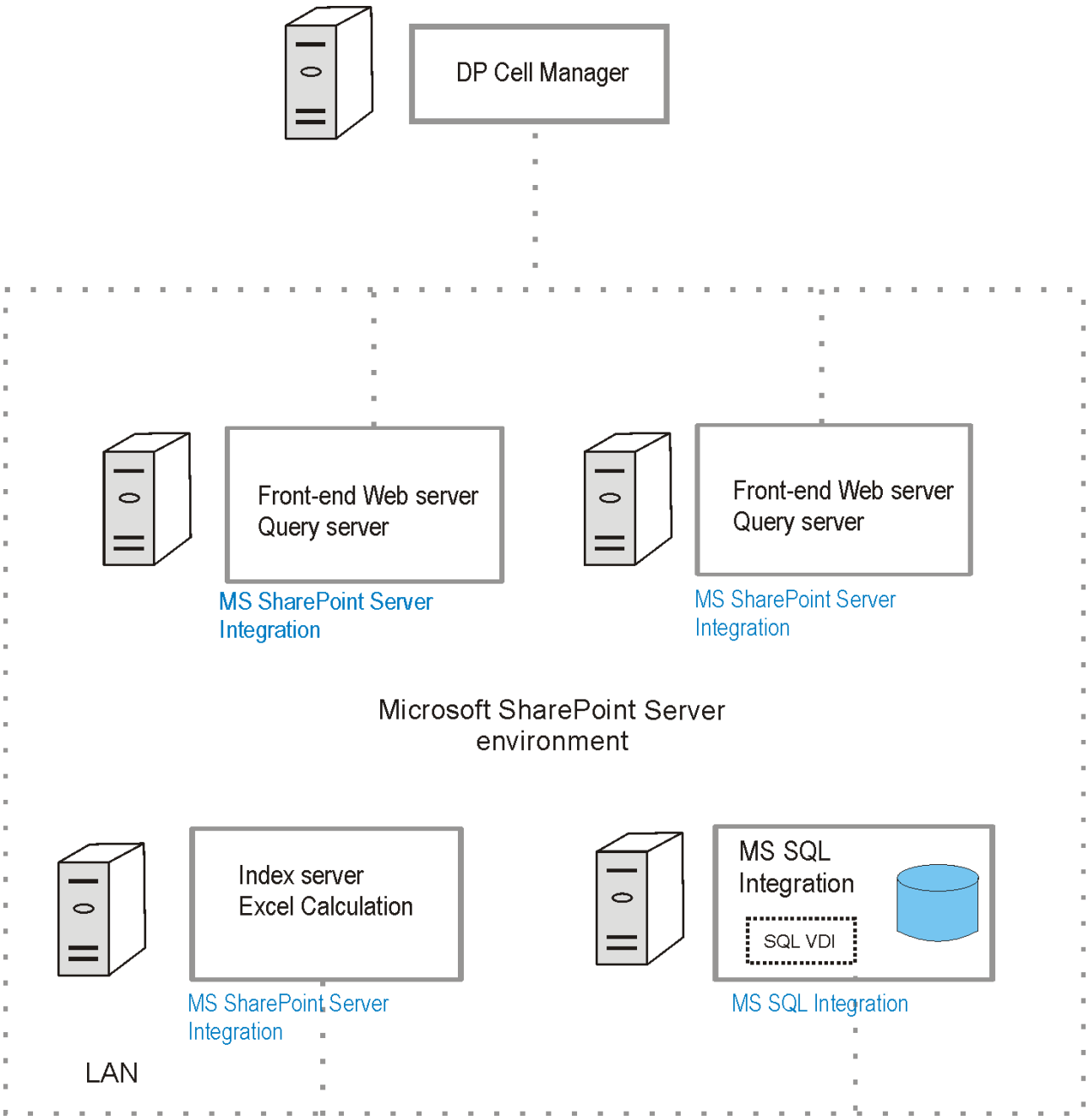
集成概念

Data Protector 通过 Data Protector Microsoft SharePoint Server 集成代理（sharepoint_bar.exe）与 Microsoft SharePoint Server 集成，该代理可在 Microsoft SharePoint Server 环境中引导 Data Protector 会话管理器与客户机之间的通信。Data Protector Microsoft SharePoint Server 集成代理使用 Data Protector Microsoft SQL Server 集成代理来备份 SQL 数据库并使用数据移动代理 (DMA) 来备份索引文件。

无论 Microsoft SharePoint Server 环境是由单个系统还是多个系统 (小型、中型或大型场) 组成，集成的体系结构基本相同。

下图介绍 Data Protector 如何与中型场集成。

Microsoft SharePoint Server 集成



图例

MS SharePoint Server 集成	Data Protector 可执行文件集，用于支持 Microsoft SharePoint Server 和 Data Protector 介质之间的数据传输
MS SQL 集成	Data Protector 可执行文件集，用于支持 Microsoft SQL Server 和 Data Protector 介质之间的数据传输
SQL VDI	Microsoft SQL Server 虚拟设备接口，Microsoft SQL Server 和 Data Protector 通过它交换控制和数据
LAN	本地局域网

下表简要介绍了可使用 Data Protector Microsoft SharePoint Server 集成进行备份和还原的 Microsoft SharePoint Server 对象。

Microsoft SharePoint Server 对象

Microsoft SharePoint Server 对象	描述
配置数据库和管理中心内容数据库	配置数据库是 Microsoft SQL Server 数据库，其中包含整个场的配置。数据库本身位于场中的一个 Microsoft SQL Server 系统上。 管理中心内容数据库是 Microsoft SQL Server 数据库，其中包含管理中心 Web 应用程序的内容。该数据库位于场中的一个 Microsoft SQL Server 系统上。
内容数据库 (Web 应用程序数据库、SSP 数据库)	存储 Web 应用程序内容的 Microsoft SQL Server 数据库。所有 Web 应用程序都可以具有一个或多个内容数据库。内容数据库包含与站点集合以及站点/Web 关联的内容和元数据。
Web 应用程序	各个站点的入口点，用于托管用户内容。场可以包含多个 Web 应用程序。

为灾难恢复做准备

为了能够执行灾难恢复，请备份以下 Microsoft SharePoint Server 对象:

必须备份哪些内容

对象	如何备份
Microsoft SharePoint Server 内容数据库	如本节所述，使用 Data Protector Microsoft SharePoint Server 集成备份备份数据库。
Microsoft SQL Server 配置	使用 Data Protector Microsoft SQL Server 集成备份备份主数据库。
自定义 (来自所有前端 Web 服务器客户机)	使用 Data Protector 文件系统备份备份自定义项。 通常，自定义文件位于以下目录中: • 14 (Microsoft SharePoint Server 2010): Program Files\Common Files\Microsoft Shared\Web server extensions\14 • 15 (Microsoft SharePoint Server 2013): Program Files\Common Files\Microsoft Shared\Web server extensions\15 • 16 (Microsoft SharePoint Server 2016 和 2019) Program Files\Common Files\Microsoft Shared\Web server extensions\16 • Internet Information Services (IIS) 虚拟目录: \Inetpub\wwwroot\wss\VirtualDirectories 要确定自定义文件在文件系统中的确切位置，请与自定义供应商联系。 或者，如果将自定义项打包为解决方案，则可以将这些解决方案包用于手动重新部署。
IIS 数据库 (来自所有前端 Web 服务器客户机)	使用 Data Protector 文件系统备份备份数据库。IIS 数据库位于客户机 CONFIGURATION 中。

灾难恢复

灾难恢复是一个极其复杂的过程，涉及到来自不同供应商的不同产品。要了解如何为其做准备，请查看操作系统和 Microsoft SharePoint Server 的说明。

以下步骤简要介绍了灾难恢复过程:

1. 重新安装操作系统、Microsoft SharePoint Server 环境和 Microsoft SQL Server。确保配置与原始配置相匹配。
2. 在新配置的环境中安装 Data Protector。
3. 还原 Microsoft SQL Server 配置，并还原主数据库。
4. 如本节所述，从 Data Protector Microsoft SharePoint Server 集成备份还原 Microsoft SharePoint Server 数据库 (至少包括配置数据库和管理中心网页内容数据库)。

5. 从 Data Protector 文件系统备份还原 IIS (Windows CONFIGURATION – IIS 数据库)。
6. 从 Data Protector 文件系统备份还原自定义项 (或重新部署手动解决方案)。

满足 Microsoft SharePoint Server 集成的先决条件

以下是 Microsoft SharePoint Server 集成的先决条件:

- 确保已正确安装和配置 Microsoft SharePoint Server 环境。
- 确保已正确安装 Data Protector。

  必须安装以下 Data Protector 组件:

  - MS SharePoint Server Integration – 在 Microsoft SharePoint Server 系统上（Microsoft SQL Server 系统除外）
  - MS SQL Integration – 在 Microsoft SQL Server 系统上

  > **注意**如果系统已安装 Microsoft SQL Server 和 Microsoft SharePoint Server，则在其上安装所有 Data Protector 组件。

  - 配置要与 Data Protector 配合使用的设备和介质。
  - 要测试 Microsoft SharePoint Server 和 Cell Manager 是否正常通信，请在场中的每个客户机上配置并运行 Data Protector 文件系统备份和还原。
- 确保 Microsoft SharePoint Server 和 Microsoft SQL Server 实例处于联机状态。
- 确保 Microsoft SharePoint Server 和 Microsoft SQL Server 实例处于联机状态，并且 Microsoft SharePoint Server 服务在 Microsoft SharePoint Server 场管理员帐户下运行。
- 如果打算将 Microsoft SQL Server 数据库还原到其他位置:
  - 确保目标 Microsoft SQL Server 系统是 Microsoft SharePoint Server 环境的一部分，并且已安装 MS SQL Integration 组件。
  - 确保目标 Microsoft SQL Server 实例存在且处于联机状态。
- 如果将加密密钥用于单点登录服务，请注意，没有原始加密密钥就无法还原单点登录数据库。
- 对于 Microsoft SharePoint Server 2016，必须安装补丁 KB3127942 和 KB3127940 才能应用 MinRole 拓扑。对于 Microsoft SharePoint Server 2019，MinRoles 包含在安装程序中。

配置集成

按如下所示配置集成:

配置用户帐户

通过 Data Protector Inet 服务启动备份和还原会话，默认情况下，这些会话使用 Windows 本地用户帐户 SYSTEM 运行。

但是，必须指定 Data Protector Inet 服务在 Microsoft SharePoint Server 场管理员 Windows 域用户帐户下启动会话。需要成为 SharePoint 服务器的 Administrator 组成员，并且是 SQL Server 中具有 SYSADM 角色的成员。

> **注意**在 Microsoft SharePoint Server 2010 环境中还原配置数据库时，Data Protector Microsoft SharePoint Server 集成代理会自动使用在 Windows 注册表中保存的预定义凭据 (用户 *PASSPHRASE* 和组 *MSSPS*)。

如下所示配置用户帐户：

1. 确保已为 Microsoft SharePoint Server 场管理员分配 Windows 本地安全策略用户权限“替换进程级别令牌”。
2. 将 Microsoft SharePoint Server 场管理员添加至 Data Protector admin 或 operator 用户组。
3. 将 Microsoft SharePoint Server 场管理员及其密码保存至所有 Microsoft SharePoint Server 系统和所有 Microsoft SQL Server 系统上的 Windows 注册表。

   > **注意**要在 Microsoft SharePoint Server 2010 环境中还原配置数据库，请将预定义凭据 (用户 *PASSPHRASE* 和组 *MSSPS*) 保存到所有 Microsoft SharePoint Server 系统和所有 Microsoft SQL Server 系统上的 Windows 注册表。

   要保存用户帐户，请使用:

- Data Protector GUI。
- Data Protector CLI，通过使用 omniinetpasswd 或 omnicc 命令。

> **注意** Data Protector Inet 服务将在此用户帐户下启动会话。

示例

要在场中客户机组上的 Windows 注册表中保存用户 PASSPHRASE、组 MSSPS 和密码 passphrase ，请登录 Cell Manager 并执行以下操作:

```
omnicc -impersonation -add_user -user *PASSPHRASE*@*MSSPS* -host Client1 -host Client2 -host Client3 -passwd passphrase
```

也可以在客户机上本地执行以下命令，将用户 PASSPHRASE 和组 MSSPS 添加至 Windows 注册表:

```
omniinetpasswd -add *PASSPHRASE*@*MSSPS*
```

相关主题

备份 Microsoft SharePoint Server 集成
还原 Microsoft SharePoint Server 集成
Microsoft SharePoint Server 集成故障诊断
安装 Microsoft SharePoint Server 客户机

安装 Microsoft SharePoint Server 客户机

This feature is available in the Premium Edition

需要在 Microsoft SharePoint Server 环境中安装的 Data Protector 组件会因您要使用的备份和还原解决方案而异。可以从下列解决方案中选择：

- Data Protector Microsoft SharePoint Server 集成
- 基于 Data Protector Microsoft SharePoint Server VSS 的解决方案
- Data Protector Microsoft 卷影复制服务集成
- 用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension

.NET Framework 要求

- 安装 Microsoft SharePoint Server 客户机需要 .NET Framework 2.0 或更高版本。
- 安装适用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension 需要 .NET Framework 3.5.1 或更高版本。

Data Protector Microsoft SharePoint Server 集成

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。为了能够备份 Microsoft SharePoint Server 对象，请安装以下 Data Protector 组件：

- MS SharePoint Integration – 在 Microsoft SharePoint Server 系统上（Microsoft SQL Server 系统除外）
- MS SQL Integration – 在 Microsoft SQL Server 系统上

> 注意如果系统已安装 Microsoft SQL Server 和 Microsoft SharePoint Server，则在其上安装所有 Data Protector 组件。

基于 Data Protector Microsoft SharePoint Server VSS 的解决方案

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。为了能够备份 Microsoft SharePoint Server 对象，请安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration 在 Microsoft SQL Server 系统和至少启动了以下服务之一的 Microsoft SharePoint Server 系统上：

  Microsoft SharePoint Server 2010 :

  - SharePoint Foundation Database
  - SharePoint Foundation Help Search
  - SharePoint Server Search

  Microsoft SharePoint Server 2013 :

  - SharePoint Foundation Database
  - SharePoint Server Search

- 在安装了 Data Protector MS 卷影复制集成组件并且计划要在其上配置和启动备份的 Microsoft SharePoint Server 系统之一上安装 Data Protector 用户界面组件。

Data Protector Microsoft 卷影复制服务集成

请参阅安装 Microsoft 卷影复制服务客户机。

用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。为了能够恢复各个 Microsoft SharePoint Server 对象，请在 Microsoft SharePoint Server Central Administration 系统上安装 MS SharePoint Granular Recovery Extension。

- 本地安装该组件时，Data Protector 安装向导将显示“MS SharePoint GRE 选项”对话框。指定场管理员用户名和密码。
- 要远程安装此组件，请选择 MS SharePoint Granular Recovery Extension，单击“配置”，并在“MS SharePoint GRE 选项”对话框中指定场管理员用户名和密码。
- 您只可以将 Granular Recovery Extension 安装到已安装 Microsoft SharePoint Server 的系统上。
- 确保备份 Microsoft SharePoint Server 数据所需的 Data Protector 组件也安装在 Microsoft SharePoint Server 环境中。
- 在前端 Web 服务器上安装 CC 组件，以便成功运行 Sharepoint GRE。
- 建议在升级 SharePoint 客户机时关闭 SharePoint Server 管理中心 Web 控制台，因为 SharePoint 使用缓存内存呈现 Web 内容，这可

能会干扰其品牌自定义。

备份 Microsoft SharePoint Server 集成

This feature is available in the Premium Edition

可备份以下 Microsoft SharePoint Server 对象:

- 配置数据库
- 集中管理的内容数据库
- Web 应用程序

> **注意**Microsoft SharePoint Server 集成不支持备份 Microsoft SharePoint Server 搜索组件。

> **注意**Microsoft SharePoint Server 集成不支持备份 Microsoft SharePoint Server 单点登录数据库。

备份概念

在备份 Microsoft SharePoint Server 对象之前，应考虑每个组件的以下细节。

- **Web 应用程序**

  Data Protector Microsoft SharePoint Server 集成代理使用 Data Protector Microsoft SQL Server 集成代理来备份 Web 应用程序内容数据库。支持使用 Data Protector Microsoft SQL Server 集成代理的功能执行完整、差异和增量 (事务日志) 备份类型。还会备份 Web 应用程序设置，以简化重定向还原或灾难恢复时重新启动服务的操作。请注意，Data Protector 不会备份为 SharePoint Web 应用程序设置的用户权限。

- **配置数据库和管理中心数据库**

  配置数据库和管理中心内容数据库已同步，必须一起备份。

备份类型

集成提供以下类型的联机备份:

备份类型

完整	*Microsoft SQL Server 数据库：*执行 Microsoft SQL Server 完整数据库备份；将备份整个数据库。 *索引文件：*对所有索引文件执行完整文件系统备份。
增量	*Microsoft SQL Server 数据库：*会执行一次 Microsoft SQL Server 事务日志备份。备份自上次备份 Microsoft SQL Server 数据库的事务日志备份以来所创建的事务日志 (.log)，然后截断事务日志。 *索引文件：*仅备份自任意类型的上次备份以来所更改或创建的索引文件。 注意: 如果 Microsoft SQL Server 数据库处于简单恢复模式 (无任何事务日志)，则将改为对数据库执行差异备份。 对于 Microsoft SharePoint Server 组件的元数据，因为数据量较小，所以始终执行完整备份。
差异	*Microsoft SQL Server 数据库：*对数据库执行 Microsoft SQL Server 差异备份；备份自上次完整备份以来对数据库进行的更改。 *索引文件：*备份自上次完整备份以来已更改的索引文件。

> **注意**如果尚未执行完整备份，则无法执行增量备份或差异备份。

创建备份规范

使用 Data Protector GUI (**Data Protector Manager**) 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS SharePoint Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 MS SharePoint Server 备份”模板，然后单击“确定”。
4. 指定应在其下执行备份会话的 Microsoft SharePoint Server 场管理员的“用户名”和“组/域名”。

   从“客户机”下拉列表中，选择任何 Microsoft SharePoint Server 系统。该列表包含安装了 Data Protector MS SharePoint Server Integration 组件的所有客户机。

   将在此处指定的客户机上启动备份。

   系统会自动选择“应用程序数据库”(通过 Microsoft SharePoint Server 集成)。

   > **注意**应用程序数据库相当于 Microsoft SharePoint Server 配置数据库

   单击“下一步”。
5. 选择要备份的对象。

   > **注意**如果未显示任何组件，请确保在第 4 步中指定的用户名和域名正确。

   单击“下一步”。
6. 选择用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。

   单击“下一步”。
7. 设置备份选项。

   单击“下一步”。
8. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

特定于应用程序的备份选项

选项	描述
Pre-exec、**Post-exec**	指定要在备份之前 (pre-exec) 或之后 (post-exec) 执行的命令行。 命令行在启动了备份会话的 Microsoft SharePoint Server 系统上执行 (在该系统上还启动了 Data Protector Microsoft SharePoint Server 集成代理 (sharepoint_bar.exe))。只键入命令的名称并确保命令位于同一系统上的默认 Data Protector 命令目录中。不要使用双引号。
并发流	指定用于备份 Microsoft SQL Server 数据库的并行备份流数量。 **注意**可在单独的备份流中备份每个 Microsoft SQL Server 数据库。 可以指定的最大值应等于选择用于备份的设备数。如果更改了设备数，请确保同时更改并发性。
脱机备份	在开始备份之前停止 Microsoft SharePoint Server 场。 **注意**如果选中，则可以避免还原限制。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以将备份会话计划为在特定时间自动启动或定期启动。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS SharePoint Server”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用如配置集成所述配置的用户帐户，登录 Cell Manager 或安装了 Data Protector 用户界面组件的任何客户机。
2. 执行：

   ```
   omnib -mssharepoint_list BackupSpecificationName -test_bar
   ```

预览期间会发生什么?

测试以下内容:

- 启动备份会话的 Microsoft SharePoint Server 系统与 Data Protector Cell Manager 之间的通信
- 如果正确指定设备
- 如果必要的介质位于设备中
- 备份规范的语法

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

要启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”和“MS SharePoint Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 使用如配置集成所述配置的用户帐户，登录 Cell Manager 或安装了 Data Protector 用户界面组件的任何客户机。
2. 执行：

   ```
   omnib -mssharepoint_list BackupSpecificationName [-barmode MSSharePointMode][ListOptions ]
   ```

   其中， MSSharePointMode 是以下备份类型之一:

   ```
   full|diff|incr
   ```

   如果未指定 -barmode 选项，则执行完整备份。

   有关 ListOptions 的信息，请参阅 omnib 手册页。

   示例

   要使用备份规范 myBackup 启动完整备份，请执行以下命令:

   ```
   omnib -mssharepoint_list myBackup -barmode full
   ```

   要使用相同的备份规范启动差异备份，请执行以下命令:

   ```
   omnib -mssharepoint_list myBackup -barmode diff
   ```

相关主题

Microsoft SharePoint Server 集成
还原 Microsoft SharePoint Server 集成
Microsoft SharePoint Server 集成故障诊断
安装 Microsoft SharePoint Server 客户机

还原 Microsoft SharePoint Server 集成

This feature is available in the Premium Edition

可以使用 Data Protector GUI 或 CLI 还原 Microsoft SharePoint Server 对象。

> **注意** 不支持 Microsoft SharePoint Server 2013 配置还原。

还原概念

在还原 Microsoft SharePoint Server 对象之前，应考虑每个组件的以下细节。

- **Web 应用程序**

  还原 Web 应用程序时，可以选择整个 Web 应用程序或单个内容数据库。二者均可还原到新位置。如果同时还原，则 Data Protector Microsoft SharePoint Server 集成会在还原到新位置后重新连接 Web 应用程序及其内容数据库。Web 应用程序的还原内容需要重新爬网才能进行搜索。

- **配置数据库和管理中心数据库**

  配置数据库和管理中心内容数据库包含 Microsoft SharePoint Server 场状态的描述，包括客户机名称。因此，仅支持还原到原始位置。要确保数据一致性，必须同时还原这些数据库。

  > **注意**进行灾难恢复时，Data Protector Microsoft SharePoint Server 集成代理会自动断开与所有 Microsoft SharePoint Server 客户机的连接，还原数据库，然后重新连接场客户机以使场恢复为运行状态。还原配置数据库之后，各个 Microsoft SharePoint Server 客户机上的某些 Microsoft SharePoint Windows 服务仍保持禁用状态。需要从本地客户机服务控制台手动重新启动这些服务，或者通过还原相应的组件；系统会向您发送一条警告消息。Microsoft SharePoint 管理、计时器和跟踪服务会自动启动。

还原选项

常规还原选项

GUI/CLI 中的选项	描述
还原客户机/ -destination	指定应启动 Data Protector Microsoft SharePoint Server 集成代理的客户机。它还指定组件还原到的场。下拉列表中包含安装有 Data Protector Microsoft SharePoint Server 集成代理的所有客户机。
应用程序数据库	显示所选客户机所属的场的 Microsoft SharePoint Server 配置数据库名称。
用户名/ 用户组 / -user	指定应用于运行 Data Protector Microsoft SharePoint Server 集成代理的 Windows 域用户。该用户必须是场管理员。
覆盖现有 / -replace	覆盖为选定组件指定的所有现有重定向选项。执行还原到原始位置。

Web 应用程序选项

GUI/CLI 中的选项	描述
Web 应用程序/ -webapplication	显示原始 Web 应用程序名称。
Web 应用程序名称/ -as	指定应当用于还原 Web 应用程序的名称。
URL/-url	选择应将 Web 应用程序还原到的 URL。
通过现有 **Web** 应用程序进行强制还原/ -replace	覆盖驻留在目标 URL 上的现有 Web 应用程序。
用户名/ -poolusername 密码 / -poolpassword	指定应在其下运行应用程序池的 Windows 域应用程序池用户帐户。请注意，每个 Web 应用程序都有其自己的应用程序池。

Web 应用程序、SSP、SSO 内容数据库选项

GUI/CLI 中的选项	描述
数据库/ -db	允许您为不同的数据库指定不同的选项。下拉列表包含在所选间隔中备份的 Web 应用程序数据库。
客户机/ -tohost	指定应将数据库还原到的 Microsoft SQL Server 客户机。下拉列表包含安装了 MS SQL 集成组件的客户机。

GUI/CLI 中的选项	描述
实例 / -newinstance	指定应将数据库还原到的 Microsoft SQL Server 实例。会列出目标客户机上的所有已创建实例。
数据库名称 / -as	指定应当用于还原数据库的名称。
路径 / -todir	指定应将数据库文件还原到的目录的路径。
通过现有数据库进行强制还原 /-replace	覆盖位于目标 Microsoft SQL Server 实例上的现有数据库。如果已存在一个与要还原的数据库同名、但内部结构不同的数据库，则 Microsoft SQL Server 不允许在未选择此选项的情况下覆盖该数据库。
取消链接原始内容数据库 / -unlink	从场中删除原始内容数据库。仅当至少更改了一个还原重定向选项原始值时可用。
Windows 或 **SQL** 身份验证 / -sqllogin	指定用于连接数据库的身份验证类型。
登录名和密码 / -sqlpassword	仅在选择了 SQL 身份验证类型时可用。指定 Windows 域用户帐户或 Microsoft SQL Server 用户帐户。

SSP 站点选项

GUI/CLI 中的选项	描述
SSP 名称 / -as	指定应当用于还原共享服务提供程序的名称。
Web 应用程序 **URL** / -url	指定应托管 SSP 管理网页的 Web 应用程序的 URL。
我的站点 **Web** 应用程序 **URL** / -mysiteurl	指定应托管个人站点和配置文件的 Web 应用程序的 URL。
登录 / -ssplogin	指定应当用于运行 SSP 计时器作业和 Web 服务的 Windows 域用户帐户。
密码 / -ssppassword	指定登录凭据的密码。

SSP - 索引文件选项

GUI/CLI 中的选项	描述
客户机 / -tohost	指定应将所选 SSP 索引文件还原到的 Microsoft SharePoint Server 客户机。下拉列表包含安装有 Data Protector MS SharePoint Server 集成 的所有客户机。
位置 / -todir	指定应将 SSP 索引文件还原到的目录的路径。

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，依次展开“还原对象”、“MS SharePoint Server”，选择备份期间用作 Microsoft SharePoint Server 场的入口点的 Microsoft SharePoint Server 客户机，然后单击“MS SharePoint Server [Microsoft SharePoint Server]”。
3. 在“源”页中，选择要还原的 Microsoft SharePoint Server 对象。可以在指定时间间隔中按“组件”或“服务器”查看对象。

   “从”字段一定要是源的 FULL 会话，而“至”字段可以是源的 FULL/DIFF/INCR 会话。
4. 可单独为每个 Microsoft SharePoint Server 对象指定还原目标: 右键单击对象，然后单击“属性”。将显示“属性”对话框。

> **注意**
>
> - 仅当在“源”页的“查看依据”下拉列表中选择“组件”时，该菜单才可用。每个组件的“属性”对话框预填充了原始数据 (名称、位置、URL)。
> - 仅当未选择“覆盖现有”时才适用。
>
>   如果选择了“覆盖现有”选项，则组件会还原到原始位置并使用备份时采用的设置。

可以将 Web 应用程序的设置还原在其他名称下或恢复到其他 URL。

可以将内容数据库还原到不同的 Microsoft SQL Server 客户机中、不同的 Microsoft SQL Server 实例中、不同的名称下或是不同的目录中。

可以将不同名称下的 SSP 站点还原到其他 Web 应用程序 URL 或是还原到其他“我的站点 Web 应用程序 URL”。

可以将 SSP 索引文件还原到其他客户机或目录。

5. 在“选项”页中，选择 Microsoft SharePoint Server 的特定还原选项。

   必须指定“场管理员用户名”和“场管理员用户组”选项才能在 Microsoft SharePoint Server 场管理员的 Windows 域用户帐户下执行还原会话。

   > **注意**在 Microsoft SharePoint Server 2010 环境中还原配置数据库时，Data Protector Microsoft SharePoint Server 集成代理会自动使用在 Windows 注册表中保存的预定义凭据 (用户 *PASSPHRASE* 和组 *MSSPS*)。

6. 在“设备”页中，选择要用于还原的设备。
7. 单击**还原**。
8. 在“启动还原会话”对话框中，单击“下一步”。
9. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。

10. 单击**完成**启动还原。

    会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

1. 在已添加到 Data Protector admin 或 operator 用户组的用户帐户下登录 Cell Manager 或安装了 Data Protector User Interface 组件的任何客户机。
2. 执行：

```
omnir -mssharepoint -barhost HostName [-destination RestoreClientName] -user User:Group [-session BackupID] [-replace] [-byserver ServerName [-byserver ServerName...]] -farmname FarmName [Component [Component...]] [GENERAL_OPTIONS] Component -configdb | -webapplication WebApplicationName [WEB_APPLICATION_OPTIONS] [ContentDatabase [ContentDatabase...]]| -ssp SSPName [SSP_OPTIONS] [-index [INDEX_OPTIONS]] [Database [Database...]] [-webapp WebApplicationName [WEB_APPLICATION_OPTIONS] [ContentDatabase [ContentDatabase...]]]| -wsssearch [Database] | -ssodb [DB_OPTIONS] ContentDatabase -db DBName -host DBHostName [-unlink] [DB_OPTIONS] Database -db DBName -host DBHostName [DB_OPTIONS] WEB_APPLICATION_OPTIONS -as WebApplicationName -url WebApplicationURL -poolusername Username [-poolpassword Password] -replace DB_OPTIONS -sqllogin Username [-sqlpassword Password] -instance SourceInstanceName -as NewDBName -tohost DBHostName -newinstance DestinationInstanceName -todir NewDirectoryName -replace
```

```
SSP_OPTIONS -ssplogin Username [-ssppassword Password] -as SSPName -mysiteurl MySiteWebAppURL INDEX_OPTIONS -tohost IndexServerHostName -todir NewDirectoryName
```

> **注意**备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。
>
> 镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是对象*复制*会话的会话 ID。
>
> 如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

示例

要将 Web 应用程序内容数据库从最新会话还原到其他位置，请在更改其名称、Microsoft SQL Server 系统、实例和数据文件路径后，执行以下命令：

```
omnir –mssharepoint –barhost wfe1.domain.com –webapplication "SharePoint - 2224" –db "WSS_Content_2224" –as "WSS_new_DB" –tohost mosssql2.domain.com –newinstance moss1 –todir "f:\program files\SQL\data"
```

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

相关主题

Microsoft SharePoint Server 集成
备份 Microsoft SharePoint Server 集成
Microsoft SharePoint Server 集成故障诊断
安装 Microsoft SharePoint Server 客户机

基于 Microsoft SharePoint Server VSS 的解决方案

This feature is available in the Premium Edition

本主题说明如何配置和使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案 (“基于 VSS 的解决方案”)。实际上，该解决方案基于 Data Protector Microsoft 卷影复制服务集成 (“VSS 集成”)。

本主题介绍备份和还原在 Microsoft SQL Server 数据库中存储的 Microsoft SharePoint Server 2010 和 Microsoft SharePoint Server 2013 数据时需要了解的概念和方法。例如：

- 配置数据库 (SharePoint_Config)
- 内容数据库 (SharePoint_AdminContent_Label 、 WSS_Content_Label ...)
- SharePoint Service 应用程序数据库 (SSA_DB) (Microsoft SharePoint Server 2010/2013)

此外，还可以备份和还原 Microsoft SharePoint Server 搜索索引文件。

从现在开始，Microsoft SharePoint Server 的两个版本均称作“Microsoft SharePoint Server”，除非指出了差异。

备份

使用以下 Microsoft SQL Server VSS 写入程序之一备份在 Microsoft SQL Server 数据库中存储的 Microsoft SharePoint Server 数据:

- MSDE writer（适用于 Microsoft SQL Server 2000 数据库)
- SqlServerWriter（适用于 Microsoft SQL Server 2008 数据库)

使用以下 VSS 写入程序备份 Microsoft SharePoint Server 2010 搜索索引文件:

- OSearch14 VSS writer
- SPSearch4 VSS writer

使用以下 VSS 写入程序备份 Microsoft SharePoint Server 2013 搜索索引文件:

- OSearch15 VSS writer

Microsoft FAST Search Server 2010 搜索索引文件通过以下方法进行备份:

- 使用 Data Protector 磁盘代理 (当在已启用 VSS 的情况下进行标准文件系统备份时)
- 使用 Data Protector VSS 集成 (当进行 ZDB 文件系统备份时)

可使用 Data Protector PowerShell 命令创建和运行备份规范，如备份基于 Microsoft SharePoint Server VSS 的解决方案所述。

满足基于 Microsoft SharePoint Server Server VSS 的解决方案的先决条件

基于 Microsoft SharePoint Server Server VSS 的解决方案集成的先决条件如下:

- 如果打算运行 ZDB 和即时恢复 (IR) 会话，请确保所有 SSP 或 SSA 的 SPSearch 和 OSearch 索引文件以及 FAST Search 索引文件均位于磁盘阵列中。

Microsoft Office SharePoint Server

SPSearch 索引文件的默认位置如下:

```
C:\Program Files\Microsoft Office Servers\12.0\Data\Applications
```

OSearch 索引文件的默认位置如下:

C:\Program Files\Microsoft Office Servers\12.0\Data\Office Server\Applications

要将索引文件移至磁盘阵列，请执行以下操作:

1. 打开命令提示符，然后将目录更改为:

   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN>
2. 要移动 SPSearch 索引文件，请执行以下命令:

   stsadm -o spsearch -indexlocation PathToNewLocation
3. 要移动 OSearch 索引文件，请执行以下命令:

   stsadm -o editssp –title SSPname -indexlocation PathToNewLocation

Microsoft SharePoint Server 2010

SPSearch 索引文件的默认位置如下:

C:\Program Files\Microsoft Office Servers\14.0\Data\Applications

OSearch 索引文件的默认位置如下:

C:\Program Files\Microsoft Office Servers\14.0\Data\Office Server\Applications

要将索引文件移至磁盘阵列，请执行以下操作:

1. 打开命令提示符，然后将目录更改为:

   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN>
2. 要移动 SPSearch 索引文件，请执行以下命令:

   stsadm -o spsearch -indexlocation PathToNewLocation
3. 要移动 OSearch 索引文件，请使用管理中心 (修改场拓扑)。

在安装 FAST Search Server 2010 系统期间，必须将 FASTSearch 主文件夹安装到磁盘阵列中。如果有多个 FAST Search Server 系统场，请确保所有系统上的 FASTSearch 主文件夹路径相同 (驱动器和路径名)。

- 必须在所有系统上配置 Windows 远程管理服务 (用于远程启动和停止 Windows 服务，以及暂停和恢复 FAST for Microsoft SharePoint Server 2010)。

  要配置和分析 WinRM 服务，请执行 winrm quickconfig 命令。
- 如果 Microsoft SharePoint Server 2010/2013 使用 Microsoft SQL Server 2008/2012 存储数据，并且远程 Blob 存储与 FILESTREAM 提供程序一起使用，请确保将 FILESTREAM 访问级别设置为“启用完全访问”或“启用 Transact-SQL 访问”。

- 使用 Data Protector GUI 修改备份规范 (例如，添加备份设备)。
- 将简单模式用于 SQL Server 数据库。如果仍想使用完整模式，请确保截断事务日志。否则，磁盘空间可能不足。
- 每当更改场配置时，请执行新备份。
- 如果要备份单点登录数据库，切记备份加密密钥，如下所述:
  http://technet.microsoft.com/en-us/library/cc262932.aspx#Section32。

  否则，将无法还原数据库。

- 使用命令选项可将流程拆分为两部分: 首先创建备份规范，然后启动备份会话。可通过这种方式在实际启动备份之前，在 Data Protector GUI 中手动修改新建的备份规范。
- 如果 Microsoft SQL Server 实例同时供 Microsoft SharePoint Server 和其他数据库应用程序使用，请修改备份规范，以仅选择属于 Microsoft SharePoint Server 的数据库进行备份。
- 如果已启用了 Microsoft SQL Server 数据库镜像，则可能会发生故障转移，从而使其他 Microsoft SQL Server 系统变为活动状态。由于该命令仅为当前活动的 Microsoft SQL Server 系统创建备份规范，因此建议在启动备份之前，更新 (重新创建) 备份规范。

- 停止并禁用以下服务:
  - SharePoint Server Search 14（Microsoft SharePoint Server 2010）
  - SharePoint Server Search 15（Microsoft SharePoint Server 2013）

  此外，停止以下服务:

  Microsoft SharePoint Server 2010 :
  - SharePoint 2010 Administration
  - SharePoint Foundation Search V4
  - SharePoint 2010 Timer
  - SharePoint 2010 Tracing
  - FAST Search for SharePoint
  - FAST Search for SharePoint Monitoring

  Microsoft SharePoint Server 2013 :
  - SharePoint Administration
  - SharePoint Search Host Controller
  - SharePoint Timer Service
  - SharePoint Tracing Service

- 如果打算还原以下 Microsoft SQL Server 数据库之一，请将 Microsoft SQL Server 实例置于脱机状态:
  - master
  - model
  - msdb
  - 启用了 Microsoft SQL Server 镜像的数据库

注意

- 如果使用 SqlServerWriter ，则可以在 Microsoft SQL Server 实例处于联机状态时，还原 model 和 msdb 数据库。这一点优于 MSDE writer.
- *Microsoft SQL Server 镜像*: 如果原始数据库和镜像数据库位于单独的 Microsoft SQL Server 实例中，请将这两个 Microsoft SQL Server 实例置于脱机状态。

- 仅适用于 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的 Data Protector 文件系统还原。在还原 FAST Search 索引文件之前，必须保持“覆盖”选项处于选定状态才能确保数据一致。默认选中此选项。

配置集成

配置用户帐户

创建或标识要在其上执行 Data Protector 命令的 Microsoft SharePoint Server 系统具有 Windows 管理权限的 Windows 域用户帐户。还必须向此用户授予 Microsoft SharePoint Server 管理权限，并且必须将其添加至 Data Protector admin 用户组。

备份基于 Microsoft SharePoint Server VSS 的解决方案集成

This feature is available in the Premium Edition

要备份 Microsoft SharePoint Server 数据，请使用 Data Protector PowerShell 命令 SharePoint_VSS_backup.ps1 创建备份规范并启动备份会话。

执行 Data Protector PowerShell 命令 SharePoint_VSS_backup.ps1 时，Data Protector 首先会查询有关 Microsoft SharePoint Server 环境的信息。然后创建备份规范。

新建的备份规范名为 SharePoint_VSS_backup_ClientName ，并且指定了相同的备份设备 (在命令运行时指定的备份设备) 以供使用。

备份规范创建后，该命令即会启动备份会话 (每个备份规范对应一个会话)。

Microsoft SharePoint Server 2010

在 Microsoft SharePoint Server 2010 环境中，该命令将为至少启用了以下服务之一的每个 Microsoft SharePoint Server 系统创建单独的备份规范:

- SharePoint Foundation Database
- SharePoint Foundation Help Search
- SharePoint Server Search 14
- FAST Search Server 2010 for SharePoint (FAST Search)

对于启用了 SharePoint Foundation 数据库服务的系统，该命令将创建选择了 SqlServerWriter（Microsoft SQL Server 2008) 对象的备份规范。

对于启用了 SharePoint Foundation 帮助搜索和 SharePoint Server 搜索服务的系统，该命令将创建选择了 SPSearch4 VSS Writer 和 OSearch14 VSS Writer 对象的备份规范。

对于启用了 FAST Search Server 2010 服务的系统，该命令会创建选择了 FASTSearch 主文件夹 (不包括包含 FAST 可执行文件的 bin 和 lib 文件夹) 的文件系统备份规范。

对于启用了 FAST Search Server 2010 服务的系统，指定了 -hardware 选项的该命令会创建选择了整个 FASTSearch 主文件夹 (包括 bin 和 lib) 的 VSS 备份规范。

Microsoft SharePoint Server 2013

在 Microsoft SharePoint Server 2013 环境中，该命令将为至少启用了以下服务之一的每个 Microsoft SharePoint Server 系统创建单独的备份规范:

- SharePoint Foundation Database
- SharePoint Server Search 15

对于启用了 SharePoint Foundation Database 服务的系统，该命令将创建选择了 SqlServerWriter（Microsoft SQL Server 2008/2012) 对象的备份规范。

对于启用了 SharePoint Server 搜索服务的系统，该命令将创建选择了 OSearch15 VSS Writer 对象的备份规范。

命令语法

- 必须从前端 Web 服务器系统上的 Data_Protector_home\bin 目录执行命令。请确保使用如配置用户帐户所述配置的用户帐户进行登录，并使用管理权限打开命令提示符。
- 请勿在备份会话正在进行时关闭 PowerShell 控制台。如果在备份期间关闭控制台，则不会执行某些操作: 会完成已启动的备份会话，但场不会恢复原始状态。要恢复场，请首先使用 –resumefarm 选项执行该命令，然后使用 Microsoft SharePoint Server 管理中心或 stsadm 手动取消静默场。

SharePoint_VSS_backup.ps1 –help |-version SharePoint_VSS_backup.ps1 –createonly CreateOptions SharePoint_VSS_backup.ps1 –backuponly BackupOptions SharePoint_VSS_backup.ps1 –resumefarm [-preview] | -resumecert CreateOptions

{-device DevName | -hardware {no_keep|keep|ir} [-device DevName]} [-overwrite] [-prefix PrefixName] [-excludeindex] BackupOptions [-outfile PathToFile] [-prefix PrefixName] [-preview] [-snapshot {diskonly | disktape | tapeonly}] [-reduce] [-mode {full | incremental | incremental1 ...| incremental9}] [-timeout Timeout]

选项描述

-help	显示 SharePoint_VSS_backup.ps1 命令用法。
-version	显示 SharePoint_VSS_backup.ps1 版本。
–createonly	如果指定了此选项，则 Data Protector 仅创建备份规范。备份未启动。
–backuponly	如果指定了此选项，则 Data Protector 仅使用现有备份规范启动备份会话。不需要 -device 选项。
-device *DevNam*	指定要用于备份的 Data Protector 设备。只能指定一个设备。 **重要说明**如果仅使用一个设备来备份多系统场，则无法并行运行相应的备份会话。这会延长场处于只读模式的时间。具体来说，从备份会话启动时到所有 VSS 快照创建完，场都一直处于只读模式。 为了能够并行运行备份会话，请在启动备份之前，在每个备份规范中选择不同或额外的设备。
keep | ir }	指定应使用硬件提供程序 (而非指定了 -device 选项的软件提供程序) 并设置 ZDB 选项。ZDB 选项的默认值如下: • 保留复本以供即时恢复: 指定了 ir 时选中。 • 备份后保留复本: 指定了 ir 或 keep 时选中。 • 配置检查模式(G): 严格 • 复本类型: 镜像/克隆 (丛) • 循环的复本数: 3 默认 ZDB 备份类型如下 (前提是还指定了设备): • no_keep : ZDB 到磁带 • keep : ZDB 到磁盘 + 磁带 • ir : ZDB 到磁盘 + 磁带
–overwrite	默认情况下，Data Protector 不会创建备份规范 (如果已存在)。如果指定了此选项，则 Data Protector 将使用新创建的备份规范覆盖现有备份规范。指定了 –backuponly 时不适用。
-prefix *PrefixName*	指定此选项后，将使用其他名称创建备份规范: SharePoint_VSS_backup_PrefixName_ClientName 。 备份时，此选项用于指定要使用的备份规范: 名称包含 *PrefixName* 的备份规范。 *PrefixName* 中不支持非 ASCII 字符。
-outfile *PathToFile*	如果指定了此选项，则会将备份规范名称、错误、会话输出和 omnir 还原命令写入指定文件。
-preview	如果指定了此选项，则 Data Protector 将显示有关 Microsoft SharePoint Server 环境的信息并介绍相关操作，但不实际执行它们。
disktape | tapeonly }	启动 ZDB 备份会话时适用 (即，使用其中指定了要使用的硬件提供程序的备份规范的会话)。执行“ZDB 到磁盘”(diskonly)、“ZDB 到磁带”(tapeonly) 或“ZDB 到磁盘 + 磁带”(disktape) 会话。
-reduce	*Microsoft SharePoint Server 2010 :* 如果指定了此选项，则该命令会从备份中排除镜像查询组件以减小备份大小。 *Microsoft SharePoint Server 2013 :* 如果选择了此选项，则该命令将选择每个索引分区的主索引复本以减小备份大小。
-excludeindex	仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010/2013)。如果指定了此选项，则 Data Protector 将从备份规范中排除 FASTSearch 主文件夹中包含的 data_index 文件夹。这样，备份速度更快，但还原时间更长。该选项可实现备份大小和恢复时间之间的平衡。

incremental | incremental1 ... | incremental9 }	仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010/2013)。指定此选项后，可以启动完整或增量备份或者分级增量备份。默认情况下，执行完整备份。 如果指定了 incremental 选项且完整备份不存在时，将忽略该选项并启动 FAST Search 索引文件的完整文件系统备份。
-resumecert	仅适用于 Microsoft FAST Search Server 2010/2013。如果指定了此选项，则会重新安装内容和查询连接器的 FAST Search 证书。 **重要说明**在启用了 SharePoint Server Search 14 服务的 Microsoft SharePoint Server 系统上必须启动 SharePoint_VSS_backup.ps1 –resumecert 命令。
-resumefarm	还原后使用。此选项通过恢复所有后台活动以及爬网、解锁站点，然后启动 Microsoft SharePoint Server 服务，将场恢复为工作状态。 **重要说明**指定了 -resumefarm 选项的命令使用 WMI (Windows Management Instrumentation) 远程启动任何已停止的 SharePoint 服务。为确保其正常运行，必须向 Windows 默认防火墙添加远程管理例外 (用于添加 WMI 端口)，或直接添加 WMI 例外。有关详细信息，请参阅: http://support.microsoft.com/kb/154596。
-timeout *超时*	此选项用于设置超时 (以分钟为单位)，经过该超时后，将中止 FAST Search 索引文件的爬网并恢复场。如果未指定，则默认超时为 15 分钟。

启动 Windows PowerShell

1. 使用如配置用户帐户所述配置的用户帐户，登录安装了 Windows PowerShell 和用户界面组件的 Microsoft SharePoint Server 系统。
2. 打开 Windows PowerShell CLI。例如：

   “开始”>“程序”>“附件”>“Windows PowerShell”>“Windows PowerShell”
3. 如果启用了 Windows 用户帐户控制 (UAC)，请确保使用管理权限打开 CLI。否则，将无法运行 Data Protector PowerShell 命令。
4. 确保将 Windows PowerShell 执行策略设置为 RemoteSigned 或 Unrestricted 。

   显示 Data Protector PowerShell 命令语法说明如何将 Windows PowerShell 执行策略设置为 Unrestricted 以及如何显示 Data Protector PowerShell 命令语法。

创建备份规范 (示例)

1. 要创建指定使用备份设备 filelib_writer1 的备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device filelib_writer1
2. 要创建名称中包含 weekly 标签并且指定了使用备份设备 dev1 的备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device dev1 –prefix weekly
3. 要创建指定使用备份设备 dev1 和硬件提供程序 (ZDB 磁盘阵列) 并且启用了 ZDB 选项“保留复本以供即时恢复”的 ZDB 备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly -hardware ir –device dev1
4. 仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010)。

   要创建指定使用备份设备 dev1 并将包含在 FASTSearch 主文件夹中的 data_index 文件夹从 FAST Search 索引文件的备份中排除的文件系统备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device dev1 -excludeindex

修改备份规范

要修改备份规范，请打开 Data Protector GUI。在“上下文”列表中，选择“备份”，然后在“MS 卷影复制写入程序”或“文件系统”(如果要执行 FAST Search 索引文件的标准文件系统备份) 下，单击要修改的备份规范的名称。

源页

要修改备份规范的“源”页 (例如，备份各个 Microsoft SharePoint Server 数据库)，请考虑以下注意事项:

- 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份配置数据库和管理中心内容数据库两者。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份帮助搜索数据库和关联的索引文件。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份 FAST Search 索引文件和 FAST Content SSA 爬网组件。
- *Microsoft SharePoint Server 2010/2013 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份 SharePoint Service 应用程序、搜索数据库 (SSA_Search_DB) 和关联的搜索索引文件。

否则，还原后，Microsoft SharePoint Server 数据可能不一致。

目标页

在备份规范的“目标”页中，可选择其他或额外的设备并设置设备和介质选项。

选项页

在备份规范的“选项”页中，可修改备份选项。对于 FAST Search 索引文件的标准文件系统备份，请保留指定的“使用卷影复制”选项以启用 VSS。要修改 ZDB 选项，请单击“备份规范”字段中的“高级”，然后在“备份选项”对话框中，单击“高级备份选项”选项卡。

启动备份会话 (示例)

1. 要预览启动备份会话时执行的操作，请执行以下操作: SharePoint_VSS_backup.ps1 –backuponly –prefix dev –preview
2. 要使用名称中没有前缀的现有备份规范启动备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly
3. 要使用名称中包含前缀 weekly 的现有备份规范启动备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly –prefix weekly
4. 要使用名称中没有前缀的现有备份规范启动备份会话，并将会话和关联的还原命令的输出保存到文件 c:\logs\shp.log ，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly –outfile C:\logs\shp.log
5. 要使用名称中没有前缀的现有备份规范启动“ZDB 到磁盘”备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly -snapshot diskonly
6. 要启动 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的文件系统增量备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 -backuponly -mode incremental

计划备份会话

可使用 Windows 系统调度程序计划备份会话。

1. 在前端 Web 服务器系统上，创建 Windows PowerShell 计划任务。转到 :

   “开始”>“设置”>“控制面板”>“计划任务”>“添加计划任务”
2. 打开任务的高级属性。

在“运行”文本框中，输入以下内容:

Windows_PowerShell_home \powershell.exe SharePoint_VSS_backup.ps1[Options]

在“起始位置”文本框中，输入以下内容:

Data_Protector_home \bin

在“运行身份”文本框中，输入如配置用户帐户所述配置的 Windows 域用户帐户 DOMAIN\UserName 。

还原基于 Microsoft SharePoint Server VSS 的解决方案集成

This feature is available in the Premium Edition

要还原 Microsoft SharePoint Server 数据，请执行以下操作:

- 停止 Microsoft SharePoint Server 各项服务
- 还原数据。
- 将场恢复为工作状态。

有关详细信息，请参阅以下各节。

还原数据

可以使用 Data Protector GUI 或 CLI 还原 Microsoft SharePoint Server 数据。

注意事项

- 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原配置数据库和管理中心内容数据库。由于配置数据库和管理中心内容数据库包含特定于系统的信息，因此只能将它们还原到原始环境或具有完全相同配置、软件更新、服务器名称和服务器数量的环境。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原帮助搜索数据库和关联的索引文件。
- Microsoft SharePoint Server 2010 :
  - 由于 FAST 配置数据库和 FAST Search 主文件夹包含特定于系统的信息，因此只能将它们还原到原始环境或具有完全相同配置、软件更新、服务器名称和服务器数量的环境。
  - 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原 FAST Search 索引文件和 FAST Content SSA 爬网组件。
- *Microsoft SharePoint Server 2010/2013 :* 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原 SharePoint Service 应用程序、搜索数据库 (SSA_Search_DB) 和关联的索引文件。
- 下表显示适用于不同写入程序的 VSS 还原模式:

VSS 支持还原模式和写入程序

写入程序	VSS 还原模式	
还原到另一个客户机	将文件还原到临时位置	
MSDE 写入程序 SqlServerWriter	否	是 (需要手动连接)
OSearch VSS 写入程序 OSearch14 VSS 写入程序/OSearch15 VSS 写入程序	是	否
SPSearch VSS 写入程序 SPSearch4 VSS 写入程序	是	否

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“MS 卷影复制写入程序”，展开要还原数据的客户机，然后单击“MS 卷影复制写入程序”。

   如果执行 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的文件系统还原，请展开“文件系统”，展开要还原数据的客户机，然后单击文件系统对象。
3. 在“源”页中，选择要还原的数据。

4. 在“选项”页中，指定还原选项。
5. 在“设备”页中，选择要用于还原的设备。
6. 单击“还原”，查看选择，然后单击“完成”。

使用 Data Protector CLI 进行还原

可以使用 Data Protector omnir 命令还原 Microsoft SharePoint Server 数据。

如果在运行备份会话时指定了 –outfile 选项，则可以在指定的文件中查找必要的 omnir 命令。

还原之后

1. 启用服务 Office SharePoint Server Search 、 SharePoint Server Search 14 或 SharePoint Server Search 15 。
2. 使 Microsoft SQL Server 实例联机 (如果脱机)。
3. 通过执行以下命令将场恢复为工作状态 (即，恢复后台活动和爬网、解锁站点，然后启动 Microsoft SharePoint Server 服务):

   SharePoint_VSS_backup.ps1 –resumefarm

> **注意**
>
> - 该命令使用 WMI (Windows Management Instrumentation) 远程启动任何已停止的 SharePoint 服务。为确保其正常运行，请向 Windows 默认防火墙添加远程管理例外 (用于添加 WMI 端口)，或直接添加 WMI 例外。有关详细信息，请参阅: http://support.microsoft.com/kb/154596。
> - 如果内容和查询连接器的 FAST Search 证书不同步，则可通过执行以下命令重新进行安装:
>
>   SharePoint_VSS_backup.ps1 -resumecert
>
>   在启用了 SharePoint Server Search 14 服务的 Microsoft SharePoint Server 系统上启动该命令。

基于 Microsoft SharePoint Server VSS 的解决方案 - ZDB

本主题说明如何配置和使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案 (“基于 VSS 的解决方案”)。实际上，该解决方案基于 Data Protector Microsoft 卷影复制服务集成 (“VSS 集成”)。

本主题介绍备份和还原在 Microsoft SQL Server 数据库中存储的 Microsoft SharePoint Server 2010 和 Microsoft SharePoint Server 2013 数据时需要了解的概念和方法。例如：

- 配置数据库 (SharePoint_Config)
- 内容数据库 (SharePoint_AdminContent_Label 、 WSS_Content_Label ...)
- SharePoint Service 应用程序数据库 (SSA_DB) (Microsoft SharePoint Server 2010/2013)

此外，还可以备份和还原 Microsoft SharePoint Server 搜索索引文件。

从现在开始，Microsoft SharePoint Server 的两个版本均称作“Microsoft SharePoint Server”，除非指出了差异。

备份

使用以下 Microsoft SQL Server VSS 写入程序之一备份在 Microsoft SQL Server 数据库中存储的 Microsoft SharePoint Server 数据:

- MSDE writer（适用于 Microsoft SQL Server 2000 数据库)
- SqlServerWriter（适用于 Microsoft SQL Server 2008 数据库)

使用以下 VSS 写入程序备份 Microsoft SharePoint Server 2010 搜索索引文件:

- OSearch14 VSS writer
- SPSearch4 VSS writer

使用以下 VSS 写入程序备份 Microsoft SharePoint Server 2013 搜索索引文件:

- OSearch15 VSS writer

Microsoft FAST Search Server 2010 搜索索引文件通过以下方法进行备份:

- 使用 Data Protector 磁盘代理 (当在已启用 VSS 的情况下进行标准文件系统备份时)
- 使用 Data Protector VSS 集成 (当进行 ZDB 文件系统备份时)

可使用 Data Protector PowerShell 命令创建和运行备份规范，如备份基于 Microsoft SharePoint Server VSS 的解决方案所述。

满足基于 Microsoft SharePoint Server VSS 的解决方案的先决条件

基于 Microsoft SharePoint Server VSS 的解决方案集成的先决条件如下:

- 如果打算运行 ZDB 和即时恢复 (IR) 会话，请确保所有 SSP 或 SSA 的 SPSearch 和 OSearch 索引文件以及 FAST Search 索引文件均位于磁盘阵列中。

Microsoft Office SharePoint Server

SPSearch 索引文件的默认位置如下:

```
C:\Program Files\Microsoft Office Servers\12.0\Data\Applications
```

OSearch 索引文件的默认位置如下:

```
C:\Program Files\Microsoft Office Servers\12.0\Data\Office Server\Applications
```

要将索引文件移至磁盘阵列，请执行以下操作:

1. 打开命令提示符，然后将目录更改为:

   ```
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN>
   ```

2. 要移动 SPSearch 索引文件，请执行以下命令:

   ```
   stsadm -o spsearch -indexlocation PathToNewLocation
   ```

3. 要移动 OSearch 索引文件，请执行以下命令:

   ```
   stsadm -o editssp –title SSPname -indexlocation PathToNewLocation
   ```

Microsoft SharePoint Server 2010

SPSearch 索引文件的默认位置如下:

```
C:\Program Files\Microsoft Office Servers\14.0\Data\Applications
```

OSearch 索引文件的默认位置如下:

```
C:\Program Files\Microsoft Office Servers\14.0\Data\Office Server\Applications
```

要将索引文件移至磁盘阵列，请执行以下操作:

1. 打开命令提示符，然后将目录更改为:

   ```
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN>
   ```

2. 要移动 SPSearch 索引文件，请执行以下命令:

   ```
   stsadm -o spsearch -indexlocation PathToNewLocation
   ```

3. 要移动 OSearch 索引文件，请使用管理中心 (修改场拓扑)。

在安装 FAST Search Server 2010 系统期间，必须将 `FASTSearch` 主文件夹安装到磁盘阵列中。如果有多个 FAST Search Server 系统场，请确保所有系统上的 `FASTSearch` 主文件夹路径相同 (驱动器和路径名)。

- 必须在所有系统上配置 Windows 远程管理服务 (用于远程启动和停止 Windows 服务，以及暂停和恢复 FAST for Microsoft SharePoint Server 2010)。

  要配置和分析 WinRM 服务，请执行 `winrm quickconfig` 命令。

- 如果 Microsoft SharePoint Server 2010/2013 使用 Microsoft SQL Server 2008/2012 存储数据，并且远程 Blob 存储与 FILESTREAM 提供程序一起使用，请确保将 FILESTREAM 访问级别设置为“启用完全访问”或“启用 Transact-SQL 访问”。
- 使用 Data Protector GUI 修改备份规范 (例如，添加备份设备)。
- 将简单模式用于 SQL Server 数据库。如果仍想使用完整模式，请确保截断事务日志。否则，磁盘空间可能不足。
- 每当更改场配置时，请执行新备份。
- 如果要备份单点登录数据库，切记备份加密密钥，如下所述: http://technet.microsoft.com/en-us/library/cc262932.aspx#Section32。

  否则，将无法还原数据库。

- 使用命令选项可将流程拆分为两部分: 首先创建备份规范，然后启动备份会话。可通过这种方式在实际启动备份之前，在 Data Protector GUI 中手动修改新建的备份规范。
- 如果 Microsoft SQL Server 实例同时供 Microsoft SharePoint Server 和其他数据库应用程序使用，请修改备份规范，以仅选择属于 Microsoft SharePoint Server 的数据库进行备份。
- 如果已启用了 Microsoft SQL Server 数据库镜像，则可能会发生故障转移，从而使其他 Microsoft SQL Server 系统变为活动状态。由于该命令仅为当前活动的 Microsoft SQL Server 系统创建备份规范，因此建议在启动备份之前，更新 (重新创建) 备份规范。

  - 停止并禁用以下服务:
    - SharePoint Server Search 14 (Microsoft SharePoint Server 2010)
    - SharePoint Server Search 15 (Microsoft SharePoint Server 2013)

  此外，停止以下服务:

  Microsoft SharePoint Server 2010 :

  - SharePoint 2010 Administration
  - SharePoint Foundation Search V4
  - SharePoint 2010 Timer
  - SharePoint 2010 Tracing
  - FAST Search for SharePoint
  - FAST Search for SharePoint Monitoring

  Microsoft SharePoint Server 2013 :

  - SharePoint Administration
  - SharePoint Search Host Controller

        - SharePoint Timer Service
        - SharePoint Tracing Service
    - 如果打算还原以下 Microsoft SQL Server 数据库之一，请将 Microsoft SQL Server 实例置于脱机状态:
        - master
        - model
        - msdb
        - 启用了 Microsoft SQL Server 镜像的数据库

  注意

    - 如果使用 SqlServerWriter ，则可以在 Microsoft SQL Server 实例处于联机状态时，还原 model 和 msdb 数据库。这一点优于 MSDE writer.
    - *Microsoft SQL Server 镜像*: 如果原始数据库和镜像数据库位于单独的 Microsoft SQL Server 实例中，请将这两个 Microsoft SQL Server 实例置于脱机状态。

- 仅适用于 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的 Data Protector 文件系统还原。在还原 FAST Search 索引文件之前，必须保持“覆盖”选项处于选定状态才能确保数据一致。默认选中此选项。

配置集成

配置用户帐户

创建或标识要在其上执行 Data Protector 命令的 Microsoft SharePoint Server 系统具有 Windows 管理权限的 Windows 域用户帐户。还必须向此用户授予 Microsoft SharePoint Server 管理权限，并且必须将其添加至 Data Protector admin 用户组。

备份基于 Microsoft SharePoint Server VSS 的解决方案集成 - ZDB

要备份 Microsoft SharePoint Server 数据，请使用 Data Protector PowerShell 命令 SharePoint_VSS_backup.ps1 创建备份规范并启动备份会话。

执行 Data Protector PowerShell 命令 SharePoint_VSS_backup.ps1 时，Data Protector 首先会查询有关 Microsoft SharePoint Server 环境的信息。然后创建备份规范。

新建的备份规范名为 SharePoint_VSS_backup_ClientName ，并且指定了相同的备份设备 (在命令运行时指定的备份设备) 以供使用。

备份规范创建后，该命令即会启动备份会话 (每个备份规范对应一个会话)。

Microsoft SharePoint Server 2010

在 Microsoft SharePoint Server 2010 环境中，该命令将为至少启用了以下服务之一的每个 Microsoft SharePoint Server 系统创建单独的备份规范:

- SharePoint Foundation Database
- SharePoint Foundation Help Search
- SharePoint Server Search 14
- FAST Search Server 2010 for SharePoint (FAST Search)

对于启用了 SharePoint Foundation 数据库服务的系统，该命令将创建选择了 SqlServerWriter（Microsoft SQL Server 2008) 对象的备份规范。

对于启用了 SharePoint Foundation 帮助搜索和 SharePoint Server 搜索服务的系统，该命令将创建选择了 SPSearch4 VSS Writer 和 OSearch14 VSS Writer 对象的备份规范。

对于启用了 FAST Search Server 2010 服务的系统，该命令会创建选择了 FASTSearch 主文件夹 (不包括包含 FAST 可执行文件的 bin 和 lib 文件夹) 的文件系统备份规范。

对于启用了 FAST Search Server 2010 服务的系统，指定了 -hardware 选项的该命令会创建选择了整个 FASTSearch 主文件夹 (包括 bin 和 lib) 的 VSS 备份规范。

Microsoft SharePoint Server 2013

在 Microsoft SharePoint Server 2013 环境中，该命令将为至少启用了以下服务之一的每个 Microsoft SharePoint Server 系统创建单独的备份规范:

- SharePoint Foundation Database
- SharePoint Server Search 15

对于启用了 SharePoint Foundation Database 服务的系统，该命令将创建选择了 SqlServerWriter（Microsoft SQL Server 2008/2012) 对象的备份规范。

对于启用了 SharePoint Server 搜索服务的系统，该命令将创建选择了 OSearch15 VSS Writer 对象的备份规范。

命令语法

- 必须从前端 Web 服务器系统上的 Data_Protector_home\bin 目录执行命令。请确保使用如配置用户帐户所述配置的用户帐户进行登录，并使用管理权限打开命令提示符。
- 请勿在备份会话正在进行时关闭 PowerShell 控制台。如果在备份期间关闭控制台，则不会执行某些操作: 会完成已启动的备份会话，但场不会恢复原始状态。要恢复场，请首先使用 –resumefarm 选项执行该命令，然后使用 Microsoft SharePoint Server 管理中心或 stsadm 手动取消静默场。

```
SharePoint_VSS_backup.ps1 –help |-version SharePoint_VSS_backup.ps1 –createonly CreateOptions SharePoint_VSS_backup.ps1 –backuponly BackupOptions SharePoint_VSS_backup.ps1 –resumefarm [-preview] | -resumecert CreateOptions
```

```
{-device DevName | -hardware {no_keep|keep|ir} [-device DevName]} [-overwrite] [-prefix PrefixName] [-excludeindex] BackupOptions [-outfile PathToFile] [-prefix PrefixName] [-preview] [-snapshot {diskonly | disktape | tapeonly}] [-reduce] [-mode {full | incremental | incremental1 ...| incremental9}] [-timeout Timeout]
```

选项描述

-help	显示 SharePoint_VSS_backup.ps1 命令用法。
-version	显示 SharePoint_VSS_backup.ps1 版本。

–createonly	如果指定了此选项，则 Data Protector 仅创建备份规范。备份未启动。
–backuponly	如果指定了此选项，则 Data Protector 仅使用现有备份规范启动备份会话。不需要 -device 选项。
-device *DevName*	指定要用于备份的 Data Protector 设备。只能指定一个设备。 如果仅使用一个设备来备份多系统场，则无法并行运行相应的备份会话。这会延长场处于只读模式的时间。具体来说，从备份会话启动时到所有 VSS 快照创建完，场都一直处于只读模式。 为了能够并行运行备份会话，请在启动备份之前，在每个备份规范中选择不同或额外的设备。
-hardware {no_keep|keep | ir }	指定应使用硬件提供程序 (而非指定了 -device 选项的软件提供程序) 并设置 ZDB 选项。ZDB 选项的默认值如下: • 保留复本以供即时恢复: 指定了 ir 时选中。 • 备份后保留复本: 指定了 ir 或 keep 时选中。 • 配置检查模式(G): 严格 • 复本类型: 镜像/克隆 (丛) • 循环的复本数: 3 默认 ZDB 备份类型如下 (前提是还指定了设备): • no_keep : ZDB 到磁带 • keep : ZDB 到磁盘 + 磁带 • ir : ZDB 到磁盘 + 磁带
–overwrite	默认情况下，Data Protector 不会创建备份规范 (如果已存在)。如果指定了此选项，则 Data Protector 将使用新创建的备份规范覆盖现有备份规范。指定了 –backuponly 时不适用。
-prefix *PrefixName*	指定此选项后，将使用其他名称创建备份规范: SharePoint_VSS_backup_PrefixName_ClientName 。 备份时，此选项用于指定要使用的备份规范: 名称包含 *PrefixName* 的备份规范。 *PrefixName* 中不支持非 ASCII 字符。
-outfile *PathToFile*	如果指定了此选项，则会将备份规范名称、错误、会话输出和 omnir 还原命令写入指定文件。
-preview	如果指定了此选项，则 Data Protector 将显示有关 Microsoft SharePoint Server 环境的信息并介绍相关操作，但不实际执行它们。
-snapshot {disktape | tapeonly }	启动 ZDB 备份会话时适用 (即，使用其中指定了要使用的硬件提供程序的备份规范的会话)。执行“ZDB 到磁盘”(diskonly)、“ZDB 到磁带”(tapeonly) 或“ZDB 到磁盘 + 磁带”(disktape) 会话。
-reduce	*Microsoft SharePoint Server 2010 :* 如果指定了此选项，则该命令会从备份中排除镜像查询组件以减小备份大小。 *Microsoft SharePoint Server 2013 :* 如果选择了此选项，则该命令将选择每个索引分区的主索引复本以减小备份大小。
-excludeindex	仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010/2013)。如果指定了此选项，则 Data Protector 将从备份规范中排除 FASTSearch 主文件夹中包含的 data_index 文件夹。这样，备份速度更快，但还原时间更长。该选项可实现备份大小和恢复时间之间的平衡。
-mode{full|incremental | incremental1 ...| incremental9 }	仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010/2013)。指定此选项后，可以启动完整或增量备份或者分级增量备份。默认情况下，执行完整备份。 如果指定了 incremental 选项且完整备份不存在时，将忽略该选项并启动 FAST Search 索引文件的完整文件系统备份。
-resumecert	仅适用于 Microsoft FAST Search Server 2010/2013。如果指定了此选项，则会重新安装内容和查询连接器的 FAST Search 证书。 重要说明: 在启用了 SharePoint Server Search 14 服务的 Microsoft SharePoint Server 系统上必须启动 SharePoint_VSS_backup.ps1 –resumecert 命令。
-resumefarm	还原后使用。此选项通过恢复所有后台活动以及爬网、解锁站点，然后启动 Microsoft SharePoint Server 服务，将场恢复为工作状态。 指定了 -resumefarm 选项的命令使用 WMI (Windows Management Instrumentation) 远程启动任何已停止的 SharePoint 服务。为确保其正常运行，必须向 Windows 默认防火墙添加远程管理例外 (用于添加 WMI 端口)，或直接添加 WMI 例外。有关详细信息，请参阅: http://support.microsoft.com/kb/154596。
-timeout *超时*	此选项用于设置超时 (以分钟为单位)，经过该超时后，将中止 FAST Search 索引文件的爬网并恢复场。如果未指定，则默认超时为 15 分钟。

启动 Windows PowerShell

1. 使用如配置用户帐户所述配置的用户帐户，登录安装了 Windows PowerShell 和用户界面组件的 Microsoft SharePoint Server 系统。
2. 打开 Windows PowerShell CLI。例如：

   “开始”>“程序”>“附件”>“Windows PowerShell”>“Windows PowerShell”
3. 如果启用了 Windows 用户帐户控制 (UAC)，请确保使用管理权限打开 CLI。否则，将无法运行 Data Protector PowerShell 命令。
4. 确保将 Windows PowerShell 执行策略设置为 RemoteSigned 或 Unrestricted 。

创建备份规范 (示例)

1. 要创建指定使用备份设备 filelib_writer1 的备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device filelib_writer1
2. 要创建名称中包含 weekly 标签并且指定了使用备份设备 dev1 的备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device dev1 –prefix weekly
3. 要创建指定使用备份设备 dev1 和硬件提供程序 (ZDB 磁盘阵列) 并且启用了 ZDB 选项“保留复本以供即时恢复”的 ZDB 备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly -hardware ir –device dev1
4. 仅适用于 FAST Search 索引文件的 Data Protector 标准文件系统备份 (Microsoft SharePoint Server 2010)。

   要创建指定使用备份设备 dev1 并将包含在 FASTSearch 主文件夹中的 data_index 文件夹从 FAST Search 索引文件的备份中排除的文件系统备份规范，请执行以下操作:

   SharePoint_VSS_backup.ps1 –createonly –device dev1 -excludeindex

修改备份规范

要修改备份规范，请打开 Data Protector GUI。在“上下文”列表中，选择“备份”，然后在“MS 卷影复制写入程序”或“文件系统”(如果要执行 FAST Search 索引文件的标准文件系统备份) 下，单击要修改的备份规范的名称。

源页

要修改备份规范的“源”页 (例如，备份各个 Microsoft SharePoint Server 数据库)，请考虑以下注意事项:

- 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份配置数据库和管理中心内容数据库两者。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份帮助搜索数据库和关联的索引文件。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份 FAST Search 索引文件和 FAST Content SSA 爬网组件。
- *Microsoft SharePoint Server 2010/2013 :* 为了确保数据一致性，必须在从挂起 Microsoft SharePoint Server (SharePoint 场) 开始并以恢复 SharePoint 场结束的同一时间段内，备份 SharePoint Service 应用程序、搜索数据库 (SSA_Search_DB) 和关联的搜索索引文件。

否则，还原后，Microsoft SharePoint Server 数据可能不一致。

目标页

在备份规范的“目标”页中，可选择其他或额外的设备并设置设备和介质选项。

选项页

在备份规范的“选项”页中，可修改备份选项。对于 FAST Search 索引文件的标准文件系统备份，请保留指定的“使用卷影复制”选项以启用 VSS。要修改 ZDB 选项，请单击“备份规范”字段中的“高级”，然后在“备份选项”对话框中，单击“高级备份选项”选项卡。

启动备份会话 (示例)

1. 要预览启动备份会话时执行的操作，请执行以下操作: SharePoint_VSS_backup.ps1 –backuponly –prefix dev –preview
2. 要使用名称中没有前缀的现有备份规范启动备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly
3. 要使用名称中包含前缀 weekly 的现有备份规范启动备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly –prefix weekly

4. 要使用名称中没有前缀的现有备份规范启动备份会话，并将会话和关联的还原命令的输出保存到文件 c:\logs\shp.log ，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly –outfile C:\logs\shp.log

5. 要使用名称中没有前缀的现有备份规范启动“ZDB 到磁盘”备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 –backuponly -snapshot diskonly

6. 要启动 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的文件系统增量备份会话，请执行以下操作:

   SharePoint_VSS_backup.ps1 -backuponly -mode incremental

计划备份会话

可使用 Windows 系统调度程序计划备份会话。

1. 在前端 Web 服务器系统上，创建 Windows PowerShell 计划任务。转到：

   “开始”>“设置”>“控制面板”>“计划任务”>“添加计划任务”

2. 打开任务的高级属性。

在“运行”文本框中，输入以下内容:

Windows_PowerShell_home \powershell.exe SharePoint_VSS_backup.ps1[Options]

在“起始位置”文本框中，输入以下内容:

Data_Protector_home \bin

在“运行身份”文本框中，输入如配置用户帐户所述配置的 Windows 域用户帐户 DOMAIN\UserName 。

还原基于 Microsoft SharePoint Server VSS 的解决方案集成

要还原 Microsoft SharePoint Server 数据，请执行以下操作:

- 停止 Microsoft SharePoint Server 各项服务
- 还原数据。
- 将场恢复为工作状态。

有关详细信息，请参阅以下各节。

还原数据

可以使用 Data Protector GUI 或 CLI 还原 Microsoft SharePoint Server 数据。

注意事项

- 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原配置数据库和管理中心内容数据库。由于配置数据库和管理中心内容数据库包含特定于系统的信息，因此只能将它们还原到原始环境或具有完全相同配置、软件更新、服务器名称和服务器数量的环境。
- *Microsoft SharePoint Server 2010 :* 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原帮助搜索数据库和关联的索引文件。
- Microsoft SharePoint Server 2010 :
  - 由于 FAST 配置数据库和 FAST Search 主文件夹包含特定于系统的信息，因此只能将它们还原到原始环境或具有完全相同配置、软件更新、服务器名称和服务器数量的环境。
  - 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原 FAST Search 索引文件和 FAST Content SSA 爬网组件。
- *Microsoft SharePoint Server 2010/2013 :* 为了确保数据一致性，必须使用同一时间点的备份 (在 Microsoft SharePoint Server (SharePoint 场) 处于挂起模式的同一时间段内执行的备份) 还原 SharePoint Service 应用程序、搜索数据库 (SSA_Search_DB) 和关联的索引文件。
- 下表显示适用于不同写入程序的 VSS 还原模式:

VSS 支持还原模式和写入程序

写入程序	VSS 还原模式	
	还原到另一个客户机	将文件还原到临时位置
MSDE 写入程序 SqlServerWriter	否	是 (需要手动连接)
OSearch VSS 写入程序 OSearch14 VSS 写入程序/OSearch15 VSS 写入程序	是	否
SPSearch VSS 写入程序 SPSearch4 VSS 写入程序	是	否

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“MS 卷影复制写入程序”，展开要还原数据的客户机，然后单击“MS 卷影复制写入程序”。

   如果执行 FAST Search 索引文件 (Microsoft SharePoint Server 2010) 的文件系统还原，请展开“文件系统”，展开要还原数据的客户机，然后单击文件系统对象。
3. 在“源”页中，选择要还原的数据。
4. 在“选项”页中，指定还原选项。
5. 在“设备”页中，选择要用于还原的设备。
6. 单击“还原”，查看选择，然后单击“完成”。

使用 Data Protector CLI 进行还原

可以使用 Data Protector omnir 命令还原 Microsoft SharePoint Server 数据。

如果在运行备份会话时指定了 -outfile 选项，则可以在指定的文件中查找必要的 omnir 命令。

还原之后

1. 启用服务 Office SharePoint Server Search 、 SharePoint Server Search 14 或 SharePoint Server Search 15 。
2. 使 Microsoft SQL Server 实例联机 (如果脱机)。
3. 通过执行以下命令将场恢复为工作状态 (即，恢复后台活动和爬网、解锁站点，然后启动 Microsoft SharePoint Server 服务):

   ```
   SharePoint_VSS_backup.ps1 –resumefarm
   ```

   注意

   - 该命令使用 WMI (Windows Management Instrumentation) 远程启动任何已停止的 SharePoint 服务。为确保其正常运行，请向 Windows 默认防火墙添加远程管理例外 (用于添加 WMI 端口)，或直接添加 WMI 例外。有关详细信息，请参阅: http://support.microsoft.com/kb/154596。
   - 如果内容和查询连接器的 FAST Search 证书不同步，则可通过执行以下命令重新进行安装:

     ```
     SharePoint_VSS_backup.ps1 -resumecert
     ```

     在启用了 SharePoint Server Search 14 服务的 Microsoft SharePoint Server 系统上启动该命令。

Microsoft SQL Server 集成

This feature is available in the Premium Edition

本主题介绍如何配置和使用 Data Protector Microsoft SQL Server 集成。其中说明了要备份和还原 Microsoft SQL Server (SQL Server) 数据库对象所需了解的概念和方法。

Data Protector 提供以下类型的交互式备份和安排的备份：

支持的 SQL Server 联机备份类型

备份类型	描述
完整数据库备份	包括所有数据，无论上次备份后进行了什么更改。 在可用性组配置中，当触发属于可用性组辅助复本的数据库的完整备份时，备份类型会自动更改为仅复制完整备份。在进行任何其他类型的备份之前，应先进行完整备份。
事务日志备份	使用的资源比数据库备份少，因此可以更频繁地创建。通过应用事务日志备份，可以将数据库恢复到特定时间点。 在日志传送配置中，当事务日志备份触发时，备份类型将自动更改为差异数据库备份。 请注意，如果运行事务日志备份而不先运行完全备份，则将采用完全备份而不是事务日志备份。
差异数据库备份 (Differential database backup)	仅记录自上次完整数据库备份以来对数据库所做的更改。通过比完整数据库备份更频繁地创建差异备份，可以节约用于备份的介质。 运行差异备份之前，请确保存在完整备份。否则，来自此类差异备份会话的还原将失败。如果运行差异备份而不先运行完全备份，则将采用完全备份而不是差异备份。 在可用性组配置中，当触发属于可用性组辅助复本的数据库的差异备份时，备份类型会自动更改为仅复制完整备份。
仅副本数据库备份	仅副本完整备份是独立的完整备份，无需截断事务日志，并且不会影响 SQL Server 恢复链。因此，它无法充当差异备份的基础。 如果不想影响数据库备份，请运行仅副本完整备份。

Data Protector 会根据您的需要提供不同的还原类型。可以选择时间点还原、完整数据库还原，还可以将 SQL Server 数据还原到新位置、还原到其他 SQL Server 或其他 SQL Server 实例。

本节提供了此类集成的特定信息。

日志序列号 (LSN)

LSN 帮助 Data Protector 构建正确的还原链。当完整/差异/副本备份与事务日志备份并行运行时，将忽略备份时间。有关 LSN 的详细信息，请查看 Microsoft MSSQL Server 文档。

以下限制适用：

- 不支持备份预览。
- 功能的备份部分取决于 msdb 系统数据库中的备份信息，除非删除备份下的数据库，否则不应进行修改。
- 最后一个还原链始终按时间还原。变通方法：创建新的完整备份和事务备份。
- 9.07 之前的备份始终按时间还原。
- 如果 Data Protector 无法构造还原链，则 LSN Data Protector 会尝试按备份时间构造还原链。
- 如果在没有有效的完整数据库备份的情况下备份单个数据文件或文件数据集，则只能通过选择单个数据文件或文件数据集来进行还原。

请注意，由于正在通过 LSN 构造链，因此不仅要考虑最近的完整/差异备份，还要考虑旧备份。

集成概念

Data Protector 通过安装在 SQL Server 上的 Data Protector sql_bar.exe 可执行文件与 SQL Server 集成。它实施用于进行备份和还原的多个虚拟设备，并将 SQL Server 中的 SQL Server 虚拟设备接口 (VDI) 命令转换为 Data Protector 备份或还原流。

通过 VDI 体系结构，Data Protector 常规介质代理可以在 SQL Server 的内存中直接访问数据，只要设备直接连接到 SQL Server。因此，实现了高速备份和还原。

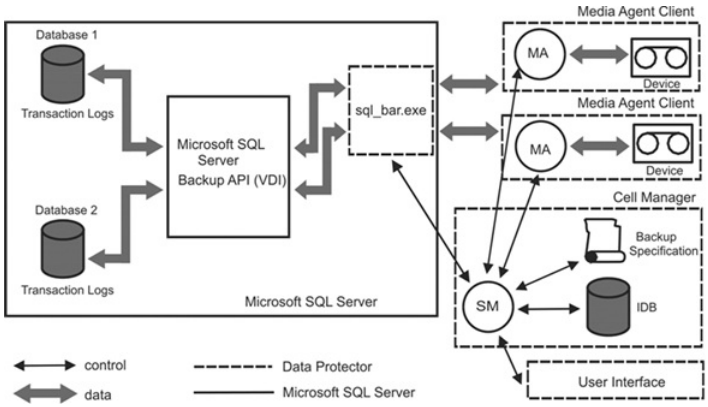
可以执行交互式和计划完整数据库备份、差异数据库备份、仅副本完整备份和事务日志备份。完整和差异备份与定期事务日志备份相结合，可在发生磁盘故障时防止数据丢失。此外，执行时间点还原也需要事务日志备份。

可以备份整个服务器、独立用户数据库、属于可用性组的用户数据库或下面列出的某些数据库:

用户数据库	包含用户数据。
主	控制用户数据库和 SQL Server 操作。跟踪用户帐户、可配置的环境变量和系统错误消息。
模型	为新用户数据库提供模板或原型。
分发	SQL Server 复制组件 (如分发代理) 用于存储数据 (包括事务、快照作业、同步状态和复制历史记录信息) 的系统数据库。
Msdb	为日程安排和备份信息提供存储。

SQL Server 支持 AlwaysOn 可用性组解决方案。Data Protector 还原数据库，以使差异备份应用于完整备份。然后，根据指定的还原选项应用事务日志备份。

Data Protector SQL Server 集成体系结构



图例

图例	描述
SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
备份 API 或 VDI	SQL Server VDI，随 SQL Server 引入的备份接口。
MA	Data Protector 常规介质代理。

并行性

可以一次备份一个以上的 SQL Server 数据库，或者使用多个流备份单个数据库。

用于 SQL Server 的并行类型有:

- 数据库并行

  如果可用设备的数量允许并行执行备份，则会备份一个以上的数据库。

  向可用设备分配流的操作是自动进行的。

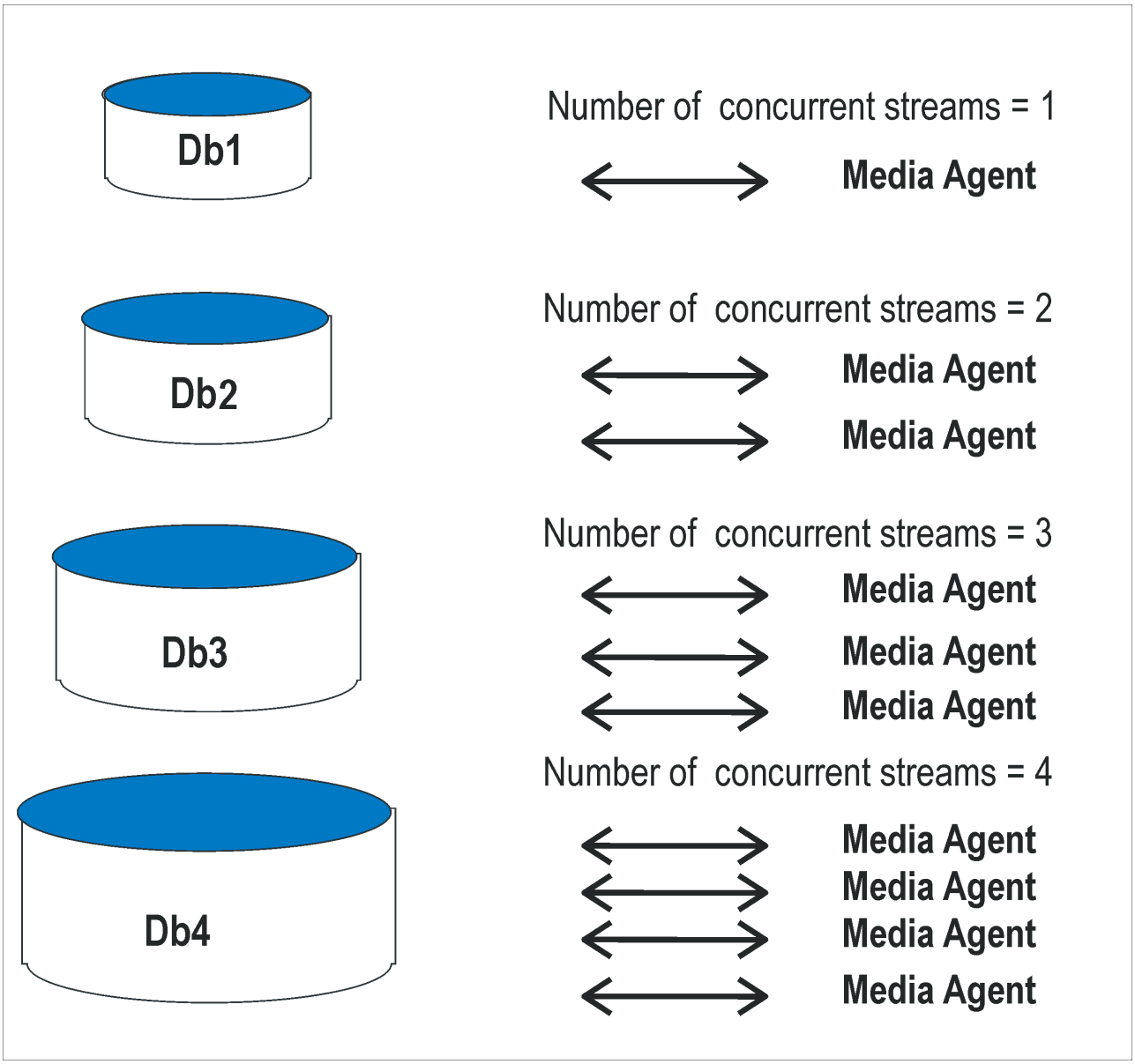
- 并发流数

  这是用于备份特定数据库或服务器的设备数。可以由用户指定或自动计算。

> 注意SQL Server 无法将多个流备份到一个设备。

数据库并行数 = 4，总并发数 = 10 显示一个会话，其中每个 SQL Server 数据库使用不同数量的并发流进行备份。

数据库并行数 = 4，总并发数 = 10


Db1
Number of concurrent streams = 1
Media Agent
Db2
Number of concurrent streams = 2
Media Agent
Media Agent
Db3
Number of concurrent streams = 3
Media Agent
Media Agent
Media Agent
Db4
Number of concurrent streams = 4
Media Agent
Media Agent
Media Agent
Media Agent

安装 Microsoft SQL Server 客户机

This feature is available in the Premium Edition

为了能够备份 Microsoft SQL Server 数据库，您需要在安装过程中选择 MS SQL 集成组件。假设 Microsoft SQL Server 已启动并正在运行。

配置 Microsoft SQL Server 集成

This feature is available in the Premium Edition

Data Protector SQL Server 配置文件

在以下系统中，Data Protector 为 Cell Manager 上的每个已配置 SQL Server 存储集成参数:

HP-UX 和 Linux 系统：

- 对于独立实例配置

  /etc/opt/omni/server/integ/config/MSSQL/ClientName%InstanceName

- 对于可用性组配置

  /etc/opt/omni/server/integ/config/MSSQL/ListenerName%AGName

/etc/opt/omni/server/integ/config/MSSQL/ClientName%InstanceName

Windows 系统：

- 对于独立实例配置

  Data_Protector_program_data\Config\Server\Integ\Config\MSSQL\ClientName%InstanceName

- 对于可用性组配置

  Data_Protector_program_data\Config\Server\Integ\Config\MSSQL\ListenerName% \ AGName

  ListenerName 可用性组侦听程序 (用于连接到 SQL Server 的虚拟客户机) 的名称。 AGName 是与所选侦听程序对应的 SQL Server 可用性组的名称。

配置参数是那些必须具有在 SQL Server 中运行备份和还原的权限 (假设使用标准安全性) 的 SQL Server 用户的用户名和密码。在集成配置期间，它们将写入 Data Protector SQL Server 配置文件。

配置文件的内容如下:

```
Login='user'; Password='encoded_password'; Domain='domain'; Port='PortNumber';
```

重要说明要避免备份问题，请确保配置文件的语法与示例一致。在可用性组配置中，还需提供可用性组侦听程序用于连接到 SQL Server 的端口号。默认值为 1433。

示例

- *SQL Server 身份验证:*

  ```
  Login='sa'; Domain=''; Password='jsk74yh80fh43kdf';
  ```

- *Windows 身份验证:*

  ```
  Login='Administrator'; Domain='IPR'; Password='dsjf08m80fh43kdf';
  ```

- *集成身份验证:*

  ```
  Login=''; Domain=''; Password='kf8u3hdgtfh43kdf';
  ```

配置 SQL Server 群集

在群集中，必须将所有节点安装为 Data Protector 群集感知的客户机，并且所有节点上的 Data Protector Inet 服务必须在也具有群集管理员权限的 Windows 域用户帐户下运行。

您必须为所有群集节点配置 Data Protector Inet 服务用户模拟。必须对使用的 Windows 域用户帐户授予以下 Windows 操作系统安全策略特

权：

- 身份验证后模拟客户机
- 替换进程级别令牌

配置 SQL Server 实例

在创建第一个备份规范期间配置 SQL Server 实例。此配置包括设置 Data Protector 连接到 SQL Server 实例时应使用的用户帐户。指定的登录信息保存到 Cell Manager 上的 Data Protector SQL Server 实例配置文件中。

如果 SQL Server 支持 AlwaysOn 可用性组解决方案，则可以为 SQL 数据库配置可用性组。可用性组包含一组读写可用性组的主复本数据库和一到四组相应可用性组的辅助复本数据库。

> **注意**确保要使用的用户帐户具有运行备份和还原的适当的 SQL Server 权限。使用 SQL Server 企业管理器检查权限。

可以按照配置集成中的说明更改配置。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS SQL Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 Microsoft SQL Server 备份”模板。

   单击**确定**。
4. 在“客户机”中，选择 SQL Server 系统。对于群集环境，选择 SQL Server 资源组的虚拟服务器。对于可用性组配置，选择相应可用性组的可用性组侦听程序。请注意，必须首先通过在“客户机”上下文中选择“虚拟主机”将可用性组侦听程序作为虚拟客户机导入。

   在“应用程序数据库”中，选择或指定 SQL Server 实例的名称。在可用性组配置中，将自动列出连接到所选可用性组侦听程序的 SQL 可用性组的名称，并且无法更改。

   如果要使用“集成身份验证”并且希望备份会话在指定的操作系统用户帐户下运行，请指定“指定 OS 用户”选项。有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 在“配置 MS SQL Server”对话框中，指定 Data Protector 要用于连接到 SQL Server 实例的用户帐户。
   - **SQL Server 身份验证**: SQL Server 用户帐户。指定用户名和密码。
   - **Windows 身份验证**: Windows 域用户帐户 (首选选项)。指定用户名、密码和域。
   - **集成身份验证**: 选择此选项可使 Data Protector 使用运行 SQL Server 系统上的 Data Protector Inet 服务的 Windows 域用户帐户连接到 SQL Server 实例。

   请确保您指定的用户帐户具有用于备份和还原 SQL Server 数据库的适当权限。

   对于可用性组配置，您还可以提供可用性组侦听程序使用的端口号。默认值为 1433。

   > **注意**建议由 SQL Server 系统管理员配置集成。

   单击“确定”确认配置。
6. SQL Server 实例即已配置。退出 GUI 或继续在创建 ZDB 备份规范创建备份规范。

使用 Data Protector CLI

执行：

- 对于独立实例配置:

  sql_bar config [-appsrv:SQLServerClient] [-instance:InstanceName] [-dbuser:SQLServerUser -password:password | -dbuser:WindowsUser -password:password -domain:domain]

- 对于可用性组配置:

  sql_bar econfig [-appsrv:ListenerName] [-ag:AGname] [-dbuser:SQLServerUser -password:password | -dbuser:WindowsUser -password:password -domain:domain]-port:PortNumber

参数描述

-appsrv:SQLServerClient	运行 SQL Server 实例的客户机系统。如果在本地执行命令，则不需要此选项。
-appsrv:ListenerName	可用性组侦听程序 (运行 SQL Server 可用性组的虚拟客户机) 的名称。
-instance:InstanceName	SQL Server 实例名称。如果省略此选项，则配置默认 SQL Server 实例。
-ag:AGname	SQL Server 可用性组名称。
-dbuser:SQLServerUser -password:password	SQL Server 用户帐户 (“SQL Server 身份验证”)
-dbuser:WindowsUser -password:password -domain:domain	Windows 域用户帐户 (“Windows 身份验证”)
-port:PortNumber	可用性组侦听程序用于连接到 SQL Server 的端口号。默认值为 1433。

注意如果未指定用户帐户，则 Data Protector 使用“集成身份验证”。

消息 *RETVAL*0 表示配置成功。

备份 Microsoft SQL Server 集成

This feature is available in the Premium Edition

运行现有 SQL Server 备份规范的联机备份:

- 使用 Data Protector 调度程序计划备份。
- 使用 Data Protector GUI 或 CLI 启动交互式备份。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS SQL Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 Microsoft SQL Server 备份”模板。
4. 在“客户机”中，选择一个 SQL Server。对于群集环境，选择 SQL Server 资源组的虚拟服务器。对于可用性组配置，选择相应可用性组的可用性组侦听程序。请注意，必须首先通过在“客户机”上下文中选择“虚拟主机”将可用性组侦听程序作为虚拟客户机导入。

   在“应用程序数据库”中，指定 SQL Server 实例的名称。在可用性组配置中，将自动列出连接到所选可用性组侦听程序的 SQL 可用性组的名称，并且无法更改。

   如果要使用“集成身份验证”并且希望备份会话在指定的操作系统用户帐户下运行，请指定“指定 OS 用户”选项。有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 如果未配置客户机，此时将显示“配置 MS SQL Server”对话框。按照配置 SQL Server 实例中的说明进行配置。
6. 选择要备份的数据库。
7. 选择要备份的数据库、文件组或数据文件。

   在 SQL Server 可用性组环境中，在创建独立实例备份规范时，Data Protector 会显示数据库的名称以及可用性组名称及其可用性组复本角色。例如，在 Data Protector GUI 中，属于名为 AG1 的可用性组主复本的名为 DB1 的数据库显示为 DB1 [AG1 primary]。请注意，数据库的名称以及可用性组名称及其可用性组复本角色仅在创建备份规范期间可见，而不是在已保存之后。

   在创建可用性组备份规范时，可以展开可用性组侦听程序以显示属于所选可用性组的可用性组复本客户机和数据库。但是，显示的客户机仅供参考，无法进行选择。只能选择要备份的数据库。

   可以通过右键单击所选的 Microsoft SQL Server 实例并选择“设置环境变量”来设置与 Data Protector Microsoft SQL Server 相关的环境变量。在“高级”对话框中，指定所需的变量及其值。单击“确定”以关闭对话框并将设置存储到 Microsoft SQL Server 配置文件中。请注意，环境变量会覆盖可在 omnirc 文件中在客户机范围内设置的 omnirc 选项。

   单击“下一步”。
8. 选择设备。单击“属性”以设置介质池和预分配策略。设备并发数设置为 1，且无法更改。有关选项的详细信息，请按 **F1**。

   要创建其他备份副本 (镜像)，请单击“添加镜像”/“删除镜像”以指定所需的数量。为每个镜像选择单独的设备。镜像的最小设备数等于用于备份的设备数。

   单击“下一步”。
9. 选择备份选项。

   单击“下一步”。
10. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

    单击“启动备份”启动备份规范。

SQL Server 的特定备份选项

通过单击“应用程序特定选项”组框中的“高级”，然后通过单击“MS SQL 集成”和“MS SQL 备份首选项”页面选择所需的选项来指定 SQL Server 的特定备份选项。

SQL Server 备份选项

Pre-exec	在备份之前，在 SQL Server 上指定带有参数的命令或由 sql_bar.exe 启动的脚本。位于默认的 Data Protector 命令目录中。在备份规范中仅文件名是必须提供的。

Post-exec	在备份之后，在 SQL Server 上指定带有参数的命令或由 sql_bar.exe 启动的脚本。位于默认的 Data Protector 命令目录中。在备份规范中仅文件名是必须提供的。	
并发流	设置用于备份的并发流数量，	
快速直接模式	用于本地连接的设备以优化性能。必须与特殊设备设置结合使用。	
检查数据库完整性	在备份之前执行数据完整性验证。如果检查失败，则会话完成，但有警告。	
SQL 备份压缩	指定 Data Protector 应该如何处理 Microsoft SQL Server 备份压缩。	
	SQL Server 设置 (默认)	根据 Microsoft SQL Server 的设置处理备份压缩。
	启用	不考虑 Microsoft SQL Server 的设置执行备份压缩。
	禁用	指定不应执行备份压缩而不考虑 Microsoft SQL Server 的设置。
从备份中排除 *(仅适用于独立实例备份)*	从备份中排除特定数据库。	
	可用性组数据库	从备份中排除属于任何可用性组的数据库。
	独立数据库	从备份中排除所有独立数据库。
	无 (默认)	不从备份中排除任何数据库。
选择备份首选项 *(仅适用于可用性组备份)*	**使用 SQL Server 设置** (默认)	按照 Microsoft SQL Server 设置执行备份。
	首选辅助复本	在可用性组辅助复本上执行可用性组数据库的备份。如果没有可用性组辅助复本可用，则在可用性组主复本上执行备份。
	仅辅助复本	在可用性组辅助复本上执行可用性组数据库的备份。如果没有可用性组辅助复本可用，则备份失败。
	主	在主复本上执行可用性组数据库的备份。
	任意复本	在可用性组中的任意可用性组复本上执行备份。
在主复本上强制进行完整备份和差异备份	选择此选项后，将始终使用可用性组主复本执行完全备份和差异备份，无论所选的备份首选项如何。“辅助副本优先”仅用于事务日志备份。 当备份属于可用性组辅助复本的数据库时，如果不选择此选项，则会执行仅副本完整备份，而不是完整备份或差异备份。	

注意不要在特定于对象的 pre-exec 和 post-exec 命令中使用双引号 (" ")。

特定于对象的选项

如果选择了一个或多个数据库进行备份 (而不是整个服务器备份)，则可以通过转到“备份规范摘要”属性页，双击对象或单击对象然后单击“属性...”，在单个数据库级别设置备份选项。

注意如果选择了整个服务器备份，则会显示与“应用程序特定选项”窗口中相同的选项。

特定于对象的选项

使用默认并发流	并发流的数量由 Data Protector 定义，并使用所有可用设备。	
并发流	设置并发流 (设备) 的数量。VDI 支持每个数据库最多 32 个虚拟设备。	
SQL 备份压缩	指定 Data Protector 应该如何处理 Microsoft SQL Server 备份压缩。	
	SQL Server 设置 (默认)	根据 Microsoft SQL Server 的设置处理备份压缩。
	启用	不考虑 Microsoft SQL Server 的设置执行备份压缩。
	禁用	指定不应执行备份压缩而不考虑 Microsoft SQL Server 的设置。
从备份中排除 *(仅适用于独立实例备份)*	从备份中排除特定数据库。	
	可用性组数据库	从备份中排除属于任何可用性组的数据库。
	独立数据库	从备份中排除所有独立数据库。
	无 (默认)	不从备份中排除任何数据库。

计划备份

您可以在特定时间或定期运行无人看管的备份。

> **注意**一段时间不活动后，防火墙会关闭 BSM 和 Inet 之间的连接。因此，建议在客户机上的 omnirc 文件中进行以下设置，以启用 keepalive 包，保持连接处于活动状态:
>
> - OB2IPCKEEPALIVE = 1
> - OB2IPCKEEPALIVETIME = 600
> - OB2IPCKEEPALIVEINTERVAL = 600
>
> 虽然在所有系统上都遵守 OB2IPCKEEPALIVE ，但某些系统可能不支持由 OB2IPCKEEPALIVETIME 和 OB2IPCKEEPALIVEINTERVAL 定义的按套接字的保持活动设置。Windows、Linux 系统: 支持 OB2IPCKEEPALIVE 和 OB2IPCKEEPALIVEINTERVAL ，HP-UX 系统: 仅支持 OB2IPCKEEPALIVETIME
> *其他系统*: 只能进行系统范围内的保持活动设置。要更改 TCP 保持活动设置，请参考相应的操作系统文档。

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS SQL Server”。右键单击要使用的备份规范，然后选择“启动备份”。
3. 选择“备份类型”和“网络负载”。有关这些选项的信息，请单击“帮助”。单击“确定”

性能调整

性能优化意味着自定义环境以提高备份和还原性能。请遵循以下指导:

1. 确保 SQL Server 数据库文件位于单独的磁盘上。
2. 计算要并行使用的设备数量。选择与传入数据流的带宽匹配的多个设备，并确定瓶颈。如果设备连接到远程系统，则可以是网络，如果设备是本地连接，则可以是 SQL Server。

   由于网络带宽通常为 ~10 MB/s (100 Mbit 以太网)，所以虽然实际吞吐量通常较低，但您不需要一个以上的快速设备 (例如用于远程备份的 DLT 7000)。

   本地连接设备有两种可能性:

   a. 设备专用于本地 SQL Server 备份，此时备份/还原性能非常重要。使用快速直接模式，字此模式下，Data Protector 可以直接从 SQL Server 共享内存中读取数据，提高本地设备的备份速度。

   b. 设备在 Data Protector 单元中共享，此时备份/还原性能不是很重要。禁用快速直接模式。

   通过备份到本地服务器上的几个空文件设备来确定最大备份速度，并选择最适于所测量性能的设备数。

   > **提示**为本地和远程设备创建单独的备份规范。建议不要在一个备份规范中同时使用它们。

3. 调整本地备份设备的块大小。
   - 启用/禁用“快速直接模式”。

     仅在需要最高性能时才使用此选项。由于特定的设备设置，不应与传统 (文件系统) 备份共享这些设备定义。因此，通常不建议使用此选项。

     如果备份性能不是非常关键和/或有其他数据备份到连接到 SQL Server 的设备，请禁用“快速直接模式”(以及特殊的本地设备设置)。

     > **注意**对于远程设备，忽略快速直接模式。

   - 设置块大小 (如果“快速直接模式”已启用)。

     调整后的块大小计算如下:

```
块大小 (kB) = 64*N + 4 (N=1,...,64) 块大小 (kB) = 68, 132, ..., 4100 kB
```

选择的所有设备必须具有相同的块大小。

通过指定大于默认值的块大小，可以获得一些性能改进。还可以逐步增加块大小，并比较每一步获得的性能。

通过选中附加的复选框并选择块大小，可以在本地设备的初始设备定义期间调整块大小。

可以稍后修改块大小；但是，必须首先使用上面的公式进行计算，然后插入“高级”选项中显示的值。

- 修改注册表。

  要使用大于 56 kB 的块大小，某些 SCSI 接口卡要求在设备所连接的系统的注册表中调整相关值。

4. 要修改现有设备的块大小:
   a. 切换到“设备和介质”上下文。

      在“范围窗格”中，展开“设备”，然后单击要修改的本地连接设备。在“结果区域”中，选择“设置”，然后单击“高级”。

   b. 在“高级选项”窗口中，单击“大小”。
5. 如果“快速直接模式”已激活，并且未对备份规范中的所有选定本地设备进行相应调整，则在保存备份规范时会收到警告:
6. 计划。

   备份计划取决于服务器上的事务数。通常，不应让事务日志文件增大到超过某个限制，这取决于特定的生产数据库及其事务日志文件的大小。以下是有关如何计划备份的一些一般规则:

   - 每周完整备份
   - 每日差异备份
   - 根据需要备份事务日志

   在服务器负载不重 (夜晚和周末) 时计划完整备份和差异备份。一天多次执行事务日志备份。

   必须根据实际的数据库配置做出最终计划决策。

更改和检查配置

可以使用 Data Protector GUI 或 CLI 检查和更改配置。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS SQL Server”。单击要更改其配置的备份规范。
3. 在“源”属性页中，右键单击 SQL Server 名称，然后选择“配置”。
4. 按照备份 Microsoft SQL Server 集成中的说明配置 SQL Server。
5. 右键单击 SQL Server，然后选择“检查配置”。

使用 Data Protector CLI

要更改配置，请再次执行配置 SQL Server 实例的命令，输入不同的数据。在可用性组配置中，请执行用于配置 SQL Server 可用性组的命令，输入不同的数据。

要检查独立实例的配置，请执行:

```
sql_bar chkconf [-instance:InstanceName]
```

如果未指定可选参数 -instance:InstanceName ，则检查默认实例。

要检查可用性组的配置，请执行:

```
sql_bar chkconf -ag agname –appsrv:ListenerName
```

如果未正确配置集成，则命令返回:

```
*RETVAL*8523
```

要获取有关独立实例的现有配置的信息，请执行:

```
sql_bar getconf [-instance:InstanceName]
```

如果未指定 -instance:InstanceName ，则 Data Protector 返回默认实例的配置。

要获取有关可用性组的现有配置的信息，请执行:

```
sql_bar getconf -ag agname –appsrv ListenerName
```

还原 Microsoft SQL Server 集成

This feature is available in the Premium Edition

Data Protector 会根据您的需要提供不同的还原类型。可以选择时间点还原、完整数据库还原，还可以将 SQL Server 数据还原到新位置、还原到其他 SQL Server 或其他 SQL Server 实例。

可以使用 Data Protector GUI 或 CLI 还原 SQL Server 数据库。

要恢复主数据库，请启动 SQL Server 灾难恢复过程。

- 验证要还原的数据库未在使用中。
- 在可用性组配置中，强制还原到其他客户机和实例。用户必须为“还原到另一个客户机”和“还原到另一个实例”字段选择具有适当值的还原选项。确保不为目标客户机选择可用性组侦听程序 (因为它不受支持)，并且目标客户机上存在所选的 SQL Server 实例。另请确保为还原选择的数据库不属于任何可用性组。
- 如果要还原的原始数据库仍存在于父实例中，则还原到另一个实例不起作用。如果还原到另一个实例需要成功，请确保已删除原始数据库或需要删除原始数据库。

使用 Data Protector GUI 进行还原

使用 Data Protector Manager 继续执行以下步骤:

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“还原对象”、“MS SQL Server”，然后选择要从中还原的 Microsoft SQL Server。此时将在“结果区域”中显示备份对象的列表。
3. 选择要还原的 SQL Server 对象。

   要还原文件组，请展开它并选择其中的所有数据文件。

   注意 在还原之前无需创建空数据库，因为数据库及其文件是由 SQL Server 自动生成的。

   重要说明必须先备份数据库的活动事务日志，然后才能还原数据文件。如果日志已损坏，则无法还原特定数据文件，并且只能还原整个数据库。

   注意选择要还原的数据文件意味着即使选择了数据库下的所有数据文件，也始终会执行文件还原。要还原整个数据库，用户应明确选择数据库级别。

   要选择特定于备份对象的选项，请右键单击该对象，然后选择“属性”。

   在“版本”选项卡中，选择要用于还原的备份版本 (备份日期) 或选择选项“还原到最新的可能状态”。后者始终还原备份链，就好像选择了“数据库的完整还原”选项一样。它包括完整、差异和事务日志备份。

   (可选) 在“高级”选项卡中，选择“以新名称还原数据库”选项并指定新的还原位置。

   重要说明在可用性组配置中，强制将数据库还原到其他位置。但是，如果数据库不属于任何可用性组，则可以使用相同的名称还原该数据库。

   根据需要选择其他还原选项。请注意，某些选项不可用于还原数据文件。

单击**确定**。

4. 在“选项”属性页中，如果要将数据还原到其他客户机或实例，请为数据库指定新位置。

> **重要说明**
>
> - 单击“选项”时，将浏览单元以运行可以成为还原的目标实例的 SQL Server 实例。如果未找到任何实例，则会禁用“还原到另一个实例”并显示消息“此客户机系统上不存在实例”。
> - 确保目标客户机上存在指定的 SQL Server 实例。否则，还原失败。

选择下列“还原操作”之一:

- **还原数据**。选择后会还原整个数据库。默认情况下选择此选项。
- **仅还原和显示文件列表**。如果不知道原始文件名，选择此选项。在这种情况下，将显示在特定会话中备份的文件。
- **仅还原和显示标头**。如果需要有关备份的特定详细信息，请选择此选项。显示 SQL Server 标头信息。

选择“启用结尾日志备份”后，将使用在下拉列表中选择的备份规范，在还原会话启动之前执行结尾日志备份会话。这将从尚未备份的结尾捕捉日志。在选择此选项之前，请确保:

- 已针对所有涉及的数据库选择**将数据库置为单用户模式 - 注销所有用户**选项。
- 选择**恢复数据**选项。

> **重要说明**将数据库还原到其他客户机或/和实例时，不建议启用结尾日志备份。因此，如果要使用可用性组配置还原备份的数据库，请不要选择“启用结尾日志备份”。

5. 在“设备”页中，选择要用于还原的设备。
6. 单击“还原 MS SQL Server”，然后单击“下一步”以选择“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
7. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

还原选项

Microsoft SQL Server 数据库还原选项

选项	描述
备份版本	指定将从中还原选定对象的备份会话。
时间点还原	此选项仅对数据库对象可用。 指定数据库状态将还原到的时间点 (还需要选择“备份版本”并设置“停止于”)。恢复后，数据库处于指定日期和时间所在的状态。 只有在指定的日期和时间之前写入的事务日志才应用于数据库。
停止在	此选项仅对数据库对象可用。 指定将停止前滚事务的具体时间。因此，要使数据库恢复到特定时间点，从中还原的备份必须是事务日志备份。不能将此选项与 **NORECOVERY** 或 **STANDBY** 一起使用。如果指定的“停止于”时间在“还原日志”操作结束后，则数据库处于未恢复状态 (如同使用 **NORECOVERY** 运行“还原日志”一样)。
仅还原此备份	如果还原了数据库版本并将其保留为不可操作或待机状态，则随后可以逐个还原差异或事务日志备份，从而使每个版本不可操作以还原其他备份。
完整还原数据库	还原所有必要的版本，其中包括最新完整备份、差异备份 (如果存在) 以及从差异备份直到所选版本为止的所有事务日志备份。
通过现有数据库进行强制还原	如果名称相同但内部结构不同的数据库已经存在于目标 Microsoft SQL Server 实例中，请选择此选项。 如果未选择此选项，则 Microsoft SQL Server 不允许覆盖现有的数据库，还原将失败。 如果从 PRIMARY 组将数据文件还原到现有数据库，则必须在数据文件级指定此选项。 使用此选项时，确保最近的日志已在还原前备份。

将数据库置为单用户模式 - 注销所有用户	断开连接到目标 Microsoft SQL Server 数据库的所有用户并将数据库设为单用户模式。请注意，如果数据库不处于简单恢复模式，则还应该选择“通过现有数据库进行强制还原”选项。
恢复完成状态	允许在恢复后选择数据库状态。可从以下选项中进行选择: • 使数据库可以继续运行。还原最后一个事务日志并完成恢复后，数据库即可运行。 • 在还原最后一个事务日志后不对数据库执行任何操作。您可以逐个还原其他事务日志。 • 将数据库保留为只读模式。您可以在数据库设置为读写模式之前还原其他事务日志。 此选项仅对数据库对象可用。
以新名称还原数据库	此选项仅对数据库对象可用。 以其他名称还原数据库。指定数据库逻辑文件名和目标文件名 (“将文件还原到新位置”的子选项)。
将文件还原到新位置	将文件还原到新位置。指定数据库逻辑文件名和指定逻辑文件名的目标文件名。使用此选项可将数据还原到其他客户机、其他实例或在同一客户机上复制数据库。
还原到最新的可能状态	还原整个备份链 (包括完整、差异和事务日志备份)。 默认情况下选择此选项。

要允许不同的还原方案，可以将常规还原选项 (例如，“将数据库还原到另一个 Microsoft SQL Server”和“使用不同设备还原”) 与对象特有的还原选项 (例如，“时间点还原”、“恢复完成状态”、“通过现有数据库进行强制还原”) 结合使用。

还原到其他 SQL Server 实例和/或其他 SQL Server

以下先决条件适用:

- 两个 SQL Server 必须具有相同的本地设置 (代码页和排序顺序)。此信息显示在每个备份的会话监视器中。
- 必须配置目标 SQL Server 并将其放置在与原始 SQL Server 相同的 Data Protector 单元中。

完成以下步骤：

1. 选择要还原的数据库及其版本。
2. 选择以下内容:
   - 要还原到其他 SQL Server 客户机，请从下拉列表中选择“还原到另一个客户机”和目标客户机。
   - 要还原到其他 SQL Server 实例，请选择“还原到另一个实例”。如果下拉列表中没有实例，请自行输入实例名称。确保目标客户机上存在指定的 SQL Server 实例。否则，还原失败。
3. 指定新的数据库位置。
4. 开始还原。

使用 Data Protector CLI 进行还原

执行：

```
omnir -mssql -barhost ClientName [-destination ClientName] [-instance SourceInstanceName] [-destinstance DestinationInstanceName] {-base DBName [-session BackupID] [MSSQL_OPTIONS]... | -base DBName -datafile GroupName/DataFileName -session BackupID [DATAFILE_OPTIONS]...}

MSSQL_OPTIONS

-asbase NewDBName {-file LogicalFileName1PhysicalFileName1 [-file LogicalFileName2PhysicalFileName2]...}

-replace

-nochain

-recovery {rec | norec}

-standby File

-tail_log BackupSpecificationName

DATAFILE_OPTIONS

-replace

-nochain

-recovery {rec | norec}
```

注意

- “BackupID”是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

  镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，必须指定原始“备份”会话的会话 ID (即备份 ID)，而不是“对象复制”会话的会话 ID。

  如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

- “SourceInstanceName”区分大小写；它必须与您在备份规范中指定的 SQL Server 实例的名称相同。

示例

要将在 SQL Server ALMA 上运行的数据库 RONA 还原到同一目标，请执行:

```
omnir -msssql -barhost ALMA -base RONA
```

要将在 SQL Server ALMA 上运行的数据库 RONA 的文件组 FILEGROUP_02 中的数据文件 DATAFILE_01 还原到同一目标，请执行:

```
omnir -MSSQL -barhost ALMA -base RONA -datafile FILEGROUP_02/DATAFILE_01 -session 2011/10/17-3
```

灾难恢复

灾难恢复是一个复杂的过程，涉及到来自不同供应商的产品。因此，需要查看数据库或应用程序供应商关于如何为灾难恢复做准备的说明。

作为第一步，执行灾难恢复中介绍的常规灾难恢复过程。接下来，还原 SQL Server 数据库。有关说明，请参阅以下小节。

重要说明

- 如果发生磁盘故障，请在执行任何其他恢复任务之前恢复操作系统。Data Protector 灾难恢复用于将操作系统恢复回受损系统。
- 重新安装 SQL Server 时，请确保使用原始本地设置。在还原到其他客户机之前，还要确保目标系统上的本地设置与原始设置一致。

恢复主数据库

主数据库保存有关 SQL Server 的重要信息。如果它被损坏或丢失，则所有其他数据库都将变为不可用。首先恢复主数据库以使 SQL Server 可运行:

1. 重建主数据库。

   创建基本主数据库:

   a. 如果 SQL Server 正在运行，请将其关闭。

   b. 启动“重建主数据库”实用程序 SQL\bin\rebuildm.exe 。

   c. 选择适当的字符集和排序顺序以匹配备份的数据。可以在最新的备份会话报告中检查此项。

   d. 重建数据库。

2. 设置用户权限或重新配置集成。

   使用 SQL Server 企业管理器设置用户权限:

   a. 启动 SQL Server 企业管理器。

   b. 右键单击所需的服务器，然后选择“注册服务器”。配置 SQL Server 以使用可信连接。

   c. 转到“安全 - 登录”然后选择适当的用户权限。

   d. 返回服务器，右键单击其名称，然后选择“注册服务器”。

在“管理 - 登录”中输入您选择的帐户。

执行运行 SQL Server 所需的任何其他管理任务。

按照创建 ZDB 备份规范中的说明重新配置 SQL Server 集成。

3. 以单用户模式启动 SQL Server 服务:
   a. 在“控制面板”中，转到“管理工具”、“服务”。
   b. 选择 MSSQL Server 服务。
   c. 停止服务。
   d. 输入 -m 作为启动参数并启动服务。
4. 使用 Data Protector Manager 还原主数据库。

重要说明要完成灾难恢复，还要还原“所有”其他数据库 (或者将磁盘上存在的数据库重新连接到最新重建的主数据库)。

恢复用户数据库

要还原用户数据库，请按还原 Microsoft SQL Server 集成中的说明继续操作。

请注意，将数据库还原到某个状态通常需要进行多阶段还原。这意味着需要还原多个版本才能检索数据。

如果采用以下备份序列:

- **F(斜体) F T(斜体)(粗体) T**: 要还原标记为 T 的版本，需还原所有斜体备份版本。通过 LSN 构建链。
- **F F(斜体) T(斜体) T(斜体)(粗体)**: 要还原标记为 T 的版本，需还原所有斜体备份版本。通过时间构建链。

当 Data Protector 无法通过 LSN 构造链时，按时间的旧公式仍按原来旧样应用。因此，必须还原最新的完整备份、最新的差异备份以及上一次完整或差异备份之后的所有事务日志备份。

示例

假设拥有以下备份序列:

F D T T D T T T *T* T

并要还原标记为 *T* 的版本，则将还原处于“斜体”的所有备份版本。

提示可以逐个还原版本，以便更好地控制还原过程。使用选项“仅还原此备份”和“恢复完成状态”来执行此操作。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话或查看以前的会话。运行交互式会话时，监视器窗口将显示会话进度。关闭 GUI 不会影响会话。

还可以从安装了“用户界面”组件的任何 Data Protector 客户机中，使用“监视器”上下文监视会话。

Microsoft SQL Server ZDB 集成

This feature is available in the Premium Edition

本主题介绍如何配置和使用 Data Protector Microsoft SQL Server 集成。其中说明了要备份和还原 Microsoft SQL Server (SQL Server) 数据库对象所需了解的概念和方法。

在备份期间，会生成 SQL Server 快照 (将冻结数据库文件，并缓存通往这些文件的事务)，因此数据库高度可用 (联机备份)。在创建复本 (拆分镜像磁盘或创建快照) 期间，数据库 I/O 处于暂挂状态。

SQL Server 快照是一个与 SQL Server 相关的术语，与磁盘阵列快照并不相同。

支持以下磁盘阵列和阵列配置:

支持的阵列	支持的配置
P9000 XP 磁盘阵列系列 (P9000 XP 阵列)	BC P9000 XP、CA P9000 XP、组合 CA+BC P9000 XP
存储阵列 (NetApp)	本地复制
存储阵列 (NetApp、Dell EMC Unity)	本地 + 远程复制

该集成支持所有 ZDB 类型 (ZDB 到磁带、ZDB 到磁盘和 ZDB 到磁盘 + 磁带)。

使用 Data Protector，您可以还原 SQL Server 数据:

- 从备份介质还原到 LAN 上的应用程序系统 (标准还原)。
- 使用即时恢复功能。

下表概述了 SQL Server 恢复方法:

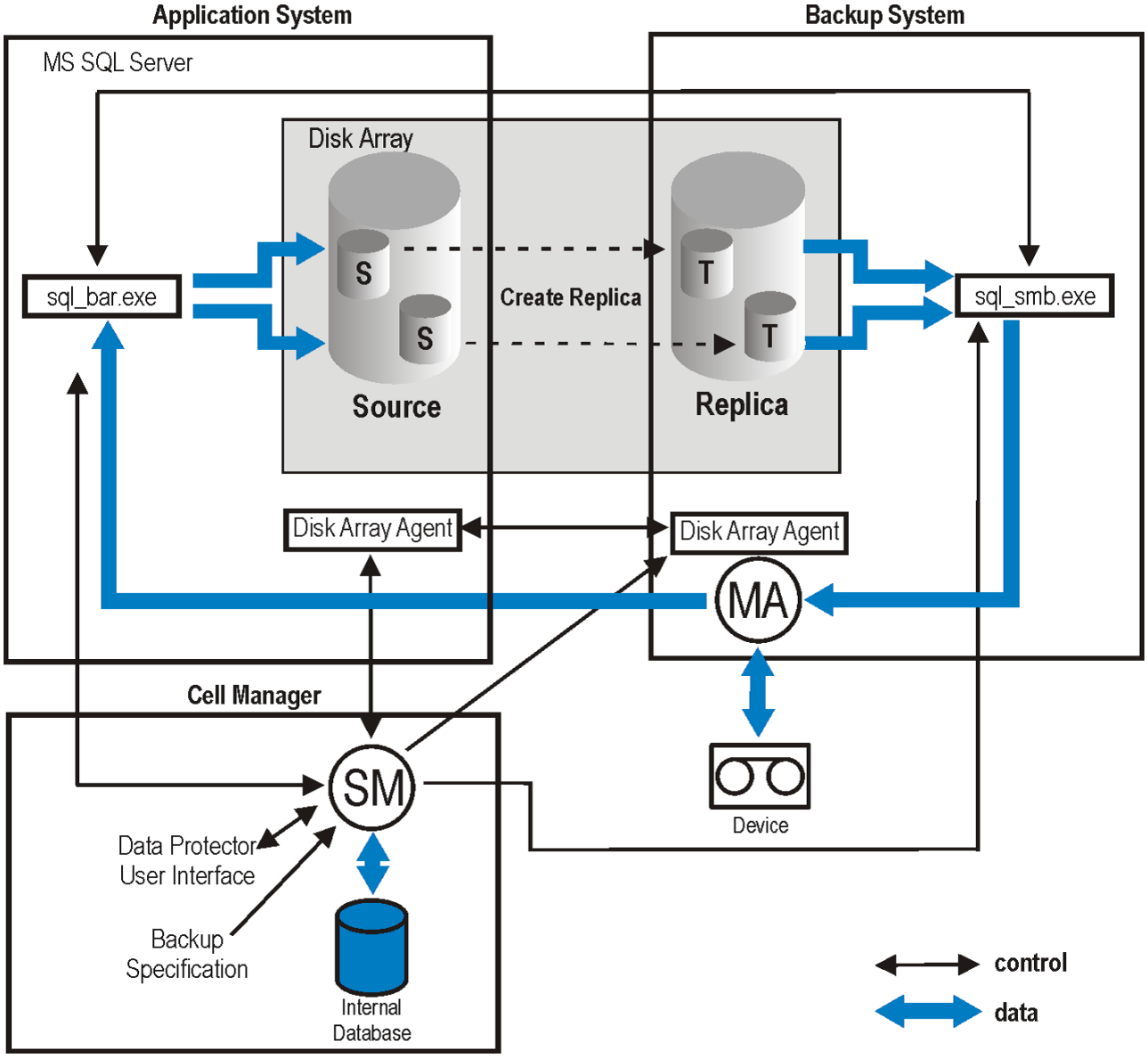
ZDB 类型	恢复方法
ZDB 到磁带	标准还原
ZDB 到磁盘	即时恢复
ZDB 到磁盘 + 磁带	标准还原、即时恢复

集成概念

Data Protector 通过安装在 SQL Server 上的 Data Protector sql_bar.exe 可执行文件与 SQL Server 集成。备份期间，在应用程序系统上启动的 sql_bar.exe 连接到 SQL Server 以查找数据库文件的位置。然后，该集成备份 SQL Server 数据库，这些数据库在磁盘阵列中替换。

还原期间， sql_bar.exe 连接到 SQL Server 以接收还原数据，该数据随后写入磁盘。

ZDB 过程取决于在拆分镜像还是快照替换中替换数据以及选定的 ZDB 类型。还原过程取决于还原类型 - 标准还原或即时恢复。


Application System
Backup System
MS SQL Server
Disk Array
S
S
Source
Create Replica
T
T
Replica
sql_bar.exe
sql_smb.exe
Disk Array Agent
Disk Array Agent
MA
Cell Manager
SM
Device
Data Protector
User Interface
Backup
Specification
Internal
Database
control
data

安装 Microsoft SQL Server ZDB 客户机

P9000 XP 与 Microsoft SQL Server 的集成

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- P9000 XP Agent
- MS SQL Integration

与 Microsoft SQL Server 的存储阵列集成

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- 在应用程序和备份系统上安装适用于存储阵列（NetApp Storage Provider）的存储提供程序
- MS SQL Integration – 仅在应用程序系统上

以下限制适用：

- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

配置 Microsoft SQL Server ZDB 集成

This feature is available in the Premium Edition

Data Protector SQL Server 配置文件

在以下系统中，Data Protector 为 Cell Manager 上的每个已配置 SQL Server 存储集成参数:

HP-UX 和 Linux 系统：

/etc/opt/omni/server/integ/config/MSSQL/ClientName%InstanceName

Windows 系统：

Data_Protector_program_data\Config\Server\Integ\Config\MSSQL\ClientName%InstanceName

配置参数是那些必须具有在 SQL Server 中运行备份和还原的权限 (假设使用标准安全性) 的 SQL Server 用户的用户名和密码。在集成配置期间，它们将写入 Data Protector SQL Server 配置文件。

配置文件的内容如下:

```
Login='user'; Password='encoded_password'; Domain='domain'; Port='PortNumber';
```

重要说明要避免备份问题，请确保配置文件的语法与示例一致。

示例

- *SQL Server 身份验证:*

  ```
  Login='sa'; Domain=''; Password='jsk74yh80fh43kdf';
  ```

- *Windows 身份验证:*

  ```
  Login='Administrator'; Domain='IPR'; Password='dsjf08m80fh43kdf';
  ```

- *集成身份验证:*

  ```
  Login=''; Domain=''; Password='kf8u3hdgtfh43kdf';
  ```

配置 SQL Server 群集

在群集中，必须将所有节点安装为 Data Protector 群集感知的客户机，并且所有节点上的 Data Protector Inet 服务必须在也具有群集管理员权限的 Windows 域用户帐户下运行。

您必须为所有群集节点配置 Data Protector Inet 服务用户模拟。必须对使用的 Windows 域用户帐户授予以下 Windows 操作系统安全策略特权：

- 身份验证后模拟客户机
- 替换进程级别令牌

配置 SQL Server 实例

在创建第一个备份规范期间配置 SQL Server 实例。此配置包括设置 Data Protector 连接到 SQL Server 实例时应使用的用户帐户。指定的登录信息保存到 Cell Manager 上的 Data Protector SQL Server 实例配置文件中。

注意确保要使用的用户帐户具有运行备份和还原的适当的 SQL Server 权限。使用 SQL Server 企业管理器检查权限。

可以按照配置集成中的说明更改配置。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS SQL Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 Microsoft SQL Server 备份”模板，然后指定备份类型。

   单击**确定**。
4. 指定特定于 ZDB 的选项。
5. 在“客户机”中，选择 SQL Server 系统。对于群集环境，选择 SQL Server 资源组的虚拟服务器。对于可用性组配置，选择相应可用性组的可用性组侦听程序。请注意，必须首先通过在“客户机”上下文中选择“虚拟主机”将可用性组侦听程序作为虚拟客户机导入。

   在“应用程序数据库”中，选择或指定 SQL Server 实例的名称。

   如果要使用“集成身份验证”并且希望备份会话在指定的操作系统用户帐户下运行，请指定“指定 OS 用户”选项。有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
6. 在“配置 MS SQL Server”对话框中，指定 Data Protector 要用于连接到 SQL Server 实例的用户帐户。
   - **SQL Server 身份验证**: SQL Server 用户帐户。指定用户名和密码。
   - **Windows 身份验证**: Windows 域用户帐户 (首选选项)。指定用户名、密码和域。
   - **集成身份验证**: 选择此选项可使 Data Protector 使用以下运行 SQL Server 系统上的 Data Protector Inet 服务的 Windows 域用户帐户连接到 SQL Server 实例。

   请确保您指定的用户帐户具有用于备份和还原 SQL Server 数据库的适当权限。

   > **注意**建议由 SQL Server 系统管理员配置集成。

   单击“确定”确认配置。
7. SQL Server 实例即已配置。退出 GUI 或继续在创建 ZDB 备份规范创建备份规范。

使用 Data Protector CLI

执行：

```
sql_bar config [-appsrv:SQLServerClient] [-instance:InstanceName] [-dbuser:SQLServerUser -password:password | -dbuser:WindowsUser -password:password -domain:domain]
```

参数描述

-appsrv:SQLServerClient	运行 SQL Server 实例的客户机系统。如果在本地执行命令，则不需要此选项。
-appsrv:ListenerName	可用性组侦听程序 (运行 SQL Server 可用性组的虚拟客户机) 的名称。
-instance:InstanceName	SQL Server 实例名称。如果省略此选项，则配置默认 SQL Server 实例。
-ag:AGname	SQL Server 可用性组名称。
-dbuser:SQLServerUser -password:password	SQL Server 用户帐户 (“SQL Server 身份验证”)
-dbuser:WindowsUser -password:password -domain:domain	Windows 域用户帐户 (“Windows 身份验证”)
-port:PortNumber	可用性组侦听程序用于连接到 SQL Server 的端口号。默认值为 1433。

> **注意**如果未指定用户帐户，则 Data Protector 使用“集成身份验证”。

消息 *RETVAL*0 表示配置成功。

备份 Microsoft SQL Server ZDB 集成

This feature is available in the Premium Edition

运行现有 SQL Server ZDB 规范的 ZDB:

- 使用 Data Protector 调度程序计划备份。
- 使用 Data Protector GUI 或 CLI 启动交互式备份。

创建 ZDB 规范

使用 Data Protector Manager 创建 ZDB 规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MS SQL Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 Microsoft SQL Server 备份”模板。

   从“备份类型”下拉列表中，选择“快照或拆分镜像备份”，然后从“子类型”下拉列表中选择适当的磁盘阵列代理。代理必须安装在应用程序系统和备份系统上。

   单击“确定”
4. 在“客户机系统”下，选择 SQL Server 系统。在群集环境中，选择 SQL Server 资源组的虚拟服务器。

   在“备份系统”下拉列表中，选择备份系统。

   选择磁盘阵列的其他特定备份选项。有关备份选项的详细信息，请按 **F1**。

   EMC:

   在 EMC GeoSpan for Microsoft 群集服务环境中，选择活动节点的备份系统并指定 TimeFinder 配置。

   将 EMC GeoSpan for MSCS 中的故障转移之后，选择当前活动节点的备份系统，然后保存备份规范。

   P9000 XP 阵列:

   要启用即时恢复，请保持选中“跟踪复本以用于即时恢复”。

   单击“下一步”。
5. 在“应用程序数据库”中，指定 SQL Server 实例的名称。

   如果要使用“集成身份验证”并且希望备份会话在指定的操作系统用户帐户下运行，请指定“指定 OS 用户”选项。有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
6. 如果未配置客户机，此时将显示“配置 MS SQL Server”对话框。按照配置 SQL Server 实例中的说明进行配置。
7. 选择要备份的数据库。
8. 选择要备份的数据库、文件组或数据文件。

   > **重要说明**要启用即时恢复，请为用户和系统数据库创建不同的备份规范。

   单击“下一步”。
9. 选择设备。单击“属性”以设置介质池和预分配策略。设备并发数设置为 1，且无法更改。有关选项的详细信息，请按 **F1**。

   要创建其他备份副本 (镜像)，请单击“添加镜像”/“删除镜像”以指定所需的数量。为每个镜像选择单独的设备。镜像的最小设备数等于用于备份的设备数。

   > **注意**不支持 ZDB 到磁盘的对象镜像。

   单击“下一步”。
10. 选择备份选项。

单击“下一步”。

11. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

    请注意，仅执行“完整”备份。

    单击“启动备份”启动备份规范。

SQL Server 的特定备份选项

通过单击“应用程序特定选项”组框页面中的“高级”，指定特定于 SQL Server 的备份选项。

SQL Server 备份选项

Pre-exec	在备份之前，在 SQL Server 上指定带有参数的命令或由 sql_bar.exe 启动的脚本。位于默认的 Data Protector 命令目录中。在备份规范中仅文件名是必须提供的。	
Post-exec	在备份之后，在 SQL Server 上指定带有参数的命令或由 sql_bar.exe 启动的脚本。位于默认的 Data Protector 命令目录中。在备份规范中仅文件名是必须提供的。	
并发流	设置用于将 SQL Server 数据库从复本备份到磁带的并发流数。适用于 ZDB 到磁带和 ZDB 到磁盘 + 磁带会话。	
快速直接模式	对于 ZDB 会话忽略该选项。	
检查数据库完整性	在备份之前执行数据完整性验证。如果检查失败，则会话完成，但有警告。	
SQL 备份压缩	指定 Data Protector 应该如何处理 Microsoft SQL Server 备份压缩。	
	SQL Server 设置 (默认)	根据 Microsoft SQL Server 的设置处理备份压缩。
	启用	不考虑 Microsoft SQL Server 的设置执行备份压缩。
	禁用	指定不应执行备份压缩而不考虑 Microsoft SQL Server 的设置。
从备份中排除 *(仅适用于独立实例备份)*	从备份中排除特定数据库。	
	可用性组数据库	从备份中排除属于任何可用性组的数据库。
	独立数据库	从备份中排除所有独立数据库。
	无 (默认)	不从备份中排除任何数据库。
	使用 SQL Server 设置 (默认)	按照 Microsoft SQL Server 设置执行备份。

> **注意**不要在特定于对象的 pre-exec 和 post-exec 命令中使用双引号 (" ")。

计划备份

您可以在特定时间或定期运行无人看管的 ZDB。

> **注意**如果在备份规范中未选择“跟踪复本以用于即时恢复”，则无法运行 ZDB 到磁盘或 ZDB 到磁盘 + 磁带。

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS SQL Server”。右键单击要使用的备份规范，然后选择“启动备份”。
3. 选择“网络负载”。有关网络负载的信息，请单击“帮助”。单击“确定”

   对于 ZDB 会话，备份类型设置为“完整”。

   对于 ZDB 到磁盘或 ZDB 到磁盘 + 磁带，请指定“拆分镜像/快照备份”选项。

使用 Data Protector CLI

要启动 ZDB 到磁带或 ZDB 到磁盘 + 磁带，请执行以下操作:

```
omnib -mssql_list ListName
```

要启动 ZDB 到磁盘，请执行以下操作:

```
omnib -mssql_list ListName -disk_only
```

其中， ListName 是备份规范的名称。

性能调整

性能优化意味着自定义环境以提高备份和还原性能。请遵循以下指导:

1. 确保 SQL Server 数据库文件位于单独的磁盘上。
2. 计算要并行使用的设备数量。选择与传入数据流的带宽匹配的多个设备，并确定瓶颈。如果设备连接到远程系统，则可以是网络，如果设备是本地连接，则可以是 SQL Server。

   由于网络带宽通常为 ~10 MB/s (100 Mbit 以太网)，所以虽然实际吞吐量通常较低，但您不需要一个以上的快速设备 (例如用于远程备份的 DLT 7000)。

   本地连接设备有两种可能性:

   a. 设备专用于本地 SQL Server 备份，此时备份/还原性能非常重要。使用快速直接模式，字此模式下，Data Protector 可以直接从 SQL Server 共享内存中读取数据，提高本地设备的备份速度。

   b. 设备在 Data Protector 单元中共享，此时备份/还原性能不是很重要。禁用快速直接模式。

   通过备份到本地服务器上的几个空文件设备来确定最大备份速度，并选择最适于所测量性能的设备数。

   > **提示**为本地和远程设备创建单独的备份规范。建议不要在一个备份规范中同时使用它们。

3. 调整本地备份设备的块大小。
   - 启用/禁用“快速直接模式”。

     仅在需要最高性能时才使用此选项。由于特定的设备设置，不应与传统 (文件系统) 备份共享这些设备定义。因此，通常不建议使用此选项。

     如果备份性能不是非常关键和/或有其他数据备份到连接到 SQL Server 的设备，请禁用“快速直接模式”(以及特殊的本地设备设置)。

     > **注意**对于远程设备，忽略快速直接模式。

   - 设置块大小 (如果“快速直接模式”已启用)。

     调整后的块大小计算如下:

     ```
     块大小 (kB) = 64*N + 4 (N=1,...,64) 块大小 (kB) = 68, 132, ..., 4100 kB
     ```

     选择的所有设备必须具有相同的块大小。

     通过指定大于默认值的块大小，可以获得一些性能改进。还可以逐步增加块大小，并比较每一步获得的性能。

     通过选中附加的复选框并选择块大小，可以在本地设备的初始设备定义期间调整块大小。

     可以稍后修改块大小；但是，必须首先使用上面的公式进行计算，然后插入“高级”选项中显示的值。

   - 修改注册表。

     要使用大于 56 kB 的块大小，某些 SCSI 接口卡要求在设备所连接的系统的注册表中调整相关值。

4. 要修改现有设备的块大小:

   a. 切换到“设备和介质”上下文。

   在“范围窗格”中，展开“设备”，然后单击要修改的本地连接设备。在“结果区域”中，选择“设置”，然后单击“高级”。

   b. 在“高级选项”窗口中，单击“大小”。

5. 如果“快速直接模式”已激活，并且未对备份规范中的所有选定本地设备进行相应调整，则在保存备份规范时会收到警告:
6. 计划。

   备份计划取决于服务器上的事务数。通常，不应让事务日志文件增大到超过某个限制，这取决于特定的生产数据库及其事务日志文件的大小。以下是有关如何计划备份的一些一般规则:

   - 每周完整备份
   - 每日差异备份
   - 根据需要备份事务日志

   在服务器负载不重 (夜晚和周末) 时计划完整备份和差异备份。一天多次执行事务日志备份。

   必须根据实际的数据库配置做出最终计划决策。

更改和检查配置

可以使用 Data Protector GUI 或 CLI 检查和更改配置。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“MS SQL Server”。单击要更改其配置的备份规范。
3. 在“源”属性页中，右键单击 SQL Server 名称，然后选择“配置”。
4. 按照备份 Microsoft SQL Server 集成中的说明配置 SQL Server。
5. 右键单击 SQL Server，然后选择“检查配置”。

使用 Data Protector CLI

要更改配置，请再次执行配置 SQL Server 实例的命令，输入不同的数据。在可用性组配置中，请执行用于配置 SQL Server 可用性组的命令，输入不同的数据。

要检查配置，请执行以下命令:

```
sql_bar chkconf [-instance:InstanceName]
```

如果未指定可选参数 -instance:InstanceName ，则检查默认实例。

如果未正确配置集成，则命令返回:

```
*RETVAL*8523
```

要获取有关独立实例的现有配置的信息，请执行:

```
sql_bar getconf [-instance:InstanceName]
```

如果未指定 -instance:InstanceName ，则 Data Protector 返回默认实例的配置。

还原 Microsoft SQL Server ZDB 集成

This feature is available in the Premium Edition

Data Protector 提供从备份介质到 LAN 上的应用程序系统的还原 (标准还原)，可以根据还原方案和即时恢复选择各种还原选项。有关详细信息，请参阅以下小节。

- 验证要还原的数据库未在使用中。
- 在可用性组配置中，强制还原到其他客户机和实例。用户必须为“还原到另一个客户机”和“还原到另一个实例”字段选择具有适当值的还原选项。确保不为目标客户机选择可用性组侦听程序 (因为它不受支持)，并且目标客户机上存在所选的 SQL Server 实例。另请确保为还原选择的数据库不属于任何可用性组。

标准还原

注意 在还原之前无需创建空数据库，因为数据库及其文件是由 SQL Server 自动生成的。

使用 Data Protector Manager 继续执行以下步骤:

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“还原对象”、“MS SQL Server”，然后选择要从中还原的客户机 (备份系统)。此时将在“结果区域”中显示备份对象的列表。
3. 选择要还原的 SQL Server 对象。

   注意选择要还原的数据文件意味着即使选择了数据库下的所有数据文件，也始终会执行文件还原。要还原整个数据库，用户应明确选择数据库级别。

   要选择特定于备份对象的选项，请右键单击该对象，然后选择“属性”。

   在“版本”选项卡中，选择要用于还原的备份版本 (备份日期)。

   根据需要选择其他还原选项。请注意，某些选项不可用于还原数据文件。

   单击**确定**。
4. 在“选项”属性页中，如果要将数据还原到其他客户机或实例，请为数据库指定新位置。

   重要说明

   - 单击“选项”时，将浏览单元以运行可以成为还原的目标实例的 SQL Server 实例。如果未找到任何实例，则会禁用“还原到另一个实例”并显示消息“此客户机系统上不存在实例”。
   - 确保目标客户机上存在指定的 SQL Server 实例。否则，还原失败。

   选择下列“还原操作”之一:

   - **还原数据**。选择后会还原整个数据库。默认情况下选择此选项。
   - **仅还原和显示文件列表**。如果不知道原始文件名，选择此选项。在这种情况下，将显示在特定会话中备份的文件。
   - **仅还原和显示标头**。如果需要有关备份的特定详细信息，请选择此选项。显示 SQL Server 标头信息。

   选择“启用结尾日志备份”后，将使用在下拉列表中选择的备份规范，在还原会话启动之前执行结尾日志备份会话。这将从尚未备份的结尾捕捉日志。在选择此选项之前，请确保:
5. 在“设备”页中，选择要用于还原的设备。
6. 单击“还原 MS SQL Server”，然后单击“下一步”以选择“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。

7. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

还原选项

Microsoft SQL Server 数据库还原选项

选项	描述
备份版本	指定将从中还原选定对象的备份会话。
时间点还原	此选项仅对数据库对象可用。 指定数据库状态将还原到的时间点 (还需要选择“备份版本”并设置“停止于”)。恢复后，数据库处于指定日期和时间所在的状态。 只有在指定的日期和时间之前写入的事务日志才应用于数据库。
停止在	此选项仅对数据库对象可用。 指定将停止前滚事务的具体时间。因此，要使数据库恢复到特定时间点，从中还原的备份必须是事务日志备份。不能将此选项与 **NORECOVERY** 或 **STANDBY** 一起使用。如果指定的“停止于”时间在“还原日志”操作结束后，则数据库处于未恢复状态 (如同使用 **NORECOVERY** 运行“还原日志”一样)。
仅还原此备份	如果还原了数据库版本并将其保留为不可操作或待机状态，则随后可以逐个还原差异或事务日志备份，从而使每个版本不可操作以还原其他备份。
完整还原数据库	还原所有必要的版本，其中包括最新完整备份、差异备份 (如果存在) 以及从差异备份直到所选版本为止的所有事务日志备份。
通过现有数据库进行强制还原	如果名称相同但内部结构不同的数据库已经存在于目标 Microsoft SQL Server 实例中，请选择此选项。 如果未选择此选项，则 Microsoft SQL Server 不允许覆盖现有的数据库，还原将失败。 如果从 PRIMARY 组将数据文件还原到现有数据库，则必须在数据文件级指定此选项。 使用此选项时，确保最近的日志已在还原前备份。
将数据库置为单用户模式 - 注销所有用户	断开连接到目标 Microsoft SQL Server 数据库的所有用户并将数据库设为单用户模式。请注意，如果数据库不处于简单恢复模式，则还应该选择“通过现有数据库进行强制还原”选项。
恢复完成状态	允许在恢复后选择数据库状态。可从以下选项中进行选择: • 使数据库可以继续运行。还原最后一个事务日志并完成恢复后，数据库即可运行。 • 在还原最后一个事务日志后不对数据库执行任何操作。您可以逐个还原其他事务日志。 • 将数据库保留为只读模式。您可以在数据库设置为读写模式之前还原其他事务日志。 此选项仅对数据库对象可用。
以新名称还原数据库	此选项仅对数据库对象可用。 以其他名称还原数据库。指定数据库逻辑文件名和目标文件名 (“将文件还原到新位置”的子选项)。
将文件还原到新位置	将文件还原到新位置。指定数据库逻辑文件名和指定逻辑文件名的目标文件名。使用此选项可将数据还原到其他客户机、其他实例或在同一客户机上复制数据库。

要允许不同的还原方案，可以将常规还原选项 (例如，“将数据库还原到另一个 Microsoft SQL Server”和“使用不同设备还原”) 与对象特有的还原选项 (例如，“时间点还原”、“恢复完成状态”、“通过现有数据库进行强制还原”) 结合使用。

还原到其他 SQL Server 实例和/或其他 SQL Server

以下先决条件适用:

- 两个 SQL Server 必须具有相同的本地设置 (代码页和排序顺序)。此信息显示在每个备份的会话监视器中。
- 必须配置目标 SQL Server 并将其放置在与原始 SQL Server 相同的 Data Protector 单元中。

完成以下步骤：

1. 选择要还原的数据库及其版本。
2. 选择以下内容:
   - 要还原到其他 SQL Server 客户机，请从下拉列表中选择“还原到另一个客户机”和目标客户机。
   - 要还原到其他 SQL Server 实例，请选择“还原到另一个实例”。如果下拉列表中没有实例，请自行输入实例名称。确保目标客户机上存在指定的 SQL Server 实例。否则，还原失败。
3. 指定新的数据库位置。
4. 开始还原。

如果采用以下备份序列:

- **F(斜体) F T(斜体)(粗体) T**: 要还原标记为 T 的版本，需还原所有斜体备份版本。通过 LSN 构建链。
- **F F(斜体) T(斜体) T(斜体)(粗体)**: 要还原标记为 T 的版本，需还原所有斜体备份版本。通过时间构建链。

当 Data Protector 无法通过 LSN 构造链时，按时间的旧公式仍按原来旧样应用。因此，必须还原最新的完整备份、最新的差异备份以及上一次完整或差异备份之后的所有事务日志备份。

即时恢复

以下先决条件适用:

对于 NetApp 和 Dell EMC Unity 阵列，以下是 MS SQL 的先决条件 (独立):

- 如果还原用户数据库，请将数据库置于脱机状态:
  1. 启动 SQL Server 企业管理器。
  2. 选择数据库，然后单击“操作”。
  3. 选择所有任务并将其置于脱机状态。
- 如果还原系统数据库，请通过启动 SQL Server 企业管理器，右键单击 SQL Server，然后单击“停止”使 SQL Server 脱机。

  在 NetApp 和 Dell EMC Unity 上进行 MS SQL 群集即时恢复的先决条件:

  1. 关闭数据库。
  2. 将与 SQL 数据库相关的群集磁盘置于维护模式。
  3. 将 omnirc 变量 SMISA_FORCE_DISMOUNT 设置为 1。
  4. 运行 IR 还原。
  5. 退出维护模式。
  6. 登录 SQL Server 并检查数据库状态是否为“联机”。

使用 Data Protector Manager 执行即时恢复:

1. 在“上下文列表”中，单击“即时恢复”。
2. 展开“MS SQL Server”，然后选择要从中还原的备份会话 (复本)。默认情况下，数据库将执行恢复，直到上次备份的事务为止。
3. 将用户数据库恢复到特定的时间点:
   a. 在“源”属性页中的“还原对象”下，右键单击数据库，然后单击“属性”。
   b. 在“备份版本”下拉列表中，选择所需的复本。默认情况下选择最新版本。

      选择“时间点还原”。从“停止于”下拉列表中，选择应该应用事务的时间点，然后单击“确定”。如果没有可用的事务日志，则此选项禁用。

      要以其他名称还原数据库，请单击“高级”，然后选择“以新名称还原数据库”。

      > **重要说明**如果未列出逻辑文件名和物理文件名，则将其添加到列表。指定与 ZDB 所用相同的名称；否则，即时恢复失败。

4. 单击“还原 MS SQL Server”。

   如果还原系统数据库，则 SQL Server 显示错误，因为其服务处于脱机状态。因此，还原完成后，使用 SQL Server 企业管理器手动启动 SQL Server。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话或查看以前的会话。运行交互式会话时，监视器窗口将显示会话进度。关闭 GUI 不会影响会话。

还可以从安装了“用户界面”组件的任何 Data Protector 客户机中，使用“监视器”上下文监视会话。

Microsoft Volume Shadow Copy Service

This feature is available in the Premium Edition

传统的备份过程基于备份应用程序与备份其数据的应用程序之间的直接通信。此备份方法要求备份应用程序为其备份的每个应用程序提供一个单独的接口。为了应对应用程序及其特定接口越来越多的问题，在 Microsoft Windows 系统上的备份和还原过程的参与程序之间引入了一种新的协调程序 -“Microsoft 卷影复制服务”。

Data Protector 通过 Data Protector Microsoft 卷影复制服务集成 (“VSS 集成”) 与卷影复制服务集成。

Data Protector 与 Microsoft 卷影复制服务集成可提供两个功能:

- 支持认证的 VSS 写入程序。有关受支持的 VSS 写入程序和提供程序的完整列表，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。
- 构成其他集成的基础，如 Data Protector Microsoft Exchange Server 2010 集成。

本节介绍如何使用通用 Data Protector VSS 集成来备份和还原写入程序的数据。有关基于 VSS 技术的应用程序集成的说明，请参阅相应的章节。

使用 VSS 集成的好处

使用 Data Protector VSS 集成的好处包括:

- 为提供写入程序的所有应用程序提供统一备份接口。
- 在应用程序级别提供数据完整性，因为它由写入程序提供。备份应用程序无需干预。
- 由于编程和用户界面的通用特性，即使在最初的 Data Protector 发布之后，也可以更轻松地添加对新应用程序、应用程序版本或磁盘阵列 (例如通过认证等) 的支持。

  另一方面，*应用程序集成* (如 Data Protector Exchange Server 2010 集成) 可提供更多功能，并且比通用 VSS 集成能更好地适合应用程序细节。但是，由于其他实现细节，与通过通用 Data Protector VSS 集成添加支持相比，开发此类集成可能需要更长时间。

集成概念

Data Protector VSS 集成使用 Microsoft 卷影复制服务和虚拟磁盘服务接口以及 VSSBAR 代理来执行应用程序数据的备份和还原。

备份类型

可用备份类型取决于所使用的 VSS 提供程序的类型及其功能:

- 使用软件提供程序，可以将数据备份到磁带 (“标准的 Data Protector 备份到磁带”)。这只能在创建卷影副本的同一系统上完成。
- 使用硬件提供程序，可以创建目标卷，可用于备份到磁带或进行即时恢复。此类备份是 Data Protector 零宕机时间备份 (ZDB)，其中硬件提供程序替换通常复制卷的磁盘阵列代理。因此，要在使用 Data Protector VSS 集成时创建 ZDB 备份规范，必须始终选择硬件提供程序。有关 ZDB (拆分镜像或快照备份) 和即时恢复概念的一般说明，请参阅《Data Protector 概念指南》。

  复本所驻留的以及从中将复本备份到磁带的备份系统可以是:

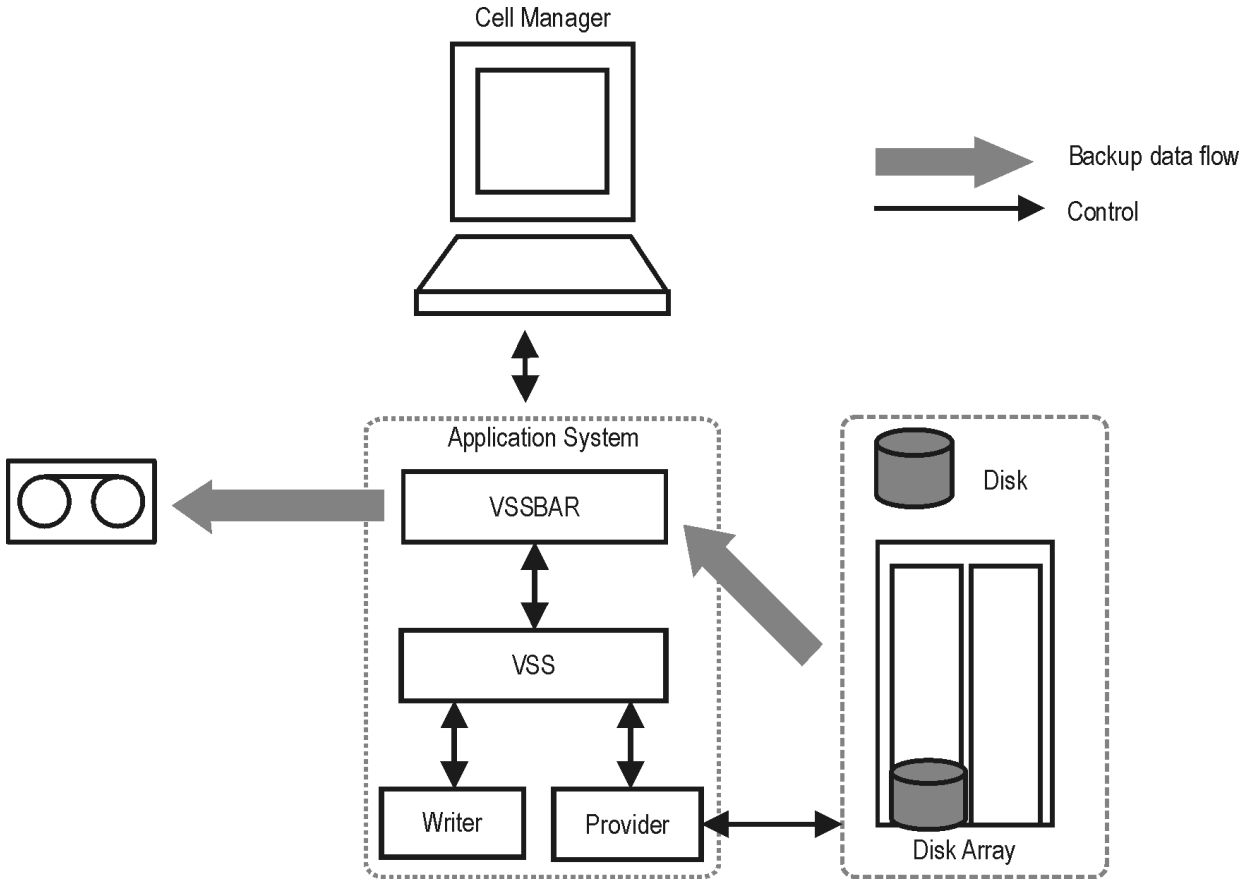
  - 专用系统 (Data Protector ZDB 术语: 双主机配置)。

    在 VSS 术语中，在此类环境中执行的备份为“可传输备份”。它只能与硬件提供程序结合使用。
  - 与应用系统相同的系统 (Data Protector ZDB 术语: 单主机配置)。

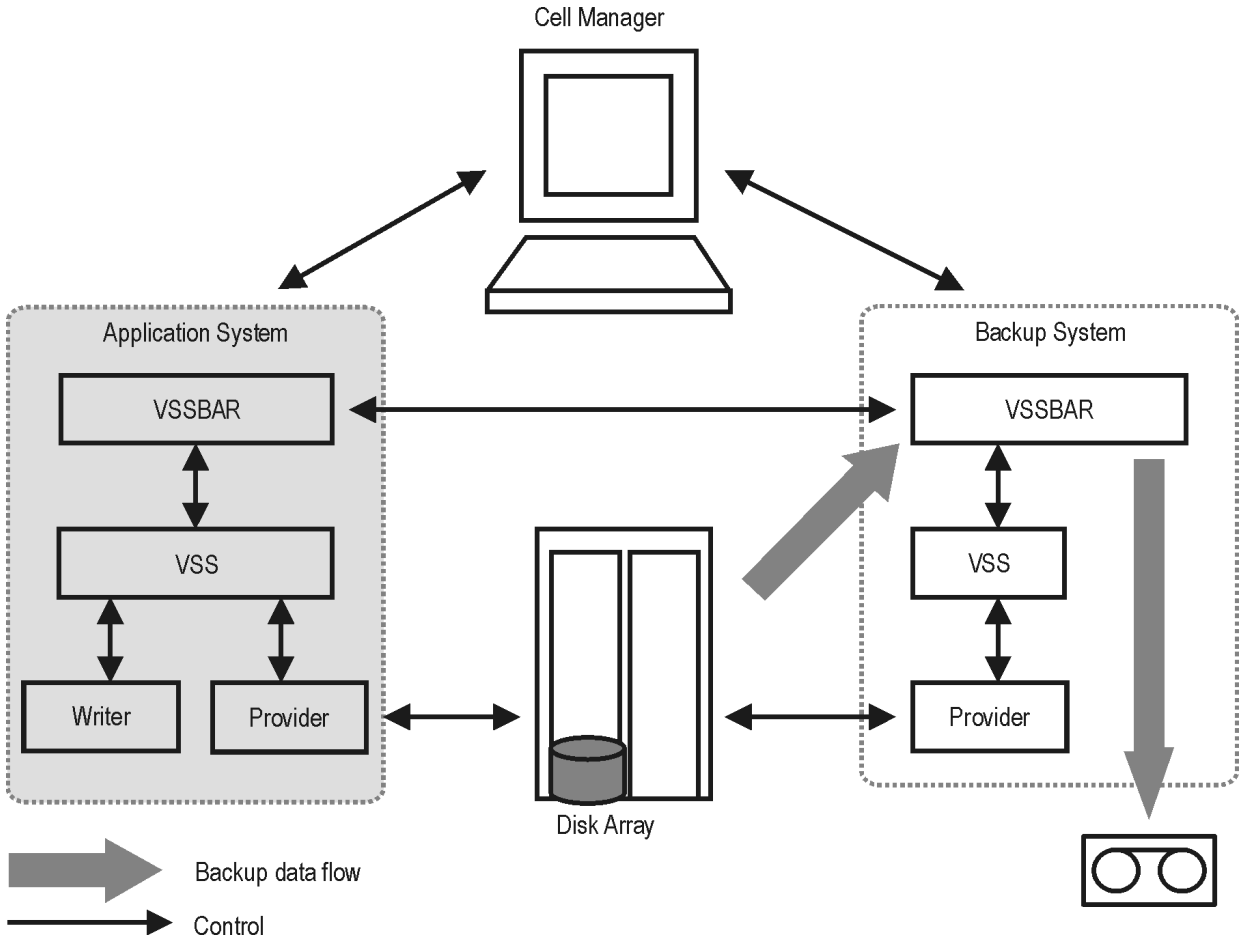
    在 VSS 术语中，在此类环境中执行的备份为“本地或网络备份”。

  本地 VSS 备份显示本地 VSS 备份的组件之间的关系。可传输 VSS 备份显示可传输 VSS 备份的组件之间的关系。

  本地 VSS 备份


Cell Manager
Backup data flow
Control
Application System
VSSBAR
VSS
Writer
Provider
Disk
Disk Array

可传输 **VSS** 备份


Cell Manager
Application System
VSSBAR
VSS
Writer
Provider
Backup System
VSSBAR
VSS
Provider
Disk Array
Backup data flow
Control

VSS 数据库

VSS 数据库 (VSSDB) 是对 Cell Manager 上的 Data Protector 内部数据库 (IDB) 的扩展。它保存有关 VSS 备份会话及其复本的特定于 VSS 集成的信息。存储的信息可用于以下目的:

- 即时恢复
- 数据挖掘 (可以保存备份组件和写入程序元数据文档)
- 列出备份会话并查看有关它们的详细信息
- 删除备份会话
- 启用 (呈现和装载) 和禁用 (卸除和隐藏) ZDB 到磁盘和 ZDB 到磁盘+磁带会话的复本

VSSDB 可保存 VSS 会话的元数据。此元数据存储在 VSSDB 的两个部分中: 永久部分和非永久部分。“永久”部分保存有关所有备份会话的信息，而“非永久”部分仅保存有关支持即时恢复的会话 (ZDB 到磁盘和 ZDB 到磁盘 + 磁带会话) 的信息。在来自支持即时恢复的会话的复本从复本集循环出来后，将从 VSSDB 的非永久部分删除有关会话的信息，并从磁盘阵列中删除会话的目标卷。有关会话的信息在 VSSDB 的永久部分中仍可用，并且只能使用 omnidbvss 命令手动删除。请注意，ZDB 到磁带会话和使用软件提供程序创建的会话始终仅记录到 VSSDB 的永久部分。

您可以使用 omnidbvss 命令查询和管理 VSSDB 的项目。有关命令语法、说明和示例的信息，请参阅《Data Protector 命令行界面参考》。

可以使用 omnidbvss 命令执行以下任务:

- 查询 VSSDB
- 删除备份会话
- 启用和禁用复本

查询 VSSDB

使用 omnidbvss 命令，可以列出:

- 所有备份会话及其详细信息。
- 基于特定备份规范的所有备份会话及其详细信息。
- 在指定日期之前创建的，记录在 VSSDB 永久部分中的所有备份会话，以及其详细信息。
- 有关特定备份会话的详细信息，由会话 ID 标识。

使用 omnidbvss 命令，可以将有关备份组件和写入程序元数据的文档保存到指定目录。

有关命令语法和示例，请参阅 omnidbvss 手册页。

删除备份会话

使用 omnidbvss 命令，可以删除:

- 由会话 ID 标识的特定支持即时恢复的备份会话 (复本版本)，从 VSSDB 的非永久部分和磁盘阵列中，或仅从 VSSDB 中删除。
- 基于特定备份规范 (复本集) 的所有支持即时恢复的备份会话，从 VSSDB 的非永久部分和磁盘阵列中，或仅从 VSSDB 中删除。
- 由会话 ID 标识的特定备份会话，从 VSSDB 的永久部分中删除。
- 基于特定备份规范的所有备份会话或在指定日期之前创建的会话，从 VSSDB 的永久部分中删除。

有关命令语法和示例，请参阅 omnidbvss 手册页。

启用和禁用复本

使用 omnidbvss 命令，您可以在备份系统上呈现和装载 (启用)，以及从备份系统卸除和隐藏 (禁用) 以下会话中的复本:

- 所有支持即时恢复的会话。
- 特定支持即时恢复的会话，由会话 ID 标识。
- 所有基于特定备份规范的支持即时恢复的会话。

环境变化

在使用 omnidbvss 命令 (删除、禁用、启用) 的 VSS 即时恢复会话或 VSSDB 维护会话期间，将在还原、删除、禁用和启用操作之前检查复本中目标卷的状态。在还原之前，还会检查应用程序系统上的源卷的状态。如果检查发现 VSSDB 中存在未跟踪到的任何更改，则会中止会话，通知您特定的更改。通过将 OB2VSS_IGNORE_BACKUP_DISK_CHANGES 和 OB2VSS_IGNORE_SOURCE_DISK_CHANGES omnirc 选项设置为 1，可以禁用

此检查。

在 VSS 备份会话期间，将创建复本并将其留在磁盘阵列上，直到达到指定循环的复本数。随后，要创建的下一复本会替换集合中最旧的复本。如果因为您手动 (未使用 Data Protector) 从备份系统中隐藏复本并将其呈现在某个其他系统上，而无法替换集合中最旧的副本，则备份会话将继续并创建新复本，并将旧复本留在阵列上。请注意，在这种情况下，如果磁盘阵列上没有用于创建新复本的空间，则备份会话也会失败。

如果将 OB2VSS_IGNORE_BACKUP_DISK_CHANGES omnirc 选项设置为 1 ，则备份会话将继续删除旧复本并在其位置上创建新复本。

安装 Microsoft 卷影复制服务客户机

This feature is available in the Premium Edition

要备份 VSS 写入程序或者只有文件系统使用 VSS，请在应用程序系统（*本地备份*）或同时在应用程序和备份系统（*可传输备份*）上安装以下 Data Protector 软件组件：

- MS Volume Shadow Copy Integration。
- 如果要使用磁盘阵列（包含硬件提供程序），则相应的磁盘阵列代理为：P4000 VSS Agent、P6000/3PAR SMI-S 代理、P9000 XP 代理或 3PAR VSS 代理。
- 对于 Data Protector Express，VEPA（虚拟环境代理）组件需要 VSS 组件才能支持 Hyper-V 备份和还原。不支持 VSS 集成备份或还原。

要执行“ZDB 到磁盘 + 磁带”或“ZDB 到磁带”会话，请在备份系统上另外安装以下 Data Protector 软件组件:

- General Media Agent

安装 VSS 集成之后，如果要执行 ZDB 到磁盘和 ZDB 到磁盘 + 磁带会话（支持即时恢复的会话），则需要解析应用程序系统上的源卷。如下从单元中的任何 VSS 客户机上运行解析操作：

```
omnidbvss –resolve {–apphost ApplicationSystem | –all}
```

但是，如果不进行解析或未能解析应用程序系统，则只要 omnirc 文件中的 OB2VSS_DISABLE_AUTO_RESOLVE 选项设置为 0（默认值），就会自动对它进行解析。在这种情况下，创建复本的备份时间会延长。

满足 Microsoft 卷影复制服务的先决条件

This feature is available in the Premium Edition

以下是 Microsoft 卷影复制服务集成的先决条件:

- 在开始之前，确保已正确安装和配置 Data Protector、写入程序。如果要执行 ZDB，还需安装和配置 VSS 和 VDS 硬件提供程序。
  - 请参阅 Web 上的最新支持矩阵，以获得受支持版本、平台、设备、磁盘阵列、限制的最新列表及其他信息。
  - 写入程序和卷影副本提供程序文档，以获得有关如何在系统上安装和配置写入程序和提供程序的说明。
- 安装任何所需的 Microsoft Windows 补丁或修补程序。

以下限制适用：

- 不支持预览以下任一类型的 VSS 会话：备份、还原、零宕机时间备份和即时恢复。
- DPM“数据库写入程序”组件不能使用“将文件还原到临时位置”模式。由于这些文件已由另一写入程序（在此情况下是指 MSDE 写入程序）进行备份，因此未显示在还原页面中。在这些情况下，只能使用“还原组件”模式。
- Microsoft SQL Writer 不支持将 Microsoft SQL 数据库还原到其他系统。如果尝试执行还原，则只能还原文件。
- 要运行 VSS 集成备份，写入程序的数据必须位于 NTFS 文件系统上。对于硬件提供商，这不是必需的。
- 不支持对将数据存储在网络共享卷上的写入程序进行 VSS 集成备份。
- Data Protector Microsoft VSS 集成没有为请求自定义还原方法的写入程序提供任何还原方法。默认情况下，Data Protector 不显示这些写入程序。
- 如果写入程序指定了自定义还原方法，则只能使用 Data Protector 功能将写入程序的数据还原为纯文件。可以手动执行自定义还原。有关还原方法的其他信息，请参阅写入程序文档。
- 备份预览仅适用于 VSS 文件系统备份会话。
- 动态磁盘 (逻辑磁盘管理器分区) 只能使用软件提供程序备份。
- Data Protector MS 卷影复制集成会跳过重新分析点。但通过 Microsoft 卷重复数据删除操作删除了重复数据的文件例外，其重新分析标记为 IO_REPARSE_TAG_DEDUP ，这些文件备份为普通文件。

可传输备份先决条件

- 必须将备份系统配置为接受来自应用程序系统的连接，反之亦然。
- 必须在应用程序和备份系统上安装和配置以下 Data Protector 和存储组件:
  - MS Volume Shadow Copy Integration
  - 相应的 Data Protector 磁盘阵列代理
  - VSS 硬件提供程序

  根据操作系统版本和磁盘阵列，可能需要以下存储组件:
  - VDS 硬件提供程序
    - 对于 ZDB，VDS 硬件提供程序为可选。
    - 对于即时恢复，可能存在某些限制，具体取决于磁盘阵列系列和操作系统版本。在某些情况下，成功执行即时恢复需要 VDS 硬件提供程序。

  如果发生了从活动管理系统到备用管理系统的故障转移，请执行如下操作:

- 如果备用和故障管理系统具有相同的主机名，则不需要执行任何操作。
- 如果备用和故障管理系统具有不同的主机名，则从 Data Protector 配置中删除故障系统，然后添加新的管理系统。

在 Microsoft Cluster 环境中使用 VSS 硬件提供程序时，如果原始卷装载在群集中，则必须将可传输卷影副本 (复本) 传输到群集之外。

因此，Data Protector 仅支持群集中的以下配置:

- 使用 VSS 软件提供程序的本地或网络备份。
- 可传输备份，其中备份系统不是群集的一部分 (不是群集节点)。
- 使用 SMI-S 阵列提供程序，Exchange 存储组不应在超过四个源卷上驻留。但是，建议的配置是事务日志驻留一个源卷上，存储驻留在另一个源卷上。如果仅丢失存储，则此配置使您能够执行前滚恢复。

为每个存储组创建一个备份规范，并在一行中计划它们。

- 在创建备份规范之前和运行备份之前，请确保 Exchange Server 副本状态为“正常”。否则，无法在创建备份规范期间浏览要备份的对象，或者备份将失败。请注意，状态“正在初始化”不可接受。
- 每次完整或增量 Microsoft Exchange Server 备份之后，事务日志文件都会被截断。但是，LCR 和 CCR 群集技术可以保证尚未复制的日志不会被删除。因此，在截断日志的模式中运行备份可能并不会实际释放空间。如果日志复制尚未完成，则可能会发生这种情况。
- 在重同步模式下使用 P9000 XP 阵列 VSS 硬件提供程序之前，请考虑此模式的所有适用限制。由于这些限制，建议在 VSS 兼容模式下使用 P9000 XP 阵列提供程序，或者使用 VSS 软件提供程序。

要还原到其他位置， Inet 必须在域帐户下运行，该帐户需要是本地系统上的以下组的成员:

- Administrators
- Exchange Server Administrators

在 Data Protector GUI 中配置还原到其他存储组时，“目标”下拉列表中仅显示已装载的存储。要为目标选择启用所有存储，请装载已卸除的存储，然后在“其他 MS Exchange 选项”中单击“重新加载”。

重要说明在还原到非 Exchange 位置和创建恢复存储组 (RSG) 期间，Data Protector 会删除可能已存在于目标位置的 RSG。

- 必须在您要备份的所有 DAG 节点上安装 Data Protector MS 卷影复制服务集成 组件。
- 对于联机备份:
  - 来宾操作系统必须安装 Hyper-V VSS 集成服务，并且不应使用动态磁盘。
  - 需要在与虚拟磁盘文件 (vhd 文件) 相同的卷上配置快照文件 (avhd 文件)。
  - 要备份的虚拟机必须联机。
  - 必须在主机 (虚拟机监控程序) 系统上启用自动装载新卷。要启用自动装载，请在虚拟机监控程序系统上执行 MOUNTVOL /E 。
- 对于脱机备份，如果满足联机备份的先决条件，则必须手动将要备份的虚拟机置于脱机或暂挂状态。

满足 3PAR StoreServ Storage 的先决条件

以下是 3PAR StoreServ Storage 配置的先决条件:

- 获取或安装存储许可证和组件:
  - 3PAR VSS 提供程序软件。

  有关安装说明，请参阅 3PAR StoreServ Storage 文档。有关受支持产品版本的信息，请参阅最新支持矩阵。
- 获取或安装 Data Protector 许可证和组件:
  - 适当的零宕机时间备份扩展和即时恢复扩展使用许可证 (LTU)。
  - 在应用程序系统和备份系统上安装 3PAR VSS 代理
- 确保在应用程序系统和备份系统上安装相同的操作系统 (及其版本)。
- 通过 SAN 将 3PAR StoreServ Storage 系列的存储系统连接到应用程序和备份系统。备份系统必须连接到与 3PAR StoreServ Storage 系列的存储系统相同的 SAN。
- 源卷必须在与之关联的存储系统的通用配置组 (CPG) 中具有“快照空间”(“副本空间”)。

3PAR StoreServ Storage 注意事项

- 下表列出适用于 3PAR StoreServ Storage 的即时恢复方法:

  3PAR StoreServ Storage 支持的即时恢复方法

即时恢复方法	3PAR VSS 代理
将快照数据还原到源卷且保留源卷	否
但不保留源卷	是

- 3PAR StoreServ Storage 复本不依赖于链中的先前复本。

满足 P4000 SAN 解决方案的先决条件

以下是 P4000 SAN 解决方案配置的先决条件:

- 获取或安装存储许可证和组件:
  - P4000 SAN Solutions VSS provider.
  - P4000 SAN 解决方案 MPIO 的 DSM (设备专用模块)。

  有关如何安装这些组件的详细信息，请参阅 P4000 Windows Solution Pack 文档。

  有关受支持产品版本的信息，请参阅最新支持矩阵。
- 获取或安装 Data Protector 许可证和组件:
  - 即时恢复许可证。
  - P4000 VSS 代理。
- 确保在应用程序系统和备份系统上安装相同的操作系统 (及其版本)。
- 通过 SAN 将 P4000 SAN 解决方案存储系统连接到应用程序和备份系统。备份系统必须连接到与 P4000 SAN 解决方案存储系统相同的 SAN。
- 对于 VSS 可传输备份，必须将源卷呈现给应用程序和备份系统。

P4000 SAN 解决方案注意事项

- 下表列出适用于 P4000 SAN 解决方案的即时恢复方法

  P4000 SAN 解决方案支持的即时恢复方法

即时恢复方法		P4000 VSS Agent
将快照数据恢复到源卷	且保留源卷	否
	但不保留源卷	是

- P4000 SAN 解决方案复本依赖于链中的先前复本。这意味着，为了还原特定复本，将删除较新的复本。执行即时恢复时，尽量使用最新的复本，然后逐步将其他复本还原到所需的时间点，以避免复本意外丢失。
- 在 Data Protector 之外创建的任何较新复本都将阻止从包含在 Data Protector 之外复制的卷的会话执行即时恢复。

满足 P9000 XP 磁盘阵列系列的先决条件

以下是 P9000 XP 磁盘阵列系列配置的先决条件:

- 获取或安装存储许可证和组件:
  - 应用程序和备份系统上的 RAID 管理器库。有关安装说明，请参阅 RAID 管理器库文档。

    RAID 管理器库与固件相关。有关要使用的 RAID 管理器库版本的信息，请咨询销售代表。
  - 适用于下限操作、基本操作和 Business Copy 操作的 Business Copy (BC) P9000 XP 微代码和许可证。
  - P9000 XP 阵列 VSS 和 VDS 提供程序。
  - 适用于 P9000 XP 磁盘阵列系列的 MPIO 完整功能 DSM (设备特定模块)

  有关受支持产品版本的信息，请参阅最新支持矩阵。
- 获取或安装 Data Protector 许可证和组件:
  - 即时恢复许可证。
  - P9000 XP 代理。

    如果未安装此代理，则无法从 P9000 XP 阵列还原数据。
- 确保在应用程序和备份系统上安装相同的操作系统和版本。
- 将应用程序和备份系统连接到同一 P9000 XP 阵列。
- 将 LUN 分配给相应的端口。
- 为创建 VSS 快照预先配置 LDEV 并将其放入 S-VOL 主机组中。如果使用 VDS 执行还原，则需要在还原之后将新的 LDEV 放入 S-VOL 主机组中，因为 VDS 还原会切换磁盘，复本将成为源卷。添加与用于还原的 LDEV 一样多的新 LDEV。

P9000 XP 阵列注意事项

- 下表列出适用于 P9000 XP 阵列的即时恢复方法:

  P9000 XP 磁盘阵列系列支持的即时恢复方法

即时恢复方法		VDS 硬件提供程序	P9000 XP 代理
切换磁盘		是	否
重新同步卷		否	是
将快照数据恢复到源卷	且保留源卷	否	否
	但不保留源卷	否	是

- 即时恢复取决于备份期间使用的 P9000 XP 阵列 VSS 硬件提供程序模式。如果使用 VSS 兼容模式，则只能使用 VDS 还原数据。如果使用重同步模式，则只能使用 SSEA 还原数据。
- 建议不要在使用同一备份规范的不同备份会话之间更改所选的 P9000 XP 阵列 VSS 硬件提供程序模式。如果在复本集循环计数设置为大于 1 时更改此模式，在以下情况下，即时恢复将失败:
  - 如果在一种模式下执行备份，然后在另一种模式下执行相同备份，则在 VSS 兼容模式中执行的备份还原 (“磁盘切换”还原) 将失败，因为在重同步模式下执行的其他备份将检测到 S-VOL 与其 P-VOL 之间的关系。在还原期间不应删除这对关系，因此无法使用复本切换

源卷。

要还原此类备份，请在还原之前执行以下操作之一:

- 使用 omnidbvss 命令手动删除备份期间在重同步模式下创建的 S-VOL。
- 在 omnirc 文件中设置 OB2VSS_FORCE_INSTANT_RECOVERY 选项，然后在 GUI 中启用“保留争议源”还原选项。选择此选项时，Data Protector 将保留备份期间在重同步模式下创建的 S-VOL 与其 P-VOL 之间的对关系。

- 如果使用重新同步执行还原 (“复制复本数据”还原)，并且系统上不存在生产源卷 (P-VOL)，则会中止还原会话。在不同模式下使用同一备份规范运行至少两个备份会话并且在“复制复本数据”还原之前运行“磁盘切换”还原之后，可能会发生这种情况。

  在这种情况下，请在还原之前执行以下操作之一:

  - 在应用程序系统上，手动呈现 P-VOL。
  - 在 omnirc 文件中设置 OB2VSS_FORCE_INSTANT_RECOVERY 选项。

- 在 VSS 兼容模式下，需要 VDS P9000 XP 阵列硬件提供程序执行即时恢复，即便在执行备份时未使用该硬件提供程序也如此。在这种情况下，请在尝试即时恢复之前安装 VDS P9000 XP 阵列硬件提供程序并执行 omnidbvss -resolve 命令:
  - 解析应用程序系统上的源卷，请执行以下操作: omnidbvss -resolve -apphost ApplicationClient
  - 要解析在备份会话中创建的目标卷，请执行以下操作: omnidbvss -resolve -session SessionID

以下还原注意事项仅适用于使用 P9000 XP 代理进行还原:

- 您无法使用应用程序系统上的同一磁盘同时启动另一个即时恢复会话。只有在前一个会话完成同步之后，才能启动会话。
- 即时恢复之后，已还原的文件系统将装载到运行备份时所使用的驱动器号。如果这些驱动器号已装载其他文件系统，则在即时恢复之前会自动卸除这些文件系统，之后会装载已还原的文件系统。

Microsoft 卷影复制服务集成配置

This feature is available in the Premium Edition

为启用即时恢复的备份会话配置应用程序系统

要能够执行启用即时恢复的备份，然后执行即时恢复，您必须使用 omnidbvss 命令解析应用程序系统。在解析操作期间，Data Protector 会联系 VDS 以获取有关应用程序系统上呈现的源卷的存储 ID 信息。如果在还原时无法收集此类信息，则在即时恢复期间需要有关存储 ID 的信息。

如果在备份会话之前未执行解析，则会发生以下情况之一:

- 如果 omnirc 文件中的 OB2VSS_DISABLE_AUTO_RESOLVE 选项设置为 0（默认值），则在备份会话期间将自动解析应用程序系统。在这种情况下，创建复本的备份时间会延长。
- 如果 OB2VSS_DISABLE_AUTO_RESOLVE 选项设置为 1 ，则 ZDB 到磁盘会话失败，并通知您在运行备份之前解析应用程序系统。
- 如果 OB2VSS_DISABLE_AUTO_RESOLVE 选项设置为 1 ，则 ZDB 到磁盘 + 磁带会话将完成，并警告仅执行备份到磁带而不将复本保留在磁盘阵列上，从而禁用即时恢复。

在以下操作之后始终执行解析操作:

- 安装或升级 Data Protector。
- 应用程序系统上的源卷配置已更改 (例如，您已修改现有源卷或已呈现新的源卷)。
- 您已添加一个新的存储对象 (例如，Microsoft Exchange Server 存储组)。

要解析应用程序系统，请在 Data Protector 单元中的任何 VSS 客户机上执行以下操作:

```
omnidbvss –resolve {-apphost ApplicationSystem | –all}
```

其中 *ApplicationSystem* 是要解析的应用程序系统的名称。在群集环境 (例如，Microsoft Exchange Server CCR) 中，提供 *ApplicationSystem* 参数的虚拟服务器名称，以在两个群集节点上启用解析操作。

要同时解析单元中的所有应用程序系统，请使用选项 –all 。

或者，您可以将 omnirc 选项 OB2VSS_ALWAYS_RESOLVE_SOURCES 设置为 1 。在这种情况下，应用程序系统上的源卷将在每个启用即时恢复的备份会话期间自动解析。但是，复本创建时间大幅延长。如果您计划仅备份数据库副本磁盘并且可以从这些磁盘最终即时恢复到生产数据库磁盘，请不要在 CCR Microsoft Exchange 环境中将此选项设置为 1 。在这种情况下，生产数据库磁盘在备份期间永远不会解析，这可能导致此类即时恢复失败。

配置 P4000 SAN 解决方案

本节介绍如何配置 Data Protector P4000 SAN 解决方案集成以与 VSS 集成一起使用。

在开始配置之前，请确保满足配置中所述的先决条件。随后，为在管理系统上运行的 SMI-S P4000 SAN 解决方案提供程序设置登录信息。

要设置、删除、列出或检查登录信息，请使用 omnidbp4000 --ompasswd 命令。有关命令语法和示例，请参阅管理的 P4000 SAN 解决方案部分，以及CLI 参考中的 omnidp4000 参考页。

您提供的信息保留在 ZDB 数据库的 P4000 SAN 解决方案部分，用于基于 SMI-S 的集成 (SMISDB)。

对于您配置的每个管理系统，将存储以下信息:

- 在 IP 网络中识别的主机名。
- P4000 VSS 代理用来通信的端口号 (默认值为 5988)。如果 SMI-S P4000 SAN 解决方案提供程序接受基于 SSL 的连接，则默认端口号为 5989。

  > 使用 StoreVirtual VSA 软件版本 12.5 时，请使用基于 SSL 的连接。

- P4000 SAN 解决方案提供程序登录帐户的管理组名称、管理组用户名和加密密码。

SMISDB 的 P4000 SAN 解决方案部分位于以下目录中的 Cell Manager 上: Data_Protector_program_data\server\db80\smisdb\p4000 (Windows 系统) 或 /var/opt/omni/server/db80/smisdb/p4000/login (UNIX 系统)。

重要说明建议使用默认端口号 (非 SSL 为 5988，基于 SSL 的 SMI-S P4000 SAN 解决方案提供程序连接设置为 5989)。

还建议在执行备份或即时恢复之前执行 omnidbp4000 --ompasswd --check [--host ClientName] 以验证 SMI-S P4000 SAN 解决方案提供程序的配置。

配置 VSS 硬件提供程序

在应用程序和备份系统上设置管理组凭据。使用 P4000 SAN 解决方案 VSS 提供程序所需的凭据包括:

- 管理组名称
- 管理组用户名和密码

根据操作系统的不同，使用身份验证控制台或编辑 Windows 注册表。有关详细信息，请参阅 P4000 SAN 解决方案 VSS 提供程序文档。

完成此过程之后，P4000 SAN 解决方案 VSS 提供程序即准备好用于零宕机时间备份和即时恢复。

配置 P9000 XP 磁盘阵列系列

本节介绍如何配置 Data Protector P9000 XP 磁盘阵列系列集成以与 Data Protector VSS 集成一起使用。

配置 VSS 硬件提供程序

运行 ZDB 会话之前，打开 XP VSS 硬件提供程序配置实用工具:

- 选择用于备份的配置模式: VSS Compliant Mode 或 Resync Mode。

  注意在备份会话之间更改模式可能影响还原。

- 启用快照 (如果 P9000 XP 阵列和 VSS 提供程序支持)，请选择“快照类型” 快照。

  Data Protector 允许重同步模式下的备份和相同源卷的快照。

有关详细信息，请参阅 P9000 XP 磁盘阵列系列 VSS 硬件提供程序文档。

配置用户身份验证数据

在以用户身份验证模式运行的磁盘阵列上运行零宕机时间备份 (ZDB) 和即时恢复 (IR) 会话之前，请将适当的用户凭据添加到 ZDB 数据库 (XPDB)。有关用户身份验证模式以及如何配置磁盘阵列用户身份验证数据的详细信息，请参阅管理。

配置 3PAR StoreServ Storage

本节介绍如何配置 Data Protector 3PAR StoreServ Storage 集成以与 Data Protector Microsoft 卷影复制服务集成一起使用。在开始配置之前，请确保满足以下章节中讨论的先决条件。

配置 Data Protector 3PAR StoreServ Storage 集成

有关配置说明，请参阅《Data Protector 零宕机时间备份管理员指南》的“3PAR StoreServ Storage”部分中的“配置”一节。

配置 3PAR VSS 硬件提供程序

您需要执行的唯一步骤是在应用程序系统和备份系统上配置 VSS 硬件提供程序用户帐户。

提供程序用户帐户必须具有与配置 Data Protector 3PAR StoreServ Storage 集成时添加的用户帐户相同的特权: 应用程序系统和源卷上的“编辑”特权级别。此类用户帐户可确保 VSS 硬件提供程序正确访问 3PAR StoreServ Storage。应用程序和备份系统上配置的用户帐户可以不同。有关说明，请参阅 3PAR StoreServ Storage 文档。

完成此过程之后，3PAR StoreServ Storage VSS 提供程序即准备好用于 Data Protector 零宕机时间备份和即时恢复会话。

备份 Microsoft 卷影复制服务集成

备份类型

对于 Data Protector VSS 集成，以下 VSS 备份类型可用:

- 本地备份
- 可传输备份

应用程序特定的备份类型

对于受支持的应用程序特定的备份类型 (例如 Full 、 Differential 等)，请参阅 VSS 写入程序中相应的写入程序特定部分。

备份流

1. 协调器 (VSS 服务) 标识支持 VSS 功能的所有写入程序，并将可用写入程序的列表及其特征 (写入程序元数据文档) 传回 Data Protector。
2. Data Protector 检查写入程序元数据，标识包含要备份的数据的卷，准备必须置于一致状态的卷列表 (卷影副本集)，并将此信息传回协调器以通知可用的写入程序。
3. VSSBAR 代理通知写入程序有关卷影副本的创建。VSS 机制可确保在创建卷影副本时不会对该卷进行写操作。

   随后，VSSBAR 代理将卷影副本创建请求传递给 VSS。
4. 在创建卷影副本之后，VSS 服务将相关信息返回 Data Protector。如果执行启用即时恢复的 ZDB，则 VSSBAR 代理会协调 VDS 代理以收集有关即时恢复所需的已创建复本的信息。
5. Data Protector 将数据从卷影副本备份到介质，然后通知 VSS 服务可以释放卷影副本。卷影副本提供程序会销毁已备份的卷影副本。

   显示本地 VSS 备份所扮演的角色之间的关系。
6. 零宕机时间备份:

   备份方案并非相互排斥，具体取决于以下情况:

   - 备份规范中选择的备份选项
   - 在备份规范中或备份开始时选择的 ZDB 类型
   - VSS 备份类型 (本地或可传输)。

   复本可以:

   - 保留在磁盘阵列上，以进行循环和即时恢复。
   - 保留在磁盘阵列上，仅用于数据挖掘。
   - 从应用程序系统 (本地备份) 或备份系统 (可传输备份) 移动到备份介质。
   - 呈现并装载到备份规范中指定的备份系统。它可以只读或读/写模式装载。
   - 如果没有保留在阵列上，则在备份会话完成之后销毁 (在复本中的数据移动到备份介质之后)。
   - 使用 Data Protector omnidbvss 命令控制。
7. 有关已完成备份会话的相关信息记录在 VSSDB 中。

创建备份规范

以下过程显示如何使用 Data Protector GUI 备份 Microsoft VSS 对象。部分写入程序具有特定的限制。有关写入程序特定先决条件、限制和其他步骤，请参阅 VSS 写入程序中的相应章节。

要为 VSS 集成创建新备份规范，请继续执行以下步骤:

1. 在 **Data Protector Manager** 中，切换到“备份”上下文。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击 **MS Volume Shadow Copy 写入程序**，并单击**添加备份**。
4. 在“创建新备份”对话框中，选择备份类型:可以从以下类型进行选择:

   - **本地或网络备份**

     此类型用于单主机 VSS 备份。要执行零宕机时间备份 (ZDB)，您需要硬件提供程序。否则，此类型的备份不需要硬件提供程序。
   - **VSS 可传输备份**

     使用此选项可在应用程序系统上创建卷影副本，并将其呈现在备份系统中 (可以执行备份到磁带)。

     此类型的备份需要硬件提供程序。
5. 在应用程序系统中，指定已安装 VSSBAR 代理的客户机的名称。

备份群集感知写入程序 (例如通过 MSDE 写入程序的 SQL Server，或者 LCR 或 CCR 环境中的 Exchange Server) 时，请指定特定写入程序资源组中给定的虚拟服务器名称。

零宕机时间备份:

指定以下选项：

- “对于本地或网络备份”，请选择“使用硬件提供程序”以启用 ZDB 并指定其他备份选项。
- “对于可传输备份”，请选择可以将卷影副本备份到磁带或者在备份后要呈现和装载卷影副本位置的备份系统名称。硬件提供程序将自动使用。
- 要在备份之后保留复本，请选择“在备份完成之后保留复本”。
- 要启用即时恢复，请选择“跟踪复本以用于即时恢复”。将自动选择“在备份完成之后保留复本”。
- 如果选择“在备份完成之后保留复本”，则可以指定复本类型:

复本类型

副本类型	描述
Plex (克隆/镜像)	创建独立于其源卷的卷影副本: • P4000 SAN 解决方案和 3PAR StoreServ Storage 硬件提供程序不支持此复本类型。 • 对于 P9000 XP 磁盘阵列系列硬件提供程序，创建的复本取决于提供程序模式 (在 VSS 符合模式的情况下克隆，或在重同步模式的情况下镜像)。将忽略选定的子类型。
差异 (快照)	创建依赖于其源卷的卷影副本。 • 对于 P4000 SAN 解决方案或 3PAR StoreServ Storage 硬件提供程序，将创建快照。 • 对于 P9000 XP 磁盘阵列系列硬件提供程序，将创建快照。
默认值	复本类型由 VSS 硬件提供程序配置确定。 不适用于即时恢复。

- 提供程序可能支持一个或所有类型。如果选择不受支持的复本类型，则备份将失败。
- 要在备份系统上装载复本，请选择“在备份系统上装载复本”。
- 要更改复本管理和装载选项，请单击“设置”以打开“复本管理”或“装载”对话框。

> **注意**每当您更改影响其他设置的页面上的选项时，按钮都会标有星号 (*)。打开设置窗口并查看或修改选项之后，将删除星号。

有关复本选项的说明，请参阅复本管理选项，或者按 **F1**。

有关装载选项的说明，请参阅装载选项，或者按 **F1**。

单击“下一步”。

6. 在此页面中，将显示选择的 VSS 客户机。

   在 Windows 系统上，可以指定“用户和组/域”选项。有关这些选项的信息，请按 **F1**。

   单击“下一步”。

7. 选择要备份的备份对象。确保在启用即时恢复的会话的情况下，选择驻留在将要备份的特定源卷上的所有对象 (例如，所有存储组、所有虚拟机...)。

   通过选择顶级项目 (客户机的名称) 可以指定*完整的客户机备份*，通过选择较低级别的项目，可以指定单个写入程序备份或写入程序的组件备份。

   如果选择完整客户机备份，Data Protector 将检查客户机上存在哪些写入程序，并在备份时间全部备份它们。

   如果写入程序需要备份其所有组件，则自动选择较低级别的项目。如果为备份选择此类写入程序，将备份其所有组件。如果写入程序没有要备份的组件，则它不会在写入程序列表中显示，并且在选择完整客户机时也不会备份它。

   “文件系统”项将显示所有已装载的磁盘。如果在一个磁盘上的目录已装载另一个磁盘，则该父磁盘名称将显示两次。第一个名称表示父磁盘名称 (例如 c:)，而第二个名称表示装载点的容器 (例如 c:\mnt\1)。要选择装载的磁盘，请选择装载点的容器。

8. 要备份到磁带，请选择要用于备份到磁带的设备。单击“属性”可以设置设备并发、介质池和预分配策略。有关这些选项的详细信息，请单击“帮助”。如果未选择设备，则只能使用备份到磁盘。

> **重要说明**如果未配置设备且未选择“跟踪复本以用于即时恢复”选项，则无法使用 Data Protector 还原数据。

在备份到磁带的情况下，还可以指定是否要在备份会话期间额外创建备份的其他副本 (镜像)。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。

有关对象镜像功能的详细信息，请参阅《Data Protector 帮助》。

9. 按照向导操作，选择备份选项。

> **提示**如果您不确定选择备份选项，请保留默认值。

有关所有 Data Protector 备份规范的通用选项的详细信息，请参阅《Data Protector 帮助》。

10. 定义所有备份选项之后，需要命名并保存新创建的备份规范。您现在已完成 Microsoft 卷影复制写入程序备份规范的创建。(可选) 还可以计划备份规范。
11. 可以在“备份”上下文中的指定备份规范组下检查最近创建和保存的备份规范。
12. 可以使用下列方法之一运行备份：
    - 使用 Data Protector 调度程序计划现有 Microsoft 卷影复制写入程序备份规范的备份。
    - 启动现有 Microsoft Volume Shadow Copy 写入程序备份规范的交互备份。

备份选项

VSS 特定备份选项

选项	描述
Pre-exec	指定在创建复本之前将由应用程序系统上的 vssbar.exe 直接启动的命令。不要使用双引号。仅键入命令的名称，而非路径名。命令必须位于默认的 Data Protector 命令目录中。
Post-exec	指定在创建复本之后将由应用程序系统上的 vssbar.exe 直接启动的命令。不要使用双引号。仅键入命令的名称，而非路径名。命令必须位于默认的 Data Protector 命令目录中。

ZDB 选项

复本管理选项

选项	描述
配置检查模式	如果已选定“跟踪复本以用于即时恢复”，则指定“配置检查模式”。配置检查适用于要用于即时恢复的磁盘备份，不适用于磁带备份。
轮换的复本数量	在 ZDB 会话期间，Data Protector 创建新副本，并在阵列上保留该副本，直到达到指定的**轮换的副本数量**（选择**备份后保留副本**后指定）。在那之后，删除最旧的复本，然后创建一个新复本。 默认值： 3 Data Protector 不限制旋转的复本的数，但是如果超出限制，会话将失败。

装载选项

选项	描述
装载复本	选择此选项可在备份系统上装载复本。装载路径取决于“备份系统上装载点的根目录”和“将目录添加到装载路径”选项。
以读/写模式启用备份系统	选择此选项可允许读/写访问备份系统上所装载复本的磁盘。请注意，建议不要对以读/写模式激活的磁盘进行即时恢复，因为通过设置写入权限，可以在备份时间之后更改磁盘的数据。如果**跟踪复本以用于即时恢复**为“开启”，则为未选择，如果**在备份完成之后保留复本**为“开启”，则为已选择。
备份系统上装载点的根目录	指定将在其下装载来自复本的文件系统的根目录。装载文件系统的确切位置取决于如何指定**将目录添加到装载路径**。默认装载点为 c:\mnt 。

将目录添加到装载路径	通过此选项，可以单独控制所创建的各个装载点。在创建路径过程中使用会话 ID 时，这样可保证各个装载点唯一。这些选项定义用**备份系统上装载路径的根目录**选项指定的目录中将创建哪些子目录。 示例： 根目录： c:\mnt 应用程序系统： app.comp.com 备份会话 ID： 2008–02–22–4 应用程序系统上的装载路径： E:\disk1 如果选择**主机名**： c:\mnt\app.comp.com\E\disk1 如果选择“主机名 + 会话 ID”: c:\mnt\app.comp.com\2008–02–22–4\E\disk1 如果选择**会话 ID**： c:\mnt\2008–02–22–4\E\disk1 如果选择**会话 ID + 主机名**： c:\mnt\2008–02–22–4\app.comp.com\E\disk1 默认值：“主机名 + 会话 ID”。
在目标装载点自动卸除文件系统	如果装载点在使用中 (例如，可能装载之前会话) 并且已选择此选项，则 Data Protector 将尝试卸除装载的文件系统。如果未选择此选项且装载点在使用中，或者已选择此选项但卸除失败，则会话将失败。 默认：未选择。

计划备份会话

有关如何创建和编辑计划的详细信息，请参阅管理中的“调度程序”。

要计划 Microsoft 卷影复制写入程序备份规范，请在 Data Protector GUI 中执行以下步骤:

1. 在 **Data Protector Manager** 中，切换到“备份”上下文。
2. 在“范围窗格”中，展开“备份”，然后展开“备份规范”。单击“MS 卷影复制写入程序”。

   此时将在结果区域中显示可用备份规范的列表。
3. 右键单击要计划的备份规范，然后单击“编辑计划”。“计划程序”页面随即打开。此备份规范的所有可用计划均列在右窗格中。
4. 单击要编辑的计划，然后单击“编辑”图标。计划向导随即打开。
5. 在“选项”页面查看选项，然后单击“下一步”。“重复”页面随即打开。

   请注意，要用于即时恢复的 ZDB 会话的备份类型设置为“完整”。

   如果是“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，指定“拆分镜像/快照备份”选项。
6. 设置“重复”模式，然后单击“下一步”。“摘要”页面随即打开。
7. 在“摘要”页面查看选项，然后单击“完成”。

启动备份会话

可以使用 Data Protector GUI 按照以下步骤启动交互式备份:

1. 在 **Data Protector Manager** 中，切换到“备份”上下文。
2. 在“范围窗格”中，展开“备份”；然后展开“备份规范”和“MS 卷影复制写入程序”项。
3. 右键单击要使用的备份规范，然后从弹出菜单中选择“启动备份”。

   此时将显示“启动备份”对话框。

   选择备份类型和网络负载 (“高”、“中”或“低”)。

   请注意，要用于即时恢复的 ZDB 会话的备份类型设置为“完整”。

如果是“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，指定“拆分镜像/快照备份”选项。

有关网络负载的说明，请参阅《Data Protector 帮助》。

4. 单击**确定**。成功完成备份会话之后，将显示“会话已成功完成”消息。

检查 Microsoft 卷影复制服务集成配置

This feature is available in the Premium Edition

对于即时恢复，仅当写入程序的组件驻留在单独源卷上时，才可以有选择地还原单独的写入程序组件。单独组件的即时恢复还要求具有组件数据的卷不应包含任何其他数据。配置检查将检测卷上是否有多个组件以及除了组件数据是否还有任何其他数据。

在备份时，Data Protector 可以检查是否可以使用即时恢复功能有选择地还原单独的组件。在即时恢复时，Data Protector 可以检查组件还原所需的数据是否可用。

对于 Microsoft Exchange Server 写入程序，检查是否应还原整个存储组，或者是否可以分别还原单独的数据库存储。对于 MSDE 写入程序，检查用户、系统和日志文件是否在单独的卷上。

如果在备份期间对某个组件的检查失败，您将无法选择此组件进行即时恢复，需要恢复所有写入程序组件。如果在即时恢复期间检查失败，则即时恢复会话将失败。

配置检查模式

您可以在三种配置检查模式中进行选择:

- **严格**

  如果卷上有任何文件或文件夹不属于组件，则 ZDB 到磁盘、ZDB 到磁盘 + 磁带或即时恢复失败。

- **非严格**

  如果卷上有任何文件夹不属于组件，则 ZDB 到磁盘、ZDB 到磁盘 + 磁带或即时恢复失败。

- **禁用**

  检查将检测卷上是否有多个组件或卷上除了组件数据是否还有任何其他数据，但任何情况下会话均不会失败。

重要说明如果对于即时恢复禁用了配置检查，则将丢失不属于组件、但与组件位于相同卷上的数据。仅当无法在启用配置检查的情况下执行即时恢复时禁用配置检查，并且在禁用之前必须确保这不会导致数据丢失。如果数据丢失，不属于组件但位于同一卷上的数据将丢失。

除非无法在启用配置检查的情况下执行即时恢复，否则不应禁用配置检查。由于特定的行为，在备份和即时恢复期间，某些写入程序 (不适用于 MSDE 写入程序和 Microsoft Exchange Server 写入程序) 可能会在组件卷上创建临时文件，从而导致检查失败。在这种情况下，不禁用检查就无法执行即时恢复。

注意事项

备份 P4000 SAN 解决方案

使用 P4000 SAN 解决方案创建新快照时，将在写入新数据的阵列上分配新的磁盘空间 (这种创建快照的方法也称为“写时重定向”)。这意味着较新的快照取决于较旧的快照，并且您需要链中的所有快照才能使最后一个快照生效。

如果多个备份规范包含相同的源卷，则从一个备份规范的 ZDB 会话执行即时恢复可能会导致基于其他备份规范的较新 ZDB 会话无法进行即时恢复。

例如，备份规范 BSpec1 包含卷 C: 和 G:，备份规范 BSpec2 包含卷 G: 和 M:。

从 BSpec1 的 ZDB 会话执行即时恢复将删除卷 C: 和 G: 的所有后续快照。这也会阻止从在用于即时恢复的 BSpec1 ZDB 会话之后创建的所有 BSpec2 ZDB 会话进一步执行即时恢复会话，因为卷 G: 的快照不再可用。

因此，您必须考虑以下几点:

- 建议将备份规范中包含的卷数限制为所需的最小数量。
- 执行会话 (而不是特定卷) 的即时恢复。
- 在 Data Protector 之外创建的任何较新复本 (快照或智能克隆) 都将阻止从包含在 Data Protector 之外复制的卷的会话执行即时恢复。

复本创建和重用

创建新复本，并在未达到指定的“循环的复本数”时将其添加到复本集中。

删除集合中最旧的复本，并在达到指定的“循环的复本数”时创建新复本。

备份 P9000 XP 磁盘阵列系列

- 对于在“重新同步模式”下创建的备份 (镜像)，“循环的复本数”选项的值限制为每个源卷 (P-VOL) 最多三个复本 (S-VOL)，前提是 P9000 XP 阵列 VSS 硬件提供程序配置中的 MU# range 选项设置为 0-2 或 0, 1, 2。如果在多个备份规范中使用同一 P-VOL，则所有备份规范的“循环的复本数”选项中指定值的总和不应超过 3。

  此限制也适用于 Microsoft Exchange Server CCR 环境中选择了相同备份系统的以下备份方案: 假定使用一个备份规范在生产数据库系统上创建源卷的三个备份，然后使用其他规范在数据库副本系统上创建源卷的三个备份。这样一来，总共就会创建六个复本。但在这种情况下，Data Protector 会限制该数量，总共仅支持三个复本。因此，您可以选择只在生产数据库系统上备份源卷，或者只在数据库副本系统上备份源卷。否则，使用一个备份规范创建三个复本之后，使用第二个备份规范的下一次备份将失败。

  *快照*不限于每个源卷 3 个复本。可以在 VSS 提供程序配置中配置快照的 MU# 数量。

- 您可以在使用同一备份规范的不同备份会话之间更改 P9000 XP 阵列 VSS 硬件提供程序模式，但在使用复本集循环时不建议这样做，因为还原此类备份数据可能会失败。

备份 3PAR StoreServ Storage

- 使用 3PAR StoreServ Storage 创建新快照之后，首先将原始卷上要被新数据覆盖的数据复制到与该卷关联的快照空间 (这种创建快照的方法也称为“写时复制”)。这意味着较新的快照独立于较旧的快照。
- 建议不要在 Data Protector 创建的目标卷上手动设置保留期。一旦设置，如果 Data Protector 将某个卷从复本集循环出来，卷保留期会阻止从 3PAR StoreServ Storage 中删除该卷。在这种情况下，在复本集循环之后，该卷将成为孤立的卷，不必要地占用存储空间。由于 3PAR VSS 硬件提供程序版本 2.1.0.11 中存在问题，因此会将此类卷删除失败报告为成功。

还原 Microsoft 卷影复制服务集成

This feature is available in the Premium Edition

您可以使用 Data Protector GUI 还原 Data Protector Microsoft 卷影复制服务集成备份对象。

Data Protector 提供了两种还原写入程序的方法:

- 从备份介质还原到 LAN 上的应用程序系统 (标准还原)。
- 使用即时恢复功能。

标准还原

自定义还原方法的限制

- Data Protector Microsoft VSS 集成没有自动为请求自定义还原的写入程序提供任何还原方法。如果写入程序指定了自定义还原方法，则只能使用 Data Protector 文件还原功能将写入程序的数据还原为纯文件。您可以使用“还原至”选项为这些纯文件指定备用还原路径。然后，您可以手动从这些纯文件执行自定义还原。有关写入程序的自定义还原的信息，请参阅写入程序的文档。

还原模式

Data Protector 提供两种还原模式:

- 使用 VSS 服务进行“组件还原”
- 使用 Data Mover Agent (DMA) 而不是 VSS 进行“文件还原”

默认情况下，Data Protector 使用 VSS 服务还原写入程序组件。

组件还原

还原写入程序组件时，Data Protector 与 VSS 服务一起使用以确保数据一致性:

1. Data Protector 首先还原在备份期间收集的元数据。然后，它使用元数据来标识备份组件并确定还原方法。
2. Data Protector 按照写入程序关于任何其他检查或处理的说明，将数据从备份介质还原到备份元数据中指定的位置。
3. 从备份介质成功还原之后，Data Protector 会通知协调器，写入程序现在可以访问新还原的数据并启动内部处理，例如数据库恢复。

文件还原

要成功还原写入程序组件，必须还原组成此组件的所有文件。如果单个文件的还原失败，则整个组件的还原将失败。Data Protector 提供了一种额外的还原模式，用于还原不使用 Microsoft 卷影复制服务的单个文件，从而解决此问题。此模式还可用于还原到不支持 VSS 或未安装 VSS 写入程序的系统。

还原文件或一组文件时，将启动 DMA 并使用标准 Data Protector 文件系统还原过程还原文件。

> **重要说明**由于文件还原模式不利用 VSS 服务，因此不执行组件还原后执行的其他任务 (如数据库恢复)，并且应用程序数据可能处于不一致状态，在应用程序恢复之前需要执行其他手动过程。

使用 GUI 还原

以下过程显示如何使用 Data Protector GUI 还原 Microsoft VSS 组件。部分写入程序需要自定义还原过程和/或具有特定限制。另请参阅 VSS 写入程序中的相应章节。

要使用 Data Protector GUI 还原 Microsoft VSS 对象，请继续执行以下步骤:

1. 在 Data Protector GUI 中，切换到“还原”上下文。
2. 展开“还原对象”，展开“MS 卷影复制写入程序”，展开要从中还原数据的客户机，然后单击“MS 卷影复制写入程序”。在结果区域中，显示在此客户机上备份的写入程序的列表。
3. 选择还原模式:
   - 还原组件

     选定此选项之后，将使用卷影复制服务还原整个组件。无法选择单个文件进行还原。

- 将文件还原到临时位置

  通过此选项，可以选择使用选定写入程序备份的单个文件或文件组。文件是使用 Data Mover Agent 还原的，而不是 Volume Shadow Copy Service。

4. 在结果区域中，选择写入程序或写入程序的组件 (用于组件还原) 或文件或文件组 (用于文件还原模式)。

   您可以选择顶级项目 (完整写入程序还原) 或仅选择特定组件。如果选择完整写入程序还原，但此写入程序的某些组件未在同一会话中备份，则不可用组件带阴影，并且无法选择。要选择版本 (备份日期)，请右键单击对象名称，然后单击“属性”。默认情况下会选择最后一个可用的备份版本，但是，您可以从下拉列表中选择其他版本。

   有关特定于应用程序的选项，请参阅 VSS 写入程序。

5. 在“选项”属性页中，选择特定于 MS 卷影复制的还原选项。请参见还原选项。

6. 在“设备”和“介质”属性页中，将自动选中要还原的设备和介质。

   请注意，您可以更改用于还原的设备。因此，您可以使用不同的设备进行还原，而不是使用用于备份的设备。请参阅《Data Protector 帮助》索引: “选择还原设备”。

7. 单击**还原**。检查选择，然后单击“完成”以启动还原会话。

   结果区域中将显示还原会话消息。

8. 如果要还原需要自定义还原的 VSS 写入程序，请使用特定于写入程序的方法 (如果它由写入程序提供) 手动继续。请参阅写入程序的文档。

还原选项

以下还原选项特定于 Data Protector Microsoft 卷影复制服务集成。

> **注意**不要将这些选项用于 Microsoft Exchange Server 写入程序，因为还提供其他特定于 Exchange Server 的选项用于还原到其他位置。请参阅 Microsoft Exchange Server 写入程序详述。

还原选项

还原选项	描述
还原到另一个客户机	默认情况下，组件或文件将还原到从中备份应用程序数据的客户机。但是，如果指定“还原到另一个客户机”选项，则可以将数据还原到另一个 VSS 客户机。 Microsoft VSS 客户机必须是 Data Protector 单元的一部分。对于组件还原，它还必须在同一平台上运行并安装 MS 卷影复制集成软件组件。对于文件还原，不需要 MS 卷影复制集成软件组件。
恢复到以下目录中(I)	默认情况下，您将数据还原到从中备份它的同一目录 (它可以在原始客户机上或在选择的某些其他客户机上)。 但是，如果指定“还原到以下目录中”选项，则数据将还原到另一个目录。定义还原位置时，可以指定要还原数据的目录的路径。

使用 CLI 还原

使用 omnidbvss -get session SessionKey 命令以获取有关要用于还原的会话的详细信息。

例如：

```
omnidbvss -get session_persistent 2011/01/26-2:computer1
============================================================ 会话 ID: 2011/01/26-2 Barlist 名称:
SQL_NEW_DB_SIMPLE Bar 主机名: computer1.company.com 备份类型: FULL 即时还原: FALSE 仅磁盘: FALSE 组件名称
============================================================ [0] /SqlServerWriter(SQL Server
2008:SQLWriter)/COMPUTER1/New_DB
```

“组件名称”下将列出在此会话中备份的对象。有关详细信息，请参阅《Data Protector 命令行界面参考》中的 omnidbvss 参考页。

执行 omnir 命令:

```
omnir -vss –barhost ClientName -session BackupID -tree TreeName1 [-tree TreeName2...] -conf_check {strict|non-strict|disabled}
```

注意“BackupID”是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，必须指定原始“备份”会话的会话 ID (即备份 ID)，而不是“对象复制”会话的会话 ID。

如果存在同一对象的多个副本，则 omnir 语法不允许您指定要从哪个对象副本还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

要从上面的示例中恢复组件，请执行:

```
omnir -vss –barhost server1.company.com -session 2010/1/12-09 -tree /Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/Store1/Logs –tree /Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/Store1/File -conf_check disabled
```

即时恢复过程

1. 在 **Data Protector Manager** 中，切换到“即时恢复”上下文。
2. 在“范围窗格”中，展开“还原对象”下的“MS 卷影复制写入程序”，展开要从中还原的备份规范，然后单击要从中还原的备份会话。
3. 在“源”属性页中，指定要恢复的写入程序和/或组件。

   选择配置检查模式。

   要在恢复数据库之前即时恢复之后执行其他步骤，请选择“没有恢复”选项。Data Protector 将不执行数据库恢复，因此可以在以后手动完成恢复步骤 (如应用事务日志)。

   如果未选择此选项，则会完成所有恢复步骤。在这种情况下，无法执行其他任务。此选项取决于正在恢复的应用程序写入程序。_

   有关任何其他特定于应用程序的选项，请参阅 VSS 写入程序。
4. 在“选项”选项卡下，选择即时恢复类型:
   - 使用 Microsoft 虚拟磁盘服务进行恢复
   - 使用 Microsoft Volume Shadow Copy Service LUN 重新同步进行还原
   - 使用磁盘阵列代理还原

   要使用 VDS 硬件提供程序或磁盘代理进行即时恢复，要保留源卷，请选择“保留争议源”。

   选择使用磁盘阵列代理进行恢复时，可以使用其他选项。
   - 使用 P4000 进行还原

     还原方法: “将快照数据还原到源卷”。
   - 使用 P9000 XP 进行还原

     还原方法: “将复本数据重新同步到源卷”、“将复本数据快速重新同步到源卷 (内部交换)”或“将快照数据还原到源卷”。

     有关这些方法的详细信息，请参阅还原。
   - 使用 P10000 3PAR 进行还原

     还原方法: “将快照数据还原到源卷”。

     有关这些方法的详细信息，请参阅还原。
5. 单击**还原**。
6. 执行任何其他写入程序特定步骤。请参阅 VSS 写入程序。

群集

要在群集环境中执行即时恢复，请使用上面的即时恢复过程。选择客户机名称时，请使用虚拟客户机名称而不是物理系统。有关在群集配置中执行即时恢复的详细信息，请参阅《Data Protector 零宕机时间备份管理员指南》。

VSS 写入程序

This feature is available in the Premium Edition

本主题提供有关在备份或还原写入程序之前需要考虑的 VSS 写入程序的特定信息。

VSS 写入程序附带 Windows 操作系统或应用程序。有关受支持的 VSS 写入程序和提供程序的完整列表，请参阅最新支持矩阵。

Data Protector Microsoft VSS 集成没有为请求自定义还原的写入程序提供任何还原方法。如果写入程序指定了自定义还原方法，则只能使用 Data Protector 功能将写入程序的数据还原为纯文件。可以手动执行自定义还原。有关还原方法的其他信息，请参阅写入程序文档。

注意默认情况下，Data Protector 不显示需要自定义还原方法的写入程序。要显示所有写入程序，必须将 omnirc 选项 OB2VSS_SHOWALLWRITERS 设置为 1。

写入程序说明提供 VSS 写入程序的说明。

写入程序说明

写入程序名称	描述	恢复方法
证书颁发机构写入程序	这是一个系统写入程序，用于备份和还原证书颁发机构 (CA) 服务数据库。此服务发布、撤销和管理基于公钥的加密技术中所使用的证书。	在系统重新启动后会还原文件。
群集服务写入程序	此 VSS 写入程序使用自定义 API，用于备份和还原 Microsoft 群集服务器 (MSCS) 上的群集服务。该群集服务是 Windows Server 系统上的一个组件，用于控制群集节点上的服务器群集活动。它是群集操作的基础。	自定义还原方法
COM+ REGDB 写入程序	此 VSS 写入程序使用自定义 API，用于备份和还原 COM+ 数据库服务。此服务自动分发订阅 COM+ 组件的事件。	自定义还原方法
DHCP Jet 写入程序	这是一个系统写入程序，用于备份和还原 DHCP 服务数据库。DHCP 服务为动态主机配置协议 (DHCP) 客户机提供动态 IP 地址分配和网络配置。	在系统重新启动后会还原文件。
事件日志写入程序	这是一个系统写入程序，用于备份和还原事件日志。事件日志是 Windows 操作系统保存事件信息的文件，例如，服务启动和停止以及用户登录和注销。	在系统重新启动后会还原文件。
FRS 写入程序	此 VSS 写入程序使用自定义 API，用于备份和还原 File Replication Service 数据。File Replication Service 是一个多线程复制引擎，可复制存储在系统卷 (SYSVOL) 中的系统策略和登录脚本。FRS 还可以复制分布式文件系统 (DFS) 的数据，同时复制和维护多个服务器上的共享文件和文件夹。	自定义还原方法
IIS Metabase 写入程序	这是一个系统写入程序，用于备份和还原 Microsoft Internet Information Server (IIS)。IIS 是一种支持多协议的网络文件和应用程序服务器。IIS 主要使用超文本传输协议 (HTTP) 传输超文本标记语言 (HTML) 页中的信息。	在系统重新启动后会还原文件。
MSDE 写入程序	这是一个用于备份和还原 Microsoft SQL Server 2000 的写入程序。SQL Server 是一个数据库管理系统，可以响应使用 SQL 语言格式化的客户机查询。	
Microsoft Data Protection Manager 写入程序	这是一个用于备份和还原 Microsoft Data Protection Manager 的写入程序。Microsoft Data Protection Manager 是一个服务器，可创建和存储客户机的复本并用其恢复客户机上的数据	
Microsoft Exchange Server 写入程序	这是一个用于备份和还原 Microsoft Exchange Server 的写入程序。Microsoft Exchange Server 是一个邮件和群件服务器。	
Microsoft Virtual Server 2005 写入程序	这是一个用于备份和还原 Microsoft Virtual Server 2005 的写入程序。Microsoft Virtual Server 2005 是 Microsoft Windows Server 系统的虚拟化平台。Data Protector 支持实时备份单个虚拟机和 Virtual Server 配置，从而确保备份和还原的数据一致性。如果 Virtual Server Machine 处于联机模式，则不支持硬件提供程序；使用软件提供程序或将 Virtual Server Machine 置于脱机模式。有关 Virtual Server 联机和脱机模式的详细信息，请参阅 Microsoft Virtual Server 文档。 不支持群集配置，只能备份单个节点。	标准 VSS 还原和即时恢复。

Microsoft Hyper-V 写入程序	此写入程序用于备份和还原 Microsoft Virtual Server 2008 Hyper-V 配置以及在服务器上运行的单个或所有虚拟机。在联机和脱机备份期间，支持软件和硬件提供程序。 不支持群集感知备份。	标准 VSS 还原和即时恢复。
SharePoint Services Writer	这是一个用于备份和还原 Microsoft Office SharePoint Server 2010 (MOSS) 的引用写入程序。MOSS 2010 是一个信息门户，用于在人员和团队之间沟通与交流专业知识。 仅支持单个服务器配置 (场)。 OSearch VSS 写入程序和 SPSearch VSS 写入程序供该引用写入程序备份和还原用户和帮助内容的索引文件。它们不得用于备份和还原。	标准 VSS 还原。
NTDS 写入程序	这是一个系统写入程序，用于备份和还原 Windows Server 系统上的 Microsoft Active Directory。Active Directory Service 是一种 Windows 服务器目录服务，可用于管理通过网络分发的数据结构。例如，Active Directory Service 存储有关用户帐户、密码、电话号码，配置文件和已安装服务的信息。通过它可以存储目录数据并向网络用户和管理员提供这些数据。	要还原 Active Directory，请引导到“目录”还原模式中。如果文件可以覆盖，则会将其还原。
Registry Writer	此 VSS 写入程序使用自定义 API，用于备份和还原 Windows 注册表。Windows 注册表是包含 Windows 系统配置的信息数据库存储库。	自定义还原方法
远程存储写入程序	这是一个系统写入程序，用于备份和还原远程存储服务 (RSS)。RSS 用于自动将不常访问的文件从本地移至远程存储。打开此类文件时，将自动检索远程文件。	在系统重新启动后会还原文件。
Removable Storage Manager 写入程序	这是一个系统写入程序，用于备份和还原 Removable Storage Manager 服务。此服务管理可移动介质、驱动器和库。	在系统重新启动后会还原文件。
System Writer	这是一个系统写入程序，用于备份一组特定的 Windows 动态链接库 (DLL)。	在系统重新启动后会还原文件。
TermServLicencing 写入程序	这是一个系统写入程序，用于备份 Windows 终端服务。这些服务提供一个多会话环境，该环境使客户机系统可以访问运行在服务器上的虚拟 Windows 桌面会话和基于 Windows 的程序。	在系统重新启动后会还原文件。
WINS Jet 写入程序	这是一个系统写入程序，用于备份和还原 Windows Internet Name Service (WINS)。WINS 是一种动态复制数据库服务，可以注册并将 NetBIOS 名称解析为 TCP/IP 网络上使用的 IP 地址。	在系统重新启动后会还原文件。
WMI 写入程序	这是一个系统写入程序，用于备份和还原 Windows Management Instrumentation (WMI)。WMI 是 Windows 中用于监视系统资源的统一管理基础架构。	在系统重新启动后会还原文件。

Microsoft Data Protection Manager 写入程序详述

备份

Microsoft Data Protection Manager (DPM) 是一个服务器应用程序，可创建客户机的复本、通过 LAN 使其同步并将这些复本存储为快照。

Data Protection Manager 写入程序用于备份:

- Data Protection Manager 数据库和 Data Protection Manager 报告数据库
- DPM 复本的“最新版本”。

> **重要说明**要确保数据一致性，请在开始备份之前计划 DPM 复本同步。DPM 使用 DPM 快照进行还原。这些快照“未”备份。为了能够重新创建 DPM 快照，每次 DPM 创建新复本之后，必须手动计划复本备份。

支持两种备份类型:

- *完整* (适用于 DPM 数据库和复本)
- *增量* (仅限复本)

如果在计划备份时选择不受支持的备份类型 (“副本”或“差异”)，Data Protector 将中止备份并显示一条错误消息。

必须安装 MSDE 写入程序 (用于备份 DPM 数据库)。

以下限制适用：

- DPM 不支持硬件提供程序。

- 如果在 DPM 复本的增量同步仍在进行时启动备份，则备份会损坏，但 Data Protector 不会报告任何错误。如果与一致性检查同步，Data Protector 会自动中止备份会话。

还原

还原 DPM 写入程序时，可以:

- 先还原 DPM 服务器，然后使用 DPM 还原客户机。

  发生灾难时，如果整个 DPM 服务器丢失，请先执行标准灾难恢复过程，然后继续还原 DPM 服务器。

- 直接还原单个 DPM 客户机，而不使用 DPM 服务器 (例如，如果无法还原 DPM 服务器或者如果要避免重新创建 DPM 快照的额外步骤)。直接还原 DPM 客户机时，可以在组件还原和文件还原模式之间进行选择。请参阅直接还原 DPM 客户机。

> **注意**尽管也可以使用 MSDE 写入程序还原 Data Protection Manager 数据库，但建议不要使用此方法，因为 DPM“不”像 DPM 写入程序那样自动关闭。如果确实需要使用此写入程序，请手动关闭 DPM 服务器。

限制

- Data Protection Manager 写入程序不支持还原到其他服务器。
- 不支持并行还原到不同的客户机。

先还原 DPM 服务器

1. 启动 DPM 管理员控制台并将磁盘添加到存储池，以便有足够的可用空间来还原复本。

   确保已启动 DPM 写入程序 (服务)。

2. 切换到 Data Protector“还原”上下文。展开“还原”和“Microsoft 卷影复制写入程序”，然后选择要从中还原数据的客户机。
3. 在“结果区域”中，展开 DPM 写入程序，然后“仅”选择 Data Protection Manager 数据库。

   继续执行常规 VSS 写入程序还原。

4. 执行 DPM 命令 `DpmSync -Sync` 以重新分配复本。
5. 切换回 Data Protector“还原”上下文，然后选择并还原必要的复本。
6. 使用 DPM 还原单个客户机。

   > **重要说明**DPM 控制台不会自动检查新快照或已还原的快照。在开始还原客户机之前，必须使用 Data Protection Manager 重新创建 DPM 快照。

   a. 在 DPM 控制台中，打开“恢复”上下文。在“浏览”选项卡下，选择服务器，右键单击已还原的复本，然后选择“立即创建卷影副本”。

   b. 选择新快照并将其还原到客户机。

直接还原 DPM 客户机

1. 切换到“还原”上下文。展开“还原”和“Microsoft 卷影复制写入程序”，然后选择要从中还原数据的客户机。
2. 选择还原模式:
   - 还原组件

     仅当要还原到的客户机支持 VSS 时 (例如，如果还原到 Windows Server 2008 客户机)，才使用此模式。

     您只能还原整个复本。

   - 还原文件

     客户机不需要支持 VSS，您可以还原单个文件夹或文件。
3. 选择 DPM 写入程序进行还原时，“仅”选择“复本”组件。不要选择 DPM 数据库。
4. 单击“选项”选项卡，然后在“还原到另一个客户机”下，输入目标客户机的名称。单击“下一步”。
5. 继续执行常规 VSS 写入程序还原。

Microsoft Exchange Server 2010 写入程序详述

概念

本节提供 Microsoft Exchange Server 2010 其他功能的详细信息。

连续复制

Microsoft Exchange Server 2010 为数据保护提供 Data Protector 支持的两种复制模式。

- 本地连续复制 (LCR)

  使用 LCR，可以在存储组中创建和维护数据库的精确副本 (LCR 副本)。在数据损坏时使用 LCR 副本，因为您只需几秒钟即可将 Exchange Server 切换为使用 LCR 副本。如果 LCR 副本用于备份，并且所处于的磁盘与原始数据不同，则生产数据库上的负载极小。

- 群集连续复制 (CCR)

  CCR 与 LCR 具有相同的特征。唯一的区别是在 CCR 环境中，数据库和事务日志被复制到不同的服务器。因此，CCR 副本可用于灾难恢复。可以在 CCR 副本所在的被动 Exchange Server 节点上执行 VSS 备份，从而降低活动节点上的负载。

复制的存储组表示为 Exchange Server 写入程序的一个新实例，即 Exchange 复制服务。备份它们的方式与备份原始或生产存储组一样。

如果使用配置了备用连续复制 (SCR) 的 LCR 或 CCR，则只能在 SCR 源端执行备份。Microsoft 不支持在 SCR 目标端执行备份。有关 SCR 和支持的 SCR 配置的详细信息，请访问 Microsoft 网站。

还原到原始位置或另一个位置

使用 Microsoft Exchange Server 2010 写入程序，您不仅可以将数据还原到原始位置 (从中执行备份)，还可以还原到其他位置。您可以还原:

- 整个存储组
- 单个存储

在这两种情况下，还可以还原相应的 LCR 或 CCR 副本。

您可以将数据还原到:

- 原始存储组
- 不同存储组
- 非 Exchange 位置 - 使用此还原方法，在还原完成后，可以自动创建恢复存储组 (RSG)。
- 恢复服务器 - 此还原方法将数据还原到不同客户机和不同存储组。

如果还原到不同存储组，则可以在不同位置访问单个邮箱或电子邮件，而不更改原始存储组内容。此外，如果整个服务器被销毁，则还原到不同 Exchange Server 系统 (恢复服务器) 将最大程度地缩短邮箱不可用的时间段。

备份

备份类型

Microsoft Exchange Server 写入程序支持以下 Microsoft Exchange 备份类型:

- *完整* - 备份数据库、事务日志和检查点文件。截断事务日志。
- *增量* - 备份事务日志以记录自最后一个完整或增量备份以来的更改。截断事务日志。

  此备份类型对 VSS 硬件提供程序不可用。

- *差异* - 与增量备份相似，但不截断事务日志。

  此备份类型对 VSS 硬件提供程序不可用。

- *副本* - 与完整备份类似，区别在于不截断事务日志。此备份类型不应该用于恢复发生故障的系统。

前滚恢复要求

为确保可以从备份进行前滚恢复，请考虑以下几点:

标准还原: 必须备份事务日志才能启用前滚操作。

即时恢复: 通过对在支持即时恢复的会话 (ZDB 到磁盘和 ZDB 到磁盘 + 磁带) 中备份的对象执行增量或差异 ZDB 到磁带，可以执行存储组前滚。如果日志在磁盘上仍然可用，则上次完整备份的还原会将存储前滚到最新状态 (记录在日志中)。

一致性检查

仅当复制的数据文件的一致性检查成功时，才认为 Microsoft Exchange Server 数据库的备份成功。默认情况下启用一致性检查。要禁用一致性检查，请单击创建的备份规范，右键单击“源”选项卡中的“Microsoft Exchange Writer”，然后单击“其他选项”。在此页面中，您还可以指定在指定的输入/输出操作数之后将一致性检查暂停一秒钟。

一致性检查还可以在即时恢复之前运行。

LCR 和 CCR 环境

在 LCR 和 CCR 环境中，复制的存储组表示为 Exchange Server 写入程序的一个新实例，即“Exchange 复制服务”。备份复制的存储组的方式与备份原始 (生产) 存储组一样。

可以选择存储组的任意组合进行备份。但是，不能在同一备份规范中选择原始存储组及其复制的存储组。请参阅选择复制的 Microsoft Exchange Server 2010 存储组。

CCR 环境中的群集支持

在 CCR 环境中，可以选择要从中执行备份的群集节点，不管此节点上驻留着哪个实例 (信息存储或复制服务)。如果选择群集节点，则 Data Protector 将备份此节点上任何可用的实例，同时忽略在 GUI 中选择的实例，例如，即使选择复制的存储组 (Exchange 复制服务) 作为备份对象。

要指定群集节点，以便从中执行位于该节点上的任何实例的备份，请右键单击 Exchange Writer，然后单击“其他选项”。在“其他 MS Exchange 选项”对话框中，在“从节点备份任意可用实例”下选择该节点。。请参阅 CCR 环境中的其他 Microsoft Exchange Server 2010 选项。

备份复制服务实例时，由于以下任一原因，备份可能会失败:

- 所选节点不可用。
- 要备份的存储组的状态不是“运行正常”。
- Data Protector 未在所选节点上运行。
- Vssbar.exe 无法在所选节点上启动。

为避免会话失败，请在同一对话框中选择“在失败时恢复为活动节点”选项。将在原始服务器（活动群集节点）上重新启动备份，并且将备份原始存储组。在备份信息存储实例期间，将忽略此选项。

还原

可以通过执行标准还原或即时恢复会话来还原 Microsoft Exchange Server 数据:

- 请参见标准还原。
- 请参见即时恢复。

只能从最新备份还原单个数据库 (存储)。要将数据库还原到较早的时间点，必须还原完整存储组。

标准还原

可能出现以下情况:

- 一个或多个数据库已损坏，但日志文件未损坏。在这种情况下，将还原数据库并应用事务日志 - 从丢失的一个或多个数据库执行前滚恢复。
- 日志文件损坏或丢失。在这种情况下，需要还原所有数据库和日志文件。无法前滚恢复数据库 - 在日志文件丢失后执行时间点还原。
- 邮箱中的某些数据已丢失。例如，电子邮件被误删。需要将邮箱还原到较早的时间点。有关详细信息，请参阅还原单个邮箱。

一致性检查

（可选）要指定用于 Microsoft Exchange 写入程序一致性检查的选项，请右键单击该写入程序，并单击**其他选项**。

从丢失的一个或多个数据库前滚恢复

对于前滚恢复:

1. 使用 Microsoft Exchange System Manager 从目标存储所在的存储组中卸除所有存储。
2. 在 Data Protector GUI 中，切换到“还原”上下文。展开“还原对象”和“MS 卷影复制写入程序”，然后选择要从中还原数据的客户机。

   在“结果区域”中，展开 Microsoft Exchange Writer 并选择要恢复的存储。“日志”组件带阴影，无法选择。

> **注意**始终从最新备份还原单个存储 (数据库)。可用于指定备份版本的“属性”菜单在存储级别不可用。

3. 继续执行常规 VSS 写入程序还原。
4. 使用 Exchange System Manager 从存储驻留的存储组装载所有存储。恢复所选存储。

在日志文件丢失后执行时间点还原

要执行时间点还原，请执行以下操作:

1. 启动 Exchange System Manager，并检查是否已卸除存储组。否则，卸除整个组。
2. 切换到“还原”上下文。展开“还原对象”和“Microsoft 卷影复制写入程序”，然后选择要从中还原数据的客户机。

   在“结果区域”中，展开 Microsoft Exchange Writer 并选择整个存储组。不要选择单个存储。
3. 继续执行常规 VSS 写入程序还原。
4. 使用 Exchange System Manager 从目标存储所在的存储组装载存储。装载所有存储并使其与上次所选完整、增量或差异备份时的状态相同。

还原单个邮箱

要还原单个邮箱，请执行以下操作:

1. 打开 Data Protector GUI。在“上下文列表”中，单击**恢复**。展开“还原对象”和“MS 卷影复制写入程序”，然后选择要从中还原数据的客户机。
2. 在“结果区域”中，展开 Microsoft Exchange Writer 并选择包含此特定邮箱的存储组。右键单击该存储组，单击“属性”，然后指定所需的时间点。

   右键单击该存储组，并单击“还原为”。在“其他 MS Exchange 选项”对话框中，选择“还原到非 Exchange 位置并创建 RSG”选项。在“原始”下拉列表中，选择包含相应邮箱的数据库，单击“添加”，然后单击“确定”。
3. 按照常规 VSS 写入程序还原过程中所述继续操作。
4. 还原数据库之后，装载数据库: 打开 Exchange Management Shell 或其他某个 GUI 工具，如 Exchange Server 灾难恢复分析工具。

   要列出所有可用数据库，请执行:

   ```
   [PS] C:\>get-mailboxdatabase
   ```

   ```
   名称 服务器 存储组 恢复 ---- ------ ------------ -------- LCR_store1 TPC181 LCR_sg1 False sg3_store1 TPC181 sg3_local False store1 exchclu3 sg1 False sg3_store2 TPC181 sg3_local False sg1_store5 TPC181 First Storage Group False sg4_store1 TPC181 sg4 False sg3_store2 TPC181 DP RSG True
   ```

   在上面的示例中，已还原到恢复存储组 DP RSG 的数据库名为 sg3_store2 。

   要装载数据库，请执行:

   ```
   [PS] C:\>mount-database -identity "TPC181\DP RSG\sg3_store2"
   ```
5. 假定相关邮箱属于 John Doe。要从已还原的数据库中提取邮箱项并将这些项移动到 John Doe 邮箱的 RSG 文件夹，请执行:

   ```
   [PS] C:\>restore-mailbox -RSGMailbox "John Doe" -RSGDatabase "TPC181\DP R SG\sg3_store2" -identity "Doe" -TargetFolder RSG
   ```

   ```
   确认 是否确定要执行此操作? 将邮箱内容从恢复数据库 'TPC181\\DP RSG\\sg3_store2' 中的 邮箱 'John Doe' 恢复到 'John Doe (Doe@dp2.com)' 的邮箱。该操作可能需要很长时间才能完成。 [Y] 是 [A] 全是 [N] 否 [L] 全否 [S] 暂挂 [?]帮助 (默认为 "Y"):Y Identity : dp2.com/Users/John Doe DistinguishedName : CN=John Doe,CN=Users,DC=dp2,DC=com DisplayName : John Doe Alias : Doe LegacyExchangeDN : /o=DataProtector/ou=First Administrative Gro up/cn=Recipients/cn=Doe PrimarySmtpAddress : Doe@dp2.com SourceServer : TPC181.dp2.com SourceDatabase : TPC181\DP RSG\sg3_store2 SourceGlobalCatalog : TPC136 SourceDomainController : TargetGlobalCatalog : TPC136 TargetDomainController : TargetMailbox : dp2.com/Users/John Doe TargetServer : TPC181.dp2.com TargetDatabase : TPC181\sg3_local\sg3_store2 MailboxSize : 40553300B IsResourceMailbox : False SIDUsedInMatch : SMTPProxies : SourceManager : SourceDirectReports : SourcePublicDelegates : SourcePublicDelegatesBL : SourceAltRecipient : SourceAltRecipientBL : SourceDeliverAndRedirect : MatchedTargetNTAccountDN : IsMatchedNTAccountMailboxEnabled : MatchedContactsDNList : TargetNTAccountDNToCreate : TargetManager : TargetDirectReports : TargetPublicDelegates : TargetPublicDelegatesBL : TargetAltRecipient : TargetAltRecipientBL : TargetDeliverAndRedirect : Options : Default SourceForestCredential : TargetForestCredential : TargetFolder : \RSG\Recovered Data - John Doe - 02.1 0.2008 16:49:59 PSTFilePath : RsgMailboxGuid : 0441be6c-46f6-4d8f-8562-ab615731ae89 RsgMailboxLegacyExchangeDN : /O=DATAPROTECTOR/OU=FIRST ADMINISTRATIVE GRO UP/CN=RECIPIENTS/CN=DOE RsgMailboxDisplayName : John Doe RsgDatabaseGuid : deb5029b-4737-4fea-8c2d-ece24007e75d StandardMessagesDeleted : 0 AssociatedMessagesDeleted : 0 DumpsterMessagesDeleted : 0 MoveType : 还原 MoveStage : 已完成 StartTime : 02.10.2008 16:50:06 EndTime : 02.10.2008 16:50:12 StatusCode : 0 StatusMessage : 恢复存储组数据库中的此 邮箱已还原到目标用户 邮箱。 ReportFile : C:\Program Files\Microsoft\Exchange Server\L ogging\MigrationLogs\restore-Mailbox20081002 -164958-8141342.xml
   ```

将 LCR 或 CCR 副本还原到原始位置

如果将 LCR 或 CCR 副本还原到原始位置，则会执行到原始数据库 (Exchange 信息存储) 而不是数据库副本 (Exchange 复制服务) 的还原。

1. 右键单击一个存储组、存储或日志，并单击“还原为”。

2. 在“其他 MS Exchange 选项”对话框中，为要还原的组件选择目标位置: 目标服务器、目标存储组和目标存储。可用的选项如下：

   - **恢复到不同的存储**

     默认情况下选择此选项。

     选择此选项可为要还原的每个存储选择目标存储 (原始存储)。首先，从“目标服务器名称”下拉列表中选择目标系统，然后通过在“原始”和“目标”下拉列表中选择条目来选择所需的存储对。注意，无法仅还原存储，因此在还原会话中自动选择不同位置的日志。

   - **恢复到非 Exchange 位置**

     选择此选项以将数据还原到非 Exchange 位置。在这种情况下，还原的数据不会由 Exchange Server 管理，并且将不创建恢复存储组 (RSG)。您可以在还原会话完成后手动创建 RSG。首先，从“目标服务器名称”下拉列表中选择目标系统，然后使用“原始”下拉列表选择所需的存储。

   - **恢复到非 Exchange 位置并创建 RSG**

     选择此选项以将数据还原到非 Exchange 位置。恢复之后，Data Protector 将在目标服务器上创建名为 DP RSG 的恢复存储组。所选的存储和日志将还原到此恢复组。首先，从“目标服务器名称”下拉列表中选择目标系统，然后使用“原始”下拉列表选择所需的存储。

   默认情况下，将存储组还原到 C:\Omni 目录中。要选择另一个位置，请使用“还原到位置”选项。单击“浏览”并选择所需位置。

   > **重要说明**所选目录必须为空，或可以指定创建新目录。如果目录不为空，则还原会话失败。

   注意，只能为存储组而不能为特定存储指定还原位置。

即时恢复

使用 Microsoft Exchange Server 2010，可以将整个存储组或单个存储还原到原始位置或不同位置。有关详细信息，请参见。

请注意，如果未选择目标卷上的所有对象进行还原，则还原到原始位置将失败。例如，如果目标卷上有四个存储和事务日志，并且仅选择一个存储进行还原，则还原会话将失败。因此，还原 Microsoft Exchange Server 数据时，可能有以下配置方案:

- 事务日志和数据库存储在相同目标卷上。

  无法在 GUI 或 CLI 中为即时恢复仅选择数据库存储。如果事务日志和/或数据库存储丢失，则需要恢复整个存储组 (或目标卷上的所有对象)。

  在这种情况下，只能执行“时间点”恢复。事务日志将替换为备份事务日志。

- 事务日志和数据库存储在不同目标卷上。

  可以在 GUI 或 CLI 中为即时恢复仅选择数据库存储。如果数据库存储丢失，只要它单独位于要恢复的目标卷上，就可以单独恢复。否则，必须为还原选择目标卷上的所有存储。如果事务日志丢失，则应当恢复整个存储组。

  在这种情况下，可以执行“时间点”或者“前滚”恢复。

  要执行 Microsoft Exchange Server 写入程序的“时间点”恢复，请选择整个存储组。事务日志将替换为备份事务日志。

  要执行“前滚”恢复，请仅选择数据库存储和原始位置。现有事务日志将应用于还原的数据库。但是，如果以前执行了相同备份会话的“时间点”恢复，则不可能执行前滚恢复。

- 邮箱中的某些数据已丢失。例如，电子邮件被误删。需要将邮箱还原到较早的时间点。当事务日志和数据库驻留在同一存储卷上以及驻留在不同存储卷上时，需要执行“时间点”恢复，此操作在这两种配置中均可用。还原单个邮箱的过程与执行标准还原的过程类似 (请参阅还原单个邮箱)。但是，您还需要考虑本节中所述的特定于即时恢复的信息。

  即时恢复后步骤

  1. 手动重新装载数据库存储。如果还原到恢复存储组，请在此 RSG 中重新装载数据库存储。
  2. 如果将 LCR 或 CCR 副本还原到了原始数据库，则执行其他步骤：
     - 对于 LCR 还原，建议将还原的数据库作为种子，将原始数据库与其副本同步。

       有关详细信息，请访问网页 http://technet.microsoft.com/en-us/library/aa995973.aspx。
     - 对于 CCR 还原，您可能需要执行其他步骤。

       > ⚠ **警告**首先完成以下过程，才能将群集邮箱服务器移动到其他节点 (使用 Move-ClusteredMailboxServer cmdlet)。如果此时移动服务器，可能会发生数据丢失。

       请执行以下步骤，以启用原始和副本数据库的正常操作:

       a. 在应用程序系统上，装载还原的存储。

b. 在数据库的副本所在的被动节点上，删除事务日志。

c. 在被动节点上，使用 Update-StorageGroupCopy cmdlet 将存储组副本作为种子，或者重新同步原始存储组及其副本。

d. 在被动节点上，使用 Resume-StorageGroupCopy cmdlet 恢复存储组副本。

数据库恢复

可以从 Data Protector GUI 的“即时恢复”上下文运行数据库恢复。如果使用与在即时恢复的备份规范中相同的对象和说明为增量/差异备份创建了单独的备份规范，则此选项可用。此类增量/差异备份基于使用所选即时恢复选项的完整备份。可以在“即时恢复”上下文中选择增量/差异备份，并开始还原。这将执行即时恢复，并且事务日志将自动应用于恢复的存储组。

故障诊断

问题

备份会话等待 10 分钟完成

默认情况下，Data Protector 等待 600 秒让 Microsoft Exchange Server 2010 写入程序稳定下来。

操作

虽然 Microsoft 建议使用此稳定延迟，但您可以通过设置 OB2VSS_EXCHANGE_WRITER_STABILIZATION omnirc 选项来更改等待期间。以秒为单位指定等待期间。

Microsoft Exchange Server 2010 写入程序详述

本节介绍使用 Data Protector Microsoft Shadow Copy Service 集成时 Microsoft Exchange Server 2010 写入程序的详细信息。

> **注意**建议您使用 Data Protector Microsoft Exchange Server 2010 集成，而不是通用 VSS 集成。
>
> Data Protector Microsoft Exchange Server 2010 集成提供附加功能并简化备份配置，使您可以在一个会话中从 DAG 的不同系统备份多个数据库副本 (活动和被动) 等等。

Microsoft Exchange Server 2010 引入了数据库可用性组 (DAG)，这是 Exchange Server 2010 SCR 和 CCR 概念发展的结果。每个 DAG 最多可包含 16 个系统，这些系统可以托管多个活动和/或被动数据库副本。被动副本与主动副本保持一致，如果特定节点上的数据损坏，DAG 会自动进行自我修复。例如，如果被动副本损坏，则会重新将被动副本作为种子。如果无法再修复主动副本，则其中一个被动副本将成为主动副本。

主动副本和相关的被动副本表示同一数据库，可以在还原期间进行交换。这意味着您可以从被动副本备份还原主动副本，反之亦然。

因此，涉及 Data Protector 的最常见方案包括 (但不限于):

- 备份被动副本，从而避免在备份期间主动副本上产生额外的负载
- 还原丢失或损坏的被动副本，避免在重新将被动副本作为种子时产生大量网络流量
- 将数据库还原到时间点 (例如，用于调查目的)

有关其他还原方案，请参阅还原方案。

将 Data Protector Microsoft 卷影复制服务集成与 Exchange Server 2010 相集成

使用此集成，您可以备份 Microsoft Exchange Server 2010 写入程序。Exchange Server 2010 备份和还原使用两个写入程序:

- Microsoft Exchange Writer (用于主动副本)
- Microsoft Exchange Replica Writer (用于被动副本)

使用这些 Exchange 写入程序，只能备份来自 DAG 中物理节点 (系统) 的数据库。DAG 是一个虚拟实体，无法被 Data Protector 识别，不能进行备份。

许可

由于需要备份单个客户机时，因此必须为每个安装了 Data Protector MS 卷影复制集成组件的系统提供一个联机扩展许可证。

配置 Microsoft Exchange Server 2010

要配置 ZDB 集成并确保磁盘解析有效，建议您在要从中进行备份的客户机上运行以下命令:

omnidbvss –resolve –apphost *ClientName*

其中，*ClientName* 是 Microsoft Exchange Server 2010 系统的名称，例如 server1.company.com 。有关详细信息，请参阅 omnidbvss 参考页。

如果未事先运行该命令，Data Protector 将在第一个 ZDB 会话期间自动运行此命令，这可能会降低备份会话的速度。

备份

使用 Data Protector Microsoft 卷影复制服务集成，您可以在物理客户机或单个邮箱数据库副本 (活动或被动) 上备份 Exchange Writer 或 Exchange Replica Writer。不能单独选择邮箱数据库的数据库文件或日志。

支持以下 Microsoft Exchange Server 2010 备份类型:

- 完整
- 增量 (仅限 VSS 软件提供程序)
- 差异 (仅限 VSS 软件提供程序)
- 复制

创建备份规范

要创建备份规范，请遵循创建备份规范中描述的过程。

选择备份对象 (数据库) 时，请考虑以下几点:

- 要为主动副本创建备份规范，请选择“Microsoft Exchange Writer”。
- 要为被动副本创建备份规范，请选择“Microsoft Exchange Replica Writer”。

> **重要说明**故障转移之后，被动副本将成为主动副本，而主动副本则变为被动副本。在这种情况下，数据库备份对象将失败，因为备份规范不会自动进行更新，并且 Data Protector 尝试使用适用于被动副本的 Exchange Replica Writer 备份主动副本。您必须手动更新备份规范并选择正确的写入程序。

还原

遵循还原中所述的标准还原过程。本节中的还原方案仅介绍 Microsoft Exchange Server 2010 的详细信息。

还原方案

还原被动副本

您可以从一系列活动或被动副本备份还原被动副本。

数据库文件和日志都丢失时还原

1. 使用 Exchange 管理控制台暂挂数据库复制。
2. 右键单击要还原的数据库，然后打开“属性”窗口。在“维护”页面中，选择“还原时可以覆盖此数据库”。
3. 在 Data Protector GUI 中，选择“还原”上下文。在“范围窗格”中，单击“MS 卷影复制”，然后选择从中备份数据库的客户机。您可以选择任何客户机，而不仅仅是要还原的客户机。
4. 根据备份的是主动副本还是被动副本，展开 Microsoft Exchange Writer 或 Microsoft Exchange Replica Writer，然后选择备份的数据库副本。

   要还原到与执行备份的客户机不同的客户机，请转到“选项”页面，然后从“还原到另一个客户机”下拉列表中选择相应客户机。
5. 指定设备和介质选项。有关详细信息，请按 **F1**。
6. 启动还原。
7. 恢复复制。

仅数据库文件丢失时还原

如果仅丢失了数据库文件，但日志在系统上仍然可用，则只能还原数据库文件:

1. 使用 Exchange 管理控制台暂挂数据库复制。
2. 右键单击要还原的数据库，然后打开“属性”窗口。在“维护”选项卡中，选择“还原时可以覆盖此数据库”。
3. 在 Data Protector GUI 中，选择“还原”上下文。在“范围窗格”中，展开“MS 卷影复制”，然后选择从中备份数据库的客户机。您可以选择任何客户机，而不仅仅是要还原的客户机。
4. 根据备份的是主动副本还是被动副本，展开 Microsoft Exchange Writer 或 Microsoft Exchange Replica Writer，然后展开数据库备份副本。

   选择“文件”。

   要还原到与执行备份的客户机不同的客户机，请转到“选项”页面，然后从“还原到另一个客户机”下拉列表中选择目标客户机。请参见还原到另一个客户机。
5. 指定设备和介质选项。有关详细信息，请按 **F1**。
6. 启动还原。

7. 恢复复制

还原主动副本

您可以从主动副本或任何被动副本的完整和增量备份链中还原主动副本。

> **重要说明**由于被动副本并非总是立即更新，因此使用此类备份映像的时间点恢复 (还原数据库和事务日志文件) 可能会导致主动副本的最后状态与备份时的状态不同。

数据库文件和日志都丢失时还原

1. 使用 Exchange 管理控制台卸除数据库。
2. 暂挂数据库复制。在 Exchange 管理控制台中，右键单击将还原的数据库，然后打开“属性”窗口。在“维护”页面中，选择“还原时可以覆盖此数据库”。请参阅对数据库启用还原
3. 在 Data Protector GUI 中，选择“还原”上下文。在“范围窗格”中，展开“MS 卷影复制”，然后选择从中备份数据库的客户机。您可以选择任何客户机，而不仅仅是要还原的客户机。
4. 根据备份的是主动副本还是被动副本，展开 Microsoft Exchange Writer 或 Microsoft Exchange Replica Writer，然后选择数据库。

   如果从中备份的系统当前托管主动副本，则备份的副本将自动还原为主动副本。

   如果从中备份的系统当前托管被动副本 (例如，如果发生故障转移)，请从“还原到另一个客户机”下拉列表中选择托管当前主动副本的客户机。请参见还原到另一个客户机。
5. 指定设备和介质选项。有关详细信息，请按 **F1**。
6. 启动还原。
7. 使用 Exchange 管理控制台装载数据库。
8. 恢复复制。

仅数据库文件丢失时还原

1. 使用 Exchange 管理控制台卸除数据库。
2. 暂挂数据库复制。在 Exchange 管理控制台中，右键单击将还原的数据库，然后打开“属性”窗口。在“维护”页面中，选择“还原时可以覆盖此数据库”。请参阅对数据库启用还原。
3. 在 Data Protector GUI 中，选择“还原”上下文。在“范围窗格”中，展开“MS 卷影复制”，然后选择从中备份数据库的客户机。您可以选择任何客户机，而不仅仅是要还原的客户机。
4. 根据备份的是主动副本还是被动副本，展开 Microsoft Exchange Writer 或 Microsoft Exchange Replica Writer，然后展开备份的数据库。
5. 选择“文件”。

   如果从中备份的系统当前托管主动副本，则备份的副本将自动还原为主动副本。

   如果从中备份的系统当前托管被动副本 (例如，如果发生故障转移)，请从“还原到另一个客户机”下拉列表中选择托管当前主动副本的客户机。请参见还原到另一个客户机。
6. 指定设备和介质选项。有关详细信息，请按 **F1**。
7. 启动还原。
8. 恢复复制。

时间点还原

对于时间点还原，必须将主动副本和被动副本还原到同一时间点，或者必须为被动副本手动完整地重新设定种子。要避免为被动副本完整地重新设定种子，必须从同一备份副本还原活动和被动副本。

1. 使用 Exchange 管理控制台卸除数据库。
2. 右键单击要还原的数据库，然后打开“属性”窗口。在“维护”页面中，选择“还原时可以覆盖此数据库”。请参阅对数据库启用还原
3. 暂挂数据库复制。
4. 还原主动副本。请参阅还原主动副本。

   然后选择要用于还原的数据库备份副本，右键单击数据库并选择“属性”。选择要将主动副本还原到的时间点。
5. 如果不想为被动副本完整地重新设定种子，请还原被动副本。请参阅还原被动副本。

   选择要用于还原的数据库备份副本时，请选择用于主动副本的同一数据库备份副本，右键单击数据库，然后选择“属性”。选择与为主动副本选择的时间点相同的时间点。
6. 使用 Exchange 管理控制台装载活动数据库。
7. 恢复复制。

即时恢复

使用备份中所述的标准即时恢复过程。有关一般先决条件和条件 (例如，卸除 Microsoft Exchange Server 数据库、暂停复制)，请参阅还原方案。本节列出其他即时恢复限制。

故障诊断

有关常规 VSS 故障诊断，请参阅故障诊断。

问题

DAG 中发生故障转移之后，Data Protector 报告找不到某些 Microsoft Exchange Writer 组件:

[Major] From: OB2BAR_VSSBAR@server5.company.com "MSVSSW" Time: 12/7/2009 1:16:40 PM

Failed to find component that would match tree:

'/Microsoft Exchange Replica Writer(Exchange Replication Service)'.

操作

可以通过两种不同的方式解决此问题:

- 更新备份规范以使用正确的写入程序。
- 执行故障转移，使数据库恢复到原始状态 (活动或被动)，将不再报告该问题。

Microsoft Hyper-V 写入程序详述

Microsoft Hyper-V 写入程序是 Microsoft Virtual Server 2005 写入程序的后续版本，在 Microsoft Windows Server 2008 上受支持。它是一个 VSS 写入程序，具有一套与 Virtual Server 类似的功能。结合两者，可以执行虚拟机的备份和还原。通过 Hyper-V，可以使用硬件提供程序执行联机备份。

有关 Hyper-V 写入程序的备份和还原详细信息，请参阅备份和还原。

备份

使用 Hyper-V VSS 写入程序，可以备份:

- Hyper-V 配置
- 虚拟机

Data Protector VSS 集成支持以下两种类型的备份:

- *联机备份*

  使用软件提供程序或硬件提供程序联机备份 Hyper-V 写入程序数据。

  如果使用硬件提供程序进行联机备份过程，Hyper-V 写入程序将创建卷影副本，该副本将通过 VSS 硬件提供程序与 *vhd* 文件一起复制。之后，卷影副本将呈现给虚拟机监控程序系统。对于可传输备份，随后从虚拟机监控程序系统隐藏卷影副本，并将其呈现给备份规范中指定的备份系统。

  联机备份会话还原之后，无论还原之前的状态如何，虚拟机始终处于关闭状态。

- *脱机备份*

  在以下情况下执行脱机备份:

  - 来宾操作系统 - Hyper-V 支持的任何其他非 Microsoft 来宾操作系统 - 未启用 VSS。
  - 来宾操作系统未安装 Hyper-V VSS 集成服务。
  - 要备份的虚拟机已关闭。

  在脱机备份之前，虚拟机会自动暂挂 (如果尚未暂挂)，并在备份之后恢复。

  脱机备份会话还原之后，无论还原之前的状态如何，虚拟机都处于暂挂状态。

  脱机备份的优势在于虚拟机将还原到备份时的状态，包括备份时运行的应用程序状态。之所以能这样，是因为虚拟机在备份期间处于暂挂状态。

从物理群集节点备份

从群集节点备份时，请考虑以下几点:

- 脱机备份会触发故障转移。

  在脱机备份期间，要备份的虚拟机会暂挂一段时间。群集服务器将此识别为故障并启动群集故障转移。要避免此类故障转移，请执行以下操作之一:

  - 仅运行联机备份。
  - 在运行脱机备份之前，使用故障转移群集管理器手动将虚拟机置于“已保存”状态。

- 每次发生故障转移时，您都需要使用其他备份规范。

  故障转移之后，运行虚拟机的主机名会发生更改。由于此更改不会反映在原始备份规范中，因此您需要创建新的备份规范，以便将新主

机名指定为应用程序系统名称。

还原

可以将 Hyper-V 写入程序数据还原到原始位置或其他位置。在还原到其他位置期间，Hyper-V 写入程序会检查系统上是否已存在具有相同标识的虚拟机。如果是，则 Hyper-V 写入程序会在还原之前从系统中删除该虚拟机，并导入已还原的虚拟机。如果系统上不存在此类虚拟机，则表示正在进行到此系统的还原会话或已删除该虚拟机。可以将 Hyper-V 虚拟机还原或即时恢复到任何具有 Hyper-V 写入程序的 Hyper-V 系统。

从物理群集节点还原

可以使用标准还原过程将物理群集节点中的 ZDB 到磁带会话还原到任何群集节点。要成功将此类会话还原到群集节点，请执行以下步骤:

可以将物理群集节点中的备份会话还原到任何群集节点。要成功将此类会话还原到群集节点，请执行以下步骤:

1. 使用“故障转移群集管理”删除要还原的虚拟机的群集组。
2. 在虚拟机磁盘处于活动状态的群集节点上执行虚拟机的标准还原。有关标准还原过程，请参阅。
3. 使用“故障转移群集管理”重新创建虚拟机群集组。

故障诊断

问题

Microsoft Hyper-V 虚拟机的备份会话意外结束

备份 Microsoft Hyper-V 虚拟机时，会话意外结束，出现与下面类似的错误:

```
[重大] 来自: OB2BAR_VSSBAR@computer.company.com "MSVSSW" 时间: 2/1/2011 11:29:03 AM [145:575] 写入程序 'Microsoft Hyper-V VSS Writer' 无法准备要备份 的文件: 报告的状态: VSS_WS_FAILED_AT_POST_SNAPSHOT 预期状态: VSS_WS_WAITING_FOR_BACKUP_COMPLETE 故障代码: VSS_E_WRITERERROR_NONRETRYABLE
```

可能的原因如下:

- 主机 (虚拟机监控程序) 系统上禁用自动装载。有关详细信息，请参阅 http://support.microsoft.com/kb/2004712。
- 虚拟机内部存在问题，例如卷影副本的可用磁盘空间不足、使用了非 NTFS 文件系统等等。

操作

检查是否在主机虚拟机监控程序系统上启用了自动装载。例如：

```
diskpart.exe Microsoft DiskPart 版本 6.1.7600 版权所有 (C) 1999-2008 Microsoft Corporation。 在计算机上: TPC021 DISKPART> automount 已启用自动装载新卷。
```

如果禁用自动装载，请通过执行以下命令启用:

```
MOUNTVOL /E
```

如果即使启用了自动装载，该问题仍然存在，请检查虚拟机内的应用程序日志以确定原因。

Microsoft SharePoint Services Writer 详述

Microsoft SharePoint Services Writer 是一个与 Windows VSS 框架集成的引用写入程序，使备份应用程序可以备份和还原 Microsoft SharePoint 数据。此写入程序依赖于:

- 搜索写入程序:
  - OSearch VSS 写入程序
  - SPSearch VSS 写入程序
- SQL 写入程序:
  - MSDE Writer for Microsoft SQL Server 2000

使用 SharePoint Services Writer，您可以备份和还原:

- 配置数据库
- 集中管理的内容数据库
- 其他内容数据库
- 共享服务提供程序数据库
- 搜索数据库
- 索引文件。

备份类型

SharePoint Services Writer 支持以下 Microsoft Office SharePoint Server 2010 备份类型:

- 完整 (适用于数据库和索引文件)

限制

- 不支持多服务器 SharePoint 配置 (场)。

先决条件

- 默认情况下，不启动 SharePoint Services Writer 和 SQL Writer。确保这两个写入程序均已正确安装和注册。必须使用 SharePoint 命令行管理工具注册 SharePoint Services Writer:

```
stsadm -o registerwsswriter
```

备份

以下限制适用：

- 如果备份单个写入程序组件，为确保数据同步，必须在同一会话中备份以下项目组合:
  - 配置数据库和集中管理的内容数据库
  - 搜索数据库和相应的索引文件

  这意味着，例如，您不应仅备份搜索数据库。相反，始终也选择相应的索引文件。
- 不要使用独立 (不是引用的一部分) OSearch 和 SPSearch 写入程序备份索引文件。如果使用，则搜索索引必须重新组织索引。

还原

要确保数据同步，必须在同一会话中还原以下项目:

- 配置数据库和集中管理的内容数据库
- 搜索数据库和相应的索引文件

这意味着，例如，您不应仅还原搜索数据库。相反，始终也选择相应的索引文件。

由于配置数据库和集中管理的内容数据库包含特定于系统的信息，因此您只能将其还原到配置为完全相同的环境，包括所有软件更新、服务器名称和服务器数量。

以下先决条件适用:

- 在执行还原之前，停止以下服务:
  - Windows SharePoint Services 管理
  - Windows SharePoint Services 搜索
  - Windows SharePoint Services 计时器
  - Office SharePoint Server 搜索
- 如果还原整个场，则必须关闭 Internet Information Server (IIS)。

MSDE 写入程序详述

还原

MSDE 写入程序用于备份和还原 Microsoft SQL 数据库。

> **重要说明**在还原 SQL 系统数据库 (master 、 model 、 msdb 和 pub) 之前，必须停止 SQL 服务。

在“结果区域”中展开“MSDE 写入程序”项时，将显示所有 Microsoft SQL Server 实例。每个实例均包括其所含的全部数据库。系统数据库 (master 、model、msdb 和 pub) 始终列在此处。

> **重要说明**如果还原系统数据库，则将更改整个内部数据库结构。

> **注意**只能进行时间点还原。不支持前滚还原。

仅当可以覆盖文件时才会还原用户数据库。MSDE 写入程序将在还原之前使用户数据库脱机，而 SQL 服务必须手动停止才能还原系统数据库。

MySQL 集成

This feature is available in the Premium Edition

本节提供特定于 Data Protector MySQL 集成的信息。其中介绍如何将 Data Protector 与 MySQL 数据库管理系统集成。此外还说明了为 MySQL 数据设置高效数据保护策略时需要考虑的概念和方法，以及以最少的工作量和宕机时间还原此类数据所需遵循的方法和过程。Data Protector MySQL 集成还支持备份和还原多主群集和/或主从群集。

备份

Data Protector 支持 MySQL 数据的热备份和温备份，具体取决于用于所选 MySQL 数据库表的基础存储引擎。热备份允许读取和更改涉及的数据库表，而温备份会锁定此类表以防写入，因此只能在会话期间进行读取。Data Protector 提供以下类型的交互式备份和安排的备份：

Data Protector 中的可用 MySQL 备份类型

备份类型	描述
完整备份	包括 MySQL 实例中的所有选定表和数据库，无论最近是否已对其进行修改。
增量备份	仅包括自上次备份 (完整备份或增量备份) 以后更改的数据。通过以高于完整备份映像的频率创建增量备份映像，可节省备份存储上的存储空间。增量备份数据将与先前创建备份的内容合并。
事务日志备份	仅包括选定 MySQL 实例的二进制日志。可通过保留事务日志备份映像并将其用于还原，依原样重新创建特定时间点的 MySQL 数据。

使用完整备份和增量备份可精确选择要包括在备份映像中的对象: 特定数据库和/或特定数据库表或整个实例。

Data Protector MySQL 集成不支持零宕机时间备份。

还原

为应对不同的使用案例和需求，Data Protector 提供不同的方法来还原 MySQL 数据。从备份映像还原数据之前，可定义还原过程的以下方面:

- 范围

  除了还原从 MySQL 实例备份的所有内容之外，还可以将还原范围缩小到特定数据库和数据库表。

- 数据目标

  已还原数据的目标位置可以是其原始位置，也可以是源客户机或其他客户机上的其他路径。对于整个实例还原，Data Protector 会根据还原的数据新建 MySQL 实例。

- 暂存

  Data Protector 可以直接将数据还原到目标位置 (就地还原)，也可以将数据还原到中间位置 (暂存还原)。对于暂存还原，稍后可以将还原的数据复制到或移至目标数据区域，或者可以保持存储在中间位置，使生产数据区域保持完好。就地还原需要的存储空间更少，但是，在出现问题时暂存还原可以更好地防止数据不一致。

- 还原数据的最终状态

  如果存在适当的还原链 (包括相应二进制日志的备份映像)，则可以重新创建以下时间的 MySQL 实例、数据库或数据库表:

  - 在所选完整备份或增量备份时
  - 在所选的稍后时间 (使用前滚的还原时间点)
  - 在其上次事务日志备份时 (前滚到可能的最新状态)

  对于时间点还原，将过滤还原的 MySQL 二进制日志中的事务，并仅将其应用于选择进行还原的对象 (整个实例、特定数据库)。

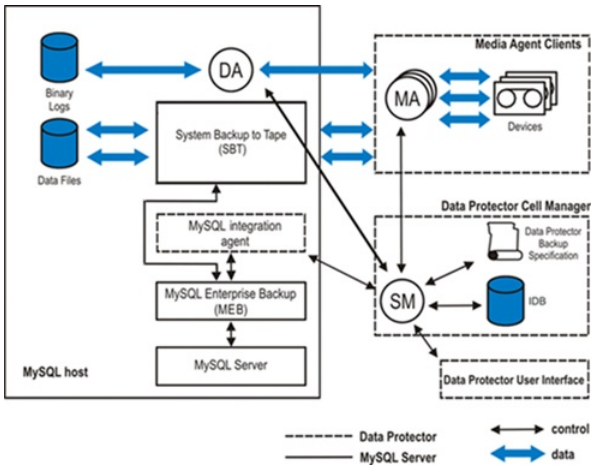
数据迁移

可通过 Data Protector MySQL 集成的还原功能迁移 MySQL 数据。此类迁移可以包括整个 MySQL 实例或者一个或多个数据库。根据选择进行迁移的内容，数据迁移过程会有所不同。

集成概念

Data Protector MySQL 集成通过系统备份到磁带 (SBT) 接口，利用 MySQL 企业备份 (MEB) 为 MySQL 提供企业级备份和恢复。Data Protector 使用 MySQL 集成代理与 MySQL 集成，该代理用于为 MEB 提供 Data Protector 接口。

MySQL 集成体系结构



图例

SM	Data Protector 会话管理器，在备份会话期间，作为备份会话管理器；在还原会话期间，作为还原会话管理器。
IDB	Data Protector 内部数据库，用于存储有关 Data Protector 会话的所有信息，包括会话消息、对象、数据以及所用的备份设备和备份介质。
MySQL 集成代理	MySQL 集成代理，在具有将使用 Data Protector 进行备份的 MySQL 数据库的系统上安装。
DA	Data Protector 磁盘代理，用于在磁盘卷中读取和写入数据。
MA	Data Protector 常规介质代理，用于从备份设备读取数据并将其写入备份介质。

满足 MYSQL 的先决条件

MySQL 集成的先决条件如下:

- 确保已正确安装和配置 MySQL 数据库管理系统:
- 确保已正确安装 Data Protector。
- 确保已根据 MySQL 数据保护策略配置 Data Protector 备份设备和备份介质。
- 确保选择用于运行 MySQL 备份和还原会话的 MySQL 操作系统用户帐户已在 Data Protector admin 或 operator 用户组中配置相应的 Data Protector 用户。
- 确保 Data Protector 文件系统备份和还原会话位于 MySQL 主机上。
- 确定 MySQL 主机上的 mysqlbackup 命令二进制文件的绝对路径。
- 必须在将使用 Data Protector 事务备份进行数据备份的所有 MySQL 实例上启用 MySQL 二进制日志。

> ⚠ **警告**要避免发生灾难时丢失数据，一定要在启用相应的二进制日志后立即执行 MySQL 实例的完整备份。

- 定义备份策略的范围时，还要考虑同一数据库的表通常相互关联。
- 对于增量备份，MySQL 备份范围应与上一次完整备份的范围相同。否则，还原链可能会断开，并且在还原期间数据可能会丢失。
- 对于基于 MySQL 数据创建的所有新备份对象，Data Protector 会在同一会话中创建伪备份对象。此额外实体用于存储原始备份对象的元数据。可根据其名称中的后缀 :METADATA 识别伪备份对象。
- 为了能够使用基础 InnoDB 存储引擎导入 (使用“将表导入到目标实例”选项进行还原) 数据库或数据库表，应启用按每个表的 MySQL 文件设置。
- 如果完整暂存还原的会话失败，请检查暂存目录中是否存在 Data Protector 可能留下的残留数据。手动删除此类数据以释放磁盘上的存储空间。
- 定义还原范围时，需要考虑同一数据库中的表通常相互关联。仅还原特定数据库的几个部分可能会导致该数据库中的数据不一致。
- 在暂存还原之后，MySQL 企业备份相关数据位于临时暂存目录中。
- 执行实例还原时，目标实例应处于脱机状态。如果将数据库和表导入现有实例，则目标实例应处于联机状态。
- 如果将数据还原到非原始客户机 (MySQL 主机):
  - 确保目标 MySQL 主机已安装 Data Protector MySQL 集成组件，并且属于 Data Protector 单元。
  - 确保已在 Data Protector 中配置目标 MySQL 实例。。

以下限制适用：

- 使用 Data Protector 无法备份具有循环二进制日志实施的 MySQL 配置。

- 增量备份类型仅可用于 InnoDB 数据库表。当增量备份会话中包含使用其他 MySQL 存储引擎的表时，系统将对此类表执行完整备份。
- MySQL 数据仅可还原到与备份数据的系统托管相同 MySQL 版本的系统。
- 仅当为备份启用 MySQL 独立表设置时，才可导入（用**将表导入到目标实例**选项还原）使用 InnoDB 存储引擎的数据库或数据库表。
- 使用 CLI (config 或 econfig) 或 GUI 重新配置 MySQL 集成会覆盖 MySQL 实例的现有配置文件。因此，您可能会丢失环境信息，例如 MEB 自定义选项、定义的 OB2BARHOSTNAME、数据库登录凭据和端口，具体取决于输入参数。使用 util_cmd –putopt 命令或 GUI 再次添加信息。

配置集成

在开始配置 Data Protector MySQL 集成之前，请检查先决条件。

要在 Data Protector 中配置 MySQL 实例，请在 Data Protector GUI 中执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MySQL”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在“结果”区域的“客户机”下拉列表中，选择 MySQL 主机。
5. 在“应用程序数据库”文本框中，输入 MySQL 实例名称或从下拉列表中选择现有名称。下拉列表显示所有正在运行的数据库实例的列表，即 Data Protector 中配置的数据库实例以及 Data Protector 中未配置的数据库实例。对于每个连接，实例名称 (MySQL 主机和通信端口的组合) 应具唯一性。未配置的正在运行的数据库实例将以下列格式显示: 未配置 <端口> [状态] (例如，未配置: 3434 [正在运行])。单击“下一步”。
6. 如果尚未配置实例，则将打开“配置”对话框。右键单击 MySQL 实例，然后选择“配置”。
7. 在“配置 MySQL 实例”对话框中，配置连接参数。执行以下某个操作：
   - 指定具有足够权限 (至少为 SUPER 权限) 的 MySQL 数据管理系统用户帐户的用户名和密码，以及实例使用的端口 (默认为 3306) 。

     > **注意**如果未在 MySQL 主机上启用 TCP/IP 协议，则指定套接字名称 (Linux) 或管道名称 (Windows)，而非端口号。

   - 选择“使用自定义 MySQL 配置文件中的参数”选项，并在从中获取参数的 MySQL 主机上指定自定义 MySQL 配置文件 (选项文件) 的路径。

     > **警告**当 Data Protector MySQL 集成提供的 MySQL 配置选项不足时，自定义 MySQL 配置选项文件是必需的。创建和编辑 MySQL 选项文件时，请特别注意。如果不能正确修改文件，不仅会导致 Data Protector 无法成功备份和恢复 MySQL 数据，通常还会导致 MySQL 数据库管理系统无法运行。

   在“mysqlbackup 命令的路径”文本框中，输入 MySQL 主机上 mysqlbackup 命令二进制文件的绝对路径。

   单击“确定”关闭对话框。
8. (可选) 使用 Data Protector util_cmd 命令指定其他 MySQL 连接参数和特定于 MySQL 的备份参数:

   > 必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。
   >
   > 设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

   - 用于设置 MySQL 连接参数:

     util_cmd -putopt MySQL InstanceName Key Value -sublist MYSQL_PARAM

     例如：

     util_cmd -putopt MySQL MYSQL56 "socket" "MySQL" -sublist MYSQL_PARAM

   - 用于设置特定于 MySQL 的备份参数:

     util_cmd -putopt MySQL InstanceName Key Value -sublist MEB_PARAM

     例如：

     util_cmd -putopt MySQL MYSQL56 "verbose" "TRUE" -sublist MEB_PARAM

配置完成后，Data Protector 会将指定的参数存储在 Cell Manager 上的相应配置文件中，并验证实例连接。

安装 MySQL 客户机

This feature is available in the Premium Edition

要将 Data Protector 与 MySQL 数据库管理系统集成并且希望能够备份 MySQL 实例和数据，请在 MySQL 主机上安装以下 Data Protector 组件：

- MySQL Integration

  此组件可用于执行 MySQL 数据库的集成备份和还原。

- Disk Agent

  此组件可用于备份和还原 MySQL 二进制日志，以满足执行 MySQL 数据库恢复的前提条件。它还可以用于执行 MySQL 数据的非集成备份，以便解决安装了 MySQL 的 Data Protector 客户机所存在的问题。

备份 MySQL 集成

This feature is available in the Premium Edition

Data Protector MySQL 集成提供 MySQL 数据库、数据库表和 MySQL 二进制日志的联机备份。可在创建备份规范时定义备份范围。

创建备份规范

要在 Data Protector GUI 中创建 MySQL 备份规范，请继续执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“MySQL”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，设置负载均衡和重复数据删除首选项。单击**确定**。
4. 在“结果”区域的“客户机”下拉列表中，选择 MySQL 主机。在“应用程序数据库”下拉列表中，选择要备份的 MySQL 实例。

   选择“指定 OS 用户”选项。在“用户名”和“组/域名”文本框中，输入相应的 MySQL 用户帐户。有关详细信息，请按 **F1**。

   单击“下一步”。
5. 选择要备份的数据库、数据库表或整个 MySQL 实例。单击“下一步”。
6. 选择用于备份会话的备份设备。如果需要，更改其顺序并调整负载均衡和对象镜像设置。

   右键单击该设备，然后选择“属性”以设置介质池、预分配策略和其他备份设备选项。有关选项的说明，请按 **F1**。单击**确定**。

   要创建其他备份副本 (镜像)，请通过单击“添加镜像”或“删除镜像”指定所需的数量。为每个镜像选择单独的设备。镜像的最小设备数等于用于备份的设备数。

   单击“下一步”。
7. 指定备份选项。

   单击“下一步”。
8. 单击“另存为”。
9. 在“将备份另存为”对话框的“名称”文本框中，输入备份规范的名称。在“组”下拉列表中，选择备份规范组。单击“确定”，保存备份规范。

   (可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

> **提示**要优化 MySQL 备份规范的组织，可通过将其保存在自行创建的同一专用 Data Protector 备份规范组中。

特定于应用程序的备份选项

下表列出特定于 MySQL 集成的备份选项。

选项	描述
常规选项	
Pre-exec、**Post-exec**	此选项用于指定在备份之前 (pre-exec) 或之后 (post-exec) 执行的命令行。 命令行将在运行备份会话的 MySQL 系统 (在此系统上启动了 Data Protector MySQL 集成代理) 上执行。 仅输入命令名称和所需参数，并确保该命令位于同一系统上的默认 Data Protector 命令目录中。不要使用双引号。
InnoDB 存储引擎选项	

启用备份数据压缩	此选项指定 Data Protector 是否应要求 MySQL 企业备份压缩从 MySQL 获取的备份数据。只能对基于 InnoDB 存储引擎的 MySQL 数据库表进行压缩。源于基于不同存储引擎的表的数据保存在未压缩的 MySQL 备份映像中。 默认: 未启用。
级别	此选项指定 MySQL 企业备份在将 MySQL 数据存储在 Data Protector 备份映像中前，用于压缩这些数据的压缩级别。 默认值：1.
二进制日志选项	
并行性	此选项指定在 Data Protector 事务日志备份会话中可并行备份的同一 MySQL 实例的二进制日志文件数。如果备份基础架构的所有部分都允许足够高的吞吐量，则可通过增加此选项的值，缩短对应的备份窗口。 默认值：1.
成功备份之后清除日志	此选项指定成功执行二进制日志备份后，Data Protector 是否应请求清理。清理二进制日志后，已成功备份的日志文件将从系统中删除，然后 MySQL 会开始在新的二进制日志中记录事务。 选择此选项可有效地减小二进制日志的备份映像大小并限制占用的存储空间的卷。备份中包括的二进制日志文件列表是在备份会话前，从 MySQL 服务器接收的。将仅备份自上次事务日志备份以后有更改的二进制日志文件。 默认：未选择。

MySQL 的规范选项:

util_mysqldb.pl -version|-help

util_mysqldb.pl -app

util_mysqldb.pl -chkconf <INSTANCE NAME>

util_mysqldb.pl -objs0 <INSTANCE NAME>

-objs1 <INSTANCE NAME> <DATABASE NAME>

列出所有实例的输出片段:

C:\Program Files\OmniBack\bin>perl -I ..\lib\perl util_mysqldb.pl -app

INS1 3306 [RUNNING]

Not-configured: 3434 [RUNNING]

*RETVAL*0

C:\Program Files\OmniBack\bin>

修改备份规范

有关修改 MySQL 备份规范的信息，请参阅《Data Protector 帮助》索引: “备份规范, 修改”。

多主数据库备份

进行群集备份的过程与在多主数据库节点设置中备份单个节点相同。任何多主数据库节点均可用于备份整个群集。

> **注意**Data Protector 管理数据备份，但不配置（创建或删除）群集。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

启动备份会话

还可以按需运行备份会话。此类会话 (称为交互式备份会话) 可用于紧急、即时数据保护以及重新启动失败的备份。

检查配置

可使用 Data Protector GUI 检查 Data Protector 中 MySQL 实例的配置。请执行以下操作：

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份规范”和“MySQL”，然后选择 MySQL 实例的备份规范。
3. 在“结果”区域中，右键单击 MySQL 实例，然后选择“检查配置”。如果配置检查成功，将显示以下消息：Integration is properly configured.

还原 MySQL 集成

This feature is available in the Premium Edition

Data Protector MySQL 集成支持还原 MySQL 数据库和二进制日志。还原范围在启动还原会话时进行定义。

在还原期间，如果使用 Windows Cell Manager 连接 Linux Cell Manager，则必须使用相同的代理配置两个 Cell Manager。

通过以下任意方式还原 MySQL 对象:

- 使用 Data Protector GUI。
- 使用 Data Protector CLI。
- 使用 REST API。

为了能够还原 MySQL 数据，首先从 Data Protector 内部数据库 (IDB) 检索有关 MySQL 备份会话的信息，例如备份类型、所用备份介质以及会话期间报告的消息。为此，请使用 Data Protector GUI 或 CLI。

- 使用 Data Protector GUI

  1. 在上下文列表中，单击**内部数据库**。
  2. 在“范围窗格”中，展开“对象”或“会话”。

     在对象树中，备份对象根据原始系统 (MySQL 主机) 进行分组。MySQL 主机按字母顺序进行排序。在会话树中，备份对象根据其创建会话进行分组，最新会话位于顶部。

     要查看备份对象详细信息，请右键单击该对象，然后单击“属性”。要查看报告的会话消息，请单击“消息”选项卡。

- 使用 Data Protector CLI 打开命令提示符窗口，然后运行 Data Protector omnidb -integ MySQL 命令。该命令用于检索使用 Data Protector 备份的 MySQL 对象的列表。然后，可以通过指定其他命令选项列出相应的会话和备份介质。

使用 Data Protector GUI 进行还原

要使用 Data Protector GUI 还原 MySQL 数据，请执行以下步骤:

1. 在“上下文列表”中，单击“还原”。
2. 在“范围窗格”中，依次展开“还原对象”、“MySQL”和从其中备份数据的 MySQL 客户机。此时将在“结果区域”中显示备份对象的列表。选择要还原的对象，然后双击它。
3. 在“源”属性页中，选择是要还原“数据库和/或表”还是“二进制文件”。
4. 根据进行的选择，指定相关选项和还原范围。有关详细信息，请按 **F1**。
5. 在“选项”属性页中，指定还原选项。有关特定于 MySQL 的选项的信息，请按 **F1**。**注意:** 在“选项”页中，“还原为实例”下拉列表显示所有实例的状态。 如果选择任何正在运行的实例并单击“还原”，则会弹出消息，要求您确认是否要先停止所选实例，然后再继续还原。如果选择“是”，则数据库实例将停止并且还原将继续，否则还原过程将终止。停止的实例以下列格式显示: <实例名称> <端口> <[已停止]> 暂存和导入表 (联机还原) 选项不会显示弹出窗口。如果所选实例未在运行，则还原将正常进行。
6. 查看还原所需的介质和设备并验证其可用性。
7. 单击**还原**。
8. 在“开始还原会话”对话框中，单击**下一步**。
9. 指定“报告级别”和“网络负载”。**注意:** 选择“显示统计信息”选项以查看会话输出中的还原配置文件消息。
10. 单击**完成**启动还原。成功还原数据库后，如果选中“还原后不启动服务”**复选框**，则服务不启动。会话结束时将显示会话统计信息和消息会话成功完成。

使用 Data Protector CLI 进行还原

要还原 MySQL 实例、数据库和/或数据库表，请在安装了 Data Protector 用户界面组件的系统上运行以下命令:

```
omnir SESSION_OPTIONS [-noexpand] -integ MySQL -barhost TargetMySQLHostname -appname TargetInstanceName [-user Username:GroupName] -options -source_client SourceMySQLHostname -source_database SourceInstanceName -database -session SessionID {-staging [CustomStagePath] [-copy_back [-target_dir NonOriginalTargetPath] | -import] | -inplace [-target_dir NonOriginalTargetPath ] } [-include {DatabaseName | DatabaseName.TableName} ...] [-roll_forward [EndDateTime]] [GENERAL_OPTIONS]
```

要还原一个或多个 MySQL 二进制日志文件，请在安装了 Data Protector 用户界面组件的系统上运行以下命令:

```
omnir SESSION_OPTIONS [-noexpand] -integ MySQL -barhost TargetMySQLHostname -appname TargetInstanceName -user Username:GroupName -options -source_client SourceMySQLHostname -source_database SourceInstanceName -binary_log {-include BinaryLogFilename ...} [-target_dir NonOriginalTargetPath] [GENERAL_OPTIONS]
```

有关选项说明和命令调用示例，请参阅 omnir 命令页。

多主数据库还原

要使用 Data Protector GUI 还原 MySQL 群集数据，请执行以下步骤:

1. 将数据还原到群集。
    1. 将群集备份数据还原到群集的所有单个节点。
    2. 从所有群集节点删除群集数据库以清除旧的群集配置。
        - 设置 SQL_LOG_BIN=0；
        - 删除数据库 mysql_innodb_cluster_metadata；
        - 设置 SQL_LOG_BIN=1；
2. 确保在安装了 MySQL 5.7.X 和 MySQL Shell 8.x 以及 MySQL Router 8.x 的群集中至少有三个 Windows / Linux 节点可用。
3. 向每个 MySQL 节点（MySQL 客户机）授予权限。在每个 MySQL 节点上执行以下命令。下面是根用户的示例：
    - GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY 'password';
    - GRANT ALL PRIVILEGES ON mysql_innodb_cluster_metadata.* TO root@'%' WITH GRANT OPTION;
    - GRANT RELOAD, SHUTDOWN, PROCESS, FILE, SUPER, REPLICATION SLAVE, REPLICATION CLIENT, CREATE USER ON *.* TO root@'%' WITH GRANT OPTION;
    - GRANT ALL PRIVILEGES ON mysql.* TO root@'%' WITH GRANT OPTION;
    - GRANT SELECT ON *.* TO root@'%' WITH GRANT OPTION;
4. 使用 MySQL Shell 检查实例配置。在任何节点上执行以下命令。这将验证节点配置。
    - dba.checkInstanceConfiguration ('root@Node1:3306, {password: 'password'})
    - dba.checkInstanceConfiguration ('root@Node2:3306, {password: 'password'})
    - dba.checkInstanceConfiguration ('root@Node3:3306', {password: 'password'})
5. 使用 MySQL Shell 配置本地实例。在单个 MySQL Shell 中执行以下命令，并将更改保存在配置文件中。
    - dba.configureLocalInstance ('root@Node1:3306')
    - dba.configureLocalInstance ('root@Node2:3306')
    - dba.configureLocalInstance ('root@Node3:3306')
    1. 使用 MySQL SHELL 创建群集。连接到一个 MySQL 节点，然后添加其他实例。例如：
    - shell.connect('root@Node1:3306', "password")
    - var cluster = dba.createCluster('backup', {multiMaster: true, force: true}) # Multimaster
    - var cluster = dba.createCluster('backup') # Single master
    - cluster.addInstance('root@Nod2:3306', {password: 'password'});
    - cluster.addInstance('root@Node3:3306', {password: 'password'});
6. 检查群集状态。如果断开了 MYSQL Shell 节点会话的连接，请使用以下命令连接到节点并获取群集：
    - shell.connect('root@Node1:3306', "password")
    - var cluster = dba.getCluster()
    - 要检查群集的状态，请使用 cluster.status(); command.

7. 执行以下命令来配置和启动 MYSQL 路由器：
    - Windows： "C:/Program Files/MySQL/MySQL Router 8.x/bin/mysqlrouter.exe" --bootstrap root@Node1:3306 --directory C:\6446 --conf-base-port 6446 powershell.exe C:\6446\start.ps1
    - Linux： mysqlrouter --bootstrap root@Node1:3310 --directory /opt/myrouter –user=root

使用 REST API 进行还原

还原 API 进行实例的备份，并获取用户提供的 MySQL 备份的详细信息。还原 API 支持 GET 和 RESTORE 方法。

GET

该 API 用于针对每个主机获取有关备份对象的信息。**GET** 没有任何输入参数。

- API 调用
    - https://CMHost:7116/idb/restoretree/mysql/restorecomponents?databasetables
    - https://CMHost:7116/idb/restoretree/mysql/restorecomponents?binarylogs
- 输入：无
- 输出：
- 参数说明:
    - End_time: 备份结束时间。
    - Mountpoint: 源对象名称。
    - Owner: 系统用户。
    - Session_name: 备份会话 ID。
    - Start_time: 备份开始时间。
- 查询响应：
    - Status: 成功或失败
    - Session_id: 备份会话名称。

输出示例

```
{ End_time: “05/03/2019 16:55:00.0000”, End_time: “05/03/2019 16:55:00.0000”, Mountpoint: “MYSQL#1”, Owner: “ADMINISTRATOR”, Session_name : “2019/03/05-6”, Start_time : “05/03/2019 16:50:00.0000” }
```

RESTORE

- API call: https://CMHost:7116/idb/restore

原位恢复

使用原位参数还原备份会话。

- 输入：
  - 输入参数：
    - Type: 代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。
    - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
      - Session: 会话 ID。
      - Restore_method: 原位
      - Target_dir: 应该还原备份的目录。
      - Custom_stage_dir: 应在其中还原备份的其他目录。
      - Include: Include 列表是备份的表级还原所必需的，否则是可选参数。可以提供以下选项
        - 数据库名称
        - 表名。
      - Roll_forward: 还原/恢复时间。
      - Appname: 备份实例名称。
      - Username: 系统的用户名。
      - Groupname: 域名。
- **输出**：无
- 查询响应：
  - Status: 成功或失败
  - Session_id: 还原会话 ID。

输入示例

```
{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL", "target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "inplace", "target_dir": "c:\\InplaceTest" "include": [ "mysql", "performance_schema.accounts" ], "roll_forward": "2019-02-28 11:54:36", }, "username": "ADMINISTRATOR" "groupname": "WIN-6IDTHL5ITKO" }
```

仅暂存选择性还原

使用仅暂存参数来还原备份会话。

- **输入**：
  - **输入参数**:
    - 类型：代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。
    - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
      - Session: 会话 ID。
      - Restore_method: 暂存。
      - Staging_option: 仅暂存
      - Include: Include 列表是备份的表级还原所必需的，否则是可选参数。可以提供以下选项
        - 数据库名称
        - 表名。
      - Target_dir: 应在其中还原备份的目录
    - Appname: 备份实例名称。
    - 用户名: 系统的用户名。
    - Groupname: 域名。
- 输出：无
- 查询响应：
  - Status: 成功或失败
  - Session_id: 还原会话 ID。

输入示例

```
{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL", "target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option": "staging-only", "include": [ "mysql", "performance_schema.accounts" ], "target_dir": "c:\\Test" }, "username": "ADMINISTRATOR", "groupname": "WIN-6IDTHL5ITKO" }
```

仅使用 custom_stage_dir 还原进行暂存

通过仅使用 custom_stage_dir 参数进行暂存来还原备份会话。

- 输入：
  - 输入参数：
    - 类型：代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。

        - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
            - Session: 会话 ID。
            - Restore_method: 暂存。
            - Staging_option: 仅暂存
            - Include: Include 列表是备份的表级还原所必需的，否则是可选参数。可以提供以下选项
                - 数据库名称
                - 表名。
                - Custom_stage_dir: 应在其中还原备份的自定义目录
        - Appname: 备份实例名称。
        - 用户名: 系统的用户名。
        - Groupname: 域名。
- 输出：无
- 查询响应：
    - 状态: 成功或失败
    - Session_id: 还原会话 ID。

输入示例

```
{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL",
"target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option":
"staging-only", "include": [ "mysql", "performance_schema.accounts" ], "custom_stage_dir": "c:\\test" }, "username": "ADMINISTRATOR",
"groupname": "WIN-6IDTHL5ITKO" }
```

暂存回写还原

使用暂存回写还原参数还原备份会话。

- 输入：
    - 输入参数：
        - 类型：代理类型
        - Barhost: 进行备份的系统的主机名。
        - Source_instance: 备份实例名称。
        - Source_client: 备份可用的系统名称。
        - target_instance: 目标实例名称
        - target_client：需要还原备份的目标系统名称。
        - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
            - Session: 会话 ID。
            - Restore_method: 暂存。
            - Staging_option: 回写
            - Include: Include 列表是备份的表级还原所必需的，否则是可选参数。可以提供以下选项：
                - 数据库名称
                - 表名。
        - Appname: 备份实例名称。
        - Username: 系统的用户名。
        - groupname: 域名。
- 输出：无
- 查询响应：
    - Status: 成功或失败
    - Session_id: 还原会话 ID。

输入示例

```
{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL",
"target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option":
"copy-back" }, "username": "ADMINISTRATOR", "groupname": "WIN-6IDTHL5ITKO" }
```

使用 custom_stage_dir 回写还原进行暂存

通过使用 custom_stage_dir 回写参数进行暂存来还原备份会话。

- 输入：
    - 输入参数：
        - 类型：代理类型
        - Barhost: 进行备份的系统的主机名。
        - Source_instance: 备份实例名称。
        - Source_client: 备份可用的系统名称。
        - target_instance：目标实例名称
        - target_client：需要还原备份的目标系统名称。
        - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
            - Session: 会话 ID。
            - Restore_method：暂存。
            - Staging_option：回写
            - Custom_stage_dir: 应在其中还原备份的自定义目录
        - Appname: 备份实例名称。
        - 用户名: 系统的用户名。
        - Groupname: 域名。
- 输出：无

- 查询响应：
  - 状态: 成功或失败
  - Session_id: 还原会话 ID。

输入示例

{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL", "target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option": "copy-back", "custom_stage_dir": "c:\\Test" }, "username": "ADMINISTRATOR", "groupname": "WIN-6IDTHL5ITKO" }

使用 custom_stage_dir 导入选择性还原进行暂存

通过使用 custom_stage_dir 导入选择性参数进行暂存来还原备份会话。

- 输入：
  - 输入参数
    - 类型：代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。
    - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
      - Session: 会话 ID。
      - Restore_method: 暂存。
      - Staging_option：导入。
      - Include: Include 列表是备份的表级还原所必需的，否则是可选参数。可以提供以下选项：
        - 数据库名称
        - 表名。
      - Custom_stage_dir: 应在其中还原备份的自定义目录
      - Appname: 备份实例名称。
      - 用户名: 系统的用户名。
      - groupname: 域名。
- 输出：无
- 查询响应：
  - Status: 成功或失败
  - Session_id: 还原会话 ID。

Signature

{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL", "target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option": "import", "include": ["mysql", "performance_schema.accounts"], "custom_stage_dir": "c:\\test" }, "username": "ADMINISTRATOR", "groupname": "WIN-6IDTHL5ITKO" }

使用 custom_stage_dir 和 target_dir 回写还原进行暂存

通过使用 custom_stage_dir 和 target dir 回写参数进行暂存来还原备份会话。

- 输入：
  - 输入参数：
    - 类型：代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。
    - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
      - Session: 会话 ID。
      - Restore_method：暂存。
      - Staging_option：回写。
      - Custom_stage_dir: 应在其中还原备份的自定义目录
      - Target_dir: 应在其中还原备份的目录
    - Appname: 备份实例名称。
    - 用户名: 系统的用户名。
    - Groupname: 域名。
- 输出：无
- 查询响应：
  - Status: 成功或失败
  - Session_id: 还原会话 ID。

输入示例

{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL", "target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option": "copy-back", "custom_stage_dir": "c:\\Custom_restore", "target_dir": "c:\\Test" }, "username": "ADMINISTRATOR", "groupname": "WIN-

```
6IDTHL5ITKO" }
```

使用 custom_stage_dir 与target_dir 回写前滚还原进行暂存

通过使用 custom_stage_dir 和 target dir 回写前滚参数进行暂存来还原备份会话。

- 输入：
  - 输入参数：
    - 类型：代理类型
    - Barhost: 进行备份的系统的主机名。
    - Source_instance: 备份实例名称。
    - Source_client: 备份可用的系统名称。
    - target_instance: 目标实例名称
    - target_client：需要还原备份的目标系统名称。
    - Db_options: 需要 db_options 来获取从何处以及如何还原备份的详细信息。
      - Session: 会话 ID。
      - Restore_method：暂存。
      - Staging_option：回写。
      - Custom_stage_dir: 应在其中还原备份的自定义目录
      - Target_dir: 应在其中还原备份的目录
      - Roll_forward: 还原/恢复时间。
    - Appname: 备份实例名称。
    - Username: 系统的用户名。
    - Groupname: 域名。
- 输出：无
- 查询响应：
  - Status: 成功或失败
  - Session_id: 还原会话 ID。

输入示例

```
{ "type": "MySQL", "barhost": "win-6idthl5itko", "source_instance": "MYSQL", "source_client": "win-6idthl5itko", "target_instance": "MYSQL",
"target_client": "win-6idthl5itko", "appname": "MYSQL", "db_options": { "session": "2019/02/28-2", "restore_method": "staging", "staging_option":
"copy-back", "custom_stage_dir": "c:\\Custom_restore", "target_dir": "c:\\Test", "roll_forward": "2019-02-28 11:54:36" }, "username":
"ADMINISTRATOR", "groupname": "WIN-6IDTHL5ITKO" }
```

MySQL 数据迁移

可以将整个 MySQL实例、各个 MySQL 数据库或数据库表迁移至位于相同或不同客户机上的其他 MySQL 实例。应遵循标准还原过程以及与迁移相关的以下细节:

- 如果迁移整个实例，请选择“还原为实例”和“使用非原始目标目录”选项。还原会话期间，目标实例应处于脱机状态。
- 如果迁移 MySQL 数据库或数据库表，请选择“将表导入到目标实例”选项。还原会话期间，目标 MySQL 实例应处于联机状态，并且不应包含与原始数据库表同名的数据库表。

MySQL 还原选项

特定于 MySQL 集成的还原选项如下。

要将选定 MySQL 对象还原到同一 MySQL 数据库和实例，请保留特定于还原的选项不变。

常规选项

恢复到客户机	此选项指定要将数据恢复到的 Data Protector 客户机。可以指定托管 MySQL 数据库管理系统且安装了 Data Protector MySQL Integration 组件的任何客户机。在此客户机上，Data Protector MySQL 集成代理在恢复会话开始时启动。 默认值：源客户机的完全限定域名。
恢复为实例	此选项用于指定要将数据还原到的 MySQL 实例的名称。如果实例尚不存在，则 Data Protector 将在恢复会话结束时自动创建并启动它。如果目标实例未启动（in-place 或 copy-back 方法），则 Data Protector 将在恢复结束时自动配置并启动实例。 默认值：源实例的名称。

用户名	此选项指定要用于恢复会话的操作系统用户帐户的用户名。必须向所选帐户授予适当的 MySQL 数据库管理员权限，并且该帐户必须是具有还原方案 (启动还原、从其他用户还原、还原到其他客户机等) 的适当用户权限的 Data Protector 用户。如果未指定任何值，则将使用目标客户机上的 Data Protector Inet 帐户。 默认值：本地启动 Data Protector GUI 的用户帐户的用户名。
组/域	此选项指定要用于恢复会话的操作系统用户帐户的用户组或域。如果未指定任何值，则将使用目标客户机上 Data Protector Inet 帐户的用户组或域。 默认值：从本地启动 Data Protector GUI 的用户帐户的组/域。

恢复方法

暂存恢复	选择此选项可执行暂存恢复的一个或两个阶段，与原位恢复或迁移数据不同。 • 选中**将暂存数据复制到目标目录**选项后，完成暂存恢复。 • 选中**将表导入到目标实例**选项后，导入数据库和/或数据库表。 • 选中**仅暂存**选项后，执行暂存恢复的第一阶段（部分暂存恢复）。 默认：选择。
使用自定义暂存目录	选择此选项可使用自定义目录来暂存已恢复的数据，而非用于临时文件的 Data Protector 默认目录。指定所选目录的完整路径。 默认：未选择。
将暂存数据复制到目标目录	选择此选项可执行完整的暂存恢复。恢复链的备份映像中的数据会先放置在目标客户机上的中间位置。之后，此数据将复制到目标位置。此恢复方法需要更多的原位恢复存储空间，但是在出现故障时，能够更好地防止可能出现的数据不一致。 **注意**二进制日志将进行过滤，而且仅恢复适用于所选表格的内容。无论恢复范围如何，系统表空间将始终恢复。 默认：选择。
将表导入到目标实例 (联机还原) (适用于 MySQL 5.6.6 及更高版本。)	选择此选项可将选定 MySQL 数据库、数据库表或两者导入目标 MySQL 实例。目标实例上不得有同名的数据库表。 **注意**二进制日志将进行过滤，而且仅恢复适用于所选表格的内容。 默认：未选择。
仅暂存	选择此选项可执行暂存恢复的第一阶段。恢复链的 MySQL 备份映像中的数据会放置在目标客户机上的中间位置，使 MySQL 生产数据完好保留。 默认：未选择。

原位恢复	选择此选项可对 MySQL 数据执行原位恢复，与有一个或两个阶段的暂存恢复不同。在此情况下，恢复链的备份映像中的数据将覆盖 MySQL 生产数据（如果存在）。此类恢复过程需要整个暂存恢复的较少存储空间，但是当出现故障时，更容易出现潜在的数据不一致。 **注意**选择此选项后，无论恢复范围为何，都只能将整个备份映像恢复到目标位置。 默认：未选择。

恢复重定向

使用非原始目标目录	选择此选项可将数据库、数据库表或二进制日志文件的恢复重定向到不同于原始位置的位置，或者到迁移数据。指定所选目录的完整路径。 对现有实例执行还原时，请确保提供到此实例上的数据库根目录（datadir）的有效路径。 默认：未选择。

数据库恢复

使用二进制日志执行恢复	选择此选项后，可通过使用相应二进制日志文件中的事务来前滚已还原的 MySQL 实体（实例、数据库或数据库表），执行该已还原 MySQL 实体的恢复。这些日志文件根据需要存储在同一会话中。 默认：未选择。
前滚直到最新的可用状态	如果选择此选项，Data Protector 将从二进制日志应用事务，并通过将恢复的 MySQL 实体置于最新的可用状态来执行恢复。恢复仅包括所选的实例、数据库或数据库表。 默认：选择。
前滚直到	如果选择此选项，Data Protector 将通过仅应用二进制日志中的事务来执行恢复，这些事务可将恢复的 MySQL 实体置于其在所选时间点的状态。日期和时间解释为源客户机上的本地日期和时间。恢复仅包括所选的实例、数据库或数据库表。 默认：未选择。
不启动数据库实例	如果您不想在目标端口上启动数据库实例，请选中此复选框。仅当源实例和目标实例不同时，才启用此选项。 如果尚未选择“不启动数据库实例”，则还原将以旧样式进行。 此选项不适用于将表导入到目标实例 (联机还原) 和仅暂存选项。

MySQL 代理切换

代理切换提供在新旧代理之间切换的能力。切换是通过编辑 global 文件完成的，因此会影响所有用户。切换是特定于代理的，因此可以灵活地在 MySQL 代理之间进行切换。

要切换代理，请完成以下步骤:

1. 打开任何文本编辑器。
2. 在文本编辑器中，打开位于以下路径中的 global 文件:
   - Windows： <PROGRAMDATA>\Config\Server\Options .例如： C:\ProgramData\OmniBack\Config\Server\Options.
   - Linux： /etc/opt/omni/server/options.
3. 找到代理切换 EnableLegacyMySqlAgent 的选项。如果未激活该选项，请删除选项名称前的 **#** 标记。
4. 设置代理切换的值。
   - EnableLegacyMySqlAgent = **1** 表示使用旧代理
   - EnableLegacyMySqlAgent = **0** 表示使用新代理
     - 默认情况下，新代理将处于活动状态。
5. 以 Unicode 格式保存文件。
6. 关闭并重新启动 Data Protector GUI 以应用新设置。

NDMP 服务器集成

This feature is available in the Premium Edition

本节说明如何配置和使用 Data Protector 网络数据管理协议 (NDMP) 服务器集成。其中说明对网络连接存储设备执行文件系统备份和还原时需要了解的概念和方法。

网络数据管理协议 (NDMP) 是一种用于管理网络连接存储 (NAS) 设备上备份和还原操作的协议。NDMP 使用客户机服务器模型，其中 Data Protector NDMP 介质代理客户机用于控制备份，而 NDMP 服务器用于执行实际的备份操作。

Data Protector NDMP 服务器集成提供以下类型的交互式和计划文件系统备份:

- 完整
- 增量 1

Data Protector NDMP 服务器集成提供两种还原类型:

- 标准文件系统还原
- 直接访问还原

Data Protector NDMP 服务器集成支持以下两种类型的备份:

- 对于 **Celerra** (所有受支持的 Dell EMC 设备):
  - 转储

    默认备份类型，用于在文件级别备份数据。
  - NDMP 卷备份 (**NVB**)

    特定于 Dell EMC 的 NDMP 备份类型，用于在卷级别备份数据块。
- 对于 Network Appliance (**NetApp**):
  - 转储

    默认备份类型，用于在文件级别备份数据。
  - 将镜像捕捉到磁带备份 (“SMTape 备份”)

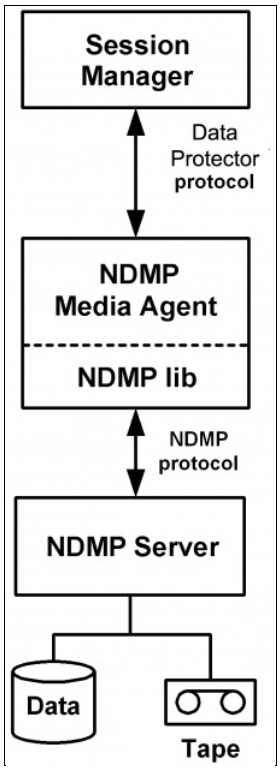
    特定于 NetApp 的 NDMP 备份类型，用于创建源卷的快照并备份当前及之前所有快照副本。

> **注意**要备份其他供应商的 NAS 设备，请使用 NetApp 转储模式。

集成概念

Data Protector 通过 Data Protector NDMP 库和 NDMP 介质代理与 NDMP 集成。Data Protector NDMP 库通过 NDMP 接口引导 Data Protector 会话管理器与 NDMP 服务器之间的通信。Data Protector NDMP 服务器集成体系结构显示集成的体系结构。

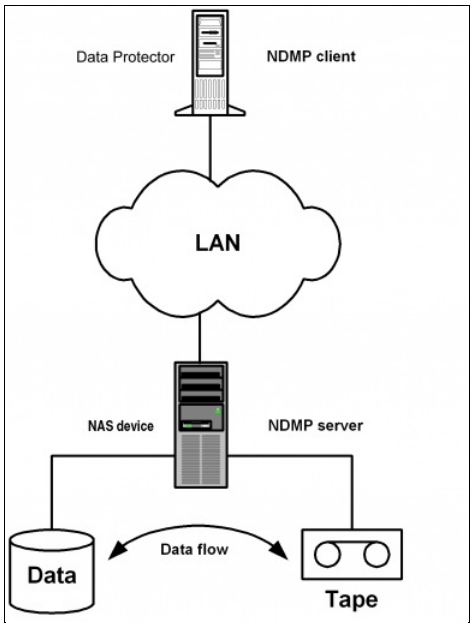
Data Protector NDMP 服务器集成体系结构



图例	
会话管理器	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。由于整个功能已在 NDMP 介质代理中实现，因此会话中不会涉及任何 Data Protector 磁盘代理。
NDMP 介质代理	NDMP 客户机，包含名为“NDMP 库”的层。该库允许 NDMP 介质代理通过 NDMP 接口与 NDMP 服务器进行通信。

在典型的 NDMP 环境配置中，NDMP 服务器系统和安装了 NDMP 介质代理的 Data Protector 客户机 (“NDMP 客户机”) 均连接到 LAN。但是，NDMP 服务器磁盘中的数据不会流经 LAN，而是备份到与 NDMP 服务器系统连接的磁带设备。NDMP 客户机启动、监视和控制数据管理，NDMP 服务器执行这些操作，直接控制与其连接的设备以及备份和还原速度。

NDMP 环境配置



NDMP 编目处理的设计使得 Data Protector 会将整个编目缓存到 NDMP 客户机，然后将其存储到 Data Protector 内部数据库 (IDB)。由于编目大小可能会显着增加，因此 NDMP 客户机会将编目的一部分缓存到“文件历史记录交换文件”中，该文件位于默认的 Data Protector 临时文件目录中。

直接访问还原

直接访问还原是一种经过优化的数据恢复操作。可在磁带还原过程中直接访问备份的数据。要实现此操作，可在备份期间将备份数据分区为多个段

并记录其起始地址。还原期间，Data Protector 首先计算哪个段包含所请求的文件或目录，然后定位该段，最后开始通读整个段以定位文件或目录的开头。

使用其他设备进行还原

您可以使用除备份时所用设备之外的设备进行还原。

介质管理

Data Protector 介质管理功能受限，因为数据是由 NDMP 服务器以其特定数据格式备份的。

Data Protector 支持以下介质管理功能:

- 介质导入和导出。
- 介质扫描。
- 介质初始化。
- 脏驱动器检测。

Data Protector 不支持以下介质管理功能:

- 备份数据验证。

NDMP 服务器集成的先决条件

网络数据管理协议服务器集成的先决条件如下:

- 确保已正确安装和配置目标 NDMP 服务器。
- 确保已正确安装 Data Protector。必须在所有 NDMP 客户机 (控制 NDMP 服务器备份的 Data Protector 客户机) 上安装 Data Protector NDMP Media Agent 组件。
- 用于介质复制的源介质和目标介质的介质类型必须相同。
- NDMP 服务器系统必须有一个磁带驱动器与其相连，用于进行常规双向备份和还原。NDMP 服务器和 Data Protector 都必须支持该驱动器。
- 用于介质复制的源驱动器和目标驱动器应连接到之前执行备份的同一 NDMP 服务器。
- 确保 NDMP 服务器处于联机状态。
- 确保已在 3PAR 上配置文件角色并且已连接 VTL。

块大小

集成支持可变磁带块大小。在为每个 NAS 设备选择块大小之前，应考虑以下注意事项:

- 确保将 NDMP 服务器配置为支持可变块大小。
- 用于还原的设备的块大小必须等于或大于用于备份的设备的块大小。
- 对于 NetApp 上的 SMTape 备份，必须将“块大小”选项设置为介于 4kB 和 256 kB 之间的值。

  请注意: Data Protector 支持的块大小介于 8 kB 到 1024 kB 之间。默认块大小为 256 kB。
- 对于 Celerra，块大小值不应大于 Celerra readWriteBlockSizeInKB 参数。
- 请确保已格式化要使用的介质。
- 要能够从使用 ONTAP 8.1.x 操作系统的 NetApp NAS 设备还原单个文件或目录，请在还原向导中设置 ENHANCED_DAR_ENABLED NDMP 环境变量或 ENHANCED_DAR_ENABLED omnirc 选项。
- 在备份期间必须打开文件历史记录跟踪。
- 要启用直接访问还原，请将 NDMP 环境变量 DIRECT 设置为 Y。直接访问还原过程与标准还原过程相同。唯一的区别是可以浏览并选择要还原的单个文件和目录。

NDMP 环境变量

使用 Data Protector GUI 为选定 NAS 设备设置 NDMP 环境变量。

下表显示受支持的 NDMP 环境变量:

适用于 NetApp NAS 设备的 NDMP 变量

变量	值	功能
HIST	y/n 默认值： y	打开/关闭文件历史记录跟踪。

DIRECT	y/n 默认值： y	启用直接访问还原。
LEVEL	0, 1, 2, ... 9 默认值： 0（完整）	指定备份级别。
SMTAPE_SNAPSHOT_NAME	Snapshot_copy_name 默认值： Invalid	指定快照副本名称。 指定的快照和所有的旧快照副本会备份到磁带中。
SMTAPE_DELETE_SNAPSHOT	y/n 默认值： n	删除备份后创建的自动快照副本。
SMTAPE_BREAK_MIRROR	y/n 默认值： n	还原后断开与 **SnapMirror** 的连接。 注意成功还原后，还原的卷将处于受限状态并且不可写入，除非 SMTAPE_BREAK_MIRROR 变量设置为 y 。
ENHANCED_DAR_ENABLED	F/T 默认值： T	设置为 F 时，此变量允许从使用 ONTAP 8.1.x 操作系统的 NetApp NAS 设备还原各个文件或目录。

适用于 Celerra NAS 设备的 NDMP 变量 (也适用于 Isilon 和其他基于 OneFS 的设备)

变量	值	功能
HIST	y/n 默认值： y	打开/关闭文件历史记录跟踪。
DIRECT	y/n 默认值： y	启用直接访问还原。
LEVEL	0, 1, 2, ... 9 默认值： 0（完整）	指定备份级别。
BASE_DATE	*32bit level '* ***32bit date***	基于特定日期的增量备份。
RESTORE_OPTIONS	1 默认值: 0x00000004	适用于所有 Isilon 和其他运行 OneFS 8.0 及更高版本的基于 OneFS 的 NAS 设备。在对新位置执行直接访问还原 (DAR) 时，服务器会将目录的权限设置为 0700，并将 UID/GID 设置为 0。 将此环境变量设置为 1 可确保从根目录继承目录权限。
OPTIONS	LK	遵循符号链接。
	AT	保留访问时间。
	NT	保存 NT 属性。

	MI/MD/MM	还原用于本地化的冲突策略。

用于 Hitachi BlueArc 和 Hitachi NAS 设备的 NDMP 变量

变量	值	功能
HIST	y/n 默认值： y	打开/关闭文件历史记录跟踪。
DIRECT	y/n 默认值： y	启用直接访问还原。
LEVEL	0, 1, 2, ... 9 默认值： 0（完整）	指定备份级别。
TYPE	dump/tar 默认值： dump	指定备份类型。
UPDATE	y/n 默认值： y	记录备份时间。以后的增量备份可以基于此备份。
FILESYSTEM	directory_name 默认: 无	指定要备份的目录。
EXCLUDE	要从备份中排除的单独文件列表。 默认: 无	指定要从备份中排除的文件或目录。

注意也可以使用 omnirc 文件设置某些 NDMP 环境变量。

限制

以下限制适用：

- 仅文件系统备份和还原可用。
- 仅支持 Full 和 Incr1 备份这两种备份类型。
- 最大设备并发数是 1。
- 不允许选择设备和浏览文件系统。
- NDMP 设备必须使用专用介质池。
- 不能对 NetApp 特定的消息本地化。
- 无法取消选择选定要还原的树的子树。
- 无法对不同路径名的选定文件集以树形结构执行还原。
- 不支持在 NDMP 备份会话中执行 NDMP 备份对象复制和对象镜像操作。
- 在 NDMP 客户机上不支持介质头运行状况检查。
- 从特定类型（例如 NDMP-NetApp）的 NDMP Server 备份的数据无法还原到另一种类型（例如 NDMP-Celerra）的 NDMP Server。
- 当还原到另一个 NDMP 服务器时，要从中还原的设备必须直接与目标 NDMP 服务器连接，而且必须是同一类型，同时在 Data Protector GUI 或 CLI 中选择或指定为还原设备。
- 不支持还原预览。
- 不支持使用 Data Protector 按查询还原功能还原数据。
- 不支持在 log file 日志记录级别直接还原 (DIRECT=Y) NDMP 备份。要还原“日志文件”日志记录级别的 NDMP 备份，请将 Data Protector GUI 中的 NDMP 环境变量手动设置为 DIRECT=N（“还原”上下文 >“选项”选项卡 >“高级”）。
- Data Protector 不支持 NDMP 备份会话使用 IPv6，因此 NDMP 服务器应启用 IPv4 协议。
- 在 64 位 Linux 系统中，Data Protector NDMP 介质代理不支持 ADIC/GRAU DAS 库设备。
- 仅支持在具有相同的固件主要版本 (例如，ONTAP 8.x) 的文件管理器中执行三向备份或还原。
- 仅在相同群集文件管理器上支持群集感知型备份 (CAB) 或还原。Data Protector 仅支持备份和还原卷和文件；这些卷和文件与用于备份或

还原操作的设备位于相同群集文件管理器上。
- 在非群集感知型备份 (CAB) 环境中，在备份规范期间无法将三向对象与本地对象结合使用。
- 不支持 NDMP 对象复制。
- 不支持 NDMP 介质复制。

Celerra 限制

- 如果从另一个目录同时选择一个目录和单独的文件并启动还原，则仅恢复所选文件。要同时还原，请使用标准还原（将 NDMP 环境变量 DIRECT 设置为 N）。
- 目录直接访问还原 (DDAR) 不能与由所选 NDMP 卷备份 (NVB) 选项创建的备份映像配合使用。
- 通过 NVB 备份类型，仅可以备份整个文件系统。例如，您可以备份 /ufs1 ，但不能备份 /ufs1/dir1 。

- NVB 备份类型和文件或目录过滤不能一起使用。如果同时使用， NVB 将占优先而过滤器将无效。

安装 NDMP Server 客户机

This feature is available in the Premium Edition

假设 NDMP 服务器已启动并正在运行。

在安装过程中，请选择“NDMP 介质代理”，并将它安装到所有访问 NDMP 专用驱动器的 Data Protector 客户机上。

如果某个 Data Protector 客户机不用于通过 NDMP 服务器访问 NDMP 专用驱动器，而仅用于控制库的机械手，则可以在此类客户机上安装“NDMP 介质代理”或“常规介质代理”。

请注意，一台 Data Protector 客户机上只能安装一个介质代理。

配置 NDMP 服务器集成

This feature is available in the Premium Edition

要配置 Data Protector NDMP 服务器集成，请执行以下操作:

1. 将 NDMP 服务器系统导入 Data Protector 单元。
2. 为 NDMP 介质创建介质池。
3. 配置 NDMP 设备。

导入 NDMP 服务器系统

使用 Data Protector GUI 导入 NDMP 服务器系统:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 在“名称”文本框中，输入要导入的 NDMP 服务器系统的名称。

   在“类型”下拉列表中，选择“NDMP 服务器”。

   单击“下一步”。
4. 在“端口”文本框中，指定 NDMP 服务器的 TCP/IP 端口号。默认编号为 10000。

   提供 NDMP 服务器系统用户帐户，以供 Data Protector 用于连接 NDMP 服务器系统。此用户必须有读取和写入 NDMP 介质的权限。

   Data Protector NDMP 集成支持“无”、“文本”和 "MD5" NDMP 身份验证方法。Data Protector 会自动检测并使用 NDMP 服务器支持的方法。

   在“NDMP 服务器类型”下拉列表中，选择 NAS 设备类型。

   单击**完成**。

注意如果目标系统的设备类型未在下拉框中列出，但作为受支持的 NDMP 平台出现在 NAS 支持矩阵中，则可以将 NetApp 类型用作常规类。

创建介质池

为 NDMP 介质创建专用介质池。NDMP 介质池只能由使用 NDMP 数据格式的设备 (“NDMP 设备”) 使用。

配置 NDMP 设备

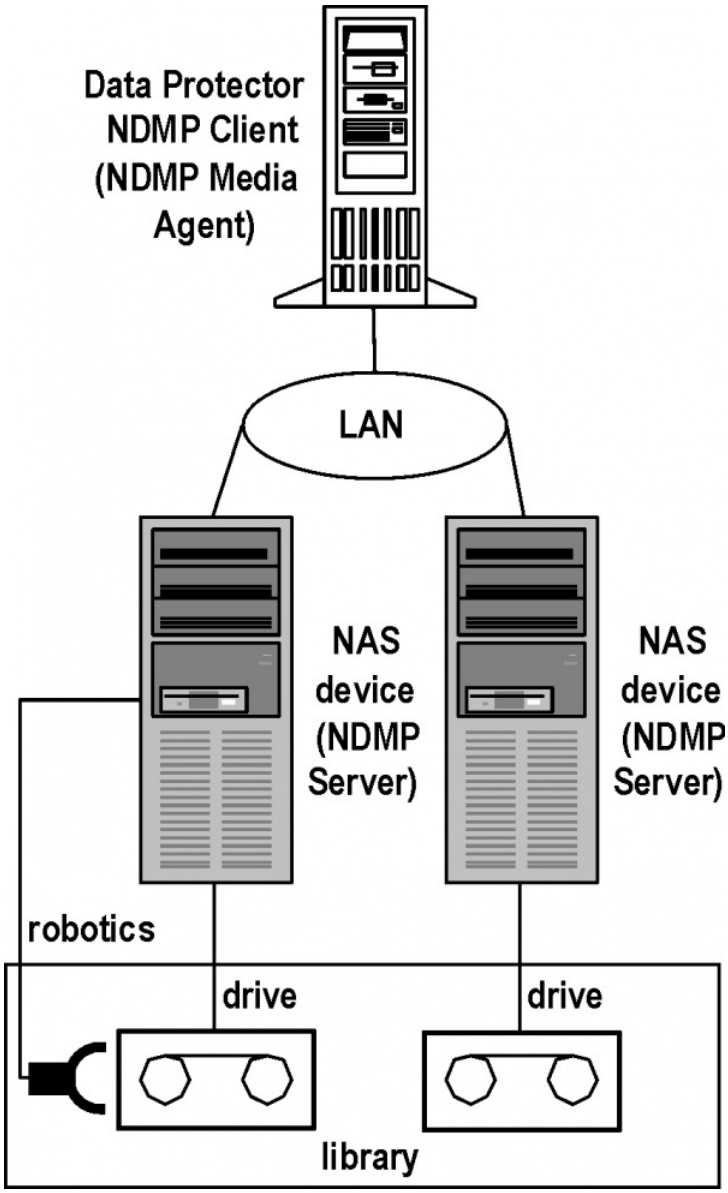
使用 Data Protector GUI 配置 NDMP 设备。

库机械手可以连接以下各项:

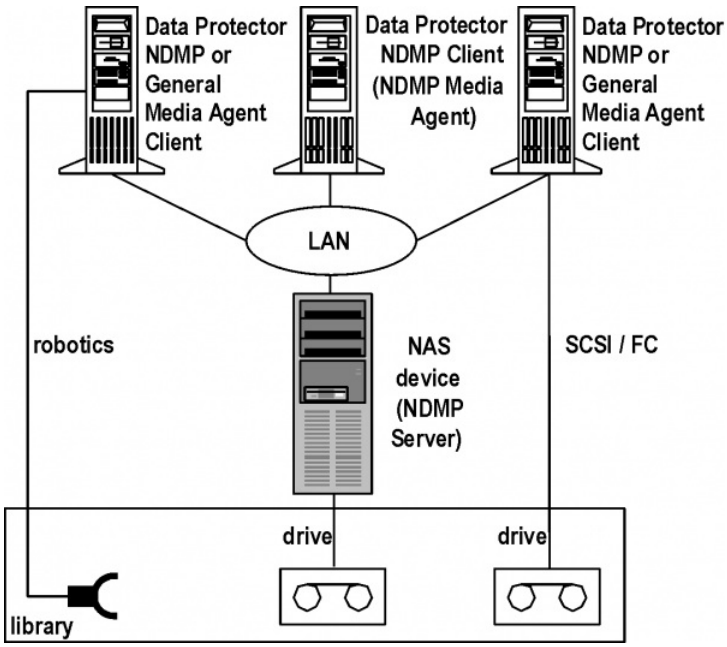
- NDMP 服务器系统 (库配置 1)。
- NDMP 客户机 (库配置 2)。
- 安装了常规介质代理 (“常规介质代理客户机”) 的 Data Protector 客户机 (库配置 2)。

如果机械手连接到 NDMP 服务器系统，则 NDMP 服务器和 Data Protector 必须都支持它。在此配置中，机械手应仅由 Data Protector NDMP 客户机控制。

库配置 1


Data Protector
NDMP Client
(NDMP Media
Agent)
LAN
NAS
device
(NDMP
Server)
NAS
device
(NDMP
Server)
robotics
drive
drive
library

库配置 2


Data Protector
NDMP or
General
Media Agent
Client
Data Protector
NDMP Client
(NDMP Media
Agent)
Data Protector
NDMP or
General
Media Agent
Client
LAN
robotics
NAS
device
(NDMP
Server)
SCSI / FC
drive
drive
library

可以将多个库驱动器连接到一个 NDMP 服务器系统。如果库机械手连接到 Data Protector NDMP 客户机，并且驱动器连接到 NDMP 服务器系统，则可以在多个 NDMP 服务器系统和常规介质代理客户机之间以及 Data Protector 和其他应用程序之间共享驱动器。另一方面，NDMP 介质无法共享。

- NDMP 设备只能使用 NDMP 介质池。

配置磁带库

要配置机械手连接到 NDMP 服务器系统的磁带库，请完成以下步骤:

1. 在上下文列表中，单击“设备和介质”。
2. 在“范围窗格”中，右键单击“设备”，然后单击“添加设备”。
3. 输入设备的名称。(可选) 描述设备。

   在“设备类型”中，选择“SCSI 库”。

   在“接口类型”中，选择使用的 NAS 设备。

   在“客户机”中，选择将通过 NDMP 服务器控制库的 NDMP 客户机。

   在“NDMP 服务器”中，选择连接了库机械手的 NDMP 服务器系统。

   (可选) 在“管理控制台 URL”中，输入库管理控制台的有效 URL。从而能够调用 Web 浏览器，然后直接从 Data Protector GUI 加载管理控制台界面。

   单击“下一步”。
4. 指定库机械手 SCSI 地址和驱动器处理方式。

   单击“下一步”。
5. 指定 Data Protector 要使用的插槽。

   单击“下一步”。
6. 在“介质类型”下拉列表中，选择在库中使用的介质类型。
7. 单击“完成”，然后单击“是”以配置库中的驱动器。
8. 输入驱动器的名称。(可选) 描述驱动器。

   在“数据格式”中，选择使用的 NAS 设备。

   在“客户机”中，选择将通过 NDMP 服务器控制库的 NDMP 客户机。

   在“NDMP 服务器”中，选择连接了库机械手的 NDMP 服务器系统。

   单击“下一步”。

   > **注意**在群集感知型备份 (CAB) 环境中，现在可以搜索磁带库和机械手。

9. 指定驱动器的 SCSI 地址。

   请勿更改驱动器索引编号。

   单击“下一步”。
10. 指定 NDMP 介质的介质池。

    要指定高级设备选项，请单击“高级”。

    > **注意**NDMP 服务器不支持多路复用数据流，并将设备并发限制为 1。

    单击“下一步”。
11. 选择新驱动器的设备策略，并指定设备标记。此项可选。

    单击**完成**。
12. 单击“是”以创建其他驱动器或“否”以完成配置。

    然后，如第 8 步到第 12 步所述配置驱动器。

配置文件库

要在文件库上配置 NDMP-NetApp 备份，请完成以下步骤:

1. 在上下文列表中，单击“设备和介质”。
2. 在“范围窗格”中，右键单击“设备”，然后单击“添加设备”。
3. 输入设备的名称。

   在“设备类型”中，选择“文件库”。

   在“接口类型”中，选择“文件库 (NDMP)”。

   在“客户机”中，选择用于控制库的 NDMP 客户机。

   单击“下一步”。

4. 指定希望库所在的目录或一组目录。单击**添加**。
5. 要更改目录的默认属性，请选择该目录，然后单击**属性**。
6. 输入文件库设备的写入程序数量。默认为所添加的目录的数量。如果所添加的写入器多于设备中的目录数，则可能将提高设备性能。这一点取决于硬件配置。需要在环境中测试这一点。单击“下一步”。
7. 文件库设备的“介质类型”为“文件”。要在此文件库中启用虚拟完整备份，请选择“使用分布式文件介质格式”。单击“下一步”。
8. 查看文件库设备配置的摘要。单击**完成**退出向导。

针对 NDMP 配置 StoreOnce

要在 StoreOnce 设备上配置 NDMP 备份，请执行以下步骤:

1. 在上下文列表中，单击“设备和介质”。
2. 在“范围窗格”中，右键单击“设备”，然后单击“添加设备”。
3. 输入设备的名称。

   在“设备类型”中，选择“备份到磁盘”。

   在“接口类型”中，选择“StoreOnce 备份系统 (NDMP)”。

4. 在**重复数据删除系统**框中，输入重复数据删除系统的 IP 地址、主机名、完全限定域名 (FQDN) 或光纤通道 (FC) 地址（重复数据删除存储所在的宿主计算机）。

   或单击**选择服务集**，查询并检索重复数据删除系统的地址。

   对于 StoreOnce 软件接口，支持 IPv4 或 IPv6 地址，或 FQDN。但是，对于 StoreOnce 备份系统接口，如果使用最新的 StoreOnce Catalyst 版本，则支持 IPv4 或 IPv6 地址、FQDN 或 FC 全局标识符。

   如果使用 FC 连接到 StoreOnce 备份系统，请指定设备的 FC 地址。确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

5. 对于 StoreOnce 备份系统设备，请输入**客户机 ID** 和密码（可选）以访问存储。可在密码中使用以下字符: [a-z][A-Z][0-9][_-.+() {}:#$*;=?@[]^|~]?
6. 单击“选择/创建存储”以选择现有的联合或非联合存储，或者创建非联合存储。从列表中选择存储名称。

   要创建加密存储，请选择**已加密存储**选项。单击**确定**。

   只能在创建存储区时启用加密功能。存储一经创建，就无法将其从已加密状态转换成未加密状态，反之亦然。StoreOnce 软件重复数据删除设备不支持存储加密。不能使用 Data Protector GUI 创建联合存储。需要使用 StoreOnce 管理控制台创建它们。

7. 选择一个网关，然后单击**添加**以显示“属性”对话框。根据需要更改任意网关属性，然后单击**确定**添加网关。如果使用 FC 连接到 StoreOnce 备份系统，请确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

   连接到 Data Protector 网关的联合成员必须是联合存储的成员。如果使用 StoreOnce 缩小了联合成员，请将 Data Protector 网关调整为连接到其他联合成员。

   要查看网关属性，请选择所需的网关然后单击**属性**。要设置其他网关选项，请单击**设置**选项卡，再单击**高级**打开“高级”属性窗口。

   在“高级属性”窗口中，要限制每个网关上的流数，请选择“每个网关的并行流的最大数量”。可以指定最多 100 个流。如果未选择此选项，则不限制流数。注意，还可以在创建备份规范时设置此选项。在这种情况下，B2D 设备创建过程中指定的值将被覆盖。

   要限制网关所使用的网络带宽，请选择**限制网关网络带宽(Kbps)** 并输入以每秒千位 (kbps) 为单位的限制。

   要启用服务器端重复数据删除，请选择**服务器端重复数据删除**。

   如果已将 IP 地址或 FQDN 配置为重复数据删除目标，则“使用 FC”和“回退至 IP”选项均可用并且默认处于选中状态。

8. 要验证连接，请单击**检查**。
9. 单击**下一步**进入“设置”窗口，在此窗口中可以指定以下选项：
   - **每个存储的最大连接数量**: 限制可以连接到每个存储的介质代理的数量。如果未选择此选项，则不限制连接数。默认情况下，不选择此值。
   - **备份大小软配额 (GB)**: 输入备份大小软配额 (GB)。如果在删除重复数据之前，数据的大小超过所设置的配额，则会话将显示一则警告，但数据仍将写入存储。该配额对备份、复制和对象合并会话有效。如果备份大小配额小于存储大小配额，将显示一则警告并且存储大小配额将无效。如果设置为 0 或字段为空，则说明未设置配额。默认情况下，未设置此字段。
   - **存储大小软配额 (GB)**: 输入存储大小软配额 (GB)。如果存储中的重复删除的数据大小超过所设置的配额，则会话将显示一则警告，但

数据仍将写入存储。该配额对备份、复制和对象合并会话有效。如果存储大小配额大于备份大小配额，将显示一则警告并且存储大小配额将无效。默认情况下，未设置此字段。如果设置为 0 或字段为空，则说明未设置配额。
    - **催化剂项目大小阈值(GB)**：为 StoreOnce Software Deduplication 和 StoreOnce 备份系统设备定义催化剂项目的阈值大小。如果当前的催化剂项目超过此大小，您将无法再向其中附加更多对象。默认情况下，催化剂项目的大小是无限制的。
    - **每个催化剂项目单个对象**：对于 StoreOnce 软件重复数据删除和 StoreOnce 备份系统设备，每个 Catalyst 项启用一个对象。默认情况下，启用此选项；无法修改此设置。
10. 单击**下一步**以显示“摘要”窗口，其中包括已配置 B2D 存储的详细信息。此外，对于联合存储，它还包括所有联合成员及其状态（联机或脱机）的列表。
11. 检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

配置独立设备

要配置独立设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，右键单击“设备”，然后单击“添加设备”。
3. 输入设备的名称。(可选) 描述设备。

   在“设备类型”中，选择“独立”。

   在“数据格式”中，选择使用的 NAS 设备。

   在“客户机”中，选择将通过 NDMP 服务器控制设备的 NDMP 客户机。

   在“NDMP 服务器”中，选择连接独立设备的 NDMP 服务器系统。

   单击“下一步”。
4. 提供设备的 SCSI 地址。

   单击“下一步”。
5. 指定介质池。

   要指定高级设备选项，请单击“高级”。

   > **注意**NDMP 服务器不支持多路复用数据流，并将设备并发限制为 1。
6. 单击**完成**。

NetApp 独立配置

磁带库中的独立磁带设备和驱动器:

要获取有关与 NDMP 服务器系统连接的独立磁带设备 (或磁带库中的驱动器) 的信息，请执行以下命令:

```
sysconfig -t
```

(在 NDMP 服务器系统上)。SCSI 地址写在输出的开头，由四部分组成。

分析驱动器的 SCSI 地址

部分	描述
{ n | u }	no rewind 和卸载/重新加载 (分别)。
rst	Raw SCSI tape (始终存在)。
{ 0 | 1 | 2 | ... }	设备编号。
{ 1 | m | h | a }	数据密度和压缩。

示例

DLT 4000 驱动器的输出如下:

```
nrst0m - no rewind device, format is:42500 bpi 6.0GB
```

库机械手

要获取与 NDMP 服务器系统连接的库机械手的 SCSI 地址，请执行以下命令:

```
sysconfig -m
```

(在 NDMP 服务器系统上)。SCSI 地址由两个部分组成。

分析库机械手的 SCSI 地址

部分	描述
mc	Media changer device（始终存在)。
{0 | 1 | 2 | ... }	设备编号。

示例

DLT 4000 库的输出如下:

```
mc0
```

NetApp ONTAP C 模式配置

您可以通过以下任一方法配置 NetApp ONTAP C-Mode 设备以进行备份和还原:

- **群集感知模式**: 仅当 ONTAP 支持群集感知备份 (CAB) 时，才适用此模式。为在 Data Protector 中成功配置此类设备，NetApp 设备必须满足特定的先决条件并进行相应配置。
- **节点范围模式**: 这类似于以前版本的 Data Protector 支持的 7 模式 ONTAP 配置。

先决条件和限制

以下是 NetApp ONTAP C-Mode 集成的先决条件:

- 群集中的每个节点必须具有群集间逻辑接口 (LIF)。
- 确保至少配置一个存储虚拟机 (SVM)。
- 创建用户并生成相应密码供 NDMP 使用。
- 介质更换器必须能够将磁带加载到任何已配置文件管理器上的任何指定驱动器。在这种情况下，介质更换器必须能够将磁带加载到 server1 和 server2 上的磁带驱动器。
- 确保 7-Mode 阵列和 C-Mode 阵列使用不同的 SMIS 提供程序系统。

以下限制适用：

- 在运行早于 6.4 的 Data ONTAP 版本的 NetApp 文件管理器上，不支持对目录的直接访问还原 (DAR)，而是执行标准还原。标准恢复仅对性能有影响。
- 在运行 Data ONTAP 8.0 或更高版本的 NetApp 文件管理器上，引入 DAR 支持后，直接访问还原 (DAR) 不适用于 Data Protector 9.05 之前进行的备份。
- 使用 SMTape 备份类型时，无法将特定集合类型的卷的备份映像用于还原到其他集合类型的卷中。
- 使用 SMTape 备份类型时，无法将常规集合中卷的备份映像用于还原到更大集合的卷中，反之亦然。
- SMTape 备份类型仅提供完整备份（level-0 备份）。
- 通过 SMTape 备份类型，仅可以备份整个文件系统。例如，您可以备份 /ufs1 ，但不能备份 /ufs1/dir1 。

配置 NetApp ONTAP C 模式

在 Data Protector 中配置 NetApp CAB 服务器

要在 Data Protector 中配置 NetApp CAB 服务器，请执行以下步骤:

1. 配置 NetApp 设备，通过禁用 node-scope-mode 启用 CAB 功能。
2. 标识需要作为 NetApp CAB 客户机导入 Data Protector 的群集管理 LIF。
3. 将群集管理 LIF 作为 NetApp CAB 服务器导入 Data Protector。

   使用以前创建的用户名和密码指定 NDMP 服务器相关信息。
4. 在 Data Protector 中使用 NetApp CAB 服务器创建逻辑设备:
5. 指定有关库 SCSI ID 和驱动器处理的所需信息。

您还可以配置 NetApp CAB 目标设备，其中库由 Data Protector 单元中的主机共享。除了在 Data Protector 中创建逻辑设备之外，上述所有配置步骤都保持不变。在这种情况下，Data Protector 中必须预先存在库逻辑定义。用户只需将相关 NDMP 驱动器手动添加到现有的库中。

1. 标识所需的驱动器连接的节点。

2. 指定驱动器名称和驱动器所连接的客户机系统。
3. 指定数据驱动器 SCSI 地址和库驱动器索引。SCSI 地址的格式必须为 /NODE_NAME/DriveAddress 。
4. 创建备份规范并将“子类型”设置为“NDMP - NetApp CAB”。
5. 选择要备份的客户机系统、驱动器、目录和文件。

Data Protector 尝试支持自动发现磁带库和驱动器。但根据供应商的不同，库并不总是能够与其驱动器关联。在这种情况下，如果特定于 NDMP CAB 的下拉菜单不显示为所选介质更换器配置的驱动器，请手动输入驱动器信息。

在 Data Protector 中配置 NetApp ONTAP C 模式 (节点范围) 设备

在 Data Protector 中对 NetApp ONTAP 群集设备进行节点范围配置与配置 NetApp 7 模式设备类似。作为先决条件，必须在配置期间应用常用设置。为完成 Data Protector 配置，需要执行以下一些额外步骤:

1. 在所有节点上启用节点范围模式和 NDMP 服务。
2. 出于安全原因，禁用明文身份验证，从而避免以纯文本格式通过网络发送 NDMP 密码。
3. 标识必须导入 Data Protector 的群集间 LIF 接口。
4. 将接口作为 NetApp 服务器导入 Data Protector。使用常用设置中配置的凭据作为两个接口的用户名和密码。
5. 设备配置也与 ONTAP 7 模式类似。Data Protector 还支持共享库，这意味着可以通过 NDMP 服务器或 Data Protector 客户机 (非 NDMP 客户机) 控制机械手。
6. 将“子类型”选为“NDMP - Netapp”，创建备份规范。

   指定属于选定节点的装载点。为标识哪个装载点属于哪个节点，请运行以下屏幕截图中所述的命令:

```
DPNetAppC::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
--------- -------- --------- ----- ------- ------ ---------------- ------------
data_aggr2  4.37TB    3.36TB   23% online       2 DPNetAppC-01     raid_dp,
                                                                    normal
data_aggr3  4.37TB    3.36TB   23% online       1 DPNetAppC-02     raid_dp,
                                                                    normal
data_aggr4  4.37TB    3.03TB   31% online       3 DPNetAppC-01     raid4,
                                                                    normal
data_aggr5  4.37TB    2.91TB   33% online       2 DPNetAppC-02     raid4,
                                                                    normal
root_aggr0  1.38TB   68.62GB   95% online       1 DPNetAppC-01     raid_dp,
                                                                    normal
root_aggr1  1.38TB   68.62GB   95% online       1 DPNetAppC-02     raid_dp,
                                                                    normal
6 entries were displayed.
```

```
DPNetAppC::> volume show
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
DPNetAppC-01
          vol0         root_aggr0   online     RW       1.31TB     1.22TB    6%
DPNetAppC-02
          vol0         root_aggr1   online     RW       1.31TB     1.22TB    6%
DPNetAppC-SVM01
          WAFL1        data_aggr2   online     RW          1TB    384.7GB   62%
DPNetAppC-SVM01
          WAFL2        data_aggr3   online     RW          1TB    803.5GB   21%
DPNetAppC-SVM01
          rootsvm01    data_aggr2   online     RW          1GB    970.8MB    5%
DPNetAppC-SVM02
          CWAFL1       -            online     RW       7.86TB     5.15TB   34%
DPNetAppC-SVM02
          rootsvm02    data_aggr4   online     RW          1GB    970.7MB    5%
7 entries were displayed.
```

   此处，WAFL1 位于集合 data_aggr2 (属于 DPNetAppC-01)。此节点 LIF 是 DPNetAppC-01_ic1，其 IP 为 a.b.c.d，专为备份规范选择。

   下一步，用户可以选择任何设备，只要设备属于同一 NetApp 群集的其中一个节点即可。如果设备与装载点属于不同节点，Data Protector 将自动切换到三向备份。如果设备与装载点位于同一节点，则在本地运行备份 (双向)。

当文件管理器共享介质更换器时，在 Data Protector 中配置 NDMP 设备

在 Data Protector 中，可以将 NDMP 设备配置为使用一个文件管理器的介质更换器，但使用另一个文件管理器的磁带驱动器。当文件管理器连接到只有一个可用介质更换器的文件库且介质更换器只连接到一个文件管理器时，使用此选项。

要将 NDMP 设备配置为两个 (或更多) 文件管理器共享一个介质更换器且介质更换器只连接一个文件管理器，请执行以下步骤:

1. 在“上下文列表”中，单击**客户机**。
2. 导入 NDMP 服务器。例如 **server1.domain.com** 和 **server2.domain.com**。
3. 在“设备和介质”上下文中，选择“设备”，然后单击“添加设备”。
4. 输入设备的名称。

在“设备类型”中，选择“SCSI 库”。

在“接口类型”中，选择“NDMP”。

> 注意配置并非 NetApp 专用。

5. 指定具有 NDMP 服务器介质更换器的服务器名称。例如，“server1.domain.com”。单击“下一步”。
6. 对于库机械手，在 server1 上指定介质更换器的 SCSI 地址。选择全部其他所需选项，然后单击“下一步”。
7. 在设备驱动器配置中，选择第二台服务器 (server2) 作为 NDMP 服务器，在 server2 上指定磁带驱动器的 SCSI 地址。

   上述设置可确保您的 Data Protector NDMP 设备使用 server1 中的介质更换器但使用 server2 中的磁带驱动器。

   然后，介质更换器可将存储库中的磁带加载到 server1 或 server2 上的指定磁带驱动器。

EMC Celerra 配置

SCSI 设备

要获取有关与 EMC Celerra NAS 设备连接的 SCSI 设备 (磁带驱动器和库机械手) 的信息，请执行以下操作:

1. 登录 Celerra 控制站。
2. 执行:

```
server_devconfig server_name -list -scsi -all
```

示例

有关 SCSI 设备的示例列表，请参阅 SCSI 设备列表示例。 c2t2l0 和 c2t3l0 是磁带库中的驱动器的 SCSI 地址，c2t0l0 是库机械手的 SCSI 地址。

SCSI 设备列表示例

名称	SCSI 地址	设备类型	信息
jbox1	c2t0l0	jbox	ATL P1000 62200001.03
tape2	c2t3l0	tape	QUANTUM DLT7000 1624q$
ttape2	c2t2l0	tape	QUANTUM DLT7000 1624q$

EMC Isilon 配置

要列出 EMC Isilon 上的设备、驱动器和别名，请执行以下命令:

```
isi tape list
```

磁带设备列表示例

磁带设备	状态	WWNN	供应商/型号/版本/序列号
tape001	已关闭	50014380271B0040	Ultrium 6-SCSI 253W HUJ5394NCC
tape002	已关闭	50014380271B0046	Ultrium 6-SCSI 253W HUJ5394ND0
tape003	已关闭	50014380271B003D	Ultrium 6-SCSI 253W HUJ5394NC8
tape004	已关闭	50014380271B0043	Ultrium 6-SCSI 253W HUJ5394N77
tape005	已关闭	5001438024B10BE5	Ultrium 4-SCSI ED41 SG1545DR01
tape006	已关闭	5001438024B10BF9	Ultrium 6-SCSI ED61 SG1545DR05
tape007	已关闭	5001438024B10BEF	Ultrium 6-SCSI ED61 SG1545DR03
tape008	已关闭	5001438024B10BF4	Ultrium 6-SCSI ED61 SG1545DR04

tape009	已关闭	5001438024B10BEA	Ultrium 6-SCSI ED61 SG1545DR02

介质 更换器	状态	WWNN	供应商/型号/版本/序列号
mc001	已关闭	50014380271B003D	MSL G3 Series 8.70 MXA542Z0P3
mc002	已关闭	5001438024B10B45	D2DBS EL01 SG1545DR45

3PAR 文件角色 (FS) 配置

3PAR 支持文件角色 (FS) 的 NDMP 备份。

要开始将 NDMP 与 3PAR 一起使用，必须先将介质代理主机作为 DMA (数据管理代理) 添加到 3PAR。使用以下命令:

```
setfsndmp conf -dma +<MA IP> -username <ndmp_user> -password <ndmp_pass> -enable_sessions true -loglevel 10 -tcpwinsize 163840 -maxsessions 128
```

添加 MA 后，可通过运行以下命令获取库机械手的 SCSI 地址和数据驱动器的 SCSI 地址:

```
showfsndmp –vtl vtltapes
```

VtlTapeId	VtlNode	VtlType	VtlConnectedHost
HP_Ultrium_4-SCSI_7615A8B9C5	/dev/nst1	TapeDevice	node0fs
HP_Ultrium_4-SCSI_7615A8B9C4	/dev/sg3	TapeDevice	node0fs
HP_Ultrium_4-SCSI_7615A8B9C8	/dev/nst0	TapeDevice	node3fs
HP_Ultrium_4-SCSI_7615A8B9C6	/dev/nst0	TapeDevice	node1fs
HP_D2DBS_7615A8B9F9	/dev/sg4	MediaChanger	node3fs
HP_Ultrium_4-SCSI_7615A8B9C5	/dev/sg5	TapeDevice	node0fs
HP_Ultrium_4-SCSI_7615A8B9C8	/dev/sg3	TapeDevice	node3fs
HP_D2DBS_7615A8B9F7	/dev/sg4	MediaChanger	node1fs
HP_Ultrium_4-SCSI_7615A8B9C6	/dev/sg5	TapeDevice	node1fs
HP_D2DBS_7615A8B9F6	/dev/sg4	MediaChanger	node0fs
HP_Ultrium_4-SCSI_7615A8B9C4	/dev/nst0	TapeDevice	node0fs

在此，介质更换器作为 **MediaChanger** 列出，数据驱动器作为 **TapeDevice** 列出。

> **注意**需要在 Data Protector 中添加 VtlTapeId (而非 VtlNode) 作为 SCSI 地址。

如果介质更换器操作 (扫描/格式化) 失败，但未显示错误消息，请确保已将介质代理主机作为 DMA 正确添加至 3PAR 设备。使用以下命令检查是否添加了该主机:

```
showfsndmp -conf
```

MA 主机 IP 应在 **DmaIpAddresses** 的逗号分隔列表中列出。

库机械手

要获取与 NDMP 服务器系统连接的库机械手的 SCSI 地址，请执行以下操作:

1. 登录 NDMP 服务器系统。
2. 获取需要为其配置设备的 NDMP 服务器系统的企业虚拟服务器 ID (EVS ID)。执行以下命令:

   evs list
3. 获取与 NDMP 服务器系统连接的库机械手的 SCSI 地址。执行以下命令:

   ndmp-devices-list -t changer -v EvsID

SCSI 地址写在 ndmp-device-list 输出的开头，由 LUN、目标和设备 ID 号组成。分析库机械手的 SCSI 地址

部分	描述
dev/ mc	Media changer device
1 | 2 | 3 ...	设备 ID 号。

示例

库机械手的介质更换器设备的输出如下:

```
5/dev/mc_d2|0 01YFPdba00 0x2001f29ccd2ca000:0 N/A
```

其中， /dev/mc_d2|0 是介质更换器设备的 SCSI 地址。

磁带库中的独立磁带设备和驱动器

要获取有关与 NDMP 服务器系统连接的磁带库中独立磁带设备或驱动器的信息，请执行以下操作:

1. 登录 NDMP 服务器系统。
2. 获取需要为其配置设备的 NDMP 服务器系统的企业虚拟服务器 ID (EVS ID)。执行以下命令:

   evs list
3. 获取有关与 NDMP 服务器系统连接的磁带库中独立磁带设备或驱动器的信息。执行以下命令:

   ndmp-devices-list -t tape -v EvsID

SCSI 地址写在 ndmp-device-list 输出的开头，由 LUN、目标和设备 ID 号组成。

分析驱动器的 SCSI 地址

部分	描述
dev/ mt	Tape device
1 | 2 | 3 ...	设备 ID 号。

示例

独立磁带设备 (或磁带库中的驱动器) 的输出如下:

```
16/dev/mt_d2|1 01YFPdba01 0x2001f29ccd2ca000:1
```

其中， /dev/mt_d2|1 是磁带设备的 SCSI 地址。

> **提示**要获取 readWriteBlockSizeInKB 参数的当前值，请执行以下命令:
>
> server_param <data mover> -facility PAX -info
>
> readWriteBlockSizeInKB -verbose

> **注意**
>
> - 如果 NAS 设备不支持设置的块大小，并且启动了备份，则 Data Protector 将显示一条错误并中止会话。

- 虽然 Data Protector 介质格式化成功完成，但并不保证 NAS 设备支持设置的块大小，备份仍然可能失败。
- 对于其他供应商的 NAS 设备，请参阅对应的产品文档以获取有关如何列出设备的信息。

备份 NDMP 服务器

Data Protector 支持网络数据管理协议 (NDMP) 服务器的以下备份类型:

备份类型	描述
本地备份或 双向备份	数据传输到备份设备，例如连接到同一文件管理器的磁带库或磁盘。
三向备份	• 磁带库**:** 数据传输到备份设备，例如连接到第二个文件管理器的磁带库或磁盘。第二个文件管理器将数据存储到其本地备份设备。这仅适用于群集感知备份 (**CAB**) 类型。 • **StoreOnce** 和文件库**:** 数据传输到与 Data Protector NDMP 介质代理系统连接的 **StoreOnce** 或“文件库” 备份设备类型。
群集感知备份 (**CAB**)	**CAB** 是 NetApp Filer 的 NDMP 协议扩展，允许在群集环境中进行数据流优化。 它支持 NDMP 服务器在链接到卷的节点上建立数据连接。反过来，Data Protector 确定是否可在群集中的同一节点找到卷和磁带设备。 NDMP 服务器提供有关具有 Data Protector 支持的 **CAB** 扩展的卷和磁带设备的相关性信息。如果可在群集中的同一节点找到卷和磁带设备，Data Protector 将使用此相关性信息执行本地备份 ，而不是 三向备份。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“文件系统”，然后单击“添加备份”。
3. 选择模板。在“备份选项”部分，执行以下操作并单击“确定”:
   - 备份类型: 选择“数据移除器备份”。
   - **负载均衡:** (可选) 为负载均衡的备份选择此选项。
   - 子类型**:** 选择 NDMP 服务器服务。例如，**NDMP-NetApp**。
4. 选择要备份的 NDMP 服务器系统，然后单击“添加/删除”。

   > **重要说明:** 在创建备份规范之前，必须确保您选择用于备份的每个 NDMP 对象包含的文件不应超过 2000 万个。要备份包含更多文件的大型卷，Micro Focus 建议您将卷拆分为多个目录，每个目录包含的文件数少于 2000 万。

   在“添加/删除磁盘装载点”对话框中，指定要备份的文件系统装载点。在“新建装载点” 选项中，指定要备份的每个目录的路径，然后单击“添加”。 要关闭对话框，请单击“确定”，然后单击“下一步”。
5. 选择用于备份的设备。

   对于 **NDMP - NetApp**、 **NDMP - NetApp CAB** 或 **NDMP - Celerra** 服务器类型，设备列表包括为 NDMP 配置的“文件库” 和 **StoreOnce** 设备以及其他支持的磁带设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。

   单击“下一步”。
6. 设置备份选项，然后单击“下一步”。
7. 查看备份规范的摘要。
   要为特定备份对象指定 NDMP 选项，请右键单击该对象，单击“属性”，然后单击“NDMP”选项卡并执行以下操作:
   a. 对于每个对象，您可以指定一个新用户帐户，以覆盖在“导入 NDMP 主机”对话框中指定的用户帐户。这要求在选定的网络连接存储 (NAS) 设备系统上设置适当的访问权限。
   b. 要设置 NDMP 环境变量，请单击“高级”。
   c. 在“NDMP 备份类型”部分，选择以下内容:
      - 对于 EMC Celerra NDMP 客户机 ，选择“转储”或“NVB”。
      - 对于 NetApp NDMP 客户机 ，选择“转储”或“SMTape”。
   d. 单击“确定”。
8. 单击“下一步” ，然后单击“另存为”以保存备份规范。指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

> **提示**在使用之前预览备份规范的备份会话。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

启动备份会话

交互式备份按需运行，对于紧急备份或重新启动失败的备份非常有用。使用 Data Protector GUI。

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开备份规范，然后展开文件系统。右键单击要使用的备份规范，然后单击“启动备份”。
3. 选择备份类型和网络负载。单击**确定**。

还原 NDMP 服务器集成

您可以使用 Data Protector GUI 或 CLI 还原网络数据管理协议 (NDMP) 服务器。

使用 Data Protector GUI 进行还原

1. 在上下文列表中，选择**还原**。
2. 在“范围窗格”中，展开“文件系统”，展开具有要还原的数据的客户机，然后单击具有该数据的对象。
3. 在“源”页中，浏览并选择要还原的对象。
4. 在“目标”页中，为每个选定对象指定还原目标客户机。默认情况下，数据将还原到数据备份的原始位置。要还原到新位置，请选择“还原到新位置”并键入新路径。
5. 在“选项”页中，指定 Data Protector 可用于连接到 NDMP 服务器系统的 NDMP 服务器系统用户帐户。此用户必须有读取和写入 NDMP 介质的权限。

   要指定 NDMP 环境变量，请单击“高级”。
6. 在“设备”页中，选择要用于还原的设备。
7. (可选) 在“介质”页中，指定介质分配优先级。
8. (可选) 在“副本”页中，指定要从中执行还原的介质集。
9. 单击**还原**。
10. 在“开始还原会话”对话框中，单击**下一步**。
11. 指定“报告级别”和“网络负载”。

    注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
12. 单击**完成**启动还原。

    会话输出的末尾会显示还原会话的统计信息和以下消息:
    Session completed successfully

使用 Data Protector CLI 进行还原

要使用 CLI 还原 NDMP，请参阅 omnir 中的“NDMP 还原”。

特定于 NDMP 的 omnirc 选项

> **注意:**
>
> - 还可以使用 Data Protector GUI 设置一些选项。GUI 设置将覆盖 omnirc 文件中的设置。
> - 还有其他 NDMP 参数也会影响还原。有关这些参数的信息，请参阅 NDMP 服务器集成。

NDMP 特定的 omnirc 选项包括以下内容:

选项	默认值	详细信息
OB2NDMPFH	Y	设置为 Y 时，将打开 NDMP 服务器文件历史记录跟踪，这是浏览和还原各个文件的先决条件。但是，这会影响此类备份所需的时间。 每次启动备份时，此设置将覆盖 NDMP 服务器上的文件历史记录设置。
OB2NDMPDIRECT	Y	设置为 Y 时，只要备份期间打开 NDMP 服务器文件历史记录跟踪，Data Protector 将使用直接访问还原功能。

OB2NDMPCATQUESIZE	5	此选项设置承载编目信息的内部缓冲区数，然后再将编目信息存储到文件历史记录交换文件。通过微调该值，可以在一定程度上提高 NDMP 备份性能。 设置为 5 时，只要有足够的系统资源 (约 1.9 GB 系统内存和 2.8 GB 磁盘空间)，NDMP 介质代理最多可以处理 2000 万文件 (位于一个备份规范)。 如果备份规范中的文件数小于 2000 万并且有足够的系统内存，则将选项设置为更高的值。 要以千字节为单位计算内存分配开销，请用选项值乘以 512。
OB2NDMPFHFILEOPT	**Windows** 系统： Data_Protector_program_data\tmp, 32, 1024 **Unix** 系统**:** /var/opt/omni/tmp, 32, 1024	此选项微调文件历史记录交换文件使用情况。其中包含三个参数，用来定义以下设置: 1. 存储文件历史记录交换文件的目录的路径。 2. NDMP 客户机磁盘上的 Data Protector 创建的最大文件历史记录交换文件数。 3. 文件历史记录交换文件的最大大小 (以 MB 为单位)。 参数以逗号分隔。您可以使用分号分隔几组参数。 **示例：** **Windows** 系统： C:\tmp, 32, 1024; D:\tmp\tmp_1, 10, 1024 **UNIX** 系统： /tmp, 10, 1024; /var/tmp, 5, 60 当第一个目录中的文件已满后，集成将数据写入下一个指定目录中的文件。如果备份期间分配的磁盘空间用尽，则备份失败。文件历史记录交换文件的大小可能显著增加。有关文件历史记录交换文件的大致磁盘消耗量的信息，请参阅文件历史记录交换文件的大致磁盘消耗量。

文件历史记录交换文件的大致磁盘消耗量

使用以下公式计算大致磁盘消耗量:

EstConsumption = (NumOfFiles + NumOfDirs) x (136 + AverageFileNameSize)

其中， NumOfFiles 是备份文件数， NumOfDirs 是备份目录数。

此计算假定:

- 目录数最多为文件总数的 10％
- 目录名称平均长度为 25 个字符
- 文件名平均长度为 10 个字符

备份文件数和目录数	文件历史记录交换文件的大致磁盘消耗量
5 百万	0.7 GB
10 百万	1.4 GB
20 百万	2.8 GB

NetApp SnapManager 解决方案

This feature is available in the Premium Edition

本节介绍 Data Protector NetApp SnapManager 解决方案，将该解决方案与标准 Data Protector 功能结合使用时，支持将 NetApp SnapManager 快照备份并还原到 Data Protector 备份介质，反之亦然。

该解决方案仅适用于 Windows 系统。

NetApp SnapManager for Microsoft Exchange (SME) 和 NetApp SnapManager for Microsoft SQL Server (SMSQL) 是两种解决方案，用来在 NetApp 存储系统上创建 Microsoft Exchange Server 和 Microsoft SQL Server 数据快照。

Data Protector 通过 omnisnapmgr.pl 脚本支持 SME 和 SMSQL，从而使您可以将现有 NetApp SnapManager 快照存档到 Data Protector 备份介质。 omnisnapmgr.pl 脚本使用 NetApp SnapDrive 命令行界面执行查询、装载及卸除卷。

要将 SME 和 SMSQL 快照备份到 Data Protector 备份介质，必须创建标准 Data Protector 文件系统备份规范，并将 omnisnapmgr.pl 脚本指定为此备份规范的 pre-exec 和 post-exec 脚本。

备份会话开始时 (pre-exec 阶段)， omnisnapmgr 将尚未存档的最新 SME 或 SMSQL 快照装载到运行它的 Windows 客户机。然后，Data Protector 磁盘代理将已装载卷中的文件备份到 Data Protector 备份设备。备份会话结束时 (post-exec 阶段)， omnisnapmgr.pl 将卸除备份会话开始时装载的卷。

满足 NetApp SnapManager 解决方案的先决条件

以下是 NetApp SnapManager 解决方案集成的先决条件:

- 将要安装 Data Protector SnapManager 解决方案的系统 (备份系统) 必须安装 Data Protector 磁盘代理，而且必须是 Data Protector 单元的成员。
- 必须在 Data Protector 单元中配置至少一个 Data Protector 备份设备。
- 必须在备份系统上安装并配置 NetApp SnapDrive。

配置

如果备份系统上的 Data Protector Inet“并非”在 SnapDrive 帐户下运行，则可以:

- 将 Data Protector 的 Inet 帐户更改为 SnapDrive 帐户。
- 配置 SnapDrive 帐户，使其可与 Data Protector 配合使用。
  - 创建一个具有足够备份权限的新 Data Protector 用户组，然后删除该权限 Backup as root:
- 将 SnapDrive 帐户添加到该组；或者，如果 SnapDrive 帐户已被添加到 Data Protector 用户列表，则将其移动到新创建的组中。

备份 NetApp SnapManager 解决方案集成

This feature is available in the Premium Edition

本主题包含以下几节:

创建备份规范

要创建 NetApp SnapManager 备份规范，请执行以下操作:

1. 为 Data Protector 将装载 SnapManager 快照的 Windows 客户机创建文件系统备份规范。

   在“源”属性页中，选择 Data Protector omnisnapmgr 脚本将装载卷的文件夹。将备份此文件夹及其下装载的所有卷。

   > **注意**即使已在备份规范中选择临时文件夹，Data Protector 也会在备份时排除某些临时文件夹。选择的文件夹不得为操作系统临时文件夹、Data Protector 临时文件夹或其子文件夹，例如 C:\Windows\Temp 或 Data_Protector_home\tmp 。

2. 指定 omnisnapmgr.pl pre-exec 和 post-exec 脚本:
   a. 在“文件系统”选项下，单击“高级”。
   b. 在“选项”窗格中，输入“Pre-exec”和“Post-exec”脚本。
3. 如果未在 SnapDrive 帐户下运行 Data Protector Inet 帐户，请将 SnapDrive 帐户指定为备份所有者:
   a. 在“文件系统”选项下，单击“高级”。
   b. 在“备份选项”窗口中的“所有权”下，输入用户名、组和客户机系统名称。
4. 保存备份规范，然后运行或计划备份会话。

omnisnapmgr.pl 参考页

概要

omnisnapmgr.pl -version | -help

omnisnapmgr.pl [-sme | -smsql] { -mount | -unmount } -apphost *ClientName* [-force] [-partial] [-preview]

omnisnapmgr.pl -query

说明

omnisnapmgr.pl 脚本用于装载或卸除 SME 或 SMSQL 快照 (作为 pre-exec 或 post-exec 脚本启动时) 或者查询 NetApp 快照 (从“命令提示符”窗口运行时)。

选项

-version	显示 Data Protector 版本。
-help	显示用法概要。
-sme	指定将备份 SME 快照。 如果未指定， omnisnapmgr 默认假定已备份 SME。
-smsql	指定将备份 SMSQL 快照。

-mount	从应用程序系统的最后一个 SnapManager 备份装载所有卷。
-unmount	卸除由 -mount 选项装载的所有卷
-apphost *ClientName*	指定应用程序服务器 (Exchange 或 SQL Server) 系统。如果未指定，则使用本地系统。
-force	即使已备份快照，也会执行快照备份。
-partial	即使无法装载某些卷，也会对 SME 或 SMSQL 快照执行备份。
-preview	显示 SnapDrive 装载命令但不执行命令。
-query	列出上次 SME/SMSQL 备份会话中包含的快照和卷。

备注

omnisnapmgr.pl 脚本仅适用于 Windows 系统。

示例

1. 要将 SnapManager Microsoft Exchange Server 快照备份到 Data Protector 备份介质 (其中，Microsoft Exchange Server 在客户机“exch1.company.com”上运行)，请指定以下两项 pre-exec 和 post-exec 命令:

   Pre-exec:

   ```
   perl omnisnapmgr.pl -sme -mount –apphost exch1.company.com
   ```

   Post-exec:

   ```
   perl omnisnapmgr.pl -sme -unmount –apphost exch1.company.com
   ```

2. 要备份 SnapManager Microsoft SQL 快照 Data Protector 备份介质 (其中，Microsoft SQL Server 在客户机“sql2.company.com”上运行，即使已备份快照；同时，确保即使不能装载某些卷，也要执行备份)，请指定以下 pre-exec 和 post-exec 命令:

   Pre-exec:

   ```
   perl omnisnapmgr.pl -smsql -mount –apphost sql2.company.com
   ```

   Post-exec:

   ```
   perl omnisnapmgr.pl -smsql -unmount –apphost sql2.company.com \
   -force -partial
   ```

还原 NetApp SnapManager 解决方案集成

This feature is available in the Premium Edition

要还原 SME 或 SMSQL 数据，请使用 Data Protector 和 SnapManager:

1. 按标准 Data Protector 还原过程将 Data Protector 备份介质中的数据库文件和日志文件还原到临时目录。

   注意一旦发生灾难导致应用程序安装程序丢失，需要先将应用程序还原或重新安装到原始位置，然后使用 SnapManager 恢复向导恢复应用程序数据。

2. 使用 SnapManager 恢复向导恢复 Microsoft Exchange Server 或 Microsoft SQL Server 数据。选择“从非托管介质还原”并按指示操作。

   有关信息，请参阅 SnapManager 文档。

Nutanix AHV 集成和 VM 备份

Nutanix 是一种超融合设备，它支持各种虚拟化，例如 VMware 和 Hyper-V。

Nutanix 有其自己的称为 Acropolis Hyper-Visor (AHV) 的虚拟机监控程序，可提供集成的虚拟化。Micro Focus Data Protector 开发了基于脚本的解决方案，使管理员可以执行 AHV VM 的备份和还原。

重要说明

- Data Protector 解决方案在数据保护方面被认证为 **Nutanix Ready AHV INTEGRATED**。有关详细信息，请转到 https://www.nutanix.com/。
- 使用这些脚本在 Nutanix 基础结构中执行 VM 的备份和还原时，您将禁用或绕过安全功能，会使系统增加安全风险。使用这些脚本即表示您了解并同意承担所有相关风险，同样使 Micro Focus 免受损失。

  Micro Focus 鼓励您添加相关的保护措施以防范与用户信息相关的风险，Micro Focus 没有提供此保护措施。若未实施相应的保护措施，您的系统可能面临更多的安全风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

Nutanix AHV 与 Data Protector 集成

Data Protector 使用脚本来执行 Nutanix AHV VM 的备份和还原。这些脚本在文件系统备份规范中用作执行前/执行后脚本。这些脚本使用 Nutanix REST API 执行 VM 管理操作 (快照、备份、还原等)。

在备份期间，pre-exec 脚本会创建 AHV VM 的实时外部快照，并将其安装在备份代理上。然后可以使用文件系统备份或磁盘映像备份来备份这些快照和装载点。

- 如果在文件级别进行备份，则可以在备份代理上还原单个文件。
- 如果将备份作为磁盘映像，则使用还原脚本只能还原整个 VM。

在备份期间，post-exec 脚本用于清除快照和临时文件。在映像级还原期间，post-exec 脚本用于还原原始数据。

先决条件

以下先决条件适用:

- 确保 Data Protector Cell Manager 的版本为 2019.05 或更高版本。
- 确保在 Linux 备份代理上安装了以下 RPM:
  - Jq
  - ntfs-3g
- 确保在备份代理中创建文件系统装载点。装载点用于在备份和还原期间存储配置数据。该装载点应是 Linux 安装代理主机上具有适当权限的文件系统目录。需要针对“Nutanix_config.sh”中引用的“$CONF”变量提及此装载点。
- 在运行备份之前，请确保已编辑“Nutanix_config.sh”脚本。
- 确保将备份代理导入到 Cell Manager。

限制

以下限制适用：

- 仅支持 Linux 备份代理。它必须是同一 AHV 基础结构的一部分。
- Nutanix AHV VM 的备份仅受 Linux Cell Manager 支持。
- 映像和文件级备份仅支持 scsi 磁盘。
- 如果是文件级备份和映像级备份，则可以创建具有 Linux 分区的 Linux VM。不支持 LVM 和 RAID。
- 如果是映像级备份，则整个磁盘作为原始映像来备份。如果是文件级备份，则备份文件系统中的所有文件。
- 如果 Data Protector Cell Manager 和备份代理是同一基础结构的一部分，则 Data Protector 不会对二者进行备份。
- 如果 VM 名称中包含“保留”一词，则该 VM 将不会备份。
- 如果使用版本 1 Nutanix 脚本备份 VM，则可以使用相同版本的脚本还原该 VM。不支持使用版本 2 脚本还原该 VM。
- 在还原配置文件之后和还原 VM 之前，您不能更改备份代理的磁盘配置。
- 不支持将单个或多个磁盘还原到同一 VM 或另一个 VM。将创建一个新 VM，并将磁盘还原到该 VM。

将 Data Protector 与 AHV 集成并配置 Data Protector

要将 Data Protector 与 AHV 集成并配置 Data Protector，请执行以下步骤:

1. 从 ITOM Marketplace 下载 AHV 脚本 zip 包。如果您有任何问题，请联系客户支持。
2. 登录 AHV 备份代理主机，并在“/opt/omni/lbin”路径中提取下载的脚本。对于文件级和映像级备份和还原，提取以下脚本:
   - *Nutanix_config.sh*
   - *Nutanix_Pre_File_Backup.sh*
   - *Nutanix_Post_Backup_Cleanup.sh*
   - *Nutanix_Pre_Image_Backup.sh*
   - *Nutanix_post_conf_Restore.sh*
   - *Nutanix_post_VM_Restore.sh*
3. 在所有 Nutanix_Pre_* 和 Nutanix_post_* AHV 脚本上，将文件权限更改为“500”。

   例如: *cd /opt/omni/lbin*

   *chmod **500** Nutanix_Pre_File_Backup.sh*

4. 将“Nutanix_config.sh”的文件权限更改为 700

   例如: *cd /opt/omni/lbin*

   chmod 700 Nutanix_config.sh

5. 使用任何文件编辑器编辑“Nutanix_config.sh”文件。

   提供用于 AHV 环境备份的变量输入。

6. 在路径“/opt/omni/lbin”下创建 VM 列表文件“Nutanix_VM_List”。该文件必须包含要备份的所有 VM 的列表。每个 VM 名称必须在新行上。

> 注意: 确保您在 *Nutanix_VM_List* 文件中输入的 VM 名称与 Prism 中提到的名称相同。这些名称区分大小写。

Data Protector 和 Nutanix AHV 集成支持以下配置:

- AHV VM 文件级备份
- AHV VM 文件级还原
- AHV VM 映像级备份
- AHV VM 映像级还原

AHV VM 文件级备份

AHV VM 文件级备份使用 Data Protector 文件系统备份功能来备份 VM。完成下列步骤以执行文件级备份:

1. 登录 Data Protector GUI 主机并连接到 Cell Manager。
2. 在客户机上下文中，将 Linux 备份代理主机导入到 Cell Manager。
3. 在设备和媒体上下文中，创建一个备份设备来存储备份数据 (文件或 VM 映像)。
4. 创建备份规范“nutanix_backup1”。
   确保在备份规范中选择先前创建的用于备份的装载点。还要在“Nutanix_config.sh”中将“$CONF”设置为此装载点。
   1. 在“选项”选项卡中，在“备份规范选项”下单击“高级”。
   2. 在“Pre-exec”脚本字段中指定“Nutanix_Pre_File_Backup.sh”。
   3. 在“在客户机上”字段中指定 Nutanix 主机。
   4. 保存并计划此备份规范。
5. 创建第二个备份规范“nutanix_backup2”。
   确保在备份规范中选择先前创建的用于备份的装载点。还要在“Nutanix_config.sh”中将“$CONF”设置为此装载点。

将“Nutanix_config.sh”中的“$NUTANIX_DATALIST”变量设置为第二个备份规范的名称。
例如 : $NUTANIX_DATALIST= nutanix_backup2。

1.
   1. 在“选项”选项卡中，在“备份规范选项”下单击“高级”。
   2. 在“Post-exec”字段中指定“Nutanix_Post_Backup_Cleanup.sh”。
      不要计划此备份规范，因为此备份将通过第一个备份规范中配置的 pre-exec 脚本运行。
   3. 在“在客户机上” 字段中指定 Nutanix 备份主机。
   4. 单击“确定”。

AHV VM 文件级还原

完成以下步骤还原 VM:

1. 在上下文列表中，单击“还原”。
2. 文件级还原可以通过多种方式完成:
   1. 在“范围窗格”中，展开“还原会话”，然后选择适当的会话。在结果区域中，从相应的磁盘中选择要还原的文件。
   2. 在“范围窗格”中，展开“还原对象”，然后展开“文件系统”。在结果区域中，选择主机和相应的磁盘以选择要还原的文件。

AHV VM 映像级备份

AHV 映像级备份使用 Data Protector 原始磁盘备份功能来备份 VM。完成下列步骤以执行映像级备份:

1. 登录 Data Protector GUI 主机并连接到 Cell Manager。
2. 在“客户机” 上下文中，将 Linux 备份代理主机导入到 Cell Manager。
3. 在“设备和介质” 上下文中，创建一个备份设备来存储备份数据 (文件或 VM 映像)。
4. 在“备份” 上下文中，创建备份规范 **nutanix_backup1**。
   确保在备份规范中选择先前创建的用于备份的装载点。还要在“Nutanix_config.sh”中将“$CONF”设置为此装载点。
   1. 在“选项” 选项卡中，在“备份规范选项”下单击“高级”。
   2. 在“Pre-exec”脚本字段中指定“Nutanix_Pre_Image_Backup.sh”。
   3. 在“在客户机上”字段中指定 Nutanix 主机。
   4. 保存并计划此备份规范。
5. 创建第二个备份规范“nutanix_backup2”。
   确保在备份规范中选择先前创建的用于备份的装载点。还要在“Nutanix_config.sh”中将“$CONF”设置为此装载点。

将“Nutanix_config.sh”中的“$NUTANIX_DATALIST”变量设置为第二个备份规范的名称。
例如 : $NUTANIX_DATALIST= nutanix_backup2。

1.
   1. 在“选项”选项卡中，在“备份规范选项”下单击“高级”。

2. 在“Post-exec”字段中指定“Nutanix_Post_Backup_Cleanup.sh”。
   不要计划此备份规范，因为此备份将通过第一个备份规范中配置的 pre-exec 脚本运行。
3. 在“在客户机上” 字段中指定 Nutanix 备份主机。
4. 单击“确定”。

AHV VM 映像级 VM 还原

单个或多个 VM 还原是一个多步骤过程。首先还原配置文件，然后还原实际的 VM 映像。

单个 VM 映像级还原

完成下列步骤以执行单个 VM 还原:

1. 启动 Data Protector，然后转到“还原” 上下文。
2. 在“范围窗格”中，展开“还原会话” 。选择要还原的磁盘映像备份。
3. 将配置数据还原到备份代理 **$CONF** 目录:
   1. 选择 **$CONF** 中提供的会话和装载点。
   2. 在“源” 选项卡中，选择 VM 目录以将配置数据还原到备份代理。
   3. 在“选项” 选项卡中，在 **Post-exec** 脚本字段中指定 *Nutanix_post_conf_Restore.sh*。
   4. 执行还原，确保还原的 VM 配置数据在备份代理上的 **$CONF** 装载点中可用。
4. 在备份代理上还原 VM 的磁盘映像:
   1. 在“还原” 上下文中，展开“还原会话”，然后选择已经为其还原了配置数据的单个 VM 的备份映像。
   2. 在“选项” 选项卡中，在 **Post-exec** 脚本字段中指定 *Nutanix_post_VM_Restore.sh*。
      该 post-exec 脚本将重命名已还原的 VM，创建新的 VM，附加已还原的磁盘和网络并启动它。
   3. 单击**还原**。

多个 VM 映像级还原

完成下列步骤以执行多个 VM 还原:

1. 启动 Data Protector，然后转到“还原” 上下文。
2. 在“范围窗格”中，展开“还原会话” 。选择要还原的磁盘映像备份。
3. 将配置数据还原到备份代理 **$CONF** 目录:
   1. 选择 **$CONF** 中提供的会话和装载点。
   2. 在“源” 选项卡中，选择所有 VM 目录以将配置数据还原到备份代理。
   3. 在“选项” 选项卡中，在 **Post-exec** 脚本字段中指定 *Nutanix_post_conf_Restore.sh*。
   4. 执行还原，确保还原的 VM 配置数据在备份代理上的 **$CONF** 装载点中可用。

   > 注意: 还原后，检查配置还原会话日志以获取 VM 磁盘映射详细信息。例如：*/dev/sdg* 映射到 */dev/sdb*。使用 Data Protector“还原为” 选项还原磁盘 */dev/sdb*。

4. 使用以下两种方法之一还原备份代理上的 VM 的磁盘映像:
   方法 1:
   1. 展开“还原会话”，然后选择已经为其还原了配置数据的多个 VM 的备份映像。
   2. 单击**还原**。
   3. 恢复完成后，在备份代理中手动运行脚本 *Nutanix_post_VM_Restore.sh*。

   方法 2:

   1. 展开“还原会话”，然后选择已经为其还原了配置数据的多个 VM 的备份映像。
   2. 确定较大的磁盘对象，然后仅在此特定磁盘对象中添加 post-exec 脚本 *Nutanix_post_VM_Restore.sh*。
   3. 单击 还原。

清理

1. 转到 Nutanix AHV Web 控制台，然后手动删除已还原 VM 的 **$VM_keep_$DATE** 后验证。
2. 使用此脚本手动清理备份代理:
   /opt/omni/lbin/**Nutanix_Post_Backup_Cleanup.sh**

参考

有关创建备份设备和备份规范的详细信息，请参阅 Data Protector 文档，网址为 https://docs.microfocus.com/?DP。

Operations Orchestration 集成

Operations Orchestration (OO) 是一个在称为流的结构化序列中创建和使用操作的系统。这些结构化序列用于对 IT 资源进行维护、故障诊断、修复和配置。使用 OO，可以对整个组织的各种服务和设备在其整个生命周期中进行管理。

Data Protector 支持与 OO 10.80 及更高版本集成。
Data Protector 的 Linux 和 HP-UX Cell Manager 已通过在 Windows 上运行的 OO 认证。

集成 OO

要集成 OO，请执行以下步骤:

1. 请联系支持人员以下载 OO。您必须具有有效的合同才能下载 OO。
   - 将 ZIP 包提取到本地文件夹。
2. 安装 OO Studio。

   有关安装 OO 的详细信息，请参阅 https://docs.microfocus.com/itom/Operations_Orchestration:10.80/Home (或对应的页面以获得更新的版本)。

   1. 浏览到所提取的文件夹，然后双击“installer-win64-studio.exe”。
   2. 在“选项选择”页面中选择“Studio”作为要安装的组件。
3. 从 https://marketplace.microfocus.com/itom/content/oo-base-content 下载“基本内容包”并将其提取到本地文件夹。
4. 从 https://marketplace.microfocus.com/itom/content/oo-solutions-content 下载 "OO Micro Focus Solutions" 内容包并将其提取到本地文件夹。
5. 启动 OO Studio。
6. 导入内容包。
   1. 单击“依赖关系”窗格中的“导入内容包”。
   2. 浏览到从基本内容包中提取的文件夹，选择 oo10-base-cp-1.12.3.jar 文件或更新的版本，然后单击“确定”。
   3. 再次单击“导入内容包”。
   4. 浏览到从 OO Micro Focus Solutions 中提取的文件夹，选择 oo10-microfocus-solutions-cp-1.13.0.jar 文件，然后单击“确定”。

   导入内容包后，将在“依赖关系”窗格下创建 OO Micro Focus Solutions 文件夹。

   “依赖关系”窗格下的 \OO Micro Focus Solutions\Library\Integrations\Micro Focus\Data Protector 文件夹列出了 Data Protector 支持的所有 OO 流。有关 Data Protector 支持的 OO 流列表，请参阅 OO 流。

   您只能部署或调试 OO 流，不能更改任何 OO 流。如果需要自定义流，请将流复制到“项目”窗格。

OO 流

支持下列 OO 流:

OO 流	描述
备份	
备份文件系统	备份 UNIX 文件系统。您必须输入要备份的源 (文件和文件夹) 和目标 (设备)。
备份 Windows 文件系统	备份 Windows 文件系统。您必须输入要备份的源 (文件和文件夹) 和目标 (设备)。
单元管理	
列出 DP 单元的客户机	提供 Cell Manager 中存在的所有客户机的详细信息。您必须提供输入 (Cell Manager 信息)。
管理 DP 服务或后台程序	启动或停止 Data Protector 服务或后台程序，显示其状态，或者打开或关闭维护模式。
配置客户机	安装、删除、升级或检查指定的 Data Protector 组件。
运行状况检查	
检查 DP 服务的状态	检查 Data Protector 服务的状态以及 Data Protector 内部数据库的一致性。
验证备份对象	验证 Data Protector 备份对象。
验证介质上的数据	验证介质上的数据。
还原	
还原文件系统	还原 UNIX 文件系统。您必须提供树路径 (作为要还原的内容)。
还原 Windows 文件系统	还原 Windows 文件系统。您必须提供树路径 (作为要还原的内容)。
会话管理	
取消活动会话	中止活动会话。
获取会话详细信息	提供会话详细信息。
获取会话状态	显示活动 Data Protector 备份和还原会话的状态。
运行 DP 命令	提供运行任何 CLI 命令的选项。指定 CLI 命令作为此流中的输入。

Oracle Server 集成

This feature is available in the Premium Edition

Data Protector 提供 Oracle Server 实例的脱机和联机备份。为了能够从联机备份进行数据库恢复，各 Oracle Server 实例必须以 ARCHIVELOG 模式运行。

联机备份概念已得到广泛接受。与脱机备份概念不同，它满足了应用程序高可用性的业务要求。在联机备份期间，数据库仍可供使用，而在脱机备份期间，应用程序则无法使用数据库。

备份类型

使用 Data Protector Oracle 集成，可以执行以下类型的备份:

- 联机备份整个数据库或其某些部分
- 联机增量备份 (Oracle 差异增量备份 1 到 4)
- 脱机备份整个数据库
- 仅备份归档重做日志
- 备份 Oracle 数据库恢复编目
- 备份 Oracle 控制文件
- 备份位于**闪回恢复区**中的**恢复文件**。

  备份闪回恢复区中的以下恢复文件:

  - 完整备份集和增量备份集
  - 控制文件自动备份 (如果使用，则包括 SPFILE)
  - 归档重做日志
  - 数据文件副本、控制文件副本

  不备份闪回日志、当前控制文件和联机重做日志。
- 在 **Oracle Data Guard** 环境中，备份“备用数据库”。

还原类型

使用 Data Protector Oracle 集成，可以还原以下各项:

- 整个数据库或其某些部分
- 将数据库还原到特定时间点
- 从增量备份进行还原
- 还原到最初所在主机以外的主机
- 将数据文件还原到其原始位置以外的位置
- 还原目录然后再还原数据库
- 从一组相关的增量备份还原

复制数据库

使用 Data Protector Oracle 集成，可以执行生产数据库的复制。

集成概念

Data Protector Oracle 集成将 Oracle 数据库管理软件与 Data Protector 相关联。从 Oracle 的角度看，Data Protector 代表一种介质管理软件。另一方面，可将 Oracle 数据库管理系统视为备份的一个数据源，其中备份使用由 Data Protector 控制的介质。

组件

备份和还原过程中涉及的软件组件包括:

- Oracle Recovery Manager (RMAN)
- Data Protector Oracle 集成软件

集成功能概述

Data Protector Oracle 集成代理 (ob2rman.pl) 与 RMAN 一起管理 Oracle 目标数据库上以下操作的所有方面:

- 数据库启动和关闭
- 备份 (备份和复制)
- 恢复 (还原、恢复和复制)

集成的工作原理

ob2rman.pl 执行 RMAN，它指导目标数据库上的 Oracle 服务器进程执行备份、还原和恢复。RMAN 在恢复编目、Oracle 中央信息存储库以及特定目标数据库的控制文件中保留有关目标数据库的必要信息。

ob2rman.pl 向 RMAN 提供的主要信息包括:

- 已分配的 RMAN 通道数
- RMAN 通道环境参数
- 有关要备份或还原的数据库对象的信息

对于备份， ob2rman.pl 使用 Oracle 目标数据库视图来获取有关可用于备份的逻辑 (表空间) 和物理 (数据文件) 目标数据库对象的信息。

对于还原， ob2rman.pl 使用当前控制文件或恢复编目 (如果使用) 来获取有关可用于还原的对象的信息。

使用 Data Protector 与 RMAN 的集成，可以备份和还原 Oracle 控制文件、数据文件和存档重做日志。

Oracle 服务器进程到 Data Protector 的接口由 Data Protector Oracle 集成介质管理库 (**MML**) 提供，该库是一组允许在常规介质代理中读取和写入数据的例程。

除了处理与介质设备的直接交互外，Data Protector 还提供计划功能、介质管理、网络备份、监视和交互式备份。

集成处理的 Oracle 备份类型

使用此集成，可以执行“Oracle 完整和增量”(最高增量级别为 4) 类型备份。

对于 Oracle 完整和增量级别 0 备份，将备份每个数据文件的所有数据块。对于 Oracle 增量备份 (级别 1 或更高级别)，将仅备份自上次备份以来所更改的数据块。

完整备份与增量级别 0 备份之间的区别在于，增量 0 是后续增量备份的基础。因此，如果在备份规范中选择完整备份类型，Data Protector 将始终执行 Oracle 增量 0 备份。

完整备份类型与备份中包含的数据文件数无关，因此，可以按单个数据文件执行。无论备份类型是什么 (完整或增量)，都由 Oracle 选择和控制所备份的数据。

Oracle 增量备份可以是差异备份或累计备份。默认情况下，Data Protector 执行“Oracle 差异增量”备份。通过更改 Data Protector 创建的默认 RMAN 脚本，还可以指定累计备份。

> **注意**无论指定哪种 Oracle 备份类型，Data Protector 始终在 Data Protector 数据库中将 Oracle 备份标记为完整备份，因为 Data Protector 增量备份概念与 Oracle 增量备份概念不同。

如果备份包含属于 Oracle Server 实例的所有数据文件和当前控制文件，则该备份称为整个数据库备份。

这些功能可用于 Oracle 目标数据库的联机或脱机备份。但是，必须确保备份对象 (例如表空间) 在备份会话之前和之后切换到适当的状态。对于联机备份，数据库实例必须在 ARCHIVELOG 模式下运行；而对于脱机备份，需要在备份规范中使用 Pre-exec 和 Post-exec 选项准备要备份的对象。

Data Protector 备份规范包含有关备份选项、RMAN 命令、Pre-exec 和 Post-exec 命令、介质和设备的信息。

使用 Data Protector 备份规范可以配置备份，然后多次使用同一规范。此外，计划的备份只能使用备份规范执行。

可以使用 Data Protector 用户界面、RMAN 实用程序或 Oracle Enterprise Manager 实用程序执行 Oracle 目标数据库的备份和还原。

Data Protector Oracle 集成的核心是 MML，它允许 Oracle Server 进程向 Data Protector 发出命令来备份或还原部分或所有 Oracle 目标数据库文件。主要目的是控制与介质和设备的直接交互。

备份流

Data Protector 备份会话管理器触发 Data Protector 计划或交互式备份，并读取备份规范，然后以备份规范中指定的操作系统用户帐户在 Oracle Server 上启动 ob2rman.pl 命令。此后，ob2rman.pl 准备环境以开始备份，并发出 RMAN 备份命令。RMAN 指示 Oracle Server 进程执行指定的命令。

Oracle Server 进程通过 MML 启动备份，从而建立与 Data Protector 备份会话管理器的连接。备份会话管理器启动常规介质代理，在 MML 与常规介质代理之间建立连接，然后监视备份过程。

Oracle Server 进程从磁盘读取数据，并通过 MML 和常规介质代理将其发送到备份设备。

RMAN 将有关备份的信息写入恢复编目 (如果使用) 或 Oracle 目标数据库的控制文件。

备份会话的消息将发送到备份会话管理器，备份会话管理器将有关备份会话的消息和信息写入 IDB。

Data Protector 常规介质代理将数据写入备份设备。

请注意，OB2BACKUPHOSTNAME 选项仅在 Data Protector 托管控制文件备份期间使用。如果您使用多个 NIC 并且想要选择特定 NIC 以避免增加生产 NIC 上的流量，则在 Oracle 客户机上的 omnirc 文件中设置此变量。

还原流

可以使用以下方式启动还原会话:

- Data Protector GUI
- RMAN CLI
- Oracle Enterprise Manager GUI

您必须指定要还原的对象。

Data Protector 还原会话管理器触发从 Data Protector 用户界面中还原，并启动 ob2rman.pl 命令。 ob2rman.pl 准备环境以开始还原，并发出 RMAN 还原命令。RMAN 检查恢复编目 (如果使用) 或控制文件以收集有关 Oracle 备份对象的信息。它还与 Oracle Server 进程进行通信，后者通过 MML 启动还原。MML 与还原会话管理器建立连接，并传递有关所需对象和对象版本的信息。

还原会话管理器将执行以下操作: 检查 IDB 以查找适合的设备和介质，启动常规介质代理，在 MML 与常规介质代理之间建立连接，监视还原，并将有关还原的消息和信息写入 IDB。

常规介质代理从备份设备读取数据，并通过 MML 将其发送到 Oracle Server 进程。Oracle Server 进程将数据写入磁盘。

数据库文件也可以通过 **Automatic Storage Management** (**ASM**) 进行管理。这些文件可以驻留在闪回恢复区中。

图例

SM	Data Protector 会话管理器；在备份会话期间为 Data Protector 备份会话管理器，在还原会话期间为 Data Protector 还原会话管理器。
RMAN	Oracle Recovery Manager。
Data Protector MML	Data Protector Oracle 集成介质管理库，它是支持在 Oracle Server 与 Data Protector 之间进行数据传输的一组例程。
备份 API	Oracle 定义的应用程序编程接口。
IDB	Data Protector 内部数据库，在其中写入有关 Data Protector 会话的所有信息，包括会话消息、对象、数据以及使用的设备和介质。
MA	Data Protector 常规介质代理，用于在介质设备中读取和写入数据。

灾难恢复

灾难恢复是一个极其复杂的过程，涉及到来自多家供应商的产品。因此，能否成功实施灾难恢复取决于涉及的所有供应商。此处提供的信息仅供参考。

有关如何为灾难恢复做准备，请查看数据库/应用程序供应商的说明。

以下是恢复应用程序的常规过程:

1. 完成操作系统的恢复。
2. 安装、配置和初始化数据库/应用程序，以便可将 Data Protector 介质上的数据加载回系统。请查看数据库/应用程序供应商文档，了解准备

数据库所需的详细过程和步骤。
3. 确保数据库/应用程序服务器已安装所需的 Data Protector 客户机软件，并且已针对数据库/应用程序进行配置。按照本节所述的过程进行操作。
4. 启动还原。完成还原后，按照数据库/应用程序供应商提供的说明执行使数据库重新联机所需的任何额外步骤。

Oracle RMAN 元数据与 Data Protector 介质管理数据库同步

本节介绍如何将 Oracle RMAN 元数据与 Data Protector 介质管理数据库同步。

RMAN 元数据包含有关目标数据库的信息。RMAN 使用此信息进行所有备份、还原和维护操作。元数据可以存储在恢复编目数据库或控制文件中。

Data Protector 是 Oracle 执行磁带存储备份和还原所需的介质管理器。

Data Protector 具有自己的数据保护策略，不会自动与 Oracle RMAN 元数据同步。要使两个编目同步，请使用 RMAN 执行以下命令:

使用 ENV:

```
allocate channel for maintenance type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=(OB2MAINTENANCE=1)';

crosscheck backup completed after "TO_DATE('01/13/06 10:30:00','MM/DD/YYHH24:MI:SS')";

release channel;
```

使用 send 命令 (建议在 Windows 上使用):

```
allocate channel for maintenance type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML';

send device type 'sbt_tape' 'OB2MAINTENANCE=1'

crosscheck backup completed after "TO_DATE('01/13/06 10:30:00','MM/DD/YYHH24:MI:SS')";

release channel;
```

应仅在 UNIX 和 Windows 系统上指定 `SBT_LIBRARY` 参数。

RMAN 检查存储库中的每个备份片，并在 MMDB 中查询该备份片的可用性。然后，RMAN 将备份片标记为已过期或可用，具体取决于介质可用性。请注意，在上面的示例中，RMAN 不会删除 MMDB 报告为已过期的备份片，而是将其标记为已过期。

要从恢复编目数据库中删除过期的备份对象，请使用 RMAN 执行以下命令:

```
delete expired backup;
```

提示建议在以下情况下执行同步:

- Data Protector 导入或导出具有 Oracle 对象的介质之后
- 只要对具有 Oracle 对象的介质的保护已过期。

满足 Oracle 服务器集成和备份的先决条件

以下是 Oracle Server 集成和备份的先决条件:

- 熟悉 Oracle 数据库管理和基本的 Data Protector 功能。
- 需要许可证才能使用 Data Protector Oracle 集成。
- 必须安装 Oracle Server 软件，并且必须打开或装载 Oracle 目标数据库。
- Microsoft Windows 上的 Oracle 数据库支持使用在安装时指定的 Oracle 主用户。此 Oracle 主用户用于为 Oracle 主目录运行 Windows 服务，类似于 Linux 上 Oracle 数据库的 Oracle 用户。

  对于备份和还原，如果 Oracle 集成代理和介质代理在同一 Windows 主机上运行，为了避免出现共享内存分配问题，应将 Oracle 主用户添加到 Windows 备份操作员组。

- 如果使用 Oracle 恢复编目数据库，请确保该数据库已正确配置并已打开。
- 必须为 Oracle 目标数据库和恢复编目 (如果使用) 正确配置并运行 Oracle 网络服务。
- 要成功备份驻留在闪回恢复区中的恢复文件，请确保已正确配置闪回恢复区。
- *Oracle Real Application Cluster (RAC):* 每个节点都必须具有一个用于存储存档日志的专用磁盘。此类磁盘必须由 NFS 装载在所有其他 RAC 节点上。

  但是，如果存档日志不在由 NFS 装载的磁盘上，则必须修改存档日志备份规范。
- *RAC :* 对于 Oracle 11.2.0.2 及更高版本，必须在共享磁盘上创建控制文件，并且可以从所有 RAC 节点访问该文件， OB2_DPMCTL_SHRLOC 环境变量必须指向这一备份控制文件的位置。
- 在 Windows 系统上，使用 Oracle 备份集 ZDB 方法时，将备份系统上的 omnirc 选项 ZDB_SMISA_AUTOMOUNTING 设置为 2 ，以便能够在本地系统上自动装载卷。
- 配置要与 Data Protector 配合使用的设备和介质。
- 测试 Oracle Server 系统和 Cell Manager 是否正常通信: 在 Oracle Server 系统上配置并运行 Data Protector 文件系统备份和还原。
- 确定 Data Protector 将用于备份的 Oracle 数据库“用户”。此用户必须获得 SYSDBA 特权。例如，它可以是在数据库创建期间创建的 Oracle 用户 sys 。必须已向用户授予 SYSBACKUP 权限。此外，您还可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。
- 在 Windows 系统上，如果 Oracle 目标数据库和 Oracle 恢复编目安装在两个不同的系统上，请在两个系统上均配置一个属于 Administrators 组成员的“域”用户帐户。

  对于受支持的 Windows 操作系统，请使用用户模拟。
- 必须在要还原或复制数据库的系统上创建 Oracle 实例。
- 如果要还原整个数据库，则数据库必须处于 Mount 状态；如果要还原控制文件或执行数据库复制，则数据库必须处于 NoMount 状态。
- 必须能够连接到数据库。
- 必须备份包含已存档日志的整个主数据库。
- 存档日志 (自上次完整备份以来尚未备份到磁带并且在复制时必须提供的日志) 必须在复制系统上可用，且其路径名与目标系统 (具有要复制的生产数据库的系统) 相同。
- 必须配置辅助实例的网络服务名称。
- 在目标数据库所在的同一系统上复制数据库时，请设置所有 *_
- ATH 、 *_DEST 、 DB_FILE_NAME_CONVERT 和 LOG_FILE_NAME_CONVERT 初始化参数。这样，重复的数据库文件便不会覆盖目标数据库文件。
- 要创建 Oracle 源端重复数据删除或备份所需的 SHM 段，运行该进程的用户必须属于以下至少一个组。
  - 进程用户安全标识符 (SID)
  - 本地管理员组
  - 本地备份操作员组

  为上述用户组的所有共享内存 (SHM) 段提供了访问控制列表 (ACL)。

满足还原的先决条件

在开始还原 Oracle 数据库之前，必须满足以下要求:

- 如果使用恢复编目数据库，请确保已打开恢复编目数据库。如果无法使恢复编目数据库联机，则可能需要还原恢复编目数据库。
- 必须有控制文件。如果没有控制文件，则必须将其还原。

  如果必须对恢复编目数据库或控制文件执行还原，则必须首先执行此还原。只有这样，您才能对 Oracle 数据库的其他部分执行还原。

  如果确定恢复编目数据库或控制文件已准备就绪，请启动恢复编目数据库。
- 确保设置了以下环境变量:
  - ORACLE_BASE
  - ORACLE_HOME
  - ORACLE_TERM
  - PATH
  - NLS_LANG
  - NLS_DATE_FORMAT

  Windows 系统示例

  ORACLE_BASE=Oracle_home

  ORACLE_HOME=Oracle_home\product\10.1.0

  ORACLE_TERM=HP

  PATH=$PATH:Oracle_home\product\10.1.0\bin

  NLS_LANG=american

NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'

UNIX 系统示例

ORACLE_BASE=/opt/oracle

ORACLE_HOME=/opt/oracle/product/10.1.0

ORACLE_TERM=HP

PATH=$PATH:/opt/oracle/product/10.1.0/bin

NLS_LANG=american

NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'

- 检查 /etc/oratab 文件是否包含以下行:

  Windows 系统： PROD:Oracle_home\product\10.1.0:N

  UNIX 系统： PROD:/opt/oracle/product/10.1.0:N

  最后一个字母用于确定启动时数据库是 (Y) 否 (N) 自动启动。

- 确保 Oracle 用户具有文件 /u01/app/gridhome/log/diag/asmcmd/user_oracle/<hostname>/alert/alert.log 的写访问权限。

限制

以下限制适用：

- 不支持 MAXPIECESIZE RMAN 参数选项，因为无法使用 Data Protector Oracle 集成还原备份期间创建的多个备份片。
- Data Protector Oracle 集成不支持通过 RMAN 磁盘备份将目标数据库备份到闪回恢复区。Data Protector Oracle 集成仅支持从闪回恢复区备份到备份设备。但是，您可以创建 RMAN 脚本，设置在 Data Protector 将闪回恢复区中的文件备份到备份设备之前或之后将目标数据库备份到闪回恢复区。创建备份规范时，可以使用 Pre-exec 或 Post-exec 选项设置脚本。
- 所有数据库的 Oracle 数据库标识符 (DBID) 在 Data Protector 单元中必须唯一。
- 在 Oracle Database 10g 版本 2 中，对于 HP-UX 系统，安装 Oracle 数据库的主机名长度将限定为 8 个字符。
- 当备份或还原 PDB 且未通过 CDB 连接时，以下限制适用:
  - 无法备份 ARCHIVELOGS 和控制文件。
  - 仅可使用正常还原模式执行 PDB 时间点。
  - PDB 并行性时间点设置为 1 且无法增加。
  - 对整个 CDB 执行时间点恢复时，需要手动打开所有 PDB。
  - 仅当打开 CDB 的所有 PDB 时，才能在 ZDB 环境中对该 CDB 进行联机备份。
  - 必须将 Windows Oracle 主用户添加到 Windows Administrators 组，以便成功执行 PDB 时间点恢复。
- Oracle Data Guard 限制:
  - 不能只配置备用数据库 (不配置主数据库)。
  - 仅支持备用数据库物理备份。
  - 备用配置需要恢复编目数据库。
  - 有关在 Oracle Data Guard 环境中执行 RMAN 备份、还原、恢复和复制的其他限制，请参阅 Oracle 文档。
- Oracle 操作系统身份验证限制: 在以下情况下，不支持执行 Oracle 操作系统身份验证:
  - Oracle ZDB 配置。
  - Oracle 恢复编目配置。
  - Oracle Data Guard 数据库配置。
- Data Protector Oracle 集成不支持在备份规范名称中使用非 ASCII 字符。
- 如果存在不受 Oracle 支持的特殊字符或密码中包含空格，Oracle 集成将失败。在 Oracle 支持的特殊字符中，部分字符因 Oracle 错误而不起作用: 空格不起作用，切勿使用三种组合 (分号和脱字号、分号和 @ 符号、分号和斜杠)。下面是在密码中使用特殊字符的两个要素:
  - 只能使用 Oracle 支持的特殊字符。
  - 不应使用任何空格或上面列出的三个组合中的任何一个。
- 在 Oracle 备份规范中使用 RMAN 脚本时，不能使用双引号 (")，必须改用单引号 (')。
- Data Protector 不会检查要还原的数据库对象是否已备份，Data Protector 内部数据库中是否存在这些对象。即可启动还原过程。
- 将表空间还原到时间点时，必须使用 RMAN 界面。
- 要恢复 Oracle 恢复编目数据库，只能使用 Oracle Restore GUI 和 Oracle RMAN。
- 使用 Data Protector GUI 将数据库还原到除该数据库原始驻留的客户机系统以外的其他客户机系统时，在新客户机系统上选择的实例名称必须与原始实例名称相同。
- 在 Windows 平台上，即使备份完成似乎没有报告任何问题，如果数据库位于原始磁盘上，也不能备份 Oracle 数据库的代理副本。
- 如果从 RMAN 恢复编目数据库删除对象，这些更改不会自动植入 IDB，反之亦然。
- 您不能使用 Data Protector GUI 配置其文件由自动存储管理 (ASM) 进行管理、且以下任一 ASM 属性与其默认值不同的 Oracle 数据库：ASM 实例的主目录、Data Protector Oracle 集成代理连接到 ASM 实例所使用的身份验证模式。

安装 Oracle Server 客户机

This feature is available in the Premium Edition

假设 Oracle Server 已启动并正在运行。为了能够备份 Oracle 数据库，您需要在安装过程中选择“Oracle 集成”组件。

OpenVMS

在 OpenVMS 上，在安装并配置 Oracle 集成之后，验证 OMNI$ROOT:[CONFIG.CLIENT]omni_info 中是否存在 -key Oracle8 条目，例如：-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath “” -uxpath “” -version 10.30

如果不存在该条目，请从 OMNI$ROOT:[CONFIG.CLIENT]omni_format 复制它。否则，Oracle 集成在 OpenVMS 客户机上不会显示为已安装。

配置 Oracle Server 集成

This feature is available in the Premium Edition

群集感知系统

在群集环境中，如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称。按如下方式在 Oracle Server 系统上设置该变量:

Windows 系统： set OB2BARHOSTNAME=virtual_server_name

UNIX 系统： export OB2BARHOSTNAME=virtual_server_name

*RAC：*在要运行备份和还原的每个节点上配置 Oracle 数据库。

使用 RAC 的 HP-UX: 如果要使用虚拟主机名，请创建一个“仅”包含虚拟 IP 和虚拟主机名参数的 Serviceguard 包，并在 RAC 节点之间分发此包。

将 Oracle Server 与 Data Protector MML 链接在一起

要使用 Data Protector Oracle 集成，需要在运行 Oracle 实例的每个系统上将 Oracle Server 软件与 Data Protector Oracle 集成“介质管理库”(MML) 链接在一起。

无需手动将 Oracle Server 与 Data Protector MML 链接在一起。使用 Data Protector GUI 或 CLI 启动备份或还原时，Data Protector 会自动将 Oracle Server 与特定于平台的相应 Data Protector MML 链接在一起。但是，出于测试目的，可以覆盖此自动选择。可以通过设置 Data Protector SBT_LIBRARY 参数来手动指定应使用哪个特定于平台的 Data Protector MML。

当 Oracle Server 需要使用 Data Protector 在设备中写入或读取数据时，它会调用 MML。

Oracle CDB 和 PDB 模式支持

为了备份和还原数据，在 Oracle 12c 中引入了一项名为可插拔数据库 (PDB) 的新功能。PDB 是体系结构、体系结构对象和非体系结构对象的可移植集合，以非容器数据库 (非 CDB) 的形式向 Oracle Net 客户机显示。CDB 包括零个、一个或多个客户创建的可插拔数据库 (PDB)。在 Oracle 12c 及更高版本中，PDB 位于容器数据库 (CDB) 下。

每个 CDB 都具有以下容器:

- 恰好一个“根”

  根用于存储 Oracle 提供的元数据和常用用户。Oracle 提供的 PL/SQL 包的源代码就是元数据的一个示例。常用用户是每个容器中已知的数据库用户。根容器名为 CDB$ROOT。

- 恰好一个“种子 PDB”

  种子 PDB 是系统提供的一个模板，CDB 使用该模板来创建新的 PDB。种子 PDB 名为 PDB$SEED。无法在 PDB$SEED 中添加或修改对象。

- **零个或多个用户创建的 PDB**

  PDB 是用户创建的实体，其中包含特定功能集所需的数据和代码。例如，PDB 可以支持特定应用程序，例如人力资源或销售应用程序。

备份存档和还原 (BAR) GUI 将列出容器数据库中的所有 PDB，应启用仅选择一个或选择多个可插拔数据库。

以下是还原方案:

- 同时还原 CDB 和 PDB
- 还原 CDB，但不还原 PDB
- 还原一个 PDB 和一个测试数据库

配置 Oracle 用户帐户

确定要用于运行备份的用户帐户。Data Protector 需要以下用户帐户:

- Oracle 操作系统用户帐户
- Oracle 数据库用户帐户

配置 Oracle 操作系统用户帐户

对于每个 Oracle 数据库，Data Protector 都需要一个具有 Oracle 权限的操作系统用户帐户才能备份数据库。此用户帐户通常属于 DBA 用户组 (“OSDBA 用户”)。用于运行 Oracle 数据库的用户帐户具有这些权限。例如，要在 UNIX 系统上查找此类用户，请执行以下命令:

ps -ef|grep ora_pmon_ *DB_NAME*

或

ps -ef|grep ora_lgwr_ *DB_NAME*

下表说明如何在不同的操作系统上配置用户:

客户机系统	描述
UNIX 系统	确保已将 Oracle Inventory 组（oinstall）中的 Oracle 用户 oracle 添加到 Data Protector admin 用户组。 将 OSDBA 用户帐户添加到 Data Protector admin 或 operator 用户组。 **注意**如果计划使用 omniintconfig.pl 命令配置 Oracle 数据库，请注意，指定的 OSDBA 用户帐户会自动添加到 Data Protector admin 用户组。
Windows 系统	在 Windows 系统上，Data Protector 使用相关系统上的 Data Protector Inet 服务连接到 Oracle 数据库。默认情况下，该服务在 Local System account“本地系统帐户”下运行，该帐户会自动添加到 Data Protector admin 用户组。但是，如果已在一个 OSDBA 用户帐户下重新启动 Data Protector Inet 服务，则需要将该新用户添加到 Data Protector admin 或 operator 用户组。

在群集环境中，确保将以下用户添加到 Data Protector admin 或 operator 用户组:

- 适用于所有物理节点的 OSDBA 用户
- 适用于虚拟服务器的 OSDBA 用户 (适用于 Serviceguard 群集)

配置 Oracle 数据库用户帐户

标识或创建以下 Oracle 数据库用户帐户。需要在配置 Oracle 数据库时提供这些用户帐户，如配置 Oracle 数据库中所述。

Oracle 数据库用户帐户

用户	描述
主数据库用户	如果已经为 CDB 和 PDB 配置了数据库，则需要登录到主数据库或 CDB。 为了成功进行配置，您应该能够作为 Oracle OS 用户使用命令 *sqlplus user @ TNSNAME as sysbackup* 登录到目标数据库。 对于 CDB 配置，允许普通用户 (例如 c##user) 连接到代表 CDB 而不是 PDB 的 TNSNAME。在这种情况下，该命令为 *sqlplus c##user@CDBTNSNAME as sysbackup*。
恢复编目用户	恢复编目的所有者 (例如， rman)。登录编目数据库时需要。使用恢复编目时需要。 确保 Oracle 恢复编目的所有者: • 被授予 CREATE ANY DIRECTORY 和 DROP ANY DIRECTORY 系统特权，使用数据抽取导出 (expdp) 和数据抽取导入 (impdp) 实用程序需要这些特权。 • 对 sys.v$instance 视图拥有 SELECT 权限。启动 SQL*Plus 并键入: grant select on v_$instance to recovery_catalog_user; • 被授予 EXEMPT ACCESS POLICY 权限
备用数据库用户	登录备用数据库时需要。仅适用于 Oracle Data Guard 环境。备份备用数据库时需要。

配置 Oracle 用户数据库

在配置 Oracle 数据库时，需要为 Data Protector 提供以下数据:

- Oracle Server 主目录
- 目标数据库的登录信息
- (可选) 恢复编目数据库的登录信息
- (可选) 备用数据库的登录信息

在配置期间， util_oracle8.pl 命令 (在 Oracle 服务器系统上启动) 将指定参数保存在 Cell Manager 上特定于 Data Protector Oracle 数据库的配置文件中。如果已创建恢复编目并且尚未在恢复编目数据库中注册 Oracle 目标数据库，则在配置期间会发生上述情况。有关 Oracle 数据库结构的信息将从 Oracle 数据库的控制文件传输到恢复编目。确保在配置过程中数据库已打开，并且您可以连接到该数据库。要配置 Oracle 数据库，可使用 Data Protector GUI 或 Data Protector CLI。

提示在具有多个 Oracle 数据库的大型环境中，请考虑使用同时配置多个 Oracle 数据库中描述的配置过程。但请注意，上述过程不能用于配置备用数据库。

备份 Oracle Server 集成

This feature is available in the Premium Edition

要配置 Oracle 备份，请执行以下步骤:

1. 配置计划用于备份的设备。
2. 配置介质池和用于备份的介质。
3. 确保您能够连接到数据库。
4. 创建 Data Protector Oracle 备份规范。

设置环境变量

使用环境变量修改备份环境以满足您的需求。环境变量特定于 Oracle 数据库。这意味着，可以针对不同的 Oracle 数据库设置不同的环境变量。指定这些变量后，它们将保存到相关的 Data Protector Oracle 数据库配置文件中。

环境变量

环境变量	默认值	描述
OB2_RMAN_COMMAND_TIMEOUT	300 s	此变量适用于 Data Protector 尝试连接到目标或编目数据库的情况。它指定 Data Protector 等待 RMAN 响应连接成功的时间 (以秒为单位)。如果 RMAN 在指定时间内没有响应，Data Protector 将中止当前会话。
OB2_SQLP_SCRIPT_TIMEOUT	300 s	此变量适用于 Data Protector 发出 SQL*Plus 查询的情况。它指定 Data Protector 等待 SQL*Plus 响应查询成功完成的时间。如果 SQL*Plus 在指定时间内没有响应，Data Protector 将中止当前会话。
OB2_DPMCTL_SHRLOC	N/A	定义控制文件的创建位置以及在 Data Protector 托管控制文件备份中备份该文件的位置。Data Protector 将控制文件复制到其临时文件目录。此变量将使用客户指定的目录覆盖默认目录。在安装了 Oracle 版本 11.2.0.2 或更高版本的 Oracle Real Application Clusters (RAC) 环境中，要启用 Data Protector 托管控制文件备份和相应的还原会话，请确保此目录位于所有 RAC 节点均可访问的共享磁盘上。

要设置环境变量，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

创建备份规范或修改现有备份规范时，可以设置一个变量:

1. 在备份规范的“源”页面中，右键单击顶部的 Oracle 数据库，然后单击“设置环境变量”。
2. 在“高级”对话框中，指定变量名称及其值，然后单击“添加”。
   单击**确定**。

使用 Data Protector CLI

必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。

设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

执行：

```
util_cmd –putopt Oracle8 DatabaseNameVariableValue –sublist Environment
```

示例

要将 Oracle 数据库 INST2 的环境变量 OB2_RMAN_COMMAND_TIMEOUT 设置为 100 秒，请执行以下命令:

```
util_cmd –putopt Oracle8 INST2 OB2_RMAN_COMMAND_TIMEOUT 100 –sublist Environment
```

创建新模板

您可以使用备份模板，以将同一组选项应用于许多备份规范。通过创建自己的模板，您可以完全按照自身要求指定选项。

这样，只需点击几下鼠标即可将所有选项应用于备份规范，而无需反复指定所有选项。此为可选任务，因为您也可以使用默认模板之一。

当使用模板创建 Oracle 备份时，模板中的分配通道语句只有一个条目。您可以根据开始时计算的动态值来编辑它，并将该条目添加到模板开头。您不能事先在模板中指定通道数和相应的条目，因为这些值在创建模板时不可用。

要创建新的备份模板，请继续执行以下步骤:

1. 在 Data Protector Manager 中，切换到“备份”上下文。
2. 在“范围窗格”中，依次展开“备份”和“模板”，然后右键单击 **Oracle Server**。
3. 单击“添加模板”。按照向导在模板中定义相应的备份选项。

创建备份规范

群集感知系统

在群集环境中执行脱机备份前，使 Oracle 数据库资源脱机，备份之后再将其重新联机。此操作可通过特定备份规范中适用于客户机系统的 Pre-exec 和 Post-exec 命令中的 Oracle fscmd 命令行界面命令或使用群集管理员来完成。

要创建 Oracle 备份规范，请执行以下操作:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Oracle Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，双击“空白 Oracle 备份”以在没有预定义选项的情况下创建备份规范，或者使用下面给出的一个预定义模板:

存档	备份存档重做日志。
Archive_Delete	备份存档重做日志，备份之后将其删除。
Whole_Online	备份数据库实例和存档重做日志。
Whole_Online_Delete	备份数据库实例和存档重做日志，然后删除存档重做日志。
Database_Archive	备份数据库实例和存档重做日志。
Database_Switch_Archive	备份数据库实例，切换联机重做日志并备份存档重做日志。
Database_Switch_ArchiveDel	备份数据库实例，切换联机重做日志并备份存档重做日志，然后删除存档重做日志。
Direct_Database	备份数据库实例和控制文件。
SMB_Proxy_Database	使用代理复制方法在 ZDB (拆分镜像或快照) 模式下备份数据库实例和控制文件。
SMB_BackupSet_Database	使用备份集方法在 ZDB (拆分镜像或快照) 模式下备份数据库实例和控制文件。

单击**确定**。

4. 在“客户机”中，选择 Data Protector Oracle 集成客户机。在群集环境中，选择虚拟服务器。

   RAC : 选择 Oracle 资源组的虚拟服务器。

   Oracle Data Guard : 选择主系统或辅助 (备用) 系统。

   在“应用程序数据库”中，键入要备份的数据库的名称。

   数据库名称可通过 SQL*Plus 来获取:

   ```
   SQL>select name from v$database;
   ```

   > **注意**在单实例配置中，数据库名称通常与其实例名称相同。在这种情况下，也可以使用实例名称。实例名称可按如下方式获取:
   >
   > ```
   > SQL>select instance_name from v$instance;
   > ```

   指定在 UNIX 和 Windows 系统上可用的“用户和组/域”选项，如下所示:

   - *UNIX 系统 :* 在“用户名”和“组/域名”中，指定要用于启动备份的 OSDBA 用户帐户 (例如，用户名 ora、组 DBA)。必须按照配置 Oracle 用户帐户中所述配置此用户。
   - *Windows 系统 :* 不必指定这些选项，而如果不指定，则以 Local System 帐户运行备份。

     在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator、域 DP)。必须设置此用户才

能模拟 Data Protector Inet 服务用户。

请确保此用户已加入 Data Protector admin 或 operator 用户组，并且具有 Oracle 数据库备份权限。此用户成为备份所有者。

> **注意**如果这不是您的第一个备份规范，Data Protector 会为您填写“用户名”和“组/域名”，并提供上次配置的 Oracle 数据库的值。

单击“下一步”。

> **注意**单击“下一步”时，Data Protector 将执行配置检查。
>
> *UNIX 系统：*以指定的 OSDBA 用户帐户启动检查。如果检查成功完成，则 OSDBA 用户和组也将保存在 Oracle 数据库特定配置文件和 Oracle 系统全局配置文件中，并覆盖以前的值 (如果存在)。
>
> 您必须为要针对其使用操作系统身份验证的用户输入用户名和组名。

5. 如果尚未将 Oracle 数据库配置为与 Data Protector 一起使用，则会显示“配置 Oracle”对话框。将 Oracle 数据库配置为与 Data Protector 一起使用，如配置 Oracle 数据库中所述
6. 选择要备份的 Oracle 数据库对象。

   例如，可以单独选择单个表空间进行备份，但是对于数据库完整联机备份，还必须选择“ARCHIVELOGS”。

   存档的日志可以驻留在闪回恢复区中。在这种情况下，如果选择要备份的“闪回恢复区”，则无需再选择“ARCHIVELOGS”。

   *Oracle Data Guard：*如果用备用连接配置数据库，则您可以备份备用数据库的控制文件，该文件可在还原备用数据库时使用。

   > **注意**由于临时表空间不包含永久数据库对象，因此 RMAN 和 Data Protector 不会备份它们。

   > **注意**如果数据库使用恢复编目，则默认在每次数据库备份后备份该目录，除非备份规范中另有约定。

   单击“下一步”。
7. 选择要用于备份的设备。单击“属性”可以设置设备并发、介质池和预分配策略。有关这些选项的详细信息，请单击“帮助”。

   还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。

   单击**下一步**继续。
8. 设置备份选项。

   有关其他备份规范选项和常见应用程序选项的信息，请按 **F1**。

   *Oracle Data Guard：*要备份备用数据库，必须在“应用程序特定选项”对话框中选择“备份备用数据库”。

   > **提示**将数据从闪回恢复区备份到磁带时，您可以在“Pre-exec”或“Post-exec”文本框中指定用于备份到闪回恢复区的 RMAN 脚本的位置。该脚本将在 Data Protector Oracle 集成每次备份到磁带之前 (**Pre-exec**) 或之后 (**Post-exec**) 执行。

   单击“下一步”。
9. 单击“另存为”以保存备份规范，指定名称和备份规范组。建议将所有 Oracle 备份规范都保存在 **Oracle** 组中。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。

   注意，仅支持“完整”备份类型。

   > **重要说明**单词 DEFAULT 为保留字，不得用于备份规范名称或任何类型的标签。因此，请勿在备份规范名称中使用标点符

> 号，因为 Oracle 通道格式从备份规范名称创建而来。

单击**确定**。

要开始备份，请参阅启动备份会话。

10. 可以在“备份”上下文中的指定备份规范组下检查最近创建和保存的备份规范。备份规范存储在 Cell Manager 上的以下文件中:

    Windows 系统： Data_Protector_program_data\Config\server\Barlists\Oracle8\ Backup_Specification_Name

    UNIX 系统： /etc/opt/omni/server/barlists/oracle8/Backup_Spec_Name

11. 建议测试备份规范。

Oracle 备份选项

禁用恢复编目自动备份	默认情况下，Data Protector 会在每个备份会话中备份恢复编目。选择此选项可禁用恢复编目的备份。
禁用 Data Protector 管理的控制文件备份	默认情况下，Data Protector 会在每个备份会话中备份 Data Protector 托管控制文件。选择此选项可禁用 Data Protector 托管控制文件的备份。
备份备用数据库	*Oracle Data Guard：*此选项适用于用备用连接配置数据库的情况。默认情况下，RMAN 备份主系统上的数据库文件和归档重做日志。选择此选项可允许在备用系统上备份数据库文件和存档日志。但是，只能在备用站点上备份配置了备用数据库之后创建的存档日志。必须在主数据库上备份配置备用数据库之前创建的存档日志。 请注意，仍将从主系统中备份当前的控制文件或用于备用的控制文件。
RMAN 脚本	您可以编辑 Data Protector Oracle 备份规范的 Oracle RMAN 脚本部分。该脚本由 Data Protector 在创建备份规范期间创建，用于反映备份规范的选择和设置。仅在保存备份规范后才能编辑该脚本。
pre-exec、post-exec	指定在备份之前（pre-exec）或之后（post-exec）将由 Oracle Server 系统中的 ob2rman.pl 启动的命令或 RMAN 脚本。RMAN 脚本的扩展名必须为 .rman。不要使用双引号。 例如，您可以提供脚本来关闭和启动 Oracle 实例。 提供命令或 RMAN 脚本的路径名。

UNIX 系统上的 pre-exec 和 post-exec 脚本示例

Pre-exec 示例

以下是关闭 Oracle 实例的脚本示例:

```
#!/bin/sh export ORACLE_HOME=$2 export ORACLE_SQLNET_NAME=$1 if [ -f $ORACLE_HOME/bin/sqlplus ]; then $ORACLE_HOME/bin/sqlplus << EOF connect sys/manager@$ORACLE_SQLNET_NAME as sysdba shutdown EOF echo "Oracle database \"$DB_NAME\" shut down." exit 0 else echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)." exit 1 fi
```

Post-exec 示例

以下是启动 Oracle 实例的脚本示例:

```
#!/bin/sh export ORACLE_HOME=$2 export ORACLE_SQLNET_NAME=$1 if [ -f $ORACLE_HOME/bin/sqlplus ]; then $ORACLE_HOME/bin/sqlplus << EOF connect sys/manager@$ORACLE_SQLNET_NAME as sysdba startup EOF echo "Oracle database \"$DB_NAME\" started." exit 0 else echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)." exit 1 fi
```

编辑 Oracle RMAN 脚本

启动 Data Protector 备份规范来备份 Oracle 对象时，会用到 RMAN 脚本。

在保存备份规范或通过单击“编辑”按钮手动编辑备份规范之前，RMAN 脚本部分不会写入至备份规范。

仅在保存 Data Protector Oracle 备份规范后，才能编辑 RMAN 脚本部分。

要编辑 Oracle RMAN 脚本，请单击“应用程序特定选项”窗口中的“编辑”，编辑脚本，然后单击“保存”以保存对脚本的更改。

Data Protector RMAN 脚本结构

Data Protector 创建的 RMAN 脚本包含以下部分:

- “Oracle 通道分配”以及每个已分配通道的 Oracle 环境参数的定义。

  分配的通道数与选定用于备份的所有设备的并发数之和相同。

  > **注意**保存备份规范后，更改并发数不会更改 RMAN 脚本中已分配通道的数量。该数量必须通过编辑 RMAN 脚本手动更改。

  > **重要说明**在 Windows 系统上，最多可以分配 32 或 64 个 (如果设备在本地) 通道。如果计算得出的数量超过此限制，则必须手动编辑 RMAN 脚本并减少分配的通道数。

  通过编辑 RMAN 脚本手动定义 Oracle 通道时，必须按以下格式添加环境参数:

  ```
  parms 'ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME, OB2BARLIST=Backup_Specification_Name)';
  ```

- 用于备份整个数据库实例的 RMAN 备份语句和/或用于备份表空间、数据文件或闪回恢复区的任何 RMAN 命令组合，具体视选定的备份对象而定。 `backup` 语句由以下部分组成:
  - 采用以下格式的备份文件的 Oracle 格式:

    ```
    format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' database;
    ```

    > **注意**通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合均可添加到不可缺少的 `%s:%t:%p` 替代变量和 `DB_NAME` 中。

  - RMAN `datafile tablespace_name*datafile_name` 命令。
- 用于备份 Oracle 存档日志的 RMAN 备份语句 (如果选择存档重做日志进行备份)。

  用于在备份存档重做日志之前切换联机重做日志的 RMAN sql 语句 (如果选择了相应模板或手动添加了语句):

  ```
  sql 'alter system archive log current';
  ```

  `backup` 语句由以下部分组成:
  - 采用以下格式的备份文件的 Oracle 格式:

    ```
    format 'Backup_Specification_NameDB_NAME_%s:%t:%p>.dbf'
    ```

    > **注意**通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合均可添加到不可缺少的 `%s:%t:%p` 替代变量和 `DB_NAME` 中。

  - RMAN `archivelog all` 命令。

  用于在备份存档重做日志之后删除这些日志的 RMAN 语句 (如果选择了相应模板或手动添加了语句):

  ```
  archivelog all delete input ;
  ```

- 用于备份 Oracle 控制文件的 RMAN 备份语句 (如果选择控制文件进行备份)。 `backup` 语句由以下部分组成:
  - 采用以下格式的备份文件的 Oracle 格式:

    ```
    format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' current controlfile;
    ```

    > **注意**通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合均可添加到不可缺少的 `%s:%t:%p` 替代变量和 `DB_NAME` 中。

  - RMAN `current controlfile` 命令。

RMAN 脚本示例

以下示例显示的是选择整个数据库后 Data Protector 基于“空白 Oracle 备份” 模板创建的 RMAN 脚本部分:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DIPSI,OB2BARLIST=New1)'; allocate channel 'dev_1' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DIPSI,OB2BARLIST=New1)'; allocate channel 'dev_2' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DIPSI,OB2BARLIST=New1)'; backup incremental level <incr_level>format 'New1<DIPSI_%s:%t:%p>.dbf' database ; backup format 'New1<DIPSI_%s:%t:%p>.dbf' archivelog all; backup format 'New1<DIPSI_%s:%t:%p>.dbf' current controlfile ; }
```

要将 RMAN 连接到目标数据库，请执行以下脚本:

```
run { allocate channel 'dev_0' type 'sbt_tape'parms
```

```
'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll,
```

```
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DatabaseName,OB2BARLIST=BarListName)'; restore archivelog all; release channel 'dev_0'; }
```

创建已备份对象的副本

Oracle 双工模式

Oracle 支持双工模式，这样您便可以将每个已备份对象的副本创建到单独的备份设备。要启用双工功能，请执行以下步骤:

1. 在任何分配通道命令之前，将以下命令添加到 RMAN 脚本中:

   set duplex=< on | 2 | ... >

   > **重要说明**如果使用多个已分配通道，则某些原始对象和复制对象可能会备份到同一介质。为了防止出现这种情况，在使用双工模式备份时，应仅使用一个已分配通道。

2. 将以下参数添加到用于备份的每个格式字符串:

   %c

3. 将用于备份的每个设备的并发性设置为 1。
4. 根据以下公式设置 MIN 和 MAX 负载均衡参数:

   (number of duplex copies)*(number of allocated channels)

   示例

   如果双工设置为 2 且以 1 个已分配通道运行备份，则 MIN 和 MAX 参数应设置为 2。

> **重要说明**如果将 MIN 和 MAX 负载均衡参数设置为较低的值，则备份会话将受阻。
>
> 如果将 MIN 和 MAX 负载均衡参数设置为较高的值，则可能会将原始对象和复制对象备份到同一介质。

测试集成

创建并保存备份规范后，应对其进行测试，然后再运行备份。该测试验证集成的两个部分: Oracle 端和 Data Protector 端。此外，还会对配置进行测试。

该过程包括检查集成的 Oracle 和 Data Protector 部分，以确保 Oracle 与 Data Protector 之间建立通信、数据传输正常且事务记录在恢复编目 (如果使用) 或控制文件中。

测试备份的详细信息 (如介质保护、备份用户和备份状态) 注册于 Data Protector 数据库和 Oracle 控制文件中。将测试备份规范的“保护”选项设置为“无”。

使用 Data Protector GUI 进行测试

按照以下过程测试 Oracle 备份规范的备份:

1. 在 **Data Protector Manager** 中，切换到“备份”上下文。
2. 在“范围窗格”中，依次展开“备份”和“备份规范”。展开“Oracle Server”，然后右键单击要预览的备份规范。
3. 单击“预览备份”。

使用 CLI 进行测试

如果系统上安装了 Data Protector 用户界面，则可以从 Oracle Server 系统上的命令行或同一 Data Protector 单元内的任何 Data Protector 客户机系统执行测试。

使用 -test_bar 选项执行 omnib 命令，如下所示:

Windows 系统： Data_Protector_home\bin\omnib -oracle8_list backup_specification_name -test_bar

HP-UX、Solaris 和 Linux 系统： /opt/omni/bin/omnib -oracle8_list bimbackup_specification_name -test_bar

其他 UNIX 系统： /usr/omni/bin/omnib -oracle8_list backup_specification_name -test_bar

ob2rman.pl 命令即会启动，进而启动 BACKUP VALIDATE DATABASE RMAN 命令。

启动备份会话

数据库备份策略有两种: 脱机或一致数据库备份以及联机或不一致数据库备份。后者也称为热备份，需要特别注意的是通过联机备份达到一致状态。

确定使用哪个数据库备份策略取决于诸多因素。如果数据库必须始终打开并可用，则只能选择联机备份。如果您能够在某个特定时间使数据库脱机，则更可能选择定期脱机备份整个数据库，并通过联机备份动态更改的表空间来加以补充。

Oracle 脱机

数据库脱机备份是指备份数据文件和控制文件，这些文件在某个特定时间点是一致的。只有彻底关闭数据库，然后在关闭或装载数据库的情况下备份文件，才能实现此一致性。

如果已关闭数据库，则可以使用 Data Protector 文件系统备份规范执行 Oracle 目标数据库的脱机备份。在这种情况下，使用的是 Data Protector 磁盘代理。

如果已装载数据库，则可以使用 Data Protector Oracle 备份规范，Data Protector 将基于该规范自动生成并执行 RMAN 脚本。在这种情况下，使用的是 Data Protector Oracle 集成软件组件。

通常情况下，您会对整个数据库执行脱机备份，即备份必须包含所有数据文件和控制文件，参数文件则为可选项。

整个数据库脱机备份的执行过程如下:

1. 彻底关闭数据库。

   彻底关闭意味着不使用 ABORT 选项关闭数据库。
2. 如果使用 RMAN 备份数据库，请装载该数据库。
3. 备份所有数据文件、控制文件以及 (可选) 参数文件。
4. 在正常联机模式下再次启动数据库。

Oracle 联机

与脱机备份相反，联机备份在数据库打开时执行。

处于打开状态的数据库的备份不具有一致性，因为在备份前进过程中，数据库的一部分会被修改并写入磁盘。数据库的此类更改也会输入到联机重做日志中。在 ARCHIVELOG 模式下运行的数据库可以存档联机重做日志。万一需要还原，此功能对于在整个还原过程中使数据库处于一致状态至关重要。

使用联机备份时，必须执行以下操作才能使数据库处于一致状态:

1. 将 (不一致的) 数据库文件还原到磁盘。
2. 执行数据库恢复，这需要应用存档重做日志。此为 Oracle 操作。

可以使用 Oracle RMAN 实用程序或 Data Protector GUI 执行 Oracle 联机数据库备份。在后一种情况下，Data Protector 会根据在 Data

Protector GUI 中输入的数据自动创建并执行 RMAN 脚本。在 Oracle 联机备份期间，当备份表空间、数据文件、控制文件和存档重做日志时，Oracle 目标数据库处于打开状态。

数据库必须在 ARCHIVELOG 模式下运行，以便将当前联机重做日志存档到存档重做日志。

重要说明在运行 Oracle 联机备份之前，请确保数据库确实在 ARCHIVELOG 模式下运行。此操作可通过启动 SQL*Plus 并发出以下命令在 Oracle 服务器系统上完成:

```
archive log list;
```

如果 Oracle 目标数据库未在 ARCHIVELOG 模式下运行，请继续执行以下步骤:

使用 SPFILE 时:

1. 关闭数据库。
2. 装载数据库。
3. 启动 SQL*Plus 并键入:

   ```
   alter database archivelog;
   alter database open;
   alter system archive log start SCOPE=SPFILE;
   ```

使用 PFILE 时:

1. 关闭数据库。
2. 更改 PFILE 以启用日志存档，设置如下:

   ```
   log_archive_start = true
   ```
3. 装载数据库。
4. 启动 SQL*Plus 并键入:

   ```
   alter database archivelog;
   alter database open;
   ```

Oracle Data Guard : 备份存档日志后生成的存档日志必须手动编制编目，这样 RMAN 才能知悉这些日志，以便在将来出现下列情况下用其进行备份:

- 重新创建主控制文件或备用控制文件。必须为存档日志重新编制编目，因为 RMAN 使用控制文件来确定必须备份哪些存档日志。
- 故障转移后主数据库角色更改为备用。必须为存档日志重新编制编目，因为数据库角色的更改会重置已装载的控制文件的版本时间。

使用 RMAN 命令 CATALOG ARCHIVELOG 'archive_log_file_name'; 手动为存档重做日志编制编目。

现在已准备好使用下列任一方法运行 Oracle 数据库联机备份:

备份过程

使用 Data Protector 用户界面启动备份时会发生以下情况:

1. Data Protector 在客户机系统上执行 ob2rman.pl 。此命令会启动 RMAN 并将 Oracle RMAN 备份命令脚本发送至 RMAN 命令的标准输入。
2. Oracle RMAN 与 Oracle Server 通信，后者通过 MML 接口与 Data Protector 通信并启动备份。
3. 在备份会话期间，Oracle Server 从磁盘读取数据并将其发送至 Data Protector 以写入备份设备。

   来自 Data Protector 备份会话的消息和 Oracle 生成的消息将记录到 Data Protector 数据库中。

除非备份规范中另有约定，否则将在每次备份 Oracle 目标数据库后自动执行 Oracle 恢复编目的备份。使用标准 Oracle 导出实用程序时，Data Protector ob2rman.pl 先将 Oracle 恢复编目导出到一个文件，然后 Data Protector 会备份该文件。

从恢复编目中删除数据

使用恢复编目数据库备份 Oracle 数据库时，有关备份、还原和数据库恢复的所有信息都存储在恢复编目中。RMAN 在还原期间会用到这些信息。如果覆盖或格式化用于备份此数据的介质，Data Protector 将从 Data Protector 数据库导出对象。登录到 RMAN 后，您必须从恢复编目中手动删除数据。

计划备份会话

可以根据您的业务需求定制备份计划。如果必须使数据库持续保持联机状态，则应经常备份数据库，包括备份存档重做日志，将数据库恢复到特定时间点时需要这些日志。

例如，您可以决定执行每日备份，并在多个不同位置创建联机重做日志和存档重做日志的多个副本。

计划生产数据库备份的示例:

- 每周完整备份
- 每日增量备份
- 存档日志备份 (根据需要)

要计划 Oracle 备份规范，请继续执行以下步骤:

1. 在 Data Protector Manager 中，切换到“备份”上下文。
2. 在“范围窗格”中，依次展开“备份规范”和 **Oracle Server**。
3. 右键单击要计划的备份规范，然后单击“编辑计划”。“计划程序”页面随即打开。此备份规范的所有可用计划均列在右窗格中。
4. 单击要编辑的计划，然后单击“编辑”图标。计划向导随即打开。
5. 在“选项”页面查看选项，然后单击“下一步”。“重复”页面随即打开。

   请注意，备份类型可以是完全备份或增量备份，增量级别可以高达增量 4。
6. 设置“重复”模式，然后单击“下一步”。“摘要”页面随即打开。
7. 在“摘要”页面查看选项，然后单击“完成”。

运行交互备份

创建并保存备份规范后，可以随时执行交互备份。可以使用 Data Protector GUI 或 CLI。

使用 GUI 启动备份

要使用 Data Protector GUI 启动 Oracle 数据库交互备份，请继续执行以下步骤:

1. 在上下文列表中，单击“备份”上下文。
2. 在“范围窗格”中，依次展开“备份规范”和“Oracle Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 在“启动备份”对话框中，选择“备份类型”和选项。有关这些选项的信息，请单击“帮助”。

   请注意，备份类型可以是完全备份或增量备份，增量级别可以高达增量 4。

   单击**确定**。

使用 CLI 启动备份

1. 在 Oracle Server 上，切换到默认的 Data Protector 用户命令目录。
2. 执行：

   omnib -oracle8_list backup_specification_name [-barmode Oracle8Mode][list_options]

   可以在以下 list_options 中选择:

   -protect { none | weeks *n* | days *n* | until *date* | permanent }

   -load { low | medium | high }

   -crc

   -no_monitor

   Oracle8Mode = {-full | -incr1 | -incr2 | -incr3 | -incr4}

示例

要使用名为 RONA 的 Oracle 备份规范启动备份，请执行以下命令:

omnib -oracle8_list RONA

使用 RMAN 启动 Oracle 备份

要使用 RMAN 启动 Oracle 备份，必须创建 Oracle 备份规范。

要使用 RMAN 启动 Oracle 备份，请执行以下操作:

1. 连接到备份规范中指定的 Oracle 目标数据库:

   如果使用恢复编目，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target Target_Database_Login catalog Recovery_Catalog_Login

   UNIX 系统： ORACLE_HOME/bin/rman target Target_Database_Login catalog Recovery_Catalog_Login

   目标数据库登录

   目标数据库登录的格式为 user_name/password@service ，

   其中：

   user_name 是用户的名称，Oracle Server 和其他用户通过该名称了解该用户。每个用户名都与一个密码关联，同时输入两者才能连接 Oracle 目标数据库。必须已向此用户授予 Oracle SYSDBA 或 SYSOPER 权限。必须已向用户授予 SYSBACKUP 权限。您也可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。

   password 必须与 Oracle 密码文件中指定的密码 (orapwd) 相同，该文件用于对执行数据库管理的用户进行身份验证。

   service 是用于标识目标数据库的 SQL*Net 服务器进程的名称。

   恢复编目登录

   恢复编目数据库登录的格式为 user_name/password@service ，

   其中用户名和密码的描述与目标数据库的登录信息相同。请注意，此处指定的 Oracle 用户必须是 Oracle 恢复编目的所有者。

   service 是用于标识恢复编目数据库的 SQL*Net 服务器进程的名称。

2. 分配 Oracle 通道。

   分配通道将告知 RMAN 启动 Oracle Server 进程以在 Oracle 目标数据库上进行备份、还原或恢复。例如：

   allocate channel 'dev_0' type 'disk';

   或

   allocate channel 'dev_1' type 'sbt_tape';

   第一种情况指定的是直接备份到磁盘，第二种情况指定的是直接备份到磁带。

   要使用 Data Protector 备份介质，请指定通道类型 SBT_TAPE 。对于此通道类型，RMAN 需要 Data Protector MML:

   Windows 和 UNIX 系统: 通过设置 SBT_LIBRARY RMAN 脚本参数，在运行时指定 Data Protector MML 的路径。

   如果指定多个 allocate channel 命令，RMAN 将建立多个登录会话，而且会并行执行多个备份集。备份和还原命令的这种“并行化”由 RMAN 在内部处理。

   > **重要说明**在 Windows 系统上，最多可以分配 32 或 64 个 (如果设备在本地) 通道。

3. 指定 parms 操作数:

   可以使用 ENV parms 或 send channel 命令指定 Data Protector MML 的参数。

   对于 Windows 上的 Oracle，建议使用 send 命令，因为使用 ENV 可能存在线程安全问题。

   使用 ENV parms:

   parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME,OB2BARLIST=backup_specification_name)';

   使用 ENV 时，如果未采用此形式指定上述参数，RMAN 脚本将无法运行。

   本文档中的示例将使用 ENV parms。

   在脚本范围内使用 send 命令:

   ```
   parms 'SBT_LIBRARY=Path_to_Data_Protector_MML';
   ```

   ```
   send device type 'sbt_tape' 'OB2BARTYPE=Oracle8';
   ```

```
send device type 'sbt_tape' 'OB2BAPPNAME=DB_NAME';
```

```
send device type 'sbt_tape' 'OB2BARLIST=backup_specification_name';
```

按通道使用 send 命令 ('send channel' 命令应用于每个已分配

通道):

```
parms 'SBT_LIBRARY=Path_to_Data_Protector_MML';
```

```
send channel '<channel_name> 'OB2BARTYPE=Oracle8';
```

```
send channel '<channel_name>' 'OB2APPNAME=DB_NAME';
```

```
send channel '<channel_name> 'OB2BARLIST=backup_specification_name';
```

不同平台上的 MML 文件名

平台	32 位	64 位
HP-UX	libob2oracle8.sl	libob2oracle8_64bit.sl
HP-UX (Itanium)	libob2oracle8.so	libob2oracle8_64bit.so
Solaris	libob2oracle8.so	libob2oracle8_64bit.so
AIX	libob2oracle8.a	libob2oracle8_64bit.a
其他 UNIX 系统	libob2oracle8.so	libob2oracle8_64bit.so
Windows	orasbt.dll	orasbt.dll

例如，在 32 位 Solaris 系统上，设置
SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so 。

4. 指定 format：

   format 'backup_specification<DB_NAME_%s:%t:%p>.dbf'

   请注意， %s:%t:%p 和 Oracle 数据库名称为必填项，而备份规范为建议填写项。

   例如，如果您已创建并保存名为 bspec1 的备份规范，用于备份由名为 inst1 的 Oracle 实例标识的 Oracle 数据库，则应输入以下字符串:

   format 'bspec1< inst1_%s:%t:%p>.dbf'

   Oracle 通道格式指定用于备份的 Oracle 备份规范。

5. (可选) 指定 backup incremental level 。

   请注意，Data Protector 完整备份与 Oracle RMAN 脚本中的增量级别 0 备份类型执行相同的操作。两者都备份曾经用过的所有块。

   如果要使用此备份作为后续增量备份的基础，则需要此选项。

要使用 RMAN 运行备份，请通过从 ORACLE_HOME 目录执行以下命令来启动 RMAN (如果使用恢复编目):

Windows 系统： bin\rman target Target_Database_Login catalog Recovery_Catalog_Login

UNIX 系统： bin/rman target Target_Database_Login catalog Recovery_Catalog_Login

RMAN 脚本示例

必须从 RMAN> 提示符执行的 RMAN 脚本的一些示例如下:

> **注意**在以下示例中， SBT_LIBRARY 参数设置为 /opt/omni/lib/libob2oracle8.so ，对于 32 位 Solaris 系统，此为正确路径。

备份单个通道

要使用名为 ora1 的备份规范来备份 Oracle 实例 ORACL，请输入以下命令序列:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; backup incremental level 0 format 'oracl1<ORACL_%s:%t>.dbf' database; }
```

并行备份三个通道

通过对同一备份规范使用三个并行通道来备份数据库的 RMAN 备份脚本如下所示:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
backup incremental level 0 format 'ora1<ORACL_%s:%t>.dbf' database; }
```

备份所有存档日志和表空间

如果要使用三个并行通道和名为 ora1 的备份规范来备份存档重做日志以及之前数据库的表空间 SYSTEM 和 RONA，RMAN 脚本应如下所示:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
backup incremental level 0 format 'ora1<ORACL_%s:%t>.dbf' tablespace SYSTEM, RONA sql 'alter system archive log current' format
'ora1<ORACL_%s:%f:%p>.dbf' archivelog all; }
```

备份特定的存档日志

要备份从序列 5 到序列 105 的所有存档重做日志，并在备份名为 ora1 的实例之后删除存档重做日志，请执行以下脚本:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
backup (archivelog sequence between 5 and 105 delete input format 'ora1<ORACL_%s:%t:%p>.dbf'); }
```

如果备份失败，则不会删除日志。

备份闪回恢复区

如果要使用三个并行通道和名为 ora1 的备份规范来备份闪回恢复区，RMAN 脚本应如下所示:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
backup format 'ora1<ORACL_%s:%t>.dbf' recovery area; }
```

在备份规范中包含控制文件

备份系统表空间的第一个数据文件时，将自动备份当前控制文件。当前控制文件也可以显式包含在备份中或单独备份。要在备份名为 COSTS，的表空间后包含当前控制文件，请执行以下脚本:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
backup format 'ora1<ORACL_%s:%t>.dbf' (tablespace COSTS current controlfile); }
```

允许某些块损坏时的备份

set maxcorrupt 命令确定在特定备份失败之前 RMAN 可以容忍的每个数据文件的块损坏数量。

如果名为 ora1 的备份规范用于备份数据库，并允许每个数据文件 /oracle/data1.dbs（UNIX 系统）或 C:\oracle\data1.dbs（Windows 系统）最多有 10 个块损坏，则相应的 RMAN 脚本将为:

在 UNIX 系统上

```
run { set maxcorrupt for datafile '/oracle/data1.dbs' to 10; allocate channel 'dev_0' type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1'
type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
allocate channel 'dev_2' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; backup incremental level 0 format 'ora1<ORACL_%s:%t>.dbf' database; }
```

在 Windows 系统上

```
run { set maxcorrupt for datafile 'C:\oracle\data1.dbs' to 10; allocate channel 'dev_0' type 'sbt_tape' parms
'SBT_LIBRARY=Oracle_home\bin\orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; allocate channel 'dev_1'
type 'sbt_tape' parms 'SBT_LIBRARY=Oracle_home\bin\orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)';
allocate channel 'dev_2' type 'sbt_tape' parms 'SBT_LIBRARY=Oracle_home\bin\orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=ORACL,OB2BARLIST=ora1)'; backup incremental level 0 format 'ora1<ORACL_%s:%t>.dbf' database; }
```

Oracle 操作系统身份验证

要连接到数据库，Data Protector 可以使用 Oracle 侦听程序和 Oracle 操作系统身份验证。对于 Oracle 操作系统身份验证，在数据库备份期间，用户必须为可用作 Oracle 操作系统数据库管理员的 Oracle 操作系统用户提供用户名和用户组。该用户必须属于 Oracle **dba/sysdba** 组。用户信息在备份规范创建期间输入。

要使用操作系统身份验证配置备份规范，请执行以下步骤:

1. 在 Oracle 主机上，创建将用于 Oracle 操作系统身份验证的操作系统用户。该用户必须位于 Oracle 操作系统 sysdba/dba 组中。有关如何创建 Oracle 操作系统数据库管理员的详细信息，请参考 Oracle 文档。
2. 在 Data Protector admin 用户组中添加用户。
    1. 对于具有 Oracle 代理和 Windows 平台的主机，请为该用户添加模拟。
3. 创建备份规范。
    1. 在“指定要备份的应用程序”屏幕上，选中“指定 OS 用户”复选框，然后为创建的用户输入用户名和组。
    2. 在主选项卡中的“配置 Oracle”对话框上，选中“使用操作系统身份验证”复选框。

> **注意**对于 Oracle RAC 环境，请在“RAC 数据库名称”文本框中输入全局数据库名称。

使用 Data Protector GUI

在为数据库创建第一个备份规范时配置 Oracle 数据库。首先执行创建备份规范中介绍的过程，并请于步骤 6 继续执行以下步骤:

1. 在“配置 Oracle”对话框和“常规”页面中，指定 Oracle Server 主目录的路径名。
2. 在“主”页面中，指定主数据库的登录信息。

    请注意，必须已向用户授予 SYSDBA 特权。必须已向用户授予 SYSBACKUP 权限。您也可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。

    在“服务”中，键入主数据库实例的网络服务名称。将对此数据库实例所在的系统执行备份。

    RAC : 列出主数据库的所有网络服务名称，以逗号分隔。

    在主选项卡中，选中“使用操作系统身份验证”复选框。
3. 在“编目”页面中，选择“使用目标数据库控制文件代替恢复编目”，以使用主数据库控制文件。

    要将恢复数据库编目用作备份历史记录的 RMAN 存储库，请选择“使用恢复编目”并指定恢复编目的登录信息。

    Oracle Data Guard : 如果要备份备用数据库，则必须使用恢复编目。

    指定的用户必须是恢复编目的所有者。

    在“服务”中，键入恢复编目的网络服务名称。
4. 在 Oracle Data Guard 环境中，如果要备份备用数据库，则还要配置备用数据库:

    在“备用”页面中，选择“配置备用数据库”并指定备用数据库的登录信息。

    在“服务”中，键入备用数据库实例的网络服务名称。

    RAC : 列出备用数据库的所有网络服务名称，以逗号分隔。
5. 单击**确定**。

Oracle 数据库配置完毕。退出 GUI 或继续在选择要备份的 Oracle 数据库对象步骤中创建备份规范。

使用 **Data Protector CLI**

1. 在 UNIX 系统上，使用 OSDBA 用户帐户登录 Oracle Server 系统。
2. 在 Oracle Server 系统上，执行:

   Windows 系统：

   perl -I..\lib\perl util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOMEPRIMARY_DB_LOGIN | USEOSAUTHENTICATION [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN] [-client CLIENT_NAME]

   UNIX 系统：

   util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOMEPRIMARY_DB_LOGIN | USEOSAUTHENTICATION [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN] [-client CLIENT_NAME]

其中：

PRIMARY_DB_LOGIN

-prmuser PRIMARY_USERNAME

-prmpasswd PRIMARY_PASSWORD

USEOSAUTHENTICATION

-useosauth USE_OS_AUT

-racdbname RAC_DB_NAME

CATALOG_DB_LOGIN 时是:

-rcuser CATALOG_USERNAME

-rcpasswd CATALOG_PASSWORD

-rcservice CATALOG_NET_SERVICE_NAME

STANDBY_DB_LOGIN 时是:

-stbuser STANDBY_USERNAME

-stbpasswd STANDBY_PASSWORD

-stbservice STANDBY_NET_SERVICE_NAME_1[,STANDBY_NET_SERVICE_NAME_2 ...]

Oracle Data Guard:如果要备份备用数据库，必须提供 STANDBY_DB_LOGIN 信息。对于备用数据库备份，必须使用恢复编目。因此，还必须提供 CATALOG_DB_LOGIN 信息。

参数描述

CLIENT_NAME	具有待配置数据库的 Oracle Server 系统的名称。必须在群集环境下指定该参数。 *RAC :* Oracle 资源组的虚拟服务器。 *Oracle Data Guard :* 主系统或辅助 (备用) 系统的名称。
DB_NAME	要配置的数据库的名称。
ORACLE_HOME	Oracle Server 主目录的路径名。
PRIMARY_USERNAMEPRIMARY_PASSWORD	用于登录目标或主数据库的用户名和密码。请注意，必须向用户授予 SYSDBA 特权。且必须向用户授予 SYSBACKUP 特权。此外，您还可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。
PRIMARY_NET_SERVICE_NAME_1 [,PRIMARY_NET_SERVICE_NAME_2, ...]	主数据库的网络服务名称。 *RAC :* 每个网络服务名称都必须解析到一个特定的数据库实例中。
USE_OS_AUT	此参数用于与配置脚本通信，以使用 Oracle 操作系统身份验证 (而不是用户名和密码身份验证)。 值应为 1。
RAC_DB_NAME	此参数用于在 Oracle RAC 环境中查找当前 Oracle RAC 节点的 Oracle SID。它代表的是 Oracle 全局数据库名称，在 Oracle RAC 平台上为必填参数。

CATALOG_USERNAMECATALOG_PASSWORD	用于登录恢复编目的用户名和密码。此为可选参数，仅在将恢复编目数据库用作备份历史记录的 RMAN 存储库时使用。
CATALOG_NET_SERVICE_NAME	恢复编目的网络服务名称。
STANDBY_USERNAMESTANDBY_PASSWORD	其用于在 Oracle Data Guard 环境中备份备用数据库。用于登录备用数据库的用户名和密码。
STANDBY_NET_SERVICE_NAME_1 [,STANDBY_NET_SERVICE_NAME_2, ...]	备用数据库的网络服务名称。

消息 *RETVAL*0 表示配置成功，即使后面还有其他消息也是如此。

> **注意**如果需要在启动 SQL*Plus、侦听程序或 RMAN 之前导出一些变量，则必须在 Data Protector Oracle 全局配置文件的 Environment 部分或使用 Data Protector GUI 定义这些变量。

示例

以下示例表示 Oracle Data Guard 环境下 Oracle 数据库及其恢复编目在 UNIX 系统上的配置。示例中使用以下名称:

- 数据库名称: oracle
- Oracle Server 主目录: /app12/oracle12/product/12.0
- 主用户名: system
- 主密码: manager
- 主网络服务名称 1: netservice1
- 主网络服务名称 2: netservice2
- 恢复编目用户名: rman
- 恢复编目密码: manager
- 恢复编目网络服务名称: catservice
- 备用用户名: system
- 备用密码: manager
- 备用网络服务名称 1: netservicesb1
- 备用网络服务名称 2: netservicesb2
- 备份系统名称: bcksys

语法

```
/opt/omni/lbin/util_oracle8.pl -config -dbname oracle -orahome /app12/oracle12/product/12.0 -prmuser system -prmpasswd manager -prmservice netservice1,netservice2 -rcuser rman -rcpasswd manager -rcservice catservice  -stbuser system -stbpasswd manager -stbservice netservicesb1,netservicesb2
```

同时配置多个 Oracle 数据库

在具有多个 Oracle 数据库的大型环境中，单独配置每个数据库会很耗时，尤其是需要频繁更新配置参数的情况。

鉴于上述原因，Data Protector 允许您在单个文件中保留多个数据库的配置参数。这样，在一处即可进行所有必需的更新。文件准备就绪时，可以执行 Data Protector omniintconfig.pl 命令，读取该文件并配置所有指定的 Oracle 数据库。这意味着，对于每个 Oracle 数据库，都会创建或更新 (如果已存在) 单独的 Data Protector 配置文件，就像使用标准配置方法一样。如果事先指定，Data Protector 还会执行配置检查。

在配置文件中，为每个 Oracle 数据库指定以下参数:

Oracle 数据库配置参数

参数	描述
MoM (可选)	Manager of managers
CellManager	Data Protector Cell Manager 默认值：本地客户机的 Cell Manager

Client	安装了 Oracle Server 的客户机。 在群集环境中指定虚拟服务器，或在 RAC 中指定其中一个群集节点。 默认: 本地客户机
Instance	Oracle 数据库实例 (必需)
OSUSER (仅限 UNIX 和 Windows 系统)	用于启动 Oracle 数据库配置和浏览的操作系统用户帐户 (用户名和组或域)。此用户将自动添加到在 Client 中指定的客户机的 Data Protector admin 用户组。
OSGROUP (仅限 UNIX 和 Windows 系统)	在 Windows 系统上，无需指定用户帐户。
ORACLE_HOME	Oracle Server 主目录
TGTUser	目标数据库的登录信息 (用户名和密码)
TGTPasswd	
TGTService	目标数据库服务。如果有多个服务，请用分号分隔 (service1;service2...)。
RCUser (可选)	恢复编目数据库的登录信息 (用户名和密码)
RCPasswd (可选)	
RCService (可选)	恢复编目数据库服务
ClusterNodes (可选)	群集节点 (适用于群集环境)。用户 OSUSER、OSGROUP 将自动添加到此处列出的每个群集节点的 Data Protector admin 用户组。使用分号分隔群集节点 (node1;node2...)。 如果未指定此参数，则需手动添加这些用户，如备份 Oracle Server 中所述。

文件格式

文件在创建时必须采用以下格式之一:

- XLS (Microsoft Office Excel 文件)
- CSV (逗号分隔值文件)

创建文件时，请考虑以下事项:

- 在第一行中，列出要指定的参数。在后续行中，列出要配置的 Oracle 数据库的参数值。
- 第一行中的参数名称不区分大小写。
- 不允许空白列。
- 允许空白行。
- 仅可选参数可以有空白单元格。

XLS 文件

在 XLS 文件中，您可以根据自身需求要格式化单元格。但是，不允许在额外的单元格中添加任何信息。

CSV 文件

CSV 文件的创建方式是以 CSV 格式 (例如， C:\My_documents\Oracle_databases.csv) 保存文本文件。文件中的参数必须用逗号分隔。可通过将两个逗号之间的位置留空来省略不适用的参数指定。

编码密码

Data Protector 要求对 Data Protector Oracle 数据库配置文件中的密码进行编码。这一点可以用两种不同的方式实现:

- 使用 Data Protector util_cmd 命令在将密码保存到 XLS 或 CSV 文件之前对密码进行编码。例如，要对密码 BlueMoon 进行编码，请执行以下命令:

- ```
  util_cmd –encode BlueMoon
  ```

  收到编码的密码后，将其复制到文件中。

  如果您的密码保持编码状态，则在执行 omniintconfig.pl 命令时无需指定 –encode 选项。

- 如果您的密码未经过编码，则在执行 omniintconfig.pl 命令时指定 –encode 选项。

重要说明确保 XLS 或 CSV 文件中的密码全部已编码或全部为纯文本。

omniintconfig.pl 命令语法

注意 omniintconfig.pl 命令可以在安装了用户界面组件的任何 Data Protector 客户机上运行。

1. 以 Data Protector admin 用户组中添加的操作系统用户帐户登录客户机系统 (实际上，用户拥有 Data Protector“用户配置”和“查看私有对象”用户权限即可)。
2. 转到下面的 Data Protector 管理命令默认编目。
3. 执行：

   Windows 系统： perl omniintconfig.pl Options

   UNIX 系统： omniintconfig.pl Options

   其中 Options 是:

   ```
   [-encode] [-chkconf] [-force] {-passwordfile FileName|Param=Value [Param=Value...]}
   ```

示例

1. 假设您登录到创建了 C:\My_documents\Oracle_instances.xls 文件的 Windows 系统。要使用该文件中的信息配置 Oracle 数据库 IN1 和 IN2，请执行以下命令:

   ```
   perl omniintconfig.pl -passwordfile C:\My_documents\Oracle_instances.xls
   ```

2. 假设您登录到 UNIX 系统。要通过在运行时指定参数来配置 Oracle 数据库 IN2，请执行以下命令:

   ```
   omniintconfig.pl –encode CellManager=galaxy Client=star Instance=IN2 ORACLE_HOME=C:\oracle\product\10.2.0\db_1 TGTUser=system TGTService=IN2_1;IN2_2 TGTPasswd=BlueMoon
   ```

   请注意，密码 BlueMoon 未经过编码。因此，必须指定选项 –encode。

   一次只能为一个 Oracle 数据库指定参数。

3. 假设您登录到 Windows 系统。要配置和检查在 C:\My_documents\Oracle_instances.xls 中指定的所有 Oracle 数据库的配置，请执行以下命令:

   ```
   perl omniintconfig.pl -chkconf –force –passwordfile C:\My_documents\Oracle_instances.xls
   ```

   如果 Oracle 数据库的配置检查失败，-force 选项将指示 Data Protector 继续配置 Oracle 数据库。

4. 假设您登录到 UNIX 系统。要检查 Oracle 数据库 IN2 的配置，请执行以下命令:

   ```
   omniintconfig.pl -chkconf CellManager=galaxy Client=star Instance=IN2
   ```

检查配置

在为数据库至少创建一个备份规范后，您可以检查 Oracle 数据库的配置。如果使用 Data Protector CLI，则不需要备份规范。
   ```

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份规范”和“Oracle Server”。单击备份规范以显示具有待检查数据库的服务器。
3. 右键单击该服务器，然后单击“检查配置”。

> **重要说明**Data Protector 不检查指定的用户是否拥有适当的 Oracle 备份权限。

使用 Data Protector CLI

1. 在 UNIX 系统上，使用 OSDBA 用户帐户登录 Oracle Server 系统。
2. 执行：

   Windows 系统：

   ```
   perl -I..\lib\perl util_oracle8.pl -chkconf _smb   -dbname DB_NAME
   ```

   UNIX 系统：

   ```
   util_oracle8.pl -chkconf _smb   -dbname DB_NAME
   ```

处理错误

如果发生错误，错误编号将以 *RETVAL*error_number 的形式显示。

要获取错误描述，请在 Cell Manager 上执行:

Windows 系统： Data_Protector_home\bin\omnigetmsg 12 error_number

UNIX 系统： /opt/omni/lbin/omnigetmsg 12 error_number

HP-UX 和 Linux 系统： /opt/omni/lbin/omnigetmsg 12 error_number

其他 UNIX 系统： /usr/omni/bin/omnigetmsg 12 error_number

> **重要说明**在 UNIX 系统上，即使您收到了 *RETVAL*0 ，备份也仍有可能失败，因为 Data Protector 不会检查指定的用户是否拥有适当的 Oracle 备份权限。

还原 Oracle Server 集成

This feature is available in the Premium Edition

可以使用以下项目还原数据库对象:

- Data Protector GUI
- RMAN

可还原的项目

可以使用 Data Protector GUI 或 RMAN 还原以下数据库对象:

- 控制文件
- 数据文件
- 表空间
- 数据库
- 恢复编目数据库

复制数据库

使用 Data Protector GUI，还可以“复制”生产数据库。

Microsoft 群集服务器系统

在开始还原群集感知 Oracle 服务器之前，使用群集管理器实用程序使 Oracle 数据库资源处于脱机状态。
验证是否已为 Oracle 资源组设置“防止回退”选项，并为 DB_NAME.world 资源 (这是 Oracle 数据库资源) 设置“不重新启动”选项。

Serviceguard 系统

从在虚拟主机上执行的备份还原数据库时，应在 RMAN 脚本中设置 OB2BARHOSTNAME 环境变量。例如：

```
run { allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=(OB2BARHOSTNAME=virtual.domain.com)';
restore datafile '/opt/ora12/oradata/MAKI/example02.dbf'; release channel dev1; }
```

使用 Data Protector GUI 还原 Oracle

对于还原，根据在 GUI 中进行的选择，生成 RMAN 脚本以及必要的命令。要使用其他命令，可直接从 RMAN 中手动使用这些命令。此外，还可以使用如何修改 RMAN 还原脚本中描述的解决方法。

在灾难恢复中还原数据库项目

在灾难恢复的情况下，必须按特定顺序还原数据库对象。以下列表显示了在还原数据库项目时必须遵守的顺序。正常情况下，可以依照任何顺序还原数据库项目。如果“已”使用恢复编目:

1. 还原恢复编目数据库 (如果已丢失)
2. 还原控制文件
3. 还原整个数据库或数据项目

如果“未”使用恢复编目:

1. 从自动备份还原控制文件。如果控制文件没有自动备份，请参阅恢复编目已丢失，无法还原控制文件。
2. 还原数据库或数据项目。

更改数据库状态

在还原任何数据库项目或执行数据库复制之前，确保数据库处于正确的状态:

所需的数据库状态

要还原的项目	数据库状态
控制文件，复制数据库	NoMount（已启动）
所有其他项目 (仅还原少量表空间或数据文件时，可以打开其中包含要脱机还原的表空间或数据文件的数据库)。	Mount

要将数据库置于正确的状态，请执行以下命令:

```
sqlplus /nolog

SQL>connect user/password@service as sysdba ;

SQL>shutdown immediate ;
```

要将数据库置于 NoMount 状态，请执行以下命令:

```
SQL>startup nomount ;
```

要将数据库置于 Mount 状态，请执行以下命令:

```
SQL>startup mount;
```

注意: 如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

还原恢复编目数据库

Oracle 恢复编目数据库使用 Oracle Export 实用程序导出到二进制文件，并由 Data Protector 进行备份。此文件必须还原回磁盘，然后使用 Oracle Import 实用程序导入 Oracle 数据库中。Data Protector 提供了一款使用 Oracle 集成自动执行此操作的工具。要还原恢复编目数据库，请执行以下操作:

1. 确保恢复编目数据库处于“打开”状态。
2. 使用 RMAN 命令 DROP CATALOG 从数据库中删除恢复编目 (如果存在)。
3. 在 Data Protector GUI 中，切换到“还原”上下文。
4. 在“还原对象”下，展开“Oracle Server” 以及要还原恢复编目的数据库所在的系统，然后单击该数据库。
5. 在“还原操作”下拉列表中，选择“执行 RMAN 存储库还原”。在结果区域中，选择“恢复编目”。如果要更改恢复编目登录信息，请右键单击“恢复编目”，然后单击“属性”。在“恢复编目设置”中，指定恢复编目的登录信息。
6. 在“选项”页中: 在“用户名”和“用户组”中，指定恢复编目数据库的用户名和密码。从“会话 ID”下拉列表中，选择会话 ID。
7. 单击**还原**。

继续还原控制文件。

还原控制文件

控制文件包含有关数据库结构的所有信息。如果控制文件已丢失，则必须先还原控制文件，然后再还原数据库的任何其他部分。数据库应处于 No Mount 状态。

根据控制文件备份的类型，还原控制文件时可以执行以下还原类型:

- 从 Data Protector 管理的控制文件备份进行还原 (“ CONTROLFILE FROM DP MANAGED BACKUP ”)

除非已选择“禁用 Data Protector 管理的控制文件备份”选项，否则在备份会话结束时 ob2rman.pl 会自动备份控制文件。

此还原选项“不”需要恢复编目。

控制文件 (ctrlDB_NAME.dbf) 将还原到默认的 Data Protector 临时文件目录。

注意: 在安装了 Oracle 11.2.0.2 及更高版本的 Oracle Real Application Cluster (RAC) 环境中，控制文件在 OB2_DPMCTL_SHRLOC 变量定义的位置进行创建、从该位置备份并还原到该位置。此目录必须驻留在共享磁盘上，并且可以从所有 RAC 节点访问，这样，还原会话才会成功进行。

- 还原后，执行以下脚本:

```
run { allocate channel 'dev0' type disk; restore controlfile from 'TMP_FILENAME'; release channel 'dev0'; }
```

其中 TMP_FILENAME 是文件将还原到的位置。

- 从 RMAN 自动备份还原 (“控制文件来自 RMAN 自动备份”)

控制文件由 RMAN 自动备份，并且恢复编目“不”可用。

请确保已正确配置 RMAN 自动备份并且可以使用正确的备份版本。如果在还原期间未找到 RMAN 自动备份会话，则该过程将会中止。

- 从 RMAN 备份集还原 (“CONTROLFILE FROM RMAN BACKUPSET”)

需要恢复编目。

- *Oracle Data Guard :* 从 RMAN 备份集还原备用控制文件 (“备用控制文件来自 RMAN 备份集”)

如果还原“备用”数据库 (不使用复制)，则必须还原此类型的控制文件。

仅当在备份规范中选择了“适用于备用的控制文件”数据库对象时，此类型的还原才可在备用配置中使用。

备份会话可以包含多种类型的控制文件备份。

要还原控制文件，请执行以下操作:

1. 打开 sqlplus 窗口并将数据库置于非装载状态。
2. 在 Data Protector GUI 中，切换到“还原”上下文。
3. 在“还原对象”下，展开“Oracle Server”以及要还原控制文件的数据库所在的系统，然后单击该数据库。
4. 在“还原操作”下拉列表中，选择“执行 RMAN 存储库还原”。在结果区域中，选择要还原的控制文件。
5. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。要将控制文件还原到与非选定数据库，请单击“设置”，然后指定目标数据库的登录信息。设置其他还原选项。
6. 单击**还原**。

继续还原 Oracle 数据库对象。

还原 Oracle 数据库对象

在还原 Oracle 数据库对象之前，确保恢复编目数据库和控制文件为最新版本。它们包含数据库结构信息。如果没有这些文件的最新版本，请按照还原恢复编目数据库和还原控制文件中所述还原这些文件。

要还原 Oracle 数据库对象，请执行以下操作:

1. 在 Oracle Data Guard 环境中，如果还原“备用”数据库，请停止管理的恢复过程 (日志应用服务):

   ```
   SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;
   ```

2. 将数据库置于装载状态。
3. 在 Data Protector GUI 中，切换到“还原”上下文。
4. 在“还原对象”下，展开“Oracle Server”以及要还原数据库对象的数据库所在的系统，然后单击该数据库。
5. 在“还原操作”下拉列表中，选择要执行的还原类型。

   > **重要说明**如果未选择“执行还原和恢复”或“仅执行恢复”，则必须使用 RMAN 手动还原数据库对象。

6. 在结果区域中，选择要还原的对象。

   如果还原的是数据文件，可以将文件还原到新位置。右键单击数据库对象，单击“还原为”，然后在“还原为”对话框中，指定新的数据文件位置。

   > **注意**如果还原到新位置，仅当您从“还原操作”下拉列表中选择“执行还原和恢复”时，才会将当前数据文件切换到已还原的数据文件副本。

   Oracle Data Guard : 如果从备用数据库备份还原“主”数据库，或者从主数据库备份还原“备用”数据库，则数据文件的位置有所不同。在“还原为”对话框中，为每个数据文件指定适当的位置。

   > **提示**如果设置 DB_FILE_NAME_CONVERT 初始化参数，则可以执行相同的操作。此参数捕获所有目标数据文件并相应地对其进行转换。

7. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理的系统。要将数据库对象还原到非选定数据库，请单击“设置”，然后指定目标数据库的登录信息。

Oracle Data Guard : 如果还原主数据库，则指定主数据库的登录信息。如果还原备用数据库，则指定备用数据库的登录信息。否则，将使用选定数据库的登录信息。

设置其他还原选项。

8. 在“设备”页中，选择要用于还原的设备。
9. 单击**还原**。

还原后:

1. 将数据库置于正确的状态。如果您在“源”页中选择了“执行还原和恢复”或“仅执行恢复”，Data Protector 会自动将数据库置于“打开”状态。
2. 如果您执行了将 Oracle 数据库还原和恢复到既定时间点之前，并且会话已成功完成，请重置数据库，以在恢复编目中注册数据库的新版本。使用 RMAN 连接到目标和恢复编目数据库并重置数据库: rman target Target_Database_Login catalog Recovery_Catalog_Login RMAN> RESET DATABASE; RMAN> exit
3. 如果您未选择使用 Data Protector 来恢复数据库对象，并且磁盘上已存档所有重做日志，请在还原数据库之后执行以下操作: 打开命令行窗口并输入以下命令: sqlplus /nolog SQL>recover database; SQL>connect user/password@service as sysdba; SQL>alter database open;
   注意**:** 如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。
4. 在 Oracle Data Guard 环境中，如果您已还原“备用”数据库，并且磁盘上已存档所有重做日志，请重新启动管理的恢复过程 (日志应用服务): SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT;

还原表空间和数据文件

要还原表空间和数据文件，请执行以下操作:

1. 如果数据库处于“打开” 状态，请打开命令行窗口并输入以下命令: sqlplus /nolog SQL>connect user/password@service as sysdba ； SQL>alter database datafile 'datafile name' offline; ；如果要还原表空间，请输入: SQL>alter tablespace tablespace_name offline;
2. 完成还原后，使用以下过程将数据文件和表空间重置为联机状态: 打开命令行窗口并输入以下命令: sqlplus /nolog SQL>connect user/password@service as sysdba ；如果要还原数据文件，请输入 SQL>alter database datafile 'datafile_name' online; ；如果要还原表空间，请输入 SQL>alter tablespace tablespace_name online; SQL>alter tablespace tablespace_name online;
   注意**:** 如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

在 Oracle Data Guard 环境中还原和恢复 Oracle 数据库

还原和恢复主数据库

可以从在主数据库或备用数据库上执行的备份中还原和恢复主数据库。该还原和恢复操作与还原和恢复独立配置中的数据库几乎相同。

还原和恢复备用数据库

可以从主数据库或备用数据库的备份中还原和恢复备用数据库。该还原和恢复操作与还原和恢复独立配置中的数据库几乎相同。

如果无法在磁盘上访问恢复操作所需的已存档重做日志文件，而只能在磁带上访问，请使用 RMAN 将还原的数据文件恢复为大于已应用到备用数据库的最后一个日志的 SCN/log 序列。

获取 UNTIL_SCN :

SQL> SELECT MAX(NEXT_CHANGE#)+1 UNTIL_SCN FROM V$LOG_HISTORY LH, V$DATABASE DB WHERE LH.RESETLOGS_CHANGE#=DB.RESETLOGS_CHANGE# AND LH.RESETLOGS_TIME = DB.RESETLOGS_TIME;

如果可以在磁盘上访问恢复操作所需的已存档重做日志，则仅还原损坏的数据文件并重新启动重做应用过程。

如果整个备用数据库已丢失，最好执行数据库的“复制”(除非只需还原少量已损坏的数据文件或表空间)。

以下情况下也请执行数据库的复制:

- 已还原或重新创建主数据库控制文件。
- 在主数据库上执行时间点恢复。
- 发生了数据库角色故障转移。

复制 Oracle 数据库

执行生产数据库复制以创建:

- 与生产 (主) 数据库具有相同 DBID 的备用数据库。这样做可以:
  - 新建备用数据库。
  - 以下情况下重新创建备用数据库:
    - 丢失整个备用数据库
    - 已还原或重新创建主数据库控制文件

    - 已在主数据库上执行数据库时间点恢复
    - 已发生数据库角色切换或故障转移
- 具有唯一 DBID 的独立副本，可用于挖掘数据或进行测试。

要复制生产数据库，请执行以下操作:

1. 在要复制选定数据库的系统上，将 Oracle 辅助数据库实例置于非装载状态。
2. 在 Data Protector GUI 的上下文列表中，单击“还原”。
3. 在“还原对象”下，展开“Oracle Server”以及生产数据库所在的系统，然后单击要复制的生产数据库。如果有多个此类系统，请选择要用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。
4. 在“还原操作”下拉列表中，选择“执行复制”。
5. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。单击“设置”以指定辅助数据库的登录信息 (用户名、密码和网络服务名称)。如果您未提供登录信息，复制会话将失败。在“用户名”和“用户组”中，指定 OSDBA 帐户的用户名和用户组，以供 Data Protector Oracle 集成代理使用。在“并行性”中，指定要为数据库复制分配的 RMAN 辅助通道的数量。设置复制选项。有关信息，请按 **F1**。如果要创建新的数据库副本 (而不是备用数据库副本)，请另外指定“在此前恢复”选项以将复制的数据库恢复到指定的时间点之前。
6. 单击**还原**。

创建备用数据库时，它将保持装载状态。手动启动管理的恢复过程 (日志应用服务)。

还原、恢复和复制选项

还原操作选项 下文介绍“源”页中的各个选项。此页面用于定义要使用 GUI 执行的还原和恢复的组合。在 Data Protector 的上下文中，“还原”是指还原数据文件。可以选择要还原的数据库、表空间或数据文件，以及希望将它们还原到哪个时间点。“恢复”是指应用重做日志。可以根据 SCN 编号、logseq 选择要应用的重做日志，也可以将所有重做日志应用到上次备份的时间。

执行还原	使用此选项只能使用 Data Protector 还原 (但不能恢复) 数据库对象。还原后，使用 RMAN 手动恢复数据库。
执行还原和恢复	使用此选项可通过 Data Protector 执行数据库对象的还原和恢复。
仅执行恢复	使用此选项只能恢复数据库。此操作只能对整个数据库执行。
执行 RMAN 存储库还原	数据库对象在“源”页中不可用时，选择此选项可以还原恢复编目或控制文件。
执行复制	此选项用于执行生产数据库的复制。此操作只能对整个数据库执行。

常规选项

客户机	此选项指定用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。
设置	单击“设置”选项可以为要还原或复制选定数据库对象的目标数据库 (在还原和恢复时) 或辅助数据库 (在复制时) 指定登录信息 (用户名、密码和网络服务名称)。如果在还原或恢复时不指定此选项，将使用位于选定系统上选定数据库的登录信息。如果在复制时不指定此选项，则复制会话将失败。
用户名、用户组 (仅限 UNIX 系统)	指定要用于启动还原的操作系统用户帐户。 确保此用户具有还原数据库的 Oracle 权限 (例如，位于 DBA 用户组中)。该用户还必须在 Data Protector 管理员或操作员用户组中 (实际上，具有“启动还原”和“查看私有对象”用户权限已足够)。
还原模式	可通过此下拉列表指定要执行的还原类型。选项如下: • Normal 当执行了使用备份集方法的传统备份或 ZDB 时，应使用此选项。 • 代理副本 当使用 Oracle RMAN 代理复制方法执行了原始 Oracle 备份时，应使用此选项。如果只执行恢复，则禁用此选项。
并行性	此字段用于指定可从备份设备中读取的并发数据流的数量。默认值为 1。在 Normal “正常”还原模式下，要优化还原性能，请使用与备份期间所用相同数量的数据流。例如，如果将备份并发设置为 3，则也要将并行数据流数量设置为 3。请注意，如果指定了非常大量的并行数据流，则这可能导致资源问题，因为要使用的内存过多。

复制选项

在选择“执行复制”时可用。

用于备用	选择此选项可以创建备用数据库。默认：选择。
DORECOVER	(在选择“适用于备用机”时可用)如果希望 RMAN 在创建数据库之后执行恢复，请选择此选项。
到数据库名称	选择此选项可以创建新数据库副本。在文本框中，指定其名称。该名称应当匹配用于启动辅助数据库实例的初始化参数文件中的名称。默认情况下，数据库名称设置为当前选定目标数据库的数据库名称。
NOFILENAMECHECK	选择此选项可禁止 RMAN 检查目标数据文件是否与所复制的数据文件同名。当目标数据文件和所复制的数据文件同名、但位于不同系统中时，选择此选项。默认：未选择。

还原直至	使用此下拉列表中的选项可以限制对适合于未完成恢复到指定时间的这些备份的选择。 **现在** 使用此选项可还原完整备份。默认情况下，选择此选项。**所选时间** 使用此选项可以指定希望向其还原数据库的确切时间。Data Protector 恢复可以在恢复中使用到指定时间的备份。**所选 logseq/线程数** logseq 数是重做日志序列数。使用此选项可以指定将充当重做日志上限以还原的特定重做日志序列和线程数。Data Protector 恢复可以在恢复中使用到指定日志序列号的备份。**选择 SCN 数** 使用此选项可以指定希望向其还原数据库的 SCN 数。Data Protector 恢复可以在恢复中使用到指定 SCN 号的备份。

在此前恢复	使用此下拉列表中的选项可指定希望恢复要执行到的时间点。 **现在** Data Protector 通过应用所有存档重做日志，启动 RMAN 将数据库恢复到尽可能最新的时间。默认情况下，选择此选项。**所选时间** 使用此选项可指定存档日志要应用到的确切时间。**所选 logseq/线程数** logseq 数是重做日志序列数。使用此选项可以指定一个特定重做日志序列，或者将充当要恢复的重做日志数上限的线程数。**选择 SCN 数** 使用此选项可指定对其执行恢复的 SCN 数。如果重置日志，也要重置数据库；否则，Oracle 将在下次备份期间尝试使用已经重置的日志，备份将失败。登录目标和恢复编目数据库并执行以下命令：rman target Target_Database_Login catalog Recovery_Catalog_Login RMAN> RESET DATABASE; RMAN> exit
恢复之后打开数据库	执行恢复后打开数据库。
重置日志	在打开数据库之后，重置存档日志。 *始终*重置日志：不完全恢复后 (不是“恢复到现在”)。如果在恢复或还原和恢复中使用控制文件的备份。以下情况下，“不要”重置日志: 在完整恢复之后 (恢复到现在)；如果在恢复或还原和恢复中未使用控制文件的备份。在主数据库上；如果存档日志用于备用数据库。但是，如果必须重置存档日志，则将需要重新创建备用数据库。如果将“在此前恢复”选项设置为“现在”时重置日志，则显示一个警告，指示仅当使用旧控制文件进行还原时才应重置日志。注意: Oracle 建议在使用“重置日志”选项打开数据库之后，立即执行完整备份。

使用 RMAN 还原 Oracle

Data Protector 充当 Oracle 系统的介质管理软件，因此 RMAN 可用于还原。本节仅介绍如何执行还原的“示例”。提供的示例不适用于需要还原的所有情况。

- 还原和恢复数据库、表空间、控制文件和数据文件。
- 复制数据库。

以下是还原示例:

- 完整数据库还原和恢复示例
- 时间点还原示例
- 表空间还原和恢复示例
- 数据文件还原和恢复示例
- 存档日志还原示例

Oracle 控制文件的还原和恢复过程是一项非常精细的操作，具体取决于您是否将恢复编目或控制文件用作中央存储库以及您所使用的 Oracle 数据库版本。

准备要还原的 Oracle 数据库

当数据库处于装载模式时，可以执行 Oracle 数据库的还原。但是，在执行表空间或数据文件的还原时，只能将 Oracle 数据库的一部分置于脱机状态。**示例中使用的连接字符串** 在下面的示例中，使用以下连接字符串:

- 用于目标数据库的目标连接字符串:

  sys/manager@PROD

  其中 sys 是用户名， manager 是密码， PROD 是网络服务名称。

- 用于恢复编目数据库的恢复编目连接字符串:

  rman/rman@CATAL

  其中 rman 是用户名和密码， CATAL 是网络服务名称。

SBT_LIBRARY 参数

在 Windows 和 UNIX 系统上，将 SBT_LIBRARY RMAN 脚本参数设置为指向正确的特定于平台的 Data Protector MML。必须分别为每个 RMAN 通道指定参数。

SBT_LIBRARY 路径参数不得包含空格，以便 RMAN 可以成功加载库。在 Windows 系统上，您可能会在配置 Oracle 备份时遇到问题，并且配置可能会失败并显示以下错误消息:

```
SBT_LIBRARY=C:/Program Files/OmniBack/bin/orasbt.dll
```

```
[...]
```

```
ORA-19554: 分配设备时出错，设备类型: SBT_TAPE，设备名称:
```

```
ORA-27209: 设备 PARMS 中的语法错误 - 关键字未知或缺失 =
```

如果在此阶段 SBT_LIBRARY 参数包含一个带有空格的路径，则必须检查路径 C:\Program Files 或 Data Protector 安装目录 *DP_HOME* 是否包含短路径 (8dot3) 表示法和 CMD 命令 <dir /X> 。

如果短路径不存在、已删除或在安装过程中已禁用，您可以使用以下命令手动添加:

```
<windows\System32\fsutil.exe file setshortname 'C:\Program Files' PROGRA~1>
```

请注意，由于在 OS 处于活动状态时 Program Files 目录正在使用中，因此，仅当您在 Oracle 计算机上运行 Windows 修复模式 CMD 时，该命令才有效。

如果由于生产数据库无法脱机以进入修复模式，因此无法添加短名称，请使用以下解决方法:

1. 使用 CMD <mklink> 创建一个指向 <DP_HOME>\bin\orasbt.dll 的符号链接，并将其保存到不含空格的路径。
2. 按照上述过程设置 Oracle 变量 SBT_LIBRARY ，并设置 util_cmd CLI 参考页。

如果由于新安装而没有 Oracle 配置，则必须指定可选参数以确保创建配置文件:

```
-local
```

```
"C:\ProgramData\OmniBack\Config\Server\Integ\Config\Oracle8\hostname.domain.suffix%SID"
```

> ⚠ **警告**如果使用上述解决方法，您需要指定符号链接的位置、安全性和访问权限。

在以下示例中， SBT_LIBRARY 参数设置为 /opt/omni/lib/libob2oracle8.so ，这是 32 位 Solaris 系统的正确路径。

完整数据库还原和恢复示例

要执行完整数据库还原和恢复，还需要还原并应用所有存档日志。要执行完整数据库还原和恢复，请执行以下操作:

1. 登录到 Oracle RMAN:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

   如果不使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog

2. 启动完整数据库还原和恢复:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore database; recover database; sql 'alter database open'; release channel 'dev1'; }
   ```

您也可以将脚本保存到文件中，并使用保存的文件执行完整数据库还原。这种情况下，操作过程如下:

1. 在默认 Data Protector 临时文件目录中创建 restore_datafile 文件。
2. 启动完整数据库还原:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_datafile

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_datafile

   如果不使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog cmdfile=Data_Protector_home\tmp\restore_datafile

UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog cmdfile=/var/opt/omni/tmp/restore_datafile

时间点还原示例

要执行时间点还原，还需要还原存档日志并将其应用于指定的时间点。要执行时间点数据库还原和恢复，请执行以下操作:

1. 登录到 Oracle RMAN:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

   如果不使用恢复编目，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog

2. 启动时间点还原:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; set until time 'Mar 14 2004 11:40:00'; restore database; recover database; sql 'alter
   database open'; release channel 'dev1'; }
   ```

3. 执行时间点还原后，请在“恢复编目”中重置数据库。

您也可以将脚本保存到文件中，并使用保存的文件执行时间点还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_PIT 文件。
2. 启动时间点还原:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore
   _PIT

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_PIT

   如果不使用恢复编目，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog cmdfile=Data_Protector_home\tmp\restore_PIT

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog cmdfile=/var/opt/omni/tmp/restore_PIT

表空间还原和恢复示例

如果表丢失或损坏，则需要对整个表空间执行还原和恢复。要还原表空间，可以仅将数据库的一部分置于脱机状态，以便数据库不必处于装载模式。可以使用恢复编目数据库或控制文件来执行表空间还原和恢复。请遵循以下步骤:

1. 登录到 Oracle RMAN:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

   如果不使用恢复编目，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog

2. 启动表空间还原和恢复。
   - 如果数据库处于打开状态，用于还原和恢复表空间的脚本应具有以下格式:

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql 'alter tablespace TEMP offline immediate'; restore tablespace TEMP; recover
     tablespace TEMP; sql 'alter tablespace TEMP online'; release channel dev1; }
     ```

   - 如果数据库处于装载状态，用于还原和恢复表空间的脚本应具有以下格式:

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore tablespace 'TEMP'; recover tablespace 'TEMP'; release channel dev1; }
     ```

您也可以将脚本保存到文件中，并使用保存的文件执行表空间还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_TAB 文件。
2. 启动表空间还原。

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_TAB

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_TAB

   如果不使用恢复编目，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog cmdfile=Data_Protector_home\tmp\restore_TAB

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog cmdfile=/var/opt/omni/tmp/restore_TAB

数据文件还原和恢复示例

要还原和恢复数据文件，可以仅将数据库的一部分置于脱机状态。

要还原和恢复数据文件，请执行以下操作:

1. 登录到 Oracle RMAN。

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

   如果不使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog

2. 启动数据文件还原和恢复:
   - 如果数据库处于打开状态，用于还原数据文件的脚本应具有以下格式:

     UNIX 系统

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql "alter database datafile ''/opt/oracle/data/oradata/DATA/temp01.dbf'' offline";
     restore datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; recover datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; sql "alter
     database datafile '/opt/oracle/data/oradata/DATA/temp01.dbf' online"; release channel dev1; }
     ```

     Windows 系统

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql "alter database datafile ''C:\oracle\data\oradata\DATA\temp01.dbf'' offline";
     restore datafile 'C:\oracle\data\oradata\DATA\temp01.dbf'; recover datafile 'C:\oracle\data\oradata\DATA\temp01.dbf'; sql "alter
     database datafile ''C:\oracle\data\oradata\DATA\temp01.dbf'' online"; release channel dev1; }
     ```

   - 如果数据库处于装载状态，用于还原和恢复数据文件的脚本应具有以下格式:

     UNIX 系统

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; recover datafile
     '/opt/oracle/data/oradata/DATA/temp01.dbf'; release channel dev1; }
     ```

     Windows 系统

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore datafile 'Oracle_home\data\oradata\DATA\temp01.dbf'; recover datafile
     'Oracle_home\data\oradata\DATA\temp01.dbf'; release channel dev1; }
     ```

您也可以将脚本保存到文件中，并使用保存的文件执行数据文件还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_dbf 文件。
2. 启动数据文件还原:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_dbf

UNIX 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_dbf

如果不使用恢复编目数据库，请执行以下命令:

Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog cmdfile=Data_Protector_home\tmp\restore_dbf

UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog cmdfile=/var/opt/omni/tmp/restore_dbf

存档日志还原示例

要还原存档日志，请执行以下操作:

1. 登录到 Oracle RMAN:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

   如果不使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog

   UNIX 系统： ORACLE_HOME /bin/rman target sys/manager@PROD nocatalog

2. 启动存档日志还原:

```
run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore archivelog all; release channel dev1;}
```

您也可以将脚本保存到文件中，并使用保存的文件执行存档日志还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_arch 文件。
2. 启动存档日志还原:

   如果使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_arch

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_arch

   如果不使用恢复编目数据库，请执行以下命令:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD nocatalog cmdfile=Data_Protector_home\tmp\restore_arch

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD nocatalog cmdfile=/var/opt/omni/tmp/restore_arch

使用不同设备还原数据库的示例

假设使用设备 dev1 对某个数据库进行了备份。要使用设备 dev2 还原该数据库，请将 send device type 'sbt_tape' 'CHDEV=dev1>dev2'; 行添加到 RMAN 脚本:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@TIN

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@TIN

2. 执行：

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; allocate
channel 'dev_2' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; send device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1'; send device
type 'sbt_tape' 'CHDEV=dev1>dev2'; restore database; }
```

> **注意**
> - device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1'; 行可禁用自动设备选择。
> - 您也可以使用 CHDEV 参数和 'CHDEV=dev1>dev2;dev3>dev4'; 语法指定多个设备重定向。

使用其他设备进行还原

Data Protector 支持从备份数据库对象时所用的设备以外的其他设备还原 Oracle 数据库对象。

按以下格式在 /etc/opt/omni/server/cell/restoredev（UNIX 系统）或 Data_Protector_program_data\Config\server\Cell\restoredev（Windows系统）文件中指定这些设备:

" DEV 1 " " DEV 2 "

其中:

DEV 1 是原始设备， DEV 2 是新设备。

在 Windows 系统上，此文件必须采用 Unicode 格式。

请注意，此文件在使用后应删除。

示例

假设您在名为 DAT1 的设备上备份了 Oracle 对象。要从名为 DAT2 的设备还原这些对象，请在 **restoredev** 文件中指定以下内容:

" DAT1 " " DAT2 "

将 Oracle CDB/PDB 还原到另一个主机

需要满足以下先决条件:

- 必须恢复 Oracle 目录结构中的所有必要信息 (用户、密码和 SID)。目标数据库使用此信息进行恢复。
- 应在 Data Protector 中为目标实例配置 Oracle 集成。
- 必须存在包含编目 (如果存在)、控制文件、数据文件和存档日志的 Oracle 备份。

要将 Oracle CDB/PDB 还原到另一个主机，请执行以下步骤:

1. 还原恢复编目数据库。
2. 从 Data Protector 管理的备份还原控制文件。
3. 还原存档日志文件。将 RMAN 连接到目标数据库并执行以下脚本:

```
run {
allocate channel 'dev_0' type 'sbt_tape'
parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll,
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DatabaseName,OB2BARLIST=BarListName)';
restore archivelog all;
release channel 'dev_0';
}
```

> **注意**数据库必须处于“装载”状态。

4. 找到 SCN 编号。连接到目标数据库并执行以下命令:

   SQL: select max(checkpoint_change#) from v$datafile;

5. 还原数据库文件。

- 从 Data Protector “还原”上下文中选择要还原的数据库。
- 在“还原”操作下拉列表中选择“执行还原”。单击“选项”选项卡，选择需要执行还原的客户机。

6. 将数据库恢复到 SCN 编号 (步骤 4)。

   在 Data Protector GUI 中，从“还原”上下文选择要恢复的数据库。在“还原”操作下拉列表中选择“仅执行恢复”。在“选项”选项卡的“恢复选项”部分，为“在此前恢复”选择“选定的 SCN 编号”并输入步骤 4 中的 SCN 编号。恢复后检查打开的数据库，并重置日志复选框。

   - 从 Data Protector “还原”上下文中选择要还原的数据库。
   - 在“还原”操作下拉列表中选择“仅执行恢复”。单击“选项”选项卡，然后输入步骤 4 中的 SCN 编号。
   - 恢复后检查打开的数据库，并重置日志复选框。

将 Oracle 还原到不同的单元/客户机

要将 Oracle 还原到不同的单元/客户机，请执行以下步骤:

1. 将 Data Protector Oracle 配置文件从源复制到目标。
2. 导出 Oracle SID。
3. 为数据库创建密码文件。
4. 设置 DBID 并在非装载状态下启动数据库。
5. 从 RMAN 恢复 **pfile**。
6. 使用已恢复的 **pfile** 在非装载状态下启动数据库。
7. 从 GUI 启动控制文件还原，并将 Data Protector 的已还原控制文件复制到控制文件位置。
8. 在装载状态下启动数据库。
9. 在目标端使用控制文件配置数据库备份。
10. 仅启动数据库还原。
11. 从目标数据库执行 sql 命令 " alter database open resetlogs " 以恢复数据库。

监视会话

在备份期间，系统消息将发送到 Data Protector 监视器。您可以从网络上安装了 Data Protector 用户界面的任何 Data Protector 客户机监视备份会话。

监视当前会话

要使用 Data Protector GUI 监视当前运行的会话，请执行以下操作:

1. 在上下文列表中，单击**监视**。

   在结果区域中，列出了所有当前运行的会话。

2. 双击要监视的会话。

清除会话

要从“监视器”上下文的“结果区域”中删除所有已完成或已中止的会话，请执行以下操作:

1. 在“范围窗格”中，单击“当前会话”。
2. 在“操作”菜单中，选择“清除会话”。或者，单击工具栏上的“清除会话”图标。

要从当前会话列表中删除特定的已完成或已中止的会话，请右键单击该会话，然后选择“从列表删除”。

> **注意**如果重新启动 Data Protector GUI，将从“监视器”上下文的“结果区域”中自动删除所有已完成或已中止的会话。

监视工具

通过使用以下 SQL 语句查询 Oracle 目标数据库，也可以监视备份和还原的进度:

```
select * from  v$SESSION_LONGOPS  where compnam='dbms_backup_restore';
```

查看先前会话

要使用 Data Protector GUI 查看先前会话，请继续执行以下步骤:

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**会话**以显示 IDB 中存储的所有会话。

   此时会话将按日期排序。每个会话都由会话 ID 标识，此标识由 YY/MM/DD 格式的日期和唯一编号组成。

3. 右键单击会话，然后选择“属性”，以查看有关会话的详细信息。
4. 单击“常规”、“消息”或“介质”选项卡，以分别显示会话的常规信息、会话消息或有关此会话所用介质的信息。

有关 Oracle 备份和还原会话的详细信息也会写入 `oracle8.log` 文件中，该文件位于 Oracle Server 系统的默认 Data Protector 日志文件目录中。

Oracle Server 会将这些日志写入 `Oracle_user_dump_directory\sbtio.log` 文件中。

恢复会话

可以恢复未成功完成的备份和还原会话。使用该功能，可以仅备份或还原原始会话中无法备份或还原的文件。因此，使用恢复会话功能 (“已恢复会话”) 启动的会话通常需要较少的时间即可完成。

可以使用 Data Protector GUI 或 CLI 来恢复会话。

恢复备份会话

恢复 Oracle Server 集成备份会话时，Data Protector 使用相同的备份规范启动新的备份会话。因此，您可以创建多个会话来完成备份。只能恢复这些会话中的最后一个会话，而无法再次恢复之前已经恢复过一次的会话。由于恢复会话功能与原始会话使用相同的备份规范，因此，对中止和恢复之间的备份规范所做的更改会影响恢复会话。

与标准备份会话相比，主要区别在于，在已恢复的会话期间，Data Protector 会在开始实际备份之前修改 RMAN 脚本，同时为每个备份命令添加 NOT BACKED UP SINCE Time 子句，其中 *Time* 是原始备份会话开始时间。请参阅以下示例:

```
run{ allocate channel 'dev_0' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORCL,OB2BARLIST=New1)'; allocate channel 'dev_1' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORCL,OB2BARLIST=New1)'; allocate channel 'dev_1' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=ORCL,OB2BARLIST=New1)'; backup incremental level <incr_level> format 'New1<ORCL_%s:%t:%p>.dbf' NOT BACKED UP SINCE TIME "TO_DATE('5/15/2009 15:30:00', 'MM/DD/YY HH24:MI:SS')" database; sql 'alter system archive log current'; backup format 'New1<ORCL_%s:%t:%p>.dbf' NOT BACKED UP SINCE TIME "TO_DATE('5/15/2009 15:30:00', 'MM/DD/YY HH24:MI:SS')" archive log all; backup format 'New1<ORCL_%s:%t:%p>.dbf' NOT BACKED UP SINCE TIME "TO_DATE('5/15/2009 15:30:00', 'MM/DD/YY HH24:MI:SS')" recovery area; backup format 'New1<ORCL_%s:%t:%p>.dbf' NOT BACKED UP SINCE TIME "TO_DATE('5/15/2009 15:30:00', 'MM/DD/YY HH24:MI:SS')" current controlfile;
```

因此，RMAN 会跳过在原始会话中已成功备份的备份集。

假设您运行以下会话:

1. 2009/05/13–1 (原始备份会话)
2. 2009/05/13–2 (恢复 2009/05/13–1)
3. 2009/05/13–3 (恢复 2009/05/13–2)

RMAN 子句 NOT BACKED UP SINCE Time 中的 *Time* 始终是原始备份会话开始时间。因此，在第三个会话 (2009/05/13–3) 中创建的 RMAN 脚本不使用会话 2009/05/13–2 的开始时间，而是使用原始备份会话 (2009/05/13–1) 的开始时间。这可确保在启动原始备份会话后仅备份每个备份集一次。

注意确保 Cell Manager 和 Oracle Server 系统保持同步。否则，如果 *Time* 不正确，恢复会话功能将无法正常工作。

注意最小的备份单元是备份集。因此，请针对 RMAN 选项 FILESPERSET 考虑以下事项:

- 如果该选项设置为 1 ，RMAN 会为每个文件创建一个单独的备份集。在这种情况下，您从恢复会话功能中的获益最多。但是，请注意，如果使用多个流来备份文件，则还原时间会显著延长。
- 如果 RMAN 仅为要备份的文件创建一个备份集，并且有些文件无法备份，则整个备份集将失败。恢复此类会话时，将再次备份整个备份集，其中包括已成功备份的文件。

恢复还原会话

恢复还原会话的主要优点是，无需再次指定要还原的内容、要使用的设备等。但是，实际上，标准还原会话和已恢复的还原会话之间没有区别。在这两种情况下，Oracle Server 首先检查要还原的文件是否已存在于目标位置，然后仅还原丢失的文件。

注意使用 RESETLOGS 选项打开 Oracle 数据库后，针对已还原旧备份 (在重置日志之前创建的备份) 的会话使用恢复会话功能毫无意义。

使用 Data Protector GUI

1. 在“内部数据库”上下文中，展开“会话”。
2. 右键单击要恢复的会话，然后单击“恢复会话”。

使用 Data Protector CLI

1. 登录到 Cell Manager 或安装了“用户界面”组件的任何系统。
2. 转到以下目录:

   Windows 系统： Data_Protector_home\bin

   HP-UX、Solaris 和 Linux 系统： /opt/omni/bin/

   其他 UNIX 系统： /usr/omni/bin/
3. 要恢复备份会话，请执行以下命令:

   omnib –resume SessionID

   要恢复还原会话，请执行以下命令:

   omnir –resume SessionID

示例

要恢复备份会话 2013/05/13–1 ，请执行以下命令:

omnib –resume 2013/05/13–1

中止会话

可通过单击“中止”按钮来中止当前运行的会话。

如果在会话期间 RMAN 或 SQL*Plus 没有对请求做出响应，Data Protector 会自动中止会话。默认情况下，Data Protector 将等待响应 5 分钟。使用 omnirc 选项或环境变量 OB2_RMAN_COMMAND_TIMEOUT 和 OB2_SQLP_SCRIPT_TIMEOUT ，可以修改此时间间隔。

Oracle Server ZDB 集成

This feature is available in the Premium Edition

您可以采用各种备份策略，以便最有效地满足系统优先级要求。例如，如果数据库可用性的优先级最高，备份策略应包括最常用的联机备份，从而尽可能缩短恢复时间。此策略可限制宕机时间，但会更密集地使用系统资源。Data Protector 零宕机时间备份 (ZDB) 功能提供联机备份功能，并最大程度地避免应用程序系统性能下降。

支持的磁盘阵列

以下磁盘阵列可用于对 Oracle Server 数据执行零宕机时间备份 (ZDB):

- P9000 XP 磁盘阵列系列 (P9000 XP 阵列)
- 非 HPE 存储阵列 (NetApp Storage、Dell EMC Unity)

注意使用 Data Protector EMC 和 Data Protector 非 HPE 存储阵列集成时，不支持即时恢复，并且 ZDB 到磁带是唯一受支持的 ZDB 形式。

在使用自动存储管理 (ASM) 的 Oracle Server 配置中，由于集成 Data Protector Dell EMC Unity 和 Data Protector P9000 XP 阵列，支持零宕机时间备份和即时恢复。

使用 Data Protector Oracle ZDB 集成的优点包括:

- ZDB 可减少应用程序系统性能下降。
- 表空间处于备份模式 (联机备份)，或者数据库仅在创建“复本”(拆分镜像磁盘或创建快照) 所需的一小段时间内关闭数据库 (脱机备份)。
- 应用程序系统的负载显著降低。创建复本后，可以使用单独的备份系统在闲置时对复制的数据启动磁带备份。

Data Protector Oracle ZDB 集成支持 Oracle Server System (应用程序系统) 联机备份和脱机备份。

联机备份概念应用广泛，因为它可以实现高应用程序可用性。脱机备份需要在创建复本时关闭数据库，因此无法实现高可用性。

ZDB 方法和 Oracle 版本

备份流的安装、升级、配置和部分因选定 Oracle ZDB 方法的不同而有所不同。酌情指示这些差异。

无论 Oracle ZDB 方法如何，配置备份规范及启动或安排备份的过程相同。

备份和还原类型

备份

- 联机“ZDB 到磁盘”、“ZDB 到磁带”和“ZDB 到磁盘 + 磁带”。

  创建复本期间，应用程序系统中的数据库处于热备份模式。如果要执行“ZDB 到磁带”和“ZDB 到磁盘 + 磁带”备份，则随后在备份系统上进行数据到磁带介质的流式传送。

- 脱机“ZDB 到磁盘”、“ZDB 到磁带”和“ZDB 到磁盘 + 磁带”。

  创建复本期间，将关闭应用程序系统中的数据库。因此，在创建复本的一小段时间内数据库不可用。如果要执行“ZDB 到磁带”和“ZDB 到磁盘 + 磁带”备份，则随后在备份系统上进行数据到磁带介质的流式传送。

使用联机和脱机“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”时，在备份系统上完成目标数据库备份之后，将自动启动恢复编目和控制文件的标准 Data Protector (非 ZDB) 备份。但是，可以在创建备份规范时禁止此行为。

注意使用“ZDB 到磁带”时，不执行恢复编目和控制文件备份。Oracle Recovery Manager 实用程序 (RMAN) 感知不到“ZDB 到磁带”会话。

重要说明使用 Data Protector Oracle ZDB 集成无法完成存档日志备份。存档日志和控制文件备份必须遵循标准 Data Protector Oracle 集成备份过程。

> **注意**在 EMC 上，只有在备份系统上安装 Oracle 二进制文件，才能执行决策支持、应用程序测试及类似任务。但在大多数情况下，Data Protector EMC 集成只要求在应用程序系统上安装应用程序二进制文件。

还原

通过使用 Data Protector 与磁盘阵列集成，可以执行以下类型的还原:

- 从备份介质还原到 LAN 上的应用程序系统 (标准 Data Protector 还原) 并对应用程序系统使用 RMAN，您可以:
  - 恢复整个数据库
  - 恢复部分数据库
  - 将整个数据库恢复到特定时间点的状态
- 对应用程序系统使用即时恢复功能和 RMAN，您可以:
  - 执行完整数据库还原和数据库恢复
  - 从增量备份进行恢复 (适用于“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”)
  - 从增量备份链进行恢复 (适用于“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”)
  - 将数据文件还原到其原始位置以外的位置

磁盘阵列	备份类型	恢复整个数据库，直到		将部分数据库恢复到当前状态
现在	时间点、Logseq 号/线程号或 SCN 号			
P9000 XP、EMC、非 HPE 存储阵列	**ZDB 到磁带 - 联机**	还原	还原	还原
	ZDB 到磁带 - 脱机	还原	还原 (必须将数据库置于存档模式)。	还原
P9000 XP、Dell EMC Unity 和 NetApp	**ZDB 到磁盘 - 联机**	即时恢复 + 数据库恢复	即时恢复 + 数据库恢复	不适用
	ZDB 到磁盘 - 脱机	即时恢复	即时恢复 + 数据库恢复 (必须将数据库置于存档模式)。	不适用
	ZDB 到磁盘 + 磁带 - 联机	• 还原 或 • 即时恢复 + 数据库恢复	• 还原 或 • 即时恢复 + 数据库恢复	还原
	ZDB 到磁盘 + 磁带 - 脱机	• 还原 或 • 即时恢复	• 还原 或 • 即时恢复 + 数据库恢复 (必须将数据库置于存档模式)	还原

图例

还原	使用 Data Protector GUI 或 RMAN 脚本将备份介质中的数据库还原到 LAN 上的应用程序系统。
即时恢复 + 数据库恢复	可能存在以下三个选项: • 首先执行即时恢复，然后从 Data Protector 即时恢复 GUI 上下文执行数据库恢复，或者 • 首先执行即时恢复，然后从 Data Protector 还原 GUI 上下文执行数据库恢复，或者 • 首先执行即时恢复，然后使用 RMAN 脚本恢复数据库。
即时恢复	无需数据库恢复即可执行即时恢复。

有关 ZDB 概念和术语的概述，请参阅关键概念。

集成概念

Data Protector Oracle 集成将 Oracle 数据库管理软件与 Data Protector 相关联。从 Oracle 的角度看，Data Protector 代表一种介质管理

软件。另一方面，可将 Oracle 数据库管理系统视为备份的一个数据源，其中备份使用由 Data Protector 控制的介质。

组件

备份和还原过程中涉及的软件组件包括:

- Oracle Recovery Manager (RMAN)
- Data Protector Oracle 集成软件

集成功能概述

Data Protector Oracle 集成代理 (ob2rman.pl) 与 RMAN 一起管理 Oracle 目标数据库上以下操作的所有方面:

- 数据库启动和关闭
- 备份 (备份和复制)
- 恢复 (还原、恢复和复制)

集成的工作原理

ob2rman.pl 执行 RMAN，它指导目标数据库上的 Oracle 服务器进程执行备份、还原和恢复。RMAN 在恢复编目、Oracle 中央信息存储库以及特定目标数据库的控制文件中保留有关目标数据库的必要信息。

ob2rman.pl 向 RMAN 提供的主要信息包括:

- 已分配的 RMAN 通道数
- RMAN 通道环境参数
- 有关要备份或还原的数据库对象的信息

对于备份， ob2rman.pl 使用 Oracle 目标数据库视图来获取有关可用于备份的逻辑 (表空间) 和物理 (数据文件) 目标数据库对象的信息。

对于还原， ob2rman.pl 使用当前控制文件或恢复编目 (如果使用) 来获取有关可用于还原的对象的信息。

使用 Data Protector 与 RMAN 的集成，可以备份和还原 Oracle 控制文件、数据文件和存档重做日志。

Oracle 服务器进程到 Data Protector 的接口由 Data Protector Oracle 集成介质管理库 (**MML**) 提供，该库是一组允许在常规介质代理中读取和写入数据的例程。

除了处理与介质设备的直接交互外，Data Protector 还提供计划功能、介质管理、网络备份、监视和交互式备份。

如果备份包含属于 Oracle Server 实例的所有数据文件和当前控制文件，则该备份称为整个数据库备份。

这些功能可用于 Oracle 目标数据库的联机或脱机备份。但是，必须确保备份对象 (例如表空间) 在备份会话之前和之后切换到适当的状态。对于联机备份，数据库实例必须在 ARCHIVELOG 模式下运行；而对于脱机备份，需要在备份规范中使用 Pre-exec 和 Post-exec 选项准备要备份的对象。

Data Protector 备份规范包含有关备份选项、RMAN 命令、Pre-exec 和 Post-exec 命令、介质和设备的信息。

使用 Data Protector 备份规范可以配置备份，然后多次使用同一规范。此外，计划的备份只能使用备份规范执行。

可以使用 Data Protector 用户界面、RMAN 实用程序或 Oracle Enterprise Manager 实用程序备份和还原 Oracle 目标数据库。

Data Protector Oracle 集成的核心是 MML，它允许 Oracle Server 进程向 Data Protector 发出命令来备份或还原部分或所有 Oracle 目标数据库文件。主要目的是控制与介质和设备的直接交互。

非 ZDB 备份流

Data Protector 备份会话管理器触发 Data Protector 计划或交互式备份，并读取备份规范，然后以备份规范中指定的操作系统用户帐户在 Oracle Server 上启动 ob2rman.pl 命令。此后， ob2rman.pl 准备环境以开始备份，并发出 RMAN 备份命令。RMAN 指示 Oracle Server 进程执行指定的命令。

Oracle Server 进程通过 MML 启动备份，从而建立与 Data Protector 备份会话管理器的连接。备份会话管理器启动常规介质代理，在 MML 与常规介质代理之间建立连接，然后监视备份过程。

Oracle Server 进程从磁盘读取数据，并通过 MML 和常规介质代理将其发送到备份设备。

RMAN 将有关备份的信息写入恢复编目 (如果使用) 或 Oracle 目标数据库的控制文件。

备份会话的消息将发送到备份会话管理器，备份会话管理器将有关备份会话的消息和信息写入 IDB。

Data Protector 常规介质代理将数据写入备份设备。

还原流

可以使用以下方式启动还原会话:

- Data Protector GUI
- RMAN CLI
- Oracle Enterprise Manager GUI

您必须指定要还原的对象。

Data Protector 还原会话管理器触发从 Data Protector 用户界面中还原，并启动 ob2rman.pl 命令。 ob2rman.pl 准备环境以开始还原，并发出 RMAN 还原命令。RMAN 检查恢复编目 (如果使用) 或控制文件以收集有关 Oracle 备份对象的信息。它还与 Oracle Server 进程进行通信，后者通过 MML 启动还原。MML 与还原会话管理器建立连接，并传递有关所需对象和对象版本的信息。

还原会话管理器将执行以下操作: 检查 IDB 以查找适合的设备和介质，启动常规介质代理，在 MML 与常规介质代理之间建立连接，监视还原，并将有关还原的消息和信息写入 IDB。

常规介质代理从备份设备读取数据，并通过 MML 将其发送到 Oracle Server 进程。Oracle Server 进程将数据写入磁盘。

数据库文件也可以通过 **Automatic Storage Management** (**ASM**) 进行管理。这些文件可以驻留在闪回恢复区中。

图例

SM	Data Protector 会话管理器；在备份会话期间为 Data Protector 备份会话管理器，在还原会话期间为 Data Protector 还原会话管理器。
RMAN	Oracle Recovery Manager。
Data Protector MML	Data Protector Oracle 集成介质管理库，它是支持在 Oracle Server 与 Data Protector 之间进行数据传输的一组例程。
备份 API	Oracle 定义的应用程序编程接口。
IDB	Data Protector 内部数据库，在其中写入有关 Data Protector 会话的所有信息，包括会话消息、对象、数据以及使用的设备和介质。
MA	Data Protector 常规介质代理，用于在介质设备中读取和写入数据。

满足 Oracle Server 的先决条件

以下是 Oracle Server 集成的先决条件:

- 熟悉 Oracle 数据库管理和基本的 Data Protector 功能。
- 需要许可证才能使用 Data Protector ZDB 集成与 Oracle 集成。即时恢复和联机扩展需要其他许可证。
- 必须正确安装并配置 Data Protector 磁盘阵列集成 (EMC、P9000 XP 阵列、Dell EMC Unity 或 NetApp Storage)。
- ***使用 ASM 的 Oracle Server 配置:*** 磁盘阵列必须支持创建具有跨卷数据一致性的复本。如果使用 P9000 XP 磁盘阵列系列磁盘阵列，必须支持最小单元拆分操作。
- 必须在应用程序系统上安装 Oracle Server 软件，并且必须在其中打开或装载 Oracle 目标数据库。
- 从 Oracle 12c 开始，Microsoft Windows 上的 Oracle 数据库支持使用在安装时指定的 Oracle 主用户。此 Oracle 主用户用于为 Oracle 主目录运行 Windows 服务，类似于 Linux 上 Oracle 数据库的 Oracle 用户。

  对于在 Oracle 12c 数据库中进行的备份和还原，如果 Oracle 集成代理和介质代理在同一 Windows 主机上运行，为了避免出现共享内存分配问题，应将 Oracle 主用户添加到 Windows 备份操作员组。
- 必须正确配置并打开 Oracle Recovery Catalog Database。
- 必须正确配置 Oracle 网络服务并在应用程序系统上对 Oracle 目标数据库和恢复编目 (如果使用) 运行。Data Protector Oracle 代理需要网络服务才能通过 Oracle 连接到应用程序系统上的 Oracle 数据库。

  请注意，Data Protector Oracle 集成使用 RMAN 进行备份和还原。RMAN 需要使用专用服务器进程连接到目标数据库。为避免配置共享服务器目标数据库时 RMAN 连接到调度程序，RMAN 使用的网络服务名称必须将 (SERVER_DEDICATED) 包含到连接字符串的 CONNECT_DATA 属性中。
- 要成功备份驻留在闪回恢复区中的恢复文件，请确保已正确配置闪回恢复区。

- *Oracle Real Application Cluster (RAC):* 每个节点都必须具有一个用于存储存档日志的专用磁盘。此类磁盘必须由 NFS 装载在所有其他 RAC 节点上。

  但是，如果存档日志不在由 NFS 装载的磁盘上，则必须修改存档日志备份规范。

- **RAC:** 必须在 Oracle RAC 的所有计算机 (节点) 上安装 Data Protector Oracle 集成。必需完成这一步，因为 RMAN 通过 Oracle 网络连接到当前活动节点，并且任何活动节点都需要 SBT 库，它是 Data Protector Oracle 集成的一部分。

- *RAC :* 对于 Oracle 11.2.0.2 及更高版本，必须在共享磁盘上创建控制文件，并且可以从所有 RAC 节点访问该文件， OB2_DPMCTL_SHRLOC 环境变量必须指向这一备份控制文件的位置。

- 在 Windows 系统上，使用 Oracle 备份集 ZDB 方法时，将备份系统上的 omnirc 选项 ZDB_SMISA_AUTOMOUNTING 设置为 2 ，以便能够在本地系统上自动装载卷。

- 配置要与 Data Protector 配合使用的设备和介质。

- 测试 Oracle Server 系统和 Cell Manager 是否正确建立通信: 在 Oracle Server 系统上配置并运行 Data Protector 文件系统备份和还原。

- 确定 Data Protector 将用于备份的 Oracle 数据库“用户”。此用户必须获得 SYSDBA 特权。例如，它可以是在数据库创建期间创建的 Oracle 用户 sys 。对于 Oracle 12c 版本，必须已授予用户 SYSBACKUP 特权。此外，您还可以在 Oracle 12c 中使用具有 SYSDBA 特权的用户，但首先必须将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。

- 在 Windows 系统上，如果 Oracle 目标数据库和 Oracle 恢复编目安装在两个不同的系统上，请在两个系统上均配置一个属于 Administrators 组成员的“域”用户帐户。

  对于受支持的 Windows 操作系统，请使用用户模拟。

- 使用备份集方法时，如果 Oracle 数据库安装在符号链接上，也可以在备份系统上创建这些符号链接。

- 在应用程序系统中，使用 SQL*Plus 通过指定用户、密码和网络连接标识符连接到目标数据库和恢复编目。以数据库管理员的身份连接到目标数据库，然后以恢复编目所有者的身份连接到恢复编目数据库。

  示例

  如果目标数据库的用户名为 system 、密码为 manager 、网络服务名称为 PROD ，恢复编目的用户名和密码为 rman 、网络服务名称为 RMANCAT ，则命令 s 将类似于:

  ```
  sqlplus /nolog
  ```

  ```
  SQL> connect system/manager@PROD as sysdba; 已连接。 SQL> connect rman/rman@RMANCAT; 已连接。
  ```

  - 仅对“联机备份”启用 Oracle 自动日志存档:

    1. 关闭应用程序系统上的 Oracle 目标数据库实例。
    2. 使用文件系统备份来备份整个数据库。
    3. 选择存档日志位置:
       - 如果使用 SPFILE:

         执行：

         ```
         alter system set log_archive_dest=path_to_archive_logs SCOPE=SPFILE;
         ```

       - 如果使用 init.ora 文件:

         执行：

         ```
         log_archive_start=true
         ```

         ```
         log_archive_dest=path_to_archive_logs
         ```

         文件的默认路径为:

         Windows 系统： ORACLE_HOME\database\initDB_NAME.ora

         UNIX 系统： ORACLE_HOME/dbs/initDB_NAME.ora

         其中 DB_NAME 是 Oracle 数据库实例的名称。
    4. 装载目标数据库并启用存档日志模式，启动 SQL*Plus，然后键入:

       ```
       startup mount alter database archivelog; alter database open;
       ```

       示例

       如果目标数据库的用户名为 system 、密码为 manager 、实例名称为 PROD ，恢复编目的用户名和密码为 rman ，则命令将类似于:

       ```
       sqlplus /nolog SQL> connect system/manager@PROD as sysdba; 已连接。 SQL> startup mount; SQL> alter database archivelog; 语句已处理。 SQL> archive log start; 语句已处理。 SQL> alter database open;
       ```

    5. 备份整个数据库。

运行 Oracle ZDB 会话之前，请考虑以下几点:

- 无法使用应用程序系统中同一源卷同时启动 ZDB、还原或即时恢复会话。只有使用应用程序系统中同一源卷的先前会话完成 ZDB 会话或还原之后，才能启动 ZDB、还原或即时恢复；否则，会话将失败。
- 对于备份集方法，如果 Oracle 数据库安装在符号链接上，则必须也在备份系统上创建这些链接。
- 在 P9000 XP 阵列上，如果使用 LVM 镜像配置，Data Protector 将在备份期间显示警告，因为应用程序系统中的卷组源卷没有分配 BC P9000 XP 对。应忽略此消息。
- 如果控制文件、SPILE 或联机重做日志与数据文件位于同一源卷，并且选择了“跟踪复本以用于即时恢复”选项，将中止备份会话。在这种情况下，需要重新配置数据库或设置 ZDB_ORA_INCLUDE_CF_OLF 、 ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECKCONF_IR omnirc 选项。

- 必须在要还原或复制数据库的系统上创建 Oracle 实例。
- 如果要还原整个数据库，则数据库必须处于 Mount 状态；如果要还原控制文件或执行数据库复制，则数据库必须处于 NoMount 状态。
- 必须能够连接到数据库。

  实现此目标的一种方法是为 Oracle 侦听程序配置静态服务信息。您可以在Oracle 数据库即时恢复失败故障诊断中查看静态服务信息配置示例。

- 在 Windows 系统上，使用 Oracle 备份集 ZDB 方法从备份执行还原时，将应用程序系统中的 omnirc 选项 ZDB_SMISA_AUTOMOUNTING 设置为 2 ，以便在本地系统上启用自动卷装载。
- 必须备份包含已存档日志的整个主数据库。
- 存档日志 (自上次完整备份以来尚未备份到磁带并且在复制时必须提供的日志) 必须在复制系统上可用，且其路径名与目标系统 (具有要复制的生产数据库的系统) 相同。
- 必须配置辅助实例的网络服务名称。
- 在目标数据库所在的同一系统上复制数据库时，请相应地设置所有 *_PATH 、 *_DEST 、 DB_FILE_NAME_CONVERT 和 LOG_FILE_NAME_CONVERT 初始化参数。这样，重复的数据库文件便不会覆盖目标数据库文件。

在开始还原 Oracle 数据库之前，必须满足以下要求:

- 确保已打开恢复编目数据库。如果无法使恢复编目数据库联机，则可能需要还原恢复编目数据库。
- 检查计划还原的备份会话使用了哪种 ZDB 方法 (proxy-copy 还是备份集)。
- 必须有控制文件。如果没有控制文件，则必须将其还原。

  如果必须对恢复编目数据库或控制文件执行还原，则必须首先执行此还原。只有这样，您才能对 Oracle 数据库的其他部分执行还原。

  如果确定恢复编目数据库或控制文件已准备就绪，请启动恢复编目数据库。

- 确保设置了以下环境变量:
  - ORACLE_BASE
  - ORACLE_HOME
  - ORACLE_TERM
  - PATH
  - NLS_LANG
  - NLS_DATE_FORMAT

  Windows 系统示例

  ```
  ORACLE_BASE=Oracle_home

  ORACLE_HOME=Oracle_home\product\10.1.0

  ORACLE_TERM=HP

  PATH=$PATH:Oracle_home\product\10.1.0\bin

  NLS_LANG=american

  NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'
  ```

  UNIX 系统示例

  ```
  ORACLE_BASE=/opt/oracle

  ORACLE_HOME=/opt/oracle/product/10.1.0

  ORACLE_TERM=HP

  PATH=$PATH:/opt/oracle/product/10.1.0/bin

  NLS_LANG=american

  NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'
  ```

- 检查 /etc/oratab 文件是否包含以下行:

Windows 系统： PROD:Oracle_home\product\10.1.0:N

UNIX 系统： PROD:/opt/oracle/product/10.1.0:N

最后一个字母用于确定启动时数据库是 (Y) 否 (N) 自动启动。

- 备份时必须可在应用程序系统上找到反映内部数据库结构的控制文件。如有必要，从磁带备份还原相应的控制文件。
- 必须打开恢复编目。

以下限制适用：

- 如果数据库安装在原始磁盘上，则不支持 Oracle 备份集 ZDB 方法。
- 仅 IPv6 客户机不支持使用 Oracle 备份集 ZDB 方法备份 Oracle 控制文件。

为 Oracle EMC Unity 复制配置 Oracle 服务器

Data Protector 提供了适用于 VMware 虚拟机 (VM) 内的代理的 Dell EMC Unity 即时恢复。仅物理原始设备映射 (RDM) 支持此功能。

要在 Linux 和 Windows 上执行即时恢复，请执行以下步骤:

1. 使用 sqlplus 命令关闭 Oracle 数据库实例。如果是 RAC，请关闭所有实例。例如：/sqlplus /nolog connect sys/oracle@APPN as sysdba sql> shutdown immediate sql> exit
2. 在应用程序主机上启用 omnirc 选项: ZDB_IR_MANUAL_AS_PREPARATION=1
3. 对于 Linux：在 IR 会话前卸除卷: # umount /dev/3PAR_ESX2/lvol0 For Windows: 在 IR会话前使磁盘脱机。
4. 准备应用程序主机以删除卷 (导出、停用和备份卷组)。
5. 从 vCenter Server 上的应用程序主机中删除硬盘。
6. 重新扫描 VM 上的卷，并确认该磁盘在应用程序主机上不再可用。
7. 执行即时恢复。**注意:** 如果您使用的是 Oracle 集成，请确保取消选中“恢复”复选框。
8. 从 vCenter Server 将硬盘添加回应用程序主机。
9. 重新扫描应用程序主机是否存在新卷。
10. 添加导出的卷组。
11. 对于 Linux：装载卷。对于 Windows：连接磁盘。
12. 遵循即时恢复后的 Oracle 数据库恢复一节中所述的步骤。

安装 Oracle Server ZDB 客户机

假设 Oracle Server 已启动并正在运行。为了能够备份 Oracle 数据库，您需要在安装过程中选择“Oracle 集成”组件。

OpenVMS

在 OpenVMS 上，在安装并配置 Oracle 集成之后，验证 OMNI$ROOT:[CONFIG.CLIENT]omni_info 中是否存在 -key Oracle8 条目，例如：-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath “” -uxpath “” -version 10.30

如果不存在该条目，请从 OMNI$ROOT:[CONFIG.CLIENT]omni_format 复制它。否则，Oracle 集成在 OpenVMS 客户机上不会显示为已安装。

P9000 XP 磁盘阵列系列与 Oracle Server 集成

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。最好将它安装在独立系统、非镜像磁盘上。使恢复编目保持为未注册状态。有关如何安装数据库的详细信息，请参见 Oracle 文档。
2. 安装以下 Data Protector 软件组件：
   - P9000 XP Agent – 在应用程序系统和备份系统上
   - Oracle Integration – 在应用程序系统和备份系统上

只有对于备份集 ZDB 方法，备份系统上才需要 Data Protector Oracle 集成组件。对于代理复制 ZDB 方法则不需要它。

在 RAC 群集环境中，Oracle 应用程序数据库通过多个 Oracle 实例进行访问。因此，请在运行 Oracle 实例的所有系统上安装 Data Protector Oracle 集成和 P9000 XP 代理组件。如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

存储阵列与 Oracle Server 的集成

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。最好将它安装在独立系统、非镜像磁盘上。使恢复编目保持为未注册状态。
2. 安装以下 Data Protector 软件组件：
   Storage Provider for the Storage Array (NetApp Storage Provider) – 在应用程序系统和备份系统上
   Oracle Integration – 在应用程序系统和备份系统上

> 注意
>
> - 只有对于备份集 ZDB 方法，备份系统上才需要 Data Protector Oracle 集成组件。对于代理复制 ZDB 方法则不需要它。
> - 如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

以下限制适用：

- 不支持 RAC 群集环境。
- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

Oracle 备份集 ZDB 概念

This feature is available in the Premium Edition

使用 Oracle 备份集 ZDB 方法时，通过 Oracle API 将要备份的全部数据提供至 Data Protector - 通过 Data Protector Oracle 集成 MML 流式传送数据。

根据 Oracle 控制文件、联机重做日志文件和 SPFILE 的位置，有以下两个可能选项:

- Oracle 控制文件、联机重做日志文件和 SPFILE 位于“不同于”Oracle 数据文件的其他卷组 (如果使用了 LVM) 或源卷。

  默认情况下，启用对此类配置进行即时恢复。

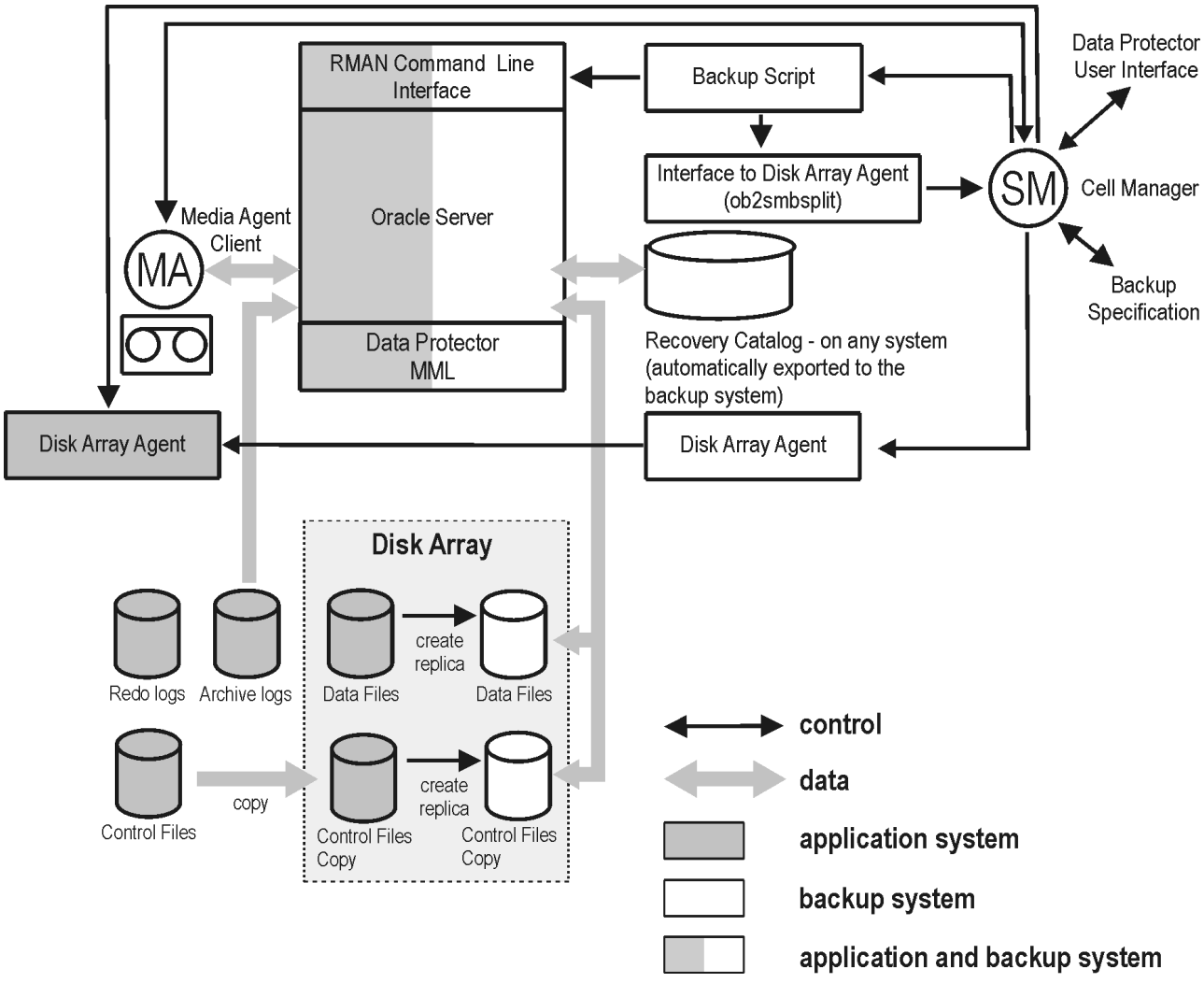
- Oracle 控制文件、联机重做日志文件、SPFILE 位于与 Oracle 数据文件“相同”的卷组 (如果使用了 LVM) 或源卷。

  默认情况下，“不”启用对此类配置进行即时恢复。可以通过将 ZDB_ORA_INCLUDE_CF_OLF 、 ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECKCONF_IR omnirc 选项设置为 1 来启用即时恢复。

> **重要说明**请注意，如果通过设置上述选项来启用即时恢复，即时恢复期间将覆盖控制文件，SPFILE 和联机重做日志。

Oracle 存档重做日志文件不一定要位于源卷上。

Oracle 备份集 ZDB 概念



Oracle 备份集 ZDB 概念仅显示默认集成行为，其中 Oracle 控制文件、联机重做日志文件和 SPFILE 位于不同于 Oracle 数据文件的其他卷组

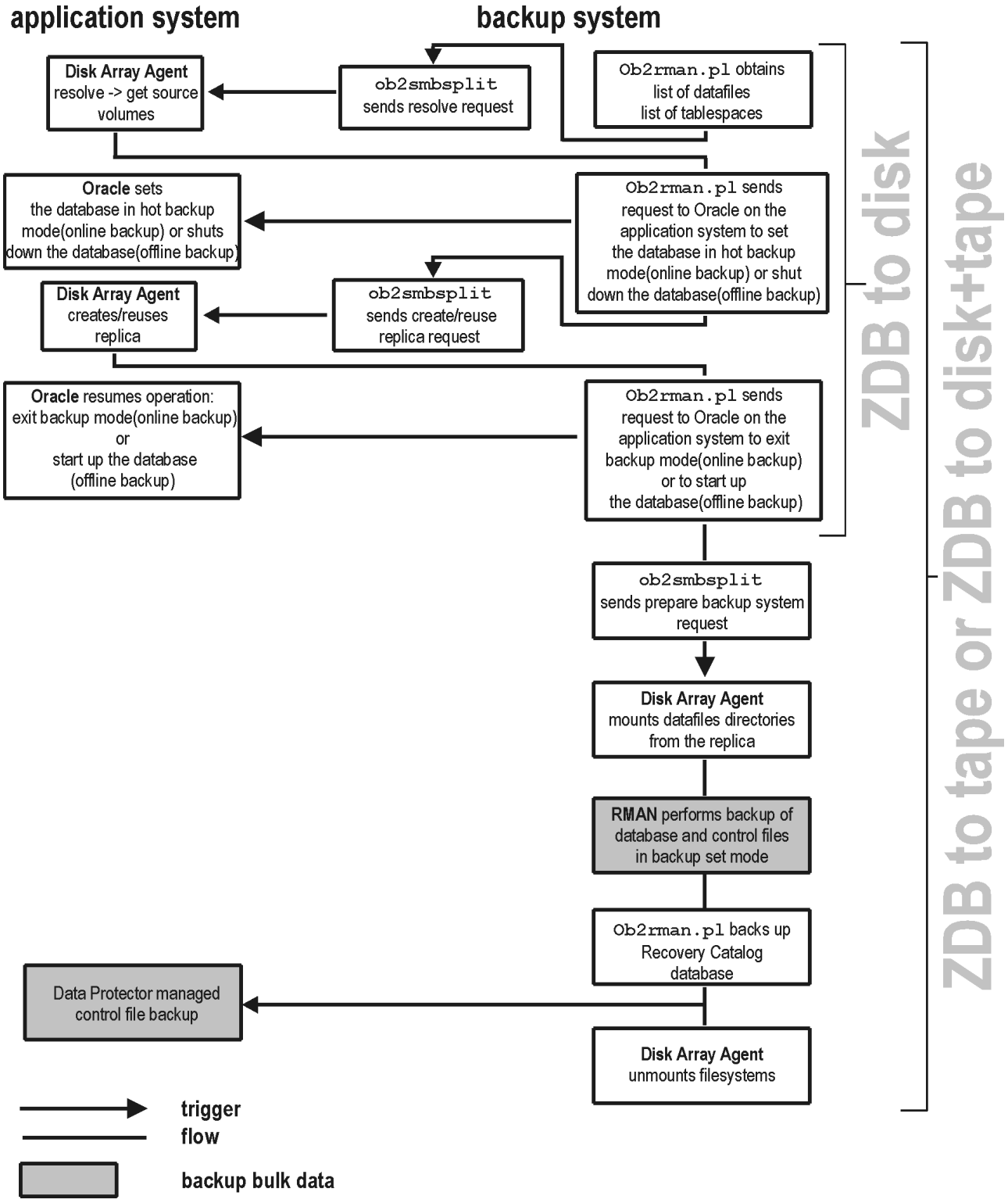
(如果使用了 LVM) 或源卷。Oracle 数据库文件也可以通过 ASM 管理，但某些限制适用于 Oracle ASM 配置。

图例

MA	常规介质代理将复本中的数据写入备份介质。常规介质代理通常驻留在备份系统上。
SM	会话管理器控制备份和还原会话，并将会话信息写入 IDB。
磁盘阵列代理	磁盘阵列代理 (ZDB 代理) 是指 SYMA (适用于 EMC)、SSEA (适用于 P9000 XP 阵列) 和 SMISA (适用于非 HPE 存储阵列)。
Data Protector MML	Data Protector Oracle 集成介质管理库，它是支持在 Oracle Server 与 Data Protector 之间进行数据传输的一组例程。这是一个链接到 Oracle 软件的 Data Protector 软件库。

备份过程

Oracle 备份集 ZDB 流



注意ZDB 代理是指 SYMA (适用于 EMC)、SSEA (适用于 P9000 XP 阵列) 和 SMISA (适用于非 HPE 存储阵列)。

本节仅提供有关 Data Protector Oracle ZDB 集成的信息。

以下复本操作（装载、激活卷/磁盘组...）依赖于 ZDB 选项，或由 ZDB 选项触发。

- Data Protector 对备份系统执行 ob2rman.pl 命令。此命令从应用程序系统的 Oracle 数据库中检索要备份的文件或磁盘映像列表，并启动解析进程。该列表仅用于确定要复制的源卷。如果配置期间指定了控制文件副本位置，则 ob2rman.pl 将控制文件复制到应用程序系统上的指定目录。此目录必须驻留在磁盘阵列源卷上。

- 执行“联机”ZDB 会话时，ob2rman.pl 通过发出 sqlplus 命令 “ALTER TABLESPACE BEGIN BACKUP 将 Oracle 目标数据库设置为备份模式，启动相应过程为安装数据库的源卷创建复本；创建复本后，发出 sqlplus 命令 “ALTER TABLESPACE END BACKUP ”使数据库退出备份模式。

  执行“脱机”ZDB 会话时，ob2rman.pl 关闭 Oracle 数据库，启动相应过程为安装数据库的源卷创建复本；创建复本后，启动 Oracle 数据库。

- ob2rman.pl 启动相应过程以在备份系统上准备复本。在此步骤中，将启用备份系统上的卷/磁盘组，除非数据库安装在原始分区，否则将装载到具有 Oracle 数据库文件的装载点。
- 然后，ZDB 代理将备份系统上的数据库装载到与应用程序系统上的装载点同名 (由 Data Protector 创建) 的装载点。

> **注意**备份系统的相关装载点上不得装载任何内容，否则解析和备份将失败。

- 如果正在执行“ZDB 到磁盘”会话，则此时将处理剩余的 ZDB 选项，并将会话详细信息写入 ZDB 数据库。会话完成。不执行此说明中的以下步骤，从而避免向 RMAN 提供有关“ZDB 到磁盘”会话的任何信息。
- 如果正在执行“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”会话，则继续进行如下处理:
  - ob2rman.pl 在备份系统上启动 Oracle 备份命令 RMAN，然后将 Oracle RMAN 备份命令脚本发送到 RMAN cmdfile (输入命令文件)。
  - RMAN 与备份系统上的 Oracle 数据库实例联系，后者通过 SBT API 与 Data Protector 联系并启动备份。
  - 备份系统上的 Oracle 数据库实例从复本读取数据并将其发送到 Data Protector 常规介质代理以写入备份设备。
  - 数据传输结束后，将禁用备份系统 (卸除所有平台的文件系统并停用 UNIX 系统的卷/磁盘组) 并重新建立链接。
  - 在备份系统上完成目标数据库备份后，将自动备份恢复编目和控制文件。但是，可以在创建备份规范时禁止此行为。

> **注意**未创建存档日志复本；因此，应按照标准 Data Protector Oracle 存档日志备份过程，从应用程序系统备份存档日志。

Oracle proxy-copy ZDB 概念

This feature is available in the Premium Edition

Data Protector Oracle 集成 MML 支持代理复制功能。这样 Data Protector 能够使用文件系统备份方法执行备份。

根据 Oracle 控制文件、联机重做日志文件和 SPFILE 的位置，有以下两个可能选项:

- Oracle 控制文件、联机重做日志文件和 SPFILE 位于“不同于”Oracle 数据文件的其他卷组 (如果使用了 LVM) 或源卷。

  默认情况下，如果在 GUI 中选择此选项，将启用即时恢复。

- Oracle 控制文件、联机重做日志文件和 SPFILE 位于与 Oracle 数据文件“相同”的卷组 (如果使用了 LVM) 或源卷。

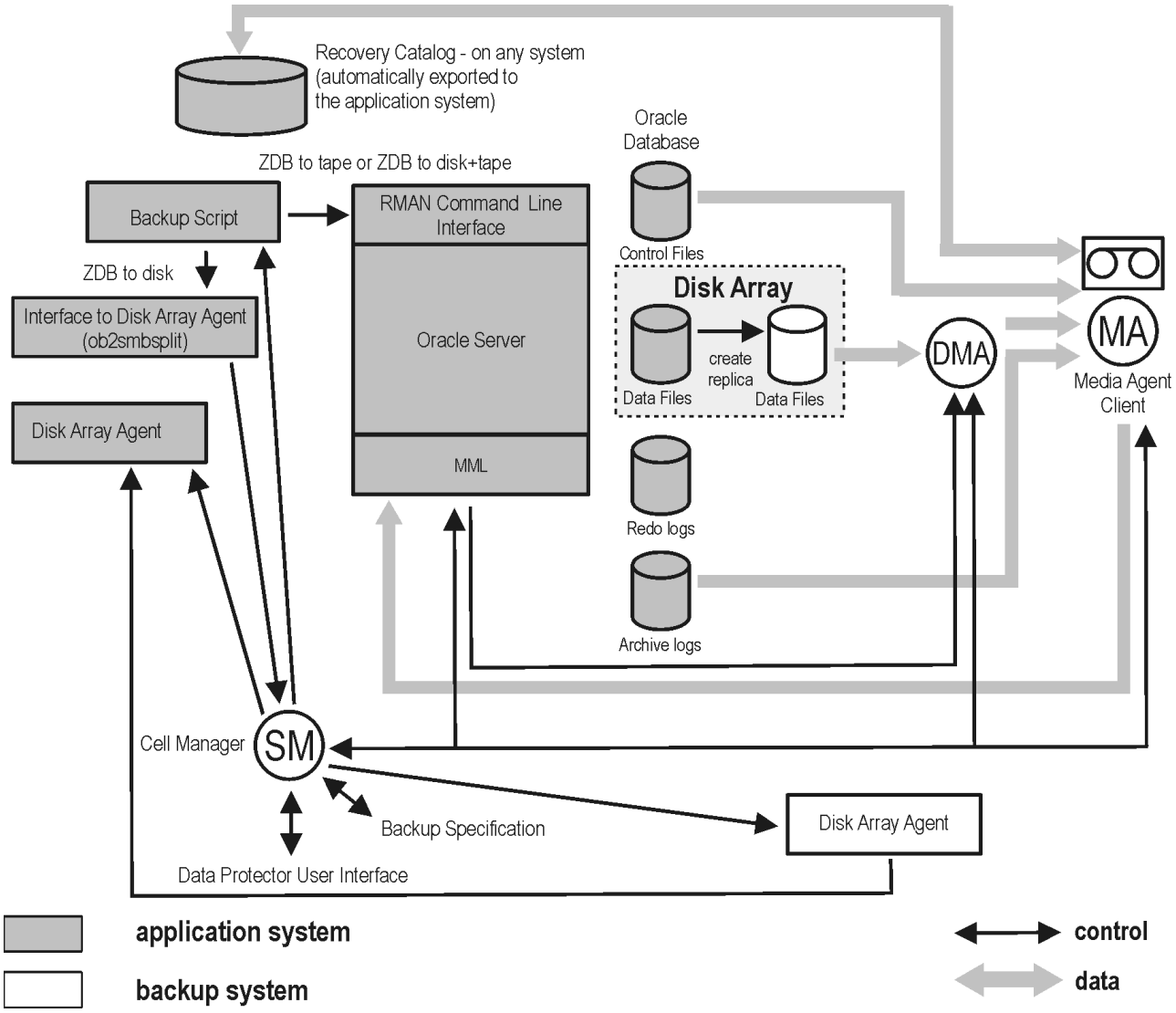
  默认情况下，即使在 GUI 中选择此选项，也“不”启用即时恢复。可以通过将 ZDB_ORA_INCLUDE_CF_OLF 、 ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECKCONF_IR omnirc 选项设置为 1 来启用即时恢复。

  重要说明请注意，如果通过设置上述选项来启用即时恢复，即时恢复期间将覆盖控制文件，SPFILE 和联机重做日志。

Oracle 存档重做日志文件不一定要位于源卷上。

Oracle proxy-copy ZDB 概念显示了 Data Protector Oracle ZDB 集成体系结构。该图阐明在备份系统上执行备份的配置。它展示了默认集成行为，其中 Oracle 控制文件、联机重做日志文件和 SPFILE 驻留在与 Oracle 数据文件不同的磁盘阵列源卷。

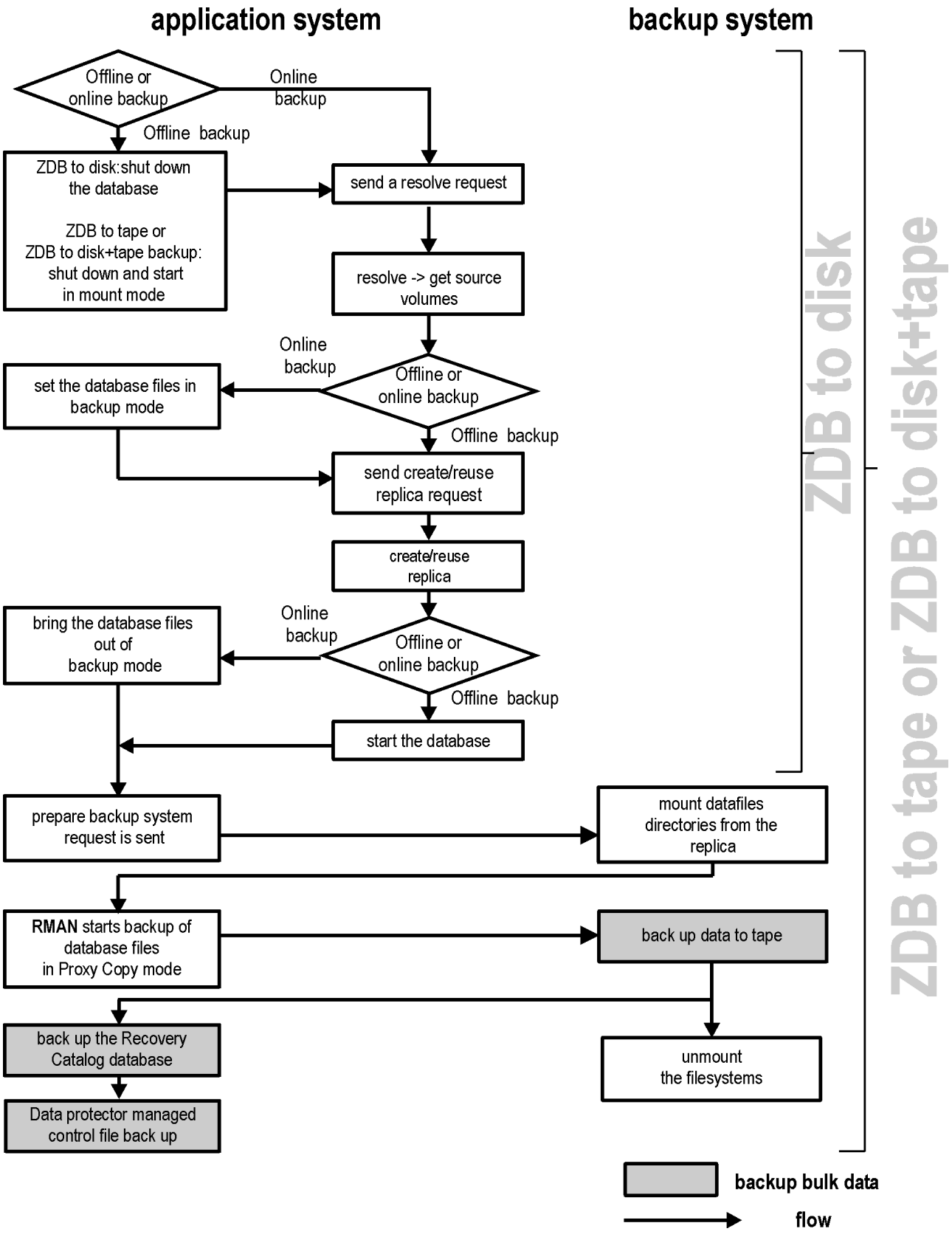
Oracle proxy-copy ZDB 概念



MA	常规介质代理将复本中的数据写入备份介质。常规介质代理通常驻留在备份系统上。
SM	会话管理器控制备份和还原会话，并将会话信息写入 IDB。
磁盘阵列代理	磁盘阵列代理 (ZDB 代理) 是指 SYMA (适用于 EMC)、SSEA (适用于 P9000 XP 阵列) 和 SMISA (适用于非 HPE 存储阵列)。
MML	Data Protector Oracle 集成介质管理库，它是支持在 Oracle Server 与 Data Protector 之间进行数据传输的一组例程。这是一个链接到 Oracle 软件的 Data Protector 软件库。

备份过程

Oracle proxy-copy ZDB 流



本节仅提供有关 Data Protector Oracle ZDB 集成的信息。

以下复本操作 (装载、激活卷/磁盘组...) 依赖于 ZDB 选项，或由 ZDB 选项触发。

- 如果是“脱机”“ZDB 到磁盘 + 磁带”和“ZDB 到磁带”会话，ob2rman.pl 将关闭处于装载状态的数据库实例，然后再将其打开。对于脱机和联机“ZDB 到磁盘 + 磁带”和“ZDB 到磁带”会话，Data Protector 将在 proxy-copy 模式下启动 RMAN。

  如果是“脱机”“ZDB 到磁盘”会话，将关闭数据库。

- Data Protector 从 Oracle 数据库中检索要纳入复本创建流程的文件或磁盘映像列表，然后启动解析过程。该列表仅用于确定要复制的源

卷。

如果是“ZDB 到磁盘”会话，若配置期间指定了控制文件副本位置，则 Data Protector 将控制文件复制到应用程序系统上的指定目录。此目录必须驻留在磁盘阵列源卷上。

- 如果是“联机”备份，Oracle 目标数据库将切换到备份模式。
- ob2smbsplit 或 MML 启动相应过程，为安装数据库的源卷创建复本。
- 如果是“联机”备份，则创建复本后数据库文件将退出备份模式。

  如果是“脱机”备份，则创建复本后发送 Oracle alter database open 命令。
- Data Protector (适用于“ZDB 到磁盘”) 或 MML (适用于“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”) 启动相应过程以在备份系统上准备复本。在此步骤中，将启用备份系统 (UNIX 系统) 上的卷/磁盘组，除非数据库安装在原始磁盘，否则将装载到包含 Oracle 数据库文件的装载点。
- 然后，ZDB 代理将备份系统上的数据库装载到与应用程序系统上的装载点同名 (由 Data Protector 创建) 的装载点。
- 如果正在执行“ZDB 到磁盘”会话，则此时将处理剩余的 ZDB 选项，并将会话详细信息写入 ZDB 数据库。会话完成。不执行此说明中的以下步骤，从而避免向 RMAN 提供有关“ZDB 到磁盘”会话的任何信息。
- 应用程序系统上的 MML 向备份系统上的 Data Protector“数据移动代理”(DMA) 发送请求，以将数据文件备份到磁带。
- DMA 从备份系统读取数据并将其发送到常规介质代理，以将实际数据写入备份设备。

  DMA 还可用于禁止常规介质代理请求访问应用程序系统。因此，由于在备份系统上执行备份，应用程序系统上运行的数据库的性能大大降低。
- 数据传输结束后，将禁用备份系统 (卸除所有平台的文件系统并停用 UNIX 系统的卷/磁盘组) 并重新建立链接。
- 在备份系统上完成目标数据库备份后，将自动备份恢复编目和控制文件。但是，可以在创建备份规范时禁止此行为。

注意未创建存档日志复本；因此，应按照标准 Data Protector Oracle 存档日志备份过程，从应用程序系统备份存档日志。

配置 Oracle Server ZDB 集成

This feature is available in the Premium Edition

备份集方法

- 确保备份系统和应用程序系统上的 Oracle 软件具有相同的目录结构。这意味着两个 Oracle 安装程序的 ORACLE_HOME 必须相同。
- 确保应用程序系统和备份系统上的以下文件相同。此外还要检查权限与应用程序系统的权限是否相同:
  - names.ora

    默认路径: ORACLE_HOME /network/admin/names.ora
  - init DB_NAME .ora

    默认路径: ORACLE_HOME /dbs/init*DB_NAME*.ora 。
  - orapw DB_NAME

    默认路径: ORACLE_HOME /dbs/orapw DB_NAME
  - admin/ DB_NAME

    默认路径: ORACLE_BASE /admin/ DB_NAME

  确保应用程序系统和备份系统上的 Oracle 网络服务具有相同的目录结构。可以通过以下方式实现: NFS 文件共享，手动将应用程序系统中的文件复制到备份系统；或者，使用 UNIX rdist 或 tar 命令来分发应用程序系统中的文件。
- 测试 Oracle 用户是否能够以 Oracle 数据库管理员的身份登录 Oracle 目标数据库，并以 Oracle 恢复编目所有者的身份从备份系统登录 Oracle 恢复编目数据库:
  1. 导出 ORACLE_HOME 、 DB_NAME ，在 UNIX 系统上还要导出 SHLIB_PATH 变量。
  2. 使用 SQL*Plus，通过指定用户 (恢复编目所有者)、密码和网络连接标识符来连接到 Oracle 恢复编目数据库。
  3. 以具有 SYSDBA 角色的 Oracle 数据库管理员的身份使用 Oracle 网络软件本地连接到 Oracle 目标数据库。

     示例

     如果目标数据库的 DB_NAME 为 PROD 、Oracle 恢复编目数据库的 DB_NAME 为 RMANCAT ，并且 ORACLE_HOME 为 /oracle/PROD ，则命令将类似于:

     ```
     su - ora id uid=101(ora) gid=101(dba) export DB_NAME=PROD oracle/PROD/bin/sqlplus SQL> connect rman/rman@RMANCAT 已连接。 SQL> connect system/manager as sysdba SQL> connect system/manager@PROD as sysdba; 已连接。
     ```
- 测试用户 root 和 Oracle 管理员 (例如，用户 oracle) 是否可以在备份系统上使用 RMAN 命令连接到目标数据库和恢复编目数据库:
  1. 以 Oracle 数据库管理员的身份登录到备份系统 (例如，用户 oracle)。
  2. 执行 RMAN 命令并连接到目标数据库和恢复编目数据库。

  示例

  如果目标数据库的 DB_NAME 为 PROD 、Oracle 恢复编目数据库的 DB_NAME 为 RMANCAT ，并且 ORACLE_HOME 为 /oracle/PROD ，则命令将类似于:

  ```
  su - ora id uid=101(ora) gid=101(dba) export DB_NAME=PROD rman target system/manager catalog rman/rman Recovery Manager: Release 10.1.0.2.0 - Production RMAN-06005: 已连接目标数据库: PROD RMAN-06008: 已连接恢复编目数据库 RMAN> exit Recovery Manager 已完成。
  ```

在 ASM 环境中配置 P9000 XP 磁盘阵列系列

在使用自动存储管理 (ASM) 的 Oracle Server 配置中，只要满足以下先决条件，则 P9000 XP 磁盘阵列系列支持 ZDB 和即时恢复:

- 数据文件、控制文件和重做日志文件必须驻留在单独的存储卷 (LUN)。如果计划执行即时恢复，则需要部署此配置。
- 磁盘阵列必须支持最小单元拆分操作:
  - 每个存储卷 (LUN) 必须由单个 LDEV 组成。
  - ASM 托管文件所在的存储卷必须属于具有唯一 ID 和非零 ID 的一致性组 (CTG)。必须在备份规范中同时选择属于同一 CTG 的多个存储卷。否则，备份会话将失败。如果计划将备份数据文件、控制文件和日志文件备份到单独的会话中，则对应的存储卷必须驻留在不同的一致性组。

    根据您的环境，在应用程序系统上设置以下 omnirc 选项:
    - SSEA_ATOMIC_SPLIT
    - SSEA_ATOMIC_SPLIT_MULTIPLE_CTGROUPS

- SSEA_ATOMIC_SPLIT_MIXED_CONFIG

必须至少设置一个选项才能启用最小单元拆分操作。

- 如果 ASM 实例名称与 +ASM 不同，请通过在应用程序系统上设置 Data Protector omnirc 选项 ORA_ASM_LCL_INSTANCE 来指定正确的名称。
- 其他即时恢复要求:
  - 在群集环境的活动群集节点中，将 Data Protector omnirc 选项 ORA_ASM_LCL_INSTANCE 设置为该节点上运行的 ASM 实例的名称。
  - 如果 Oracle ASM 实例管理多个数据库的文件，则必须重新配置 Oracle Server 以便为每个数据库使用单独的 ASM 磁盘组。
  - 备份后不得更改 ASM 磁盘组的名称。
  - 必须禁用 Oracle Server ASM 的自动扩展功能。

群集感知系统

在群集环境中，如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称。按如下方式在 Oracle Server 系统上设置该变量:

Windows 系统： set OB2BARHOSTNAME=virtual_server_name

UNIX 系统： export OB2BARHOSTNAME=virtual_server_name

*RAC：*在要运行备份和还原的每个节点上配置 Oracle 数据库。

使用 RAC 的 HP-UX: 如果要使用虚拟主机名启用即时恢复，请创建“仅”包含虚拟 IP 和虚拟主机名参数的 Serviceguard 包并将其分散到 RAC 节点。

将 Oracle Server 与 Data Protector MML 链接在一起

要使用 Data Protector Oracle 集成，需要在运行 Oracle 实例的每个系统上将 Oracle Server 软件与 Data Protector Oracle 集成“介质管理库”(MML) 链接在一起。

无需手动将 Oracle Server 与 Data Protector MML 链接在一起。使用 Data Protector GUI 或 CLI 启动备份或还原时，Data Protector 会自动将 Oracle Server 与特定于平台的相应 Data Protector MML 链接在一起。但是，出于测试目的，可以覆盖此自动选择。可以通过设置 Data Protector SBT_LIBRARY 参数来手动指定应使用哪个特定于平台的 Data Protector MML。

当 Oracle Server 需要使用 Data Protector 在设备中写入或读取数据时，它会调用 MML。

Oracle 12c CDB 和 PDB 模式支持

为了备份和还原数据，在 Oracle 12c 中引入了一项名为可插拔数据库 (PDB) 的新功能。PDB 是体系结构、体系结构对象和非体系结构对象的可移植集合，以非容器数据库 (非 CDB) 的形式向 Oracle Net 客户机显示。CDB 包括零个、一个或多个客户创建的可插拔数据库 (PDB)。在 Oracle 12c 中，PDB 位于容器数据库 (CDB) 下。

每个 CDB 都具有以下容器:

- 恰好一个“根”

  根用于存储 Oracle 提供的元数据和常用用户。Oracle 提供的 PL/SQL 包的源代码就是元数据的一个示例。常用用户是每个容器中已知的数据库用户。根容器名为 CDB$ROOT。

- 恰好一个“种子 PDB”

  种子 PDB 是系统提供的一个模板，CDB 使用该模板来创建新的 PDB。种子 PDB 名为 PDB$SEED。无法在 PDB$SEED 中添加或修改对象。

- **零个或多个用户创建的 PDB**

  PDB 是用户创建的实体，其中包含特定功能集所需的数据和代码。例如，PDB 可以支持特定应用程序，例如人力资源或销售应用程序。

备份存档和还原 (BAR) GUI 将列出容器数据库中的所有 PDB，应启用仅选择一个或选择多个可插拔数据库。

以下是还原方案:

- 同时还原 CDB 和 PDB
- 还原 CDB，但不还原 PDB
- 还原一个 PDB 和一个测试数据库

配置 Oracle 用户帐户

确定要用于运行备份的用户帐户。Data Protector 需要以下用户帐户:

- Oracle 操作系统用户帐户
- Oracle 数据库用户帐户

配置 Oracle 操作系统用户帐户

对于每个 Oracle 数据库，Data Protector 都需要一个具有 Oracle 权限的操作系统用户帐户才能备份数据库。此用户帐户通常属于 DBA 用户组 (“OSDBA 用户”)。用于运行 Oracle 数据库的用户帐户具有这些权限。例如，要在 UNIX 系统上查找此类用户，请执行以下命令:

ps -ef|grep ora_pmon_ *DB_NAME*

或

ps -ef|grep ora_lgwr_ *DB_NAME*

下表说明如何在不同的操作系统上配置用户:

客户机系统	描述
UNIX 系统	确保已将 Oracle Inventory 组 (oinstall) 中的 Oracle 用户 oracle 添加到 Data Protector admin 用户组。 将应用程序系统和备份系统中的 OSDBA 用户帐户和 root 用户帐户添加到 Data Protector admin 或 operator 用户组。备份系统上的 OSDBA 用户必须具有与应用程序系统上的 OSDBA 用户相同的数值用户 ID 和组 ID (例如， uid=101(ora) gid=101(dba))。 **提示**要查找用户 ID，请使用此用户帐户连接到系统并执行: #id
Windows 系统	在 Windows 系统上，Data Protector 使用相关系统上的 Data Protector Inet 服务连接到 Oracle 数据库。默认情况下，该服务在 Local System account “本地系统帐户”下运行，该帐户会自动添加到 Data Protector admin 用户组。但是，如果已使用 OSDBA 用户帐户重新启动应用程序系统和备份系统上的 Data Protector Inet 服务，需要将新用户添加到 Data Protector admin 或 operator 用户组。

注意只有在计划使用 Oracle 备份集 ZDB 方法时，才需要将备份系统的 OSDBA 用户帐户添加到 Data Protector 用户组。

群集

在群集环境中，确保将以下用户添加到 Data Protector admin 或 operator 用户组:

- 适用于所有物理节点的 OSDBA 用户
- 适用于虚拟服务器的 OSDBA 用户 (适用于 Serviceguard 群集)
- **UNIX 系统：** root 所有物理节点的用户

配置 Oracle 数据库用户帐户

标识或创建以下 Oracle 数据库用户帐户。需要在配置 Oracle 数据库时提供这些用户帐户，如配置 Oracle 数据库中所述。

Oracle 数据库用户帐户

用户	描述
主数据库用户	需要登录到主数据库。

恢复编目用户	恢复编目的所有者 (例如， rman)。登录编目数据库时需要。使用恢复编目时需要。 确保 Oracle 恢复编目的所有者: • 被授予 CREATE ANY DIRECTORY 和 DROP ANY DIRECTORY 系统特权，使用数据抽取导出 (expdp) 和数据抽取导入 (impdp) 实用程序需要这些特权。 • 对 sys.v$instance 视图拥有 SELECT 权限。启动 SQL*Plus 并键入: grant select on v_$instance to recovery_catalog_user; • 被授予 EXEMPT ACCESS POLICY 权限
备用数据库用户	登录备用数据库时需要。仅适用于 Oracle Data Guard 环境。备份备用数据库时需要。

配置 Oracle 数据库

在配置 Oracle 数据库时，需要为 Data Protector 提供以下数据:

- Oracle Server 主目录
- 目标数据库的登录信息
- (可选) 恢复编目数据库的登录信息
- (可选) 备用数据库的登录信息
- (可选) ASM 相关信息。
- 要使用的备份方法和相关选项

配置期间， util_oracle8.pl 命令 (在应用程序系统上启动) 将指定参数保存到 Cell Manager 的 Data Protector Oracle 数据库特定配置文件中。

确保在配置过程中数据库已打开，并且您可以连接到该数据库。

要配置 Oracle 数据库，可使用 Data Protector GUI 或 Data Protector CLI。

> **注意**使用 ASM 执行 Oracle Server 配置时，为了能够执行即时恢复，必须使用 Data Protector CLI 配置 Oracle 数据库。这是因为无法使用 Data Protector GUI 设置 ASM 相关参数。但是，如果计划仅执行 ZDB 会话但不执行即时恢复，则还可以使用 Data Protector GUI 配置数据库。

备份 Oracle Server ZDB 集成

This feature is available in the Premium Edition

要配置 Oracle ZDB 备份，请执行以下步骤:

1. 配置计划用于备份的设备。
2. 配置介质池和用于备份的介质。
3. 确保您能够连接到数据库。
4. 配置非 ZDB 备份规范并在应用程序系统上运行 Oracle 数据备份，以验证是否已正确配置 Oracle 环境。
5. 创建 Data Protector Oracle ZDB 备份规范。

设置环境变量

使用环境变量修改备份环境以满足您的需求。环境变量特定于 Oracle 数据库。这意味着，可以针对不同的 Oracle 数据库设置不同的环境变量。指定这些变量后，它们将保存到相关的 Data Protector Oracle 数据库配置文件中。注意: OpenVMS 系统不支持环境变量。

环境变量

环境变量	默认值	描述
OB2_RMAN_COMMAND_TIMEOUT	300 s	此变量适用于 Data Protector 尝试连接到目标或编目数据库的情况。它指定 Data Protector 等待 RMAN 响应连接成功的时间 (以秒为单位)。如果 RMAN 在指定时间内没有响应，Data Protector 将中止当前会话。
OB2_SQLP_SCRIPT_TIMEOUT	300 s	此变量适用于 Data Protector 发出 SQL*Plus 查询的情况。它指定 Data Protector 等待 SQL*Plus 响应查询成功完成的时间。如果 SQL*Plus 在指定时间内没有响应，Data Protector 将中止当前会话。
OB2_DPMCTL_SHRLOC	N/A	定义控制文件的创建位置以及在 Data Protector 托管控制文件备份中备份该文件的位置。Data Protector 将控制文件复制到其临时文件目录。此变量将使用客户指定的目录覆盖默认目录。在安装了 Oracle 版本 11.2.0.2 或更高版本的 Oracle Real Application Clusters (RAC) 环境中，要启用 Data Protector 托管控制文件备份和相应的还原会话，请确保此目录位于所有 RAC 节点均可访问的共享磁盘上。

要设置环境变量，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

创建备份规范或修改现有备份规范时，可以设置一个变量:

1. 在备份规范的“源”页面中，右键单击顶部的 Oracle 数据库，然后单击“设置环境变量”。
2. 在“高级”对话框中，指定变量名称及其值，然后单击“添加”。
3. 单击**确定**。

使用 Data Protector CLI

必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。

设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)。

执行：

```
util_cmd –putopt Oracle8 DatabaseNameVariableValue –sublist Environment
```

示例

要将 Oracle 数据库 INST2 的环境变量 OB2_RMAN_COMMAND_TIMEOUT 设置为 100 秒，请执行以下命令:

```
util_cmd –putopt Oracle8 INST2 OB2_RMAN_COMMAND_TIMEOUT 100 –sublist Environment
```

切换 Oracle 备份方法

您可以通过为每个数据库重新配置 Data Protector Oracle 集成来切换 Oracle 备份方法。创建备份规范期间“无法”选择方法。

重要说明: 在 Oracle 备份集与 proxy-copy 方法之间切换时，必须仔细按照下方的说明进行操作，以确保在两种方法之间自如切换，同时避免还原或恢复期间 RMAN 选择使用不同方法备份到一个恢复会话的备份对象。如果使用此类混合集，还原过程将失败。

切换备份方法:

1. 使用“当前”选定的方法成功备份整个数据库。
2. 为避免选择备份方法不同于当前备份方法的备份规范，可删除或移动属于选定数据库实例的所有 ZDB 备份规范。备份规范位于 Cell Manager 中:
   - *Windows 系统：* Data_Protector_program_data\Config\Server\BarLists\Oracle8
   - *UNIX 系统：* /etc/opt/omni/server/barlists/oracle8
3. 创建新的 Oracle ZDB 规范时，使用选定的“新方法”重新配置数据库。
4. (可选) 如果“从备份集切换到 proxy-copy”，您可以:
   1. 在 Cell Manager 上，删除文件:
      - *Windows 系统：* Data_Protector_program_data \Config\Server\Integ\Config\ Oracle8\client_name%initDB_NAME_bckp.ora
      - *UNIX 系统：* /etc/opt/omni/server/integ/config/Oracle8/ client_name%initDB_NAME_bckp.ora
   2. 从备份系统中删除 Oracle 软件。
5. 对整个数据库执行 ZDB。

重要说明: 如果需要使用新备份方法从第一次备份整个数据库开始到结束之间的某个时间执行还原，RMAN 可能尝试通过为旧方法中的文件分配的通道使用旧方法中的备份文件，还原将失败。

新建模板

您可以使用备份模板将同一组选项应用于许多备份规范。通过创建自己的模板，您可以完全按照自身要求指定选项。这样，只需点击几下鼠标即可将所有选项应用于备份规范，而无需反复指定所有选项。此为可选任务，因为您也可以使用默认模板之一。要创建新的备份模板，请继续执行以下步骤:

1. 在 Data Protector Manager 中，切换到“备份”上下文。
2. 在“范围窗格”中，依次展开“备份”和“模板”，然后右键单击 **Oracle Server**。
3. 单击“添加模板”。按照向导操作以在模板中定义相应的备份选项。

创建备份规范

联机 ZDB

要对 Oracle数据库执行联机 ZDB，必须在 ARCHIVELOG 模式下运行数据库。

脱机 ZDB

要执行脱机 ZDB，仅创建 ZDB 备份规范。

群集感知系统

在群集环境中执行脱机 ZDB 备份前，使 Oracle 数据库资源脱机，创建复本后再将其重新联机。此操作可通过特定备份规范中适用于客户机系统的 Pre-exec 和 Post-exec 命令中的 Oracle fscmd 命令行界面命令或使用群集管理员来完成。您无法执行存档重做日志文件的 ZDB。因此，需要创建两个备份规范:

- ZDB 备份规范，用于备份数据库文件
- 标准 Data Protector Oracle 集成备份规范，用于备份应用程序系统存档日志文件

要创建 ZDB 备份规范，请执行以下操作:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Oracle Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择以下各项: **备份集方法**

   要使用备份集方法对整个数据库执行 ZDB，请选择“SMB_BackupSet_Database”模板。**Proxy-copy 方法**

   要使用 proxy-copy 方法对整个数据库执行 ZDB，请选择“SMB_Proxy_Database”模板。从“备份类型”下拉列表中，选择“快照或拆分镜像备份”，然后从“子类型”下拉列表中选择适当的磁盘阵列代理。代理必须安装在应用程序系统和备份系统上。单击**确定**。
4. 在“应用程序系统”中，选择 Data Protector Oracle 集成客户机。在非 RAC 群集环境中，选择虚拟服务器。
   RAC： 选择 Oracle 资源组的虚拟服务器。
   在“备份系统”中，选择备份系统。
   选择其他特定于磁盘阵列的备份选项。有关备份选项的详细信息，请按 **F1**。
   EMC GeoSpan 详情

   在 EMC GeoSpan for Microsoft 群集服务环境中，选择活动节点的备份系统并指定 TimeFinder 配置。将 EMC GeoSpan for MSCS 中的故障转移之后，选择当前活动节点的备份系统，然后保存备份规范。
   P9000 XP 阵列详情

   要启用即时恢复，请将“跟踪复本以用于即时恢复”选项保持选中状态。如果清除此选项，则无法使用 Data Protector 运行即时恢复。
   在 Linux 上使用 P9000 XP 阵列执行 ZDB+IR+ORACLE 备份期间，建议选择“使用与应用程序系统上相同的装载点”。
   单击“下一步”。
5. 在“应用程序数据库”中，键入要备份的数据库的名称。
   数据库名称可通过 SQL*Plus 来获取:

SQL>select name from v$database;
注意: 在单实例配置中，数据库名称通常与其实例名称相同。在这种情况下，也可以使用实例名称。实例名称可按如下方式获取:
SQL>select instance_name from v$instance; 。指定在 UNIX 和 Windows 系统上可用的“用户和组/域”选项，如下所示:
- *UNIX 系统：*在“用户名”和“组/域名”中，指定要用于启动备份的 OSDBA 用户帐户 (例如，用户名 ora 、组 DBA)。必须按照配置 Oracle 用户帐户中所述配置此用户。
- *Windows 系统：*不必指定这些选项，而如果不指定，则以 Local System 帐户运行备份。

在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator 、域 DP)。必须设置此用户才能模拟 Data Protector Inet 服务用户。请确保此用户已加入 Data Protector admin 或 operator 用户组，并且具有 Oracle 数据库备份权限。此用户成为备份所有者。如果这不是您的第一个备份规范，Data Protector 会为您填写“用户名”和“组/域名”，并提供上次配置的 Oracle 数据库的值。单击“下一步”。注意: 单击“下一步”时，Data Protector 将执行配置检查。*UNIX 系统：*以指定的 OSDBA 用户帐户启动检查。如果检查成功完成，则 OSDBA 用户和组也将保存在 Oracle 数据库特定配置文件和 Oracle 系统全局配置文件中，并覆盖以前的值 (如果存在)。您必须为要针对其使用操作系统身份验证的用户输入用户名和组名。

6. 如果尚未将 Oracle 数据库配置为与 Data Protector 一起使用，则会显示“配置 Oracle”对话框。将 Oracle 数据库配置为与 Data Protector 一起使用，如配置 Oracle 数据库中所述
7. 选择要备份的 Oracle 数据库对象。注意: 由于临时表空间不包含永久数据库对象，因此 RMAN 和 Data Protector 不会备份它们。单击“下一步”。如果为此实例配置的备份方法与备份规范中的方法不对应，Data Protector 将显示警告并中止配置。
8. 选择要用于备份的设备。单击“属性”可以设置设备并发、介质池和预分配策略。有关这些选项的详细信息，请单击“帮助”。还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。不支持 ZDB 到磁盘的对象镜像。单击**下一步**继续。
9. 设置备份选项。“脱机 ZDB”。要执行脱机 ZDB，在“应用程序特定选项”对话框中选择“脱机备份”选项。此选项将在创建复本前停止数据库，并在创建复本后重新启动数据库。请注意，如果正在执行“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”会话，则在实际备份到磁带期间数据库不会处于脱机状态。单击“下一步”。
10. 单击“另存为”以保存备份规范，指定名称和备份规范组。建议将所有 Oracle 备份规范都保存在 **Oracle** 组中。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。注意，仅支持“完整”备份类型。单词 DEFAULT 为保留字，不得用于备份规范名称或任何类型的标签。因此，请勿在备份规范名称中使用标点符号，因为 Oracle 通道格式从备份规范名称创建而来。单击**确定**。要开始备份，请参阅启动备份会话。
11. 对于联机备份，还要创建标准 Data Protector Oracle 集成备份规范，用于备份应用程序系统存档日志文件。用于备份存档日志文件的备份规范可以由用于备份数据库文件的 ZDB 备份规范中定义的 **Post-Exec** 命令触发 (建议)，或在启动 ZDB 备份规范后手动启动。

Oracle 备份选项

禁用恢复编目自动备份	默认情况下，Data Protector 在每个备份会话中，在每次“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”之后，都会备份恢复编目。选择此选项可禁用恢复编目的备份。
禁用 Data Protector 管理的控制文件备份	默认情况下，Data Protector 在每个备份会话中，在每次“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”之后，都会备份 Data Protector 托管控制文件。选择此选项可禁用 Data Protector 托管控制文件的备份。
备份备用数据库	*Oracle Data Guard：*此选项适用于用备用连接配置数据库的情况。默认情况下，RMAN 备份主系统上的数据库文件和归档重做日志。选择此选项可允许在备用系统上备份数据库文件和存档日志。但是，只能在备用站点上备份配置了备用数据库之后创建的存档日志。必须在主数据库上备份配置备用数据库之前创建的存档日志。 请注意，仍将从主系统中备份当前的控制文件或用于备用的控制文件。 对于 ZDB 忽略此选项。
RMAN 脚本	您可以编辑 Data Protector Oracle 备份规范的 Oracle RMAN 脚本部分。该脚本由 Data Protector 在创建备份规范期间创建，用于反映备份规范的选择和设置。仅在保存备份规范后才能编辑该脚本。
pre-exec、post-exec	指定在备份之前 (pre-exec) 或之后 (post-exec) 将由 Oracle Server 系统中的 ob2rman.pl 启动的命令或 RMAN 脚本。RMAN 脚本的扩展名必须为 .rman 。不要使用双引号。 例如，您可以提供脚本来关闭和启动 Oracle 实例。 提供命令或 RMAN 脚本的路径名。
脱机备份	选择此选项可执行脱机 ZDB 会话。此选项将在创建复本前停止数据库，并在创建复本后重新启动数据库。

UNIX 系统上的 pre-exec 和 post-exec 脚本示例

Pre-exec 示例

以下是关闭 Oracle 实例的脚本示例:

```
#!/bin/sh export ORACLE_HOME=$2 export ORACLE_SQLNET_NAME=$1 if [ -f $ORACLE_HOME/bin/sqlplus ]; then $ORACLE_HOME/bin/sqlplus << EOF connect sys/manager@$ORACLE_SQLNET_NAME as sysdba shutdown EOF echo "Oracle database \"$DB_NAME\" shut down." exit 0 else echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)." exit 1 fi
```

Post-exec 示例

以下是启动 Oracle 实例的脚本示例:

```
#!/bin/sh export ORACLE_HOME=$2 export ORACLE_SQLNET_NAME=$1 if [ -f $ORACLE_HOME/bin/sqlplus ]; then $ORACLE_HOME/bin/sqlplus << EOF connect sys/manager@$ORACLE_SQLNET_NAME as sysdba startup EOF echo "Oracle database \"$DB_NAME\" started." exit 0 else echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)." exit 1 fi
```

编辑 Oracle RMAN 脚本

启动 Data Protector 备份规范来备份 Oracle 对象时，会用到 RMAN 脚本。

在保存备份规范或通过单击“编辑”按钮手动编辑备份规范之前，RMAN 脚本部分不会写入至备份规范。

仅在保存 Data Protector Oracle 备份规范后，才能编辑 RMAN 脚本部分。

要编辑 Oracle RMAN 脚本，请单击“应用程序特定选项”窗口中的“编辑”，编辑脚本，然后单击“保存”以保存对脚本的更改。

Data Protector RMAN 脚本结构

- “Oracle 通道分配”以及每个已分配通道的 Oracle 环境参数的定义。

对于除 Oracle proxy-copy ZDB 备份规范以外的所有备份规范，分配的通道数与选择进行备份的所有设备的并发总数相同。

保存备份规范后，更改并发数不会更改 RMAN 脚本中已分配通道的数量。该数量必须通过编辑 RMAN 脚本手动更改。

在 Windows 系统上，最多可以分配 32 或 64 个 (如果设备在本地) 通道。如果计算得出的数量超过此限制，则必须手动编辑 RMAN 脚本并减少分配的通道数。

通过编辑 RMAN 脚本手动定义 Oracle 通道时，必须按以下格式添加环境参数:

```
parms 'ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME, OB2BARLIST=Backup_Specification_Name)';
```

Proxy-copy

对于 Oracle proxy-copy ZDB 备份会话，Data Protector 分配“一个”通道。

对于 Oracle proxy-copy ZDB， OB2SMB 参数必须设置为 1。如果使用 Blank Oracle Backup 模板，则并发运行的 DMA（OB2DMAP）数将被自动计算为所有设备并发的总和；例如，如果有 4 个设备，发数设置为 3，则 OB2DMAP 将设置为 12。

如果使用 Oracle_SMB 模板，则 OB2DMAP 参数设置为 1。要提高备份和还原性能，您可能需要增大此参数的值。必须按以下格式添加环境参数:

```
parms 'ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME, OB2BARLIST=Backup_Specification_Name, OB2SMB=1, OB2DMAP=Concurrent_DMAs)';
```

即使调整设备并发，计算后 OB2DMAP 参数也不会更改。要更改 OB2DMAP ，必须手动编辑 RMAN 脚本。

- 根据选择的备份对象，**通过一个 RMAN 备份语句备份整个数据库实例，和/或通过任意 RMAN 命令组合备份表空间和数据文件**。 backup 语句由以下部分组成:
  - 采用以下格式的备份文件的 Oracle 格式: format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' database; 。通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合都可以“添加”到 %s:%t:%p 替代变量和 DB_NAME ，以上两个变量不可缺少。
  - 如果是 Oracle proxy-copy“ZDB 到磁盘 + 磁带”或“ZDB 到磁带”会话，则需要使用 PROXY ONLY 选项。只允许一个具有 proxy only 选项的 BACKUP 命令，并且只允许使用一个额外的备份命令来备份控制文件。
  - RMAN datafile tablespace_name*datafile_name 命令。
- 用于备份 Oracle 存档日志的 RMAN 备份语句 (如果选择存档重做日志进行备份)。 backup 语句包含备份文件的 Oracle 格式: format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' 通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合均可添加到不可缺少的 %s:%t:%p 替代变量和 DB_NAME 中。
- 如果为备份选择了控制文件，则为备份 Oracle 控制文件的 RMAN 备份语句。备份语句由以下各部分组成:
  - 采用以下格式的备份文件的 Oracle 格式: format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' current controlfile; 。通过编辑 RMAN 脚本手动定义或更改备份文件的 Oracle 格式时，任何用户定义的 Oracle 替代变量组合都可以添加到 %s:%t:%p 替代变量和 DB_NAME ，以上两个变量不可缺少。
  - RMAN archivelog all 命令。

对于 Oracle proxy-copy“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”，无法仅选择控制文件。您还必须选择 DATABASE 、 TABLESPACE 或 DATAFILE 对象。

Oracle proxy-copy“ZDB 到磁盘 + 磁带”RMAN 脚本示例

以下示例显示的是选择整个数据库后 Data Protector 基于“空白 Oracle 备份” 模板创建的 RMAN 脚本部分:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DIPSI,OB2BARLIST=New1,
OB2SMB=1,OB2DMAP=1)'; backup incremental level <incr_level>format 'New1<DIPSI_%s:%t:%p>.dbf' proxy only database ; backup format
'New1<DIPSI_%s:%t:%p>.dbf' controlfile; }
```

启动备份会话

要对 Oracle数据库运行“ZDB 到磁盘”、“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”备份会话，请使用以下任一方法:

备份方法

- 使用 Data Protector 调度程序计划对现有 Oracle ZDB 备份规范进行备份。
- 使用 Data Protector GUI 或 Data Protector CLI 启动对现有 Oracle ZDB 备份规范进行交互式备份。

计划备份会话

安排备份会话是指设置备份时间、日期和类型，定义日程安排选项并将其保存到备份规范后将以无人看管形式启动备份会话。

要计划 Oracle ZDB 备份规范，请继续执行以下步骤:

1. 在 Data Protector Manager 中，切换到“备份”上下文。
2. 在“范围窗格”中，依次展开“备份规范”和 **Oracle Server**。
3. 右键单击要计划的备份规范，然后单击“编辑计划”。“计划程序”页面随即打开。此备份规范的所有可用计划均列在右窗格中。
4. 单击要编辑的计划，然后单击“编辑”图标。计划向导随即打开。
5. 在“选项”页面查看选项，然后单击“下一步”。“重复”页面随即打开。

请注意，仅支持 Full 备份类型。

如果是“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，指定“拆分镜像/快照备份”选项。

只有在备份规范中选择“跟踪复本以用于即时恢复”选项时，才能运行“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。

1. 设置“重复”模式，然后单击“下一步”。“摘要”页面随即打开。
2. 在“摘要”页面查看选项，然后单击“完成”。

运行交互备份

创建并保存备份规范后，可以随时执行交互备份。可以使用 Data Protector GUI 或 CLI。

使用 GUI 启动备份

要使用 Data Protector GUI 启动 Oracle 数据库交互式 ZDB 会话备份，请继续执行以下步骤:

1. 在上下文列表中，单击“备份”上下文。
2. 在“范围窗格”中，依次展开“备份规范”和“Oracle Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 在“启动备份”对话框中，选择“备份类型”和“网络负载”选项。有关这些选项的信息，请单击“帮助”。

请注意，仅支持 Full 备份类型。

如果是“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，指定“拆分镜像/快照备份”选项。

只有在备份规范中选择“跟踪复本以用于即时恢复”选项时，才能运行“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。

单击**确定**。

使用 CLI 启动备份

要使用 Data Protector CLI 启动 Oracle“ZDB 到磁带”或“ZDB 到磁盘 + 磁带”会话，请执行: omnib -oracle8_list Name

要使用 Data Protector CLI 启动 Oracle“ZDB 到磁盘”会话，请执行:

```
omnib -oracle8_list Name -disk_only
```

其中， Name 是备份规范的名称。

如果未在备份规范中选择“跟踪复本以用于即时恢复”备份选项时，则无法运行“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。

Oracle 操作系统身份验证

要连接到数据库，Data Protector 可以使用 Oracle 侦听程序和 Oracle OS 身份验证。对于 Oracle 操作系统身份验证，在数据库备份期间，用户必须为可用作 Oracle 操作系统数据库管理员的 Oracle 操作系统用户提供用户名和用户组。该用户必须属于 Oracle **dba/sysdba** 组。用户信息在备份规范创建期间输入。

要使用操作系统身份验证配置备份规范，请执行以下步骤:

1. 在 Oracle 主机上，创建将用于 Oracle 操作系统身份验证的操作系统用户。该用户必须位于 Oracle 操作系统 sysdba/dba 组中。有关如何创建 Oracle 操作系统数据库管理员的详细信息，请参考 Oracle 文档。
2. 将用户添加到 Data Protector Admin 用户组。
   - 对于具有 Oracle 代理和 Windows 平台的主机，请为该用户添加模拟。
3. 创建备份规范。
   - 在“指定要备份的应用程序”屏幕上，选中“指定 OS 用户”复选框，然后为创建的用户输入用户名和组。
   - 在主选项卡中的“配置 Oracle”对话框上，选中“使用操作系统身份验证”复选框。

> **注意**对于 Oracle RAC 环境，请在“RAC 数据库名称”文本框中输入全局数据库名称。

使用 Data Protector GUI

为数据库创建第一个 ZDB 备份规范时，配置 Oracle 数据库。首先执行创建备份规范中介绍的过程，并请于步骤 6 继续执行以下步骤:

1. 在“配置 Oracle”对话框和“常规”页面中，指定 Oracle Server 主目录的路径名。
2. 在“主”页面中，指定主数据库的登录信息。

   请注意，必须已向用户授予 SYSDBA 特权。必须已向用户授予 SYSBACKUP 权限。您也可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。

   在“服务”中，键入主数据库实例的网络服务名称。将对此数据库实例所在的系统执行备份。

   RAC : 列出主数据库的所有网络服务名称，以逗号分隔。

   在主选项卡中，选中“使用操作系统身份验证”复选框。
3. 在“编目”页面中，选择“使用目标数据库控制文件代替恢复编目”，以使用主数据库控制文件。

   要将恢复数据库编目用作备份历史记录的 RMAN 存储库，请选择“使用恢复编目”并指定恢复编目的登录信息。

   请注意，对于 ZDB，必须使用恢复编目。

   指定的用户必须是恢复编目的所有者。

   在“服务”中，键入恢复编目的网络服务名称。
4. 如果具有适用于非 ZDB 会话的 Oracle Data Guard 配置，并且打算备份备用数据库，请同时配置备用数据库:

   在“备用”页面中，选择“配置备用数据库”并指定备用数据库的登录信息。

   在“服务”中，键入备用数据库实例的网络服务名称。

   RAC : 列出备用数据库的所有网络服务名称，以逗号分隔。
5. 在“ZDB”页中，选择“备份方法”，然后在下拉列表中选择“代理”或“备份集”。
   在“备份控制文件副本位置”中，指定源卷上在“ZDB 到磁盘”期间将制作当前控制文件的备份副本的位置。
   如果不指定位置，则 ob2rman.pl 会在需要时将控制文件的副本从应用程序系统复制到备份系统。因此，如果在复本中不需要控制文件副本，则不需要为此位置再创建一个磁盘。
   如果备份方法是“备份”集，并且数据库实例使用 PFILE (而不是 SPFILE)，请选择“参数文件 (PFILE)”选项并指定驻留在应用程序系统上的 PFILE 的路径名。
6. 单击**确定**。

Oracle 数据库配置完毕。退出 GUI 或继续在选择要备份的 Oracle 数据库对象步骤中创建备份规范。

使用 Data Protector CLI

1. 在 UNIX 系统上，使用 OSDBA 用户帐户登录 Oracle Server 系统。
2. 在 Oracle Server 系统上，执行:

Windows 系统：

perl -I..\lib\perl util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOMEPRIMARY_DB_LOGIN | USEOSAUTHENTICATION [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN] [-client CLIENT_NAME]

UNIX 系统：

util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOMEPRIMARY_DB_LOGIN | USEOSAUTHENTICATION [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN] [-client CLIENT_NAME]

其中：

PRIMARY_DB_LOGIN

-prmuser PRIMARY_USERNAME

-prmpasswd PRIMARY_PASSWORD

USEOSAUTHENTICATION

-useosauth USE_OS_AUT

-racdbname RAC_DB_NAME

CATALOG_DB_LOGIN 时是:

-rcuser CATALOG_USERNAME

-rcpasswd CATALOG_PASSWORD

-rcservice CATALOG_NET_SERVICE_NAME

STANDBY_DB_LOGIN 时是:

-stbuser STANDBY_USERNAME

-stbpasswd STANDBY_PASSWORD

-stbservice STANDBY_NET_SERVICE_NAME_1[,STANDBY_NET_SERVICE_NAME_2 ...]

ZDB_OPTIONS 为:

-zdb_method {PROXY | BACKUP_SET}

[-ctlcp_location BACKUP_CONTROL_FILE_COPY_LOCATION]

[-pfile PARAMETER_FILE]

[-bkphost BACKUP_SYSTEM]

ASM_OPTIONS 为:

[-asmhome ASM_HOME]

[-asmuser ASM_USER-asmpasswd ASM_PASSWORD-asmservice ASM_NET_SERVICE_NAME_1[,ASM_NET_SERVICE_NAME_2 ...]]

如果具有适用于“非 ZDB 会话”的 Oracle Data Guard 配置，并且打算备份备用数据库，则必须提供 STANDBY_DB_LOGIN 信息。

要为 ZDB 配置 Oracle 数据库，必须提供 ZDB_OPTIONS 信息。如果 ZDB 方法是“备份集”，还必须提供 BACKUP_SYSTEM 信息。

在使用自动存储管理 (ASM) 的 Oracle Server 配置中执行即时恢复，需要使用 ASM_OPTIONS 选项。

参数描述

CLIENT_NAME	具有待配置数据库的 Oracle Server 系统的名称。必须在群集环境下指定该参数。 *RAC :* Oracle 资源组的虚拟服务器。 *Oracle Data Guard :* 主系统或辅助 (备用) 系统的名称。
DB_NAME	要配置的数据库的名称。
ORACLE_HOME	Oracle Server 主目录的路径名。
PRIMARY_USERNAMEPRIMARY_PASSWORD	用于登录目标或主数据库的用户名和密码。请注意，必须向用户授予 SYSDBA 特权。且必须向用户授予 SYSBACKUP 特权。此外，您还可以使用具有 SYSDBA 特权的用户，但必须先将 omnirc 变量 OB2_ORACLE_USE_SYSDBA 设置为 1。
PRIMARY_NET_SERVICE_NAME_1 [,PRIMARY_NET_SERVICE_NAME_2, ...]	主数据库的网络服务名称。 *RAC :* 每个网络服务名称都必须解析到一个特定的数据库实例中。
USE_OS_AUT	此参数用于与配置脚本通信，以使用 Oracle 操作系统身份验证 (而不是用户名和密码身份验证)。 值应为 1。
RAC_DB_NAME	此参数用于在 Oracle RAC 环境中查找当前 Oracle RAC 节点的 Oracle SID。它代表的是 Oracle 全局数据库名称，在 Oracle RAC 平台上为必填参数。
CATALOG_USERNAMECATALOG_PASSWORD	用于登录恢复编目的用户名和密码。此为可选参数，仅在将恢复编目数据库用作备份历史记录的 RMAN 存储库时使用。
CATALOG_NET_SERVICE_NAME	恢复编目的网络服务名称。
STANDBY_USERNAMESTANDBY_PASSWORD	其用于在 Oracle Data Guard 环境中备份备用数据库。用于登录备用数据库的用户名和密码。
STANDBY_NET_SERVICE_NAME_1 [,STANDBY_NET_SERVICE_NAME_2, ...]	备用数据库的网络服务名称。
BACKUP_CONTROL_FILE_COPY_LOCATION	源卷上的位置，其中在“ZDB 到磁盘”之前生成当前控制文件的副本。这是可选设置，如果不指定位置，则 ob2rman.pl 会在需要时将控制文件的副本从应用程序系统复制到备份系统。因此，如果在复本中不需要控制文件副本，则不需要为此位置再创建一个磁盘。
PARAMETER_FILE	驻留在应用程序系统上的 PFILE 的完整路径名。这是可选设置，如果备份方法是备份集且数据库实例使用 PFILE (而不是 SPFILE)，则使用此方法。
BACKUP_SYSTEM	备份系统的名称。必须为 ZDB 备份集配置指定此选项。
ASM_HOME	Oracle ASM 配置中 ASM 实例的主目录。如果该值与 Oracle 数据库实例的主目录不同，请指定此选项。
ASM_USERNAME ASM_PASSWORD	用户名和密码 (身份验证凭据)，供 Data Protector Oracle 集成代理连接到 ASM 数据库使用。
ASM_NET_SERVICE_NAME_1[,ASM_NET_SERVICE_NAME_2...]	用于访问 ASM 数据库的网络服务的名称。对于涉及多项网络服务的 Oracle 环境，可以指定多个名称。

消息 *RETVAL*0 表示配置成功，即使后面还有其他消息也是如此。

> **注意**如果需要在启动 SQL*Plus、侦听程序或 RMAN 之前导出一些变量，则必须在 Data Protector Oracle 全局配置文件的 Environment 部分或使用 Data Protector GUI 定义这些变量。

示例

以下示例展示 Oracle 数据库 UNIX 系统及其恢复编目的配置，其中使用了备份集方法并指定了参数文件位置。

示例中使用以下名称:

- 数据库名称：oracle
- Oracle Server 主目录：/app12/oracle12/product/12.0
- 主用户名：system
- 主密码：manager
- 主网络服务名称 1：netservice1
- 主网络服务名称 2：netservice2
- 恢复编目用户名：rman
- 恢复编目密码：manager
- 恢复编目网络服务名称：catservice
- 备份系统名称：bcksys

语法

```
/opt/omni/lbin/util_oracle8.pl -config -dbname oracle -orahome /app12/oracle12/product/12.0 -prmuser system -prmpasswd manager -prmservice netservice1,netservice2 -rcuser rman -rcpasswd manager -rcservice catservice-zdb_method BACKUP_SET -pfile /app12/oracle12/product/12.0/dbs/pfile.ora -bkphost bcksys
```

示例

以下示例展示如何在群集环境中配置 Oracle 数据库。数据库文件通过 ASM 管理。该配置支持在 ASM 环境中执行即时恢复:

- 数据库名称：SUN
- Oracle Server 主目录：/orahome/ora/app/oracle/product/11.2.0/dbhome_1
- 主用户名：sys
- 主密码：oracle
- 主网络服务名称 1：SUN1
- 主网络服务名称 2：SUN2
- 恢复编目用户名：rman
- 恢复编目密码：manager
- 恢复编目网络服务名称：RECO
- ZDB 方法: 备份集
- Oracle Server 系统 (群集虚拟系统)：cluster.company.com
- 备份系统：backup.company.com
- ASM 主目录：/oracle/crshome/crshome/crs/app/11.2.0/grid
- ASM 用户：sys
- ASM 用户密码：oracle
- ASM 网络服务名称 1：ASMSRV1
- ASM 网络服务名称 2：ASMSRV2

要配置数据库，请执行:

```
opt/omni/lbin/util_oracle8.pl -config -dbname SUN -orahome /orahome/ora/app/oracle/product/11.2.0/dbhome_1 -prmuser sys -prmpasswd oracle -prmservice SUN1,SUN2 -rcuser rman -rcpasswd manager -rcservice RECO -zdb_method BACKUP_SET -bkphost backup.company.com -client cluster.company.com -asmhome /crshome/crs/app/11.2.0/grid –asmuser sys –asmpasswd oracle –asmservice ASMSRV1, ASMSRV2
```

检查配置

在为数据库至少创建一个备份规范后，您可以检查 Oracle 数据库的配置。如果使用 Data Protector CLI，则不需要备份规范。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份规范”和“Oracle Server”。单击备份规范以显示具有待检查数据库的服务器。
3. 右键单击该服务器，然后单击“检查配置”。

重要说明: Data Protector 不检查指定的用户是否拥有适当的 Oracle 备份权限。

使用 Data Protector CLI

1. 在 UNIX 系统上，使用 OSDBA 用户帐户登录 Oracle Server 系统应用程序系统。
2. 执行：
    1. Windows 系统： perl -I..\lib\perl util_oracle8.pl -chkconf _smb -dbname DB_NAME
    2. UNIX 系统： util_oracle8.pl -chkconf _smb -dbname DB_NAME

处理错误

如果发生错误，错误编号将以 *RETVAL*error_number 的形式显示。

要获取错误描述，请在 Cell Manager 上执行:

Windows 系统： Data_Protector_home\bin\omnigetmsg 12 error_number

UNIX 系统： /opt/omni/lbin/omnigetmsg 12 error_number

重要说明: 在 UNIX 系统上，即使您收到了 *RETVAL*0 ，备份也仍有可能失败，因为 Data Protector 不会检查指定的用户是否拥有适当的 Oracle 备份权限。

检查即时恢复配置
检查 Oracle 配置是否适合进行即时恢复。

在应用程序系统上，请执行:

Windows 系统：

```
perl util_oracle8.pl -chkconf_ir -dbname DB_NAME
```

UNIX 系统：

```
util_oracle8.pl -chkconf_ir -dbname DB_NAME
```

如果控制文件、SPFILE 和联机重做日志位于同一卷组 (如果使用 LVM) 或源卷作为数据文件，则会显示一条警告，表明无法进行即时恢复。您可以：

- 重新配置 Oracle 数据库实例。

  或

- 设置 ZDB_ORA_INCLUDE_CF_OLF 、 ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECKCONF_IR omnirc 选项并忽略此警告。但请注意，即时恢复期间将覆盖控制文件、SPFILE 和联机重做日志。

还原 Oracle Server ZDB 集成

This feature is available in the Premium Edition

可以使用 Data Protector GUI 或 RMAN 还原以下数据库对象:

- 控制文件
- 数据文件
- 表空间
- 数据库
- 恢复编目数据库

使用 Data Protector GUI，还可以“复制”生产数据库。

以下是 Data Protector 中用于还原数据库对象的可用方法:

- 标准还原，从备份介质还原到 LAN 上的应用程序系统。
- 即时恢复。

Microsoft 群集服务器系统

在开始还原群集感知 Oracle 服务器之前，使用群集管理器实用程序使 Oracle 数据库资源处于脱机状态。
验证是否已为 Oracle 资源组设置“防止回退”选项，并为 DB_NAME.world 资源 (这是 Oracle 数据库资源) 设置“不重新启动”选项。

Serviceguard 系统

从在虚拟主机上执行的备份还原数据库时，应在 RMAN 脚本中设置 OB2BARHOSTNAME 环境变量。例如：

```
run { allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=(OB2BARHOSTNAME=virtual.domain.com)';
restore datafile '/opt/orahome/oradata/MAKI/example02.dbf'; release channel dev1; }
```

从备份介质还原到 LAN 上的应用程序系统

您可以使用 Data Protector 中的以下工具之一还原数据库对象:

- Data Protector GUI。
- RMAN。

使用 Data Protector GUI 还原 Oracle

对于还原，根据在 GUI 中进行的选择，生成 RMAN 脚本以及必要的命令。要使用其他命令，可直接从 RMAN 中手动使用这些命令。此外，还可以使用如何修改 RMAN 还原脚本中描述的解决方法。

在灾难恢复中还原数据库项目

在灾难恢复的情况下，必须按特定顺序还原数据库对象。以下列表显示了在还原数据库项目时必须遵守的顺序。正常情况下，可以依照任何顺序还原数据库项目。

1. 还原恢复编目数据库 (如果已丢失)
2. 还原控制文件
3. 还原整个数据库或数据项目

更改数据库状态

在还原任何数据库项目或执行数据库复制之前，确保数据库处于正确的状态: 所需的数据库状态

要还原的项目	数据库状态
控制文件，复制数据库	NoMount（已启动）
所有其他项目 (仅还原少量表空间或数据文件时，可以打开其中包含要脱机还原的表空间或数据文件的数据库)。	Mount

要将数据库置于正确的状态，请执行以下命令:

```
sqlplus /nolog
```

SQL>connect user/password@service as sysdba ;

SQL>shutdown immediate ;

要将数据库置于 NoMount 状态，请执行以下命令:

SQL>startup nomount ;

要将数据库置于 Mount 状态，请执行以下命令:

SQL>startup mount;

> 注意: 如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

还原恢复编目数据库

Oracle 恢复编目数据库使用 Oracle Export 实用程序导出到二进制文件，并由 Data Protector 进行备份。此文件必须还原回磁盘，然后使用 Oracle Import 实用程序导入 Oracle 数据库中。Data Protector 提供了一款使用 Oracle 集成自动执行此操作的工具。

要还原恢复编目数据库，请执行以下操作:

1. 确保恢复编目数据库处于“打开”状态。
2. 使用 RMAN 命令 DROP CATALOG 从数据库中删除恢复编目 (如果存在)。
3. 在 Data Protector GUI 中，切换到“还原”上下文。
4. 在“还原对象”下，展开“Oracle Server” 以及要还原恢复编目的数据库所在的系统，然后单击该数据库。
5. 在“还原操作”下拉列表中，选择“执行 RMAN 存储库还原”。在结果区域中，选择“恢复编目”。如果要更改恢复编目登录信息，请右键单击“恢复编目”，然后单击“属性”。在“恢复编目设置”中，指定恢复编目的登录信息。
6. 在“选项”页中: 在“用户名”和“用户组”中，指定恢复编目数据库的用户名和密码。从“会话 ID”下拉列表中，选择会话 ID。
7. 单击**还原**。

继续还原控制文件。

还原控制文件

控制文件包含有关数据库结构的所有信息。如果控制文件已丢失，则必须先还原控制文件，然后再还原数据库的任何其他部分。数据库应处于 No Mount 状态。

根据控制文件备份的类型，还原控制文件时可以执行以下还原类型:

- 从 Data Protector 管理的控制文件备份进行还原 (“CONTROLFILE FROM DP MANAGED BACKUP”)

除非已选择“禁用 Data Protector 管理的控制文件备份”选项，否则在备份会话结束时 ob2rman.pl 会自动备份控制文件。

此还原选项“不”需要恢复编目。

控制文件 (ctrlDB_NAME.dbf) 将还原到默认的 Data Protector 临时文件目录。

在安装了 Oracle 11.2.0.2 及更高版本的 Oracle Real Application Cluster (RAC) 环境中，控制文件在 OB2_DPMCTL_SHRLOC 变量定义的位置进行创建、从该位置备份并还原到该位置。此目录必须驻留在共享磁盘上，并且可以从所有 RAC 节点访问，这样，还原会话才会成功进行。

还原后，执行以下脚本:

```
run { allocate channel 'dev0' type disk; restore controlfile from 'TMP_FILENAME'; release channel 'dev0'; }
```

其中， TMP_FILENAME 是文件还原到的位置。

- 从 RMAN 备份集还原 (“CONTROLFILE FROM RMAN BACKUPSET”)

需要恢复编目。

备份会话可以包含多种类型的控制文件备份。

要还原控制文件，请执行以下操作:

1. 打开 sqlplus 窗口并将数据库置于非装载状态。
2. 在 Data Protector GUI 中，切换到“还原”上下文。
3. 在“还原对象”下，展开“Oracle Server”以及要还原控制文件的数据库所在的系统，然后单击该数据库。
4. 在“还原操作”下拉列表中，选择“执行 RMAN 存储库还原”。
5. 在结果区域中，选择要还原的控制文件。
6. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理（ob2rman.pl）的系统。要将控制文件还原到与非选定数据库，请单击“设置”，然后指定目标数据库的登录信息。设置其他还原选项。
7. 单击**还原**。

继续还原 Oracle 数据库对象。

还原 Oracle 数据库对象

在还原 Oracle 数据库对象之前，确保恢复编目数据库和控制文件为最新版本。它们包含数据库结构信息。如果没有这些文件的最新版本，请按照还原恢复编目数据库和还原控制文件中所述还原这些文件。

要还原 Oracle 数据库对象，请执行以下操作:

1. 将数据库置于装载状态。
2. 在 Data Protector GUI 中，切换到“还原”上下文。
3. 在“还原对象”下，展开“Oracle Server”以及要还原数据库对象的数据库所在的系统，然后单击该数据库。
4. 在“还原操作”下拉列表中，选择要执行的还原类型。如果未选择“执行还原和恢复”或“仅执行恢复”，则必须使用 RMAN 手动还原数据库对象。如果未选择“执行还原和恢复”或“仅执行恢复”，则必须使用 RMAN 手动还原数据库对象。
5. 在结果区域中，选择要还原的对象。如果还原的是数据文件，可以将文件还原到新位置。右键单击数据库对象，单击“还原为”，然后在“还原为”对话框中，指定新的数据文件位置。如果还原到新位置，仅当您从“还原操作”下拉列表中选择“执行还原和恢复”时，才会将当前数据文件切换到已还原的数据文件副本。
6. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理的系统。要将数据库对象还原到非选定数据库，请单击“设置”，然后指定目标数据库的登录信息。设置其他还原选项。
7. 在“设备”页中，选择要用于还原的设备。
8. 单击**还原**。

还原后:

1. 将数据库置于正确的状态。如果您在“源”页中选择了“执行还原和恢复”或“仅执行恢复”，Data Protector 会自动将数据库置于“打开”状态。
2. 如果您执行了将 Oracle 数据库还原和恢复到既定时间点之前，并且会话已成功完成，请重置数据库，以在恢复编目中注册数据库的新版本。使用 RMAN 连接到目标和恢复编目数据库并重置数据库：rman target Target_Database_Login catalog Recovery_Catalog_Login RMAN> RESET DATABASE; RMAN> exit
3. 如果您未选择使用 Data Protector 来恢复数据库对象，并且磁盘上已存档所有重做日志，请在还原数据库之后执行以下操作: 打开命令行窗口并输入以下命令：sqlplus /nolog SQL>recover database; SQL>connect user/password@service as sysdba; SQL>alter database open; 。如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

还原表空间和数据文件

要还原表空间和数据文件，请执行以下操作:

1. 如果数据库处于“打开” 状态，请打开命令行窗口并输入以下命令：sqlplus /nolog SQL>connect user/password@service as sysdba ； SQL>alter database datafile 'datafile name' offline; ；如果要还原表空间，请输入：SQL>alter tablespace tablespace_name offline;
2. 完成还原后，使用以下过程将数据文件和表空间重置为联机状态: 打开命令行窗口并输入以下命令：sqlplus /nolog SQL>connect user/password@service as sysdba 。如果要还原数据文件，请输入：SQL>alter database datafile 'datafile_name' online; 。如果要还原表空间，请输入：SQL>alter tablespace tablespace_name online; SQL>alter tablespace tablespace_name online;

如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

复制 Oracle 数据库

执行生产数据库复制以创建:

- 与生产 (主) 数据库具有相同 DBID 的备用数据库。这样做可以:
  - 新建备用数据库。
  - 以下情况下重新创建备用数据库:
    - 丢失整个备用数据库
    - 已还原或重新创建主数据库控制文件
    - 已在主数据库上执行数据库时间点恢复
    - 已发生数据库角色切换或故障转移
- 具有唯一 DBID 的独立副本，可用于挖掘数据或进行测试。

要复制生产数据库，请执行以下操作:

1. 在要复制选定数据库的系统上，将 Oracle 辅助数据库实例置于非装载状态。
2. 在 Data Protector GUI 的上下文列表中，单击“还原”。
3. 在“还原对象”下，展开“Oracle Server”以及生产数据库所在的系统，然后单击要复制的生产数据库。如果有多个此类系统，请选择要用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。
4. 在“还原操作”下拉列表中，选择“执行复制”。
5. 在“选项”页上，从“客户机”下拉列表中选择用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。单击“设置”以指定辅助数据库的登录信息 (用户名、密码和网络服务名称)。如果您未提供登录信息，复制会话将失败。在“用户名”和“用户组”中，指定 OSDBA 帐户的用户名和用户组，以供 Data Protector Oracle 集成代理使用。在“并行性”中，指定要为数据库复制分配的 RMAN 辅助通道的数量。设置复制选项。有关信息，请按 **F1**。如果要创建新的数据库副本 (而不是备用数据库副本)，请另外指定“在此前恢复”选项以将复制的数据库恢复到指定的时间点之前。
6. 单击**还原**。

创建备用数据库时，它将保持装载状态。手动启动管理的恢复过程 (日志应用服务)。

还原、恢复和复制选项

还原操作选项

以下内容描述“源”页中的各个选项。此页面用于定义要使用 GUI 执行的还原和恢复的组合。

在 Data Protector 的上下文中，“还原”是指还原数据文件。可以选择要还原的数据库、表空间或数据文件，以及希望将它们还原到哪个时间点。“恢复”是指应用重做日志。可以根据 SCN 编号、logseq 选择要应用的重做日志，也可以将所有重做日志应用到上次备份的时间。

执行还原	使用此选项只能使用 Data Protector 还原 (但不能恢复) 数据库对象。还原后，使用 RMAN 手动恢复数据库。
执行还原和恢复	使用此选项可通过 Data Protector 执行数据库对象的还原和恢复。
仅执行恢复	使用此选项只能恢复数据库。此操作只能对整个数据库执行。
执行 RMAN 存储库还原	数据库对象在“源”页中不可用时，选择此选项可以还原恢复编目或控制文件。
执行复制	此选项用于执行生产数据库的复制。此操作只能对整个数据库执行。

常规选项

客户机	此选项指定用于启动 Data Protector Oracle 集成代理 (ob2rman.pl) 的系统。
设置	单击“设置”选项可以为要还原或复制选定数据库对象的目标数据库 (在还原和恢复时) 或辅助数据库 (在复制时) 指定登录信息 (用户名、密码和网络服务名称)。 如果在还原或恢复时不指定此选项，将使用位于选定系统上选定数据库的登录信息。如果在复制时不指定此选项，则复制会话将失败。
用户名、用户组 (仅限 UNIX 系统)	指定要用于启动还原的操作系统用户帐户。确保此用户具有还原数据库的 Oracle 权限 (例如，位于 DBA 用户组中)。该用户还必须在 Data Protector 管理员或操作员用户组中 (实际上，具有“启动还原”和“查看私有对象”用户权限已足够)。
还原模式	可通过此下拉列表指定要执行的还原类型。选项如下: • Normal 当执行了使用备份集方法的传统备份或 ZDB 时，应使用此选项。 • 代理副本 当使用 Oracle RMAN 代理复制方法执行了原始 Oracle 备份时，应使用此选项。如果只执行恢复，则禁用此选项。
并行性	此字段用于指定可从备份设备中读取的并发数据流的数量。默认值为 1。在 Normal “正常”还原模式下，要优化还原性能，请使用与备份期间所用相同数量的数据流。例如，如果将备份并发设置为 3，则也要将并行数据流数量设置为 3。请注意，如果指定了非常大量的并行数据流，则这可能导致资源问题，因为要使用的内存过多。对于 Oracle proxy-copy ZDB 会话，禁用此选项，Data Protector 将并发数据流的数量设置为备份时使用的值。如果要还原使用以前版本的 Data Protector 创建的备份，则将并行性设置为用于备份的设备数，无论这些设备的并发数为多少都是如此。

复制选项

在选择“执行复制”时可用。

用于备用	选择此选项可以创建备用数据库。 默认：选择。

DORECOVER	(在选择“适用于备用机”时可用) 如果希望 RMAN 在创建数据库之后执行恢复，请选择此选项。
到数据库名称	选择此选项可以创建新数据库副本。在文本框中，指定其名称。该名称应当匹配用于启动辅助数据库实例的初始化参数文件中的名称。默认情况下，数据库名称设置为当前选定目标数据库的数据库名称。
NOFILENAMECHECK	选择此选项可禁止 RMAN 检查目标数据文件是否与所复制的数据文件同名。 当目标数据文件和所复制的数据文件同名、但位于不同系统中时，选择此选项。 默认：未选择。

还原和恢复选项

还原直至	使用此下拉列表中的选项可以限制对适合于未完成恢复到指定时间的这些备份的选择。 • **现在** 使用此选项可还原完整备份。默认情况下，选择此选项。 • **所选时间** 使用此选项可以指定希望向其还原数据库的确切时间。Data Protector 恢复可以在恢复中使用到指定时间的备份。 • 还原的重做日志的上限。Data Protector 恢复可以在恢复中使用到指定日志序列号的备份。 • **选定的 SCN 编号**使用此选项可以指定希望向其还原数据库的 SCN 数。Data Protector 恢复可以在恢复中使用到指定 SCN 号的备份。
在此前恢复	使用此下拉列表中的选项可指定希望恢复要执行到的时间点。 • **现在** Data Protector 通过应用所有存档重做日志，启动 RMAN 将数据库恢复到尽可能最新的时间。默认情况下，选择此选项。 • **所选时间** 使用此选项可指定存档日志要应用到的确切时间。 • **选定的日志序列号/线程编号**logseq 号是重做日志序列号。使用此选项可以指定一个特定重做日志序列，或者将充当要恢复的重做日志数上限的线程数。 • **选定的 SCN 编号**使用此选项可指定对其执行恢复的 SCN 号。 如果重置日志，也要重置数据库；否则，Oracle 将在下次备份期间尝试使用已经重置的日志，备份将失败。登录目标和恢复编目数据库并执行以下命令: rman target Target_Database_Login catalog Recovery_Catalog_Login RMAN> RESET DATABASE; RMAN> exit
恢复之后打开数据库	执行恢复后打开数据库。
重置日志	在打开数据库之后，重置存档日志。 *始终*重置日志： • 不完全恢复后 (不是“恢复到现在”)。 • 如果在恢复或还原和恢复中使用控制文件的备份。 以下情况下，“不要”重置日志: • 在完整恢复之后 (恢复到现在)；如果在恢复或还原和恢复中未使用控制文件的备份。 • 在主数据库上；如果存档日志用于备用数据库。但是，如果必须重置存档日志，则将需要重新创建备用数据库。如果将“在此前恢复”选项设置为“现在”时重置日志，则显示一个警告，指示仅当使用旧控制文件进行还原时才应重置日志。 Oracle 建议在使用“重置日志”选项打开数据库之后，立即执行完整备份。

使用 RMAN 还原 Oracle

Data Protector 充当 Oracle 系统的介质管理软件，因此 RMAN 可用于还原。

本节仅介绍如何执行还原的“示例”。提供的示例不适用于需要还原的所有情况。

- 还原和恢复数据库、表空间、控制文件和数据文件。
- 复制数据库。

以下是还原示例:

- 完整数据库还原和恢复示例
- 时间点还原示例
- 表空间还原和恢复示例
- 数据文件还原和恢复示例
- 存档日志还原示例

Oracle 控制文件的还原和恢复过程是一项非常精细的操作，取决于使用恢复编目还是控制文件作为中央存储库，以及使用的 Oracle 数据库的版本。

准备要还原的 Oracle 数据库

当数据库处于装载模式时，可以执行 Oracle 数据库的还原。但是，在执行表空间或数据文件的还原时，只能将 Oracle 数据库的一部分置于脱机状态。

示例中使用的连接字符串

在下面的示例中，使用以下连接字符串:

- 用于目标数据库的目标连接字符串:

  sys/manager@PROD

  其中 sys 是用户名， manager 是密码， PROD 是网络服务名称。

- 用于恢复编目数据库的恢复编目连接字符串:

  rman/rman@CATAL

  其中 rman 是用户名和密码， CATAL 是网络服务名称。

SBT_LIBRARY 参数

在 Windows 和 UNIX 系统上，将 SBT_LIBRARY RMAN 脚本参数设置为指向正确的特定于平台的 Data Protector MML。必须分别为每个 RMAN 通道指定参数。

SBT_LIBRARY 路径参数不得包含空格，以便 RMAN 可以成功加载库。在 Windows 系统上，您可能会在配置 Oracle 备份时遇到问题，并且配置可能会失败并显示以下错误消息:

```
SBT_LIBRARY=C:/Program Files/OmniBack/bin/orasbt.dll
```

```
[...]
```

```
ORA-19554: 分配设备时出错，设备类型: SBT_TAPE，设备名称:
```

```
ORA-27209: 设备 PARMS 中的语法错误 - 关键字未知或缺失 =
```

如果在此阶段 SBT_LIBRARY 参数包含一个带有空格的路径，则必须检查路径 C:\Program Files 或 Data Protector 安装目录 *DP_HOME* 是否包含短路径 (8dot3) 表示法和 CMD 命令 <dir /X> 。

如果短路径不存在、已删除或在安装过程中已禁用，您可以使用以下命令手动添加:

```
<windows\System32\fsutil.exe file setshortname 'C:\Program Files' PROGRA~1>
```

请注意，由于在 OS 处于活动状态时 Program Files 目录正在使用中，因此，仅当您在 Oracle 计算机上运行 Windows 修复模式 CMD 时，该命令才有效。

如果由于生产数据库无法脱机以进入修复模式，因此无法添加短名称，请使用以下解决方法:

1. 使用 CMD <mklink> 创建一个指向 <DP_HOME>\bin\orasbt.dll 的符号链接，并将其保存到不含空格的路径。
2. 按照上述过程设置 Oracle 变量 SBT_LIBRARY ，并设置 util_cmd CLI 参考页。

如果由于新安装而没有 Oracle 配置，则必须指定可选参数以确保创建配置文件:

```
-local
```

```
"C:\ProgramData\OmniBack\Config\Server\Integ\Config\Oracle8\hostname.domain.suffix%SID"
```

> ⚠ **警告**如果使用上述解决方法，您需要指定符号链接的位置、安全性和访问权限。

在以下示例中， SBT_LIBRARY 参数设置为 /opt/omni/lib/libob2oracle8.so ，这是 32 位 Solaris 系统的正确路径。

完整数据库还原和恢复示例

要执行完整数据库还原和恢复，还需要还原并应用所有存档日志。要执行完整数据库还原和恢复，请执行以下操作:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. 启动完整数据库还原和恢复:

   对于非 ZDB 或 ZDB 备份集会话:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore database; recover database; sql 'alter database open'; release channel 'dev1'; }
   ```

   对于 ZDB proxy-copy 会话:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)'; restore database; recover database; sql 'alter database open';
   release channel 'dev1'; }
   ```

您也可以将脚本保存到文件中，并使用保存的文件执行完整数据库还原。这种情况下，操作过程如下:

1. 在默认 Data Protector 临时文件目录中创建 restore_datafile 文件。
2. 启动完整数据库还原:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_datafile

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_datafile

时间点还原示例

要执行时间点还原，还需要还原存档日志并将其应用于指定的时间点。要执行时间点数据库还原和恢复，请执行以下操作:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. 启动时间点还原:

   对于非 ZDB 或 ZDB 备份集会话:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; set until time 'Mar 14 2004 11:40:00'; restore database; recover database; sql 'alter
   database open'; release channel 'dev1'; }
   ```

   对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于数据库恢复。恢复之前，释放 proxy-copy 通道:

   ```
   run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
   (OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)'; allocate channel 'dev2' type 'sbt_tape' parms
   'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)'; set until time 'Mar 14 2006
   11:40:00'; restore database; release channel 'dev1'; recover database; sql 'alter database open'; release channel 'dev2'; }
   ```

3. 执行时间点还原后，请在“恢复编目”中重置数据库。

您也可以将脚本保存到文件中，并使用保存的文件执行时间点还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_PIT 文件。
2. 启动时间点还原:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_PIT

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_PIT

表空间还原和恢复示例

如果表丢失或损坏，则需要对整个表空间执行还原和恢复。要还原表空间，可以仅将数据库的一部分置于脱机状态，以便数据库不必处于装载模式。可以使用恢复编目数据库或控制文件来执行表空间还原和恢复。请遵循以下步骤:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. 启动表空间还原和恢复。

   - 如果数据库处于打开状态，用于还原和恢复表空间的脚本应具有以下格式:

     对于非 ZDB 或 ZDB 备份集会话:

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql 'alter tablespace TEMP offline immediate'; restore tablespace TEMP; recover
     tablespace TEMP; sql 'alter tablespace TEMP online'; release channel dev1; }
     ```

     对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于数据库恢复。恢复之前，释放 proxy-copy 通道:

     ```
     run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)'; allocate channel 'dev2' type 'sbt_tape' parms
     'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)'; sql 'alter tablespace TEMP
     offline immediate'; restore tablespace TEMP; release channel 'dev1'; recover tablespace TEMP; sql 'alter tablespace TEMP online';
     release channel 'dev2'; }
     ```

   - 如果数据库处于装载状态，用于还原和恢复表空间的脚本应具有以下格式:

     对于非 ZDB 或 ZDB 备份集会话:

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore tablespace 'TEMP'; recover tablespace 'TEMP'; release channel dev1; }
     ```

     对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于数据库恢复。恢复之前，释放 proxy-copy 通道:

     ```
     run{ allocate channel 'dev1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)'; allocate channel 'dev2' type 'sbt_tape' parms
     'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)'; restore tablespace 'TEMP';
     release channel 'dev1'; recover tablespace 'TEMP'; release channel 'dev2'; }
     ```

您也可以将脚本保存到文件中，并使用保存的文件执行表空间还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_TAB 文件。
2. 启动表空间还原。

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_TAB

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_TAB

数据文件还原和恢复示例

要还原和恢复数据文件，可以仅将数据库的一部分置于脱机状态。

要还原和恢复数据文件，请执行以下操作:

1. 登录到 Oracle RMAN。

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. 启动数据文件还原和恢复:

   - 如果数据库处于打开状态，用于还原数据文件的脚本应具有以下格式:

     UNIX 系统

     对于非 ZDB 或 ZDB 备份集会话:

     ```
     run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
     (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql "alter database datafile ''/opt/oracle/data/oradata/DATA/temp01.dbf'' offline";
     restore datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; recover datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; sql "alter
     database datafile '/opt/oracle/data/oradata/DATA/temp01.dbf' online"; release channel dev1; }
     ```

对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于数据库恢复。恢复之前，释放 proxy-copy 通道:

```
run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; allocate channel dev2 type 'sbt_tape' parms
'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)'; sql "alter
database datafile ''/opt/oracle/data/oradata/DATA/temp01.dbf'' offline"; restore datafile '/opt/oracle/data/oradata/DATA/temp01.dbf';
release channel dev2; recover datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; sql "alter database datafile
'/opt/oracle/data/oradata/DATA/temp01.dbf' online"; release channel dev1; }
```

Windows 系统

对于非 ZDB 或 ZDB 备份集会话:

```
run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; sql "alter database datafile ''C:\oracle\data\oradata\DATA\temp01.dbf'' offline";
restore datafile 'C:\oracle\data\oradata\DATA\temp01.dbf'; recover datafile 'C:\oracle\data\oradata\DATA\temp01.dbf'; sql "alter
database datafile ''C:\oracle\data\oradata\DATA\temp01.dbf'' online"; release channel dev1; }
```

对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于恢复流程。恢复之前，释放 proxy-copy 通道:

```
run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; allocate channel dev2 type 'sbt_tape' parms
'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)'; sql
"alter database datafile ''Oracle_home\data\oradata\DATA\temp01.dbf'' offline"; restore datafile
'Oracle_home\data\oradata\DATA\temp01.dbf'; release channel dev2; recover datafile 'Oracle_home\data\oradata\DATA\temp01.dbf';
sql "alter database datafile ''Oracle_home\data\oradata\DATA\temp01.dbf'' online"; release channel dev1; }
```

- 如果数据库处于装载状态，用于还原和恢复数据文件的脚本应具有以下格式:

  UNIX 系统

  对于非 ZDB 或 ZDB 备份集会话:

  ```
  run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
  (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; recover datafile
  '/opt/oracle/data/oradata/DATA/temp01.dbf'; release channel dev1; }
  ```

  对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于恢复流程。恢复之前，释放 proxy-copy 通道:

  ```
  run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
  (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; allocate channel dev2 type 'sbt_tape' parms
  'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)'; restore
  datafile '/opt/oracle/data/oradata/DATA/temp01.dbf'; release channel dev2; recover datafile
  '/opt/oracle/data/oradata/DATA/temp01.dbf'; release channel dev1; }
  ```

  Windows 系统

  对于非 ZDB 或 ZDB 备份集会话:

  ```
  run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
  (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore datafile 'Oracle_home\data\oradata\DATA\temp01.dbf'; recover datafile
  'Oracle_home\data\oradata\DATA\temp01.dbf'; release channel dev1; }
  ```

  对于 ZDB proxy-copy 会话，分配一个通道用于还原 proxy-copy 会话，分配一个通道用于恢复流程。恢复之前，释放 proxy-copy 通道:

  ```
  run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=
  (OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; allocate channel dev2 type 'sbt_tape' parms
  'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)';
  restore datafile 'Oracle_home\data\oradata\DATA\temp01.dbf'; release channel dev2; recover datafile
  'Oracle_home\data\oradata\DATA\temp01.dbf'; release channel dev1; }
  ```

您也可以将脚本保存到文件中，并使用保存的文件执行数据文件还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_dbf 文件。
2. 启动数据文件还原:

   Windows 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_dbf

   UNIX 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_dbf

存档日志还原示例

要还原存档日志，请执行以下操作:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. 启动存档日志还原:

```
run{ allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; restore archivelog all; release channel dev1;}
```

您也可以将脚本保存到文件中，并使用保存的文件执行存档日志还原:

1. 在默认 Data Protector 临时文件目录中创建 restore_arch 文件。
2. 启动存档日志还原:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=Data_Protector_home\tmp\restore_arch

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_arch

使用不同设备还原数据库的示例

假设使用设备 dev1 对某个数据库进行了备份。要使用设备 dev2 还原该数据库，请将 send device type 'sbt_tape' 'CHDEV=dev1>dev2'; 行添加到 RMAN 脚本:

1. 登录到 Oracle RMAN:

   Windows 系统： ORACLE_HOME\bin\rman target sys/manager@TIN

   UNIX 系统： ORACLE_HOME/bin/rman target sys/manager@TIN

2. 执行：

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; allocate channel 'dev_1' type 'sbt_tape' parms
'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; allocate
channel 'dev_2' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)'; send device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1'; send device
type 'sbt_tape' 'CHDEV=dev1>dev2'; restore database; }
```

> **注意**
> - device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1'; 行可禁用自动设备选择。
> - 您也可以使用 CHDEV 参数和 'CHDEV=dev1>dev2;dev3>dev4'; 语法指定多个设备重定向。

使用其他设备进行还原

Data Protector 支持从备份数据库对象时所用的设备以外的其他设备还原 Oracle 数据库对象。

按以下格式在 /etc/opt/omni/server/cell/restoredev（UNIX 系统）或 Data_Protector_program_data\Config\server\Cell\restoredev（Windows系统）文件中指定这些设备:

" DEV 1 " " DEV 2 "

其中:

DEV 1 是原始设备， DEV 2 是新设备。

在 Windows 系统上，此文件必须采用 Unicode 格式。

请注意，此文件在使用后应删除。

示例

假设您在名为 DAT1 的设备上备份了 Oracle 对象。要从名为 DAT2 的设备还原这些对象，请在 **restoredev** 文件中指定以下内容:

" DAT1 " " DAT2 "

将 Oracle 还原到不同的单元/客户机

要将 Oracle 还原到不同的单元/客户机，请执行以下步骤:

1. 将 Data Protector Oracle 配置文件从源复制到目标。
2. 导出 Oracle SID。
3. 为数据库创建密码文件。
4. 设置 DBID 并在非装载状态下启动数据库。
5. 从 RMAN 恢复 **pfile**。
6. 使用已恢复的 **pfile** 在非装载状态下启动数据库。
7. 从 GUI 启动控制文件还原，并将 Data Protector 的已还原控制文件复制到控制文件位置。
8. 在装载状态下启动数据库。
9. 在目标端使用控制文件配置数据库备份。
10. 仅启动数据库还原。
11. 从目标数据库执行 sql 命令 " alter database open resetlogs " 以恢复数据库。

即时恢复和数据库恢复

Data Protector 即时恢复功能仅用于还原数据库文件所在的目标卷。数据库恢复部分在 RMAN 实用程序即时恢复之后执行。数据库恢复期间，从磁带还原“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”之后执行的增量备份和存档日志备份。仅还原未驻留于目标卷上的存档日志。

请注意，如果 Oracle 控制文件、联机重做日志和 SPFILE 与数据文件位于同一源卷上，并且通过设置 omnirc 选项启用即时恢复，即时恢复期间将覆盖控制文件、SPFILE 和联机重做日志。

RAC 准备步骤

如果是 RAC，请在 omnirc 文件中设置以下选项：ZDB_IR_VGCHANGE=vgchange -a s 即时恢复过程与无 RAC 相同。但是，如果要对除备份节点以外的其他某个节点执行即时恢复，则必须在标准即时恢复过程之前执行以下过程:

1. 确保在目标节点上运行 SG 虚拟包。
2. 从命令行运行配置之前，将 OB2BARHOSTNAME 环境变量设置为虚拟主机名：export OB2BARHOSTNAME=virtual_hostname

使用 Data Protector GUI 即时恢复

要执行即时恢复，请执行以下操作:

1. 使用 sqlplus 将 Oracle 数据库实例置于无装载状态。如果是 RAC，请将所有实例设置为无装载状态。例如： sqlplus sql> shutdown immediate sql> startup nomount sql> exit
2. 在“上下文列表”中，单击“即时恢复”。
3. 展开“Oracle Server”，然后选择要从中执行还原的“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。
4. 在“源”选项卡中，选择要恢复的对象。只能选择整个数据库。对于 P9000 XP 磁盘阵列系列，建议将“在还原完成之后保留复本”选项保留为设置状态，以支持重新启动即时恢复会话。设置其他 P9000 XP 磁盘阵列系列选项。有关详细信息，请按 **F1**。
5. 此时，您可以决定是否在即时恢复后立即执行数据库恢复:
   - 要仅执行即时恢复，请单击“还原”。

   您可以稍后从 Data Protector Manager 还原上下文执行数据库恢复，也可以使用 RMAN CLI 手动执行数据库恢复。
   - 要在即时恢复后立即执行数据库恢复，请单击“选项”选项卡，选择“恢复”，然后选择数据库恢复选项。对于恢复到选定时间、logseq 号/线程号或 SCN 号，建议重置日志文件。
6. 单击“还原”或“预览”。请注意，预览仅检查能否还原复本。不会检查数据库恢复是否成功。

Data Protector 在执行即时恢复后恢复数据库，方法是将数据库切换到装载状态，从磁带还原必要的增量备份和存档重做日志，然后应用重做日志。

如果重置日志，请重置数据库；否则，Oracle 将在下一次备份期间尝试使用已经重置的日志，备份将失败。登录目标和恢复编目数据库并执行以下命令:

```
rman target Target_Database_Login  catalog Recovery_Catalog_Login
```

```
RMAN> RESET DATABASE;
```

```
RMAN> exit
```

在即时恢复后执行 Oracle 数据库恢复

要在执行即时恢复后恢复 Oracle 数据库，请执行以下步骤:

1. 从 sqlplus 连接到目标数据库，然后运行以下命令，将 Oracle 数据库置于装载状态: startup mount
2. 要恢复数据库，可以使用以下两个选项。从 Data Protector Manager 还原上下文进行恢复:

a. 展开“Oracle Server”并选择要恢复的数据库。在“源”选项卡的“还原操作”下，选择“仅执行恢复”。
b. 在“选项”选项卡中，选择恢复选项。
c. 单击**还原**。

使用 RMAN 执行手动数据库恢复。

运行以下 RMAN 脚本以恢复数据库:

```
run { allocate channel dev1 type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; recover database; sql 'alter database open'; release channel dev1; }
```

Veritas Cluster 中的 Oracle 即时恢复

如果应用程序系统上的 Oracle 在 Veritas Cluster 中运行，则必须在执行即时恢复之前禁用以下两类 Veritas Cluster 资源并在完成即时恢复后启用资源，以防止 Oracle Veritas 群集服务组故障转移:

- 适用于 Oracle 应用程序的 Veritas Cluster 应用程序资源，以及
- 适用于 Oracle 数据库文件的 Veritas Cluster 装载点资源。

按照以下步骤对 Oracle 位于 Veritas Cluster 中的应用程序系统执行即时恢复:

1. 在应用程序系统上，输入以下命令以禁用两类 Veritas Cluster 资源:
   a. hares -offline application_resource_name -sys system 其中， application_resource_name 是 Oracle 应用程序的 Veritas Cluster 应用程序资源的名称， system 是活动节点的名称。 hares -offline mountpoint_resource_name -sys system 其中， mountpoint_resource_name 是 Oracle 数据库文件的 Veritas Cluster 装载点资源的名称， system 是活动节点的名称。
   b. hares -modify application_resource_name Enabled 0，其中 application_resource_name 是 Oracle 应用程序的 Veritas Cluster 应用程序资源的名称。 hares -modify mountpoint_resource_name Enabled 0，其中 mountpoint_resource_name 是 Oracle 数据库文件的 Veritas Cluster 装载点资源的名称。
2. 执行即时恢复。
3. 如果仅在未执行数据库恢复的情况下执行即时恢复，请使用 RMAN 将 Oracle 数据库置于一致状态。
4. 在应用程序系统上，输入以下命令以启用两类 Veritas Cluster 资源:
   a. hares -modify mountpoint_resource_name Enabled 1 其中， mountpoint_resource_name 是 Oracle 数据库文件的 Veritas Cluster 装载点资源的名称。 hares -modify application_resource_name Enabled 1，其中 application_resource_name 是 Oracle 应用程序的 Veritas Cluster 应用程序资源的名称。
   b. hares -online application_resource_name -sys *system*，其中 application_resource_name 是 Oracle 应用程序的 Veritas Cluster 应用程序资源的名称， system 是活动节点的名称。 hares -online mountpoint_resource_name -sys *system*，其中 mountpoint_resource_name 是 Oracle 数据库文件的 Veritas Cluster 装载点资源的名称， system 是活动节点的名称。

中止会话

可通过单击“中止”按钮来中止当前运行的会话。

如果在会话期间 RMAN 或 SQL*Plus 没有对请求做出响应，Data Protector 会自动中止会话。默认情况下，Data Protector 将等待响应 5 分钟。使用 omnirc 选项或环境变量 OB2_RMAN_COMMAND_TIMEOUT 和 OB2_SQLP_SCRIPT_TIMEOUT，可以修改此时间间隔。

PostgreSQL 集成

This feature is available in the Premium Edition

本节提供与 Data Protector PostgreSQL 集成有关的信息。它解释了如何将 Data Protector 与 PostgreSQL 数据库服务器集成。此外，它还说明了为 PostgreSQL 数据设置有效数据保护策略时需要考虑的概念和方法，以及采用哪些方法和步骤来最大限度减少还原此类数据时所需的工作量和宕机时间。

备份

Data Protector 可联机备份 PostgreSQL 实例和相关的预写日志文件 (WAL 文件)。WAL 文件备份可确保 PostgreSQL 数据的完整性。执行此备份期间，仍可在会话期间主动使用所涉及的数据库表，甚至可以修改它们。Data Protector 提供以下类型的交互式备份和计划备份功能:

Data Protector 中提供的 PostgreSQL 备份类型

备份类型	描述
完整备份	包括 PostgreSQL 实例中的所有数据库。
事务备份	仅包括自上次完整备份或事务备份以来存档的 WAL 文件。相比完整备份，它的备份大小要小得多，备份速度也更快。通过更频繁地创建事务备份映像，同时减小完整数据库备份映像的创建频率，可以节省备份介质上的存储空间。恢复前，事务备份数据将与上一次备份的内容（WAL 应用于完整备份映像）合并。

Data Protector PostgreSQL 集成不支持零宕机时间备份。

还原

为了适应不同的用例和需求，Data Protector 提供了不同的方法来还原 PostgreSQL 数据。从备份映像还原数据之前，可定义还原过程的以下方面:

- 范围

  只能还原整个实例。

- 数据目标

  您可以将数据还原到其原始位置，还原到源客户机上的其他路径，或还原到其他客户机。还原到不同的位置时，Data Protector 可使用还原的数据创建一个新的 PostgreSQL 实例。

- 还原数据的最终状态

  在存在适当的还原链 (包括完整备份映像以及相应 WAL 文件的备份) 的前提下，您可以重新创建以下时点的 PostgreSQL:

  - 最后一次事务备份时 (前滚到最新的可能状态)
  - 所选的时间点 (同时使用时间点还原和前滚)
  - 所选完整或事务备份成功执行时

数据迁移

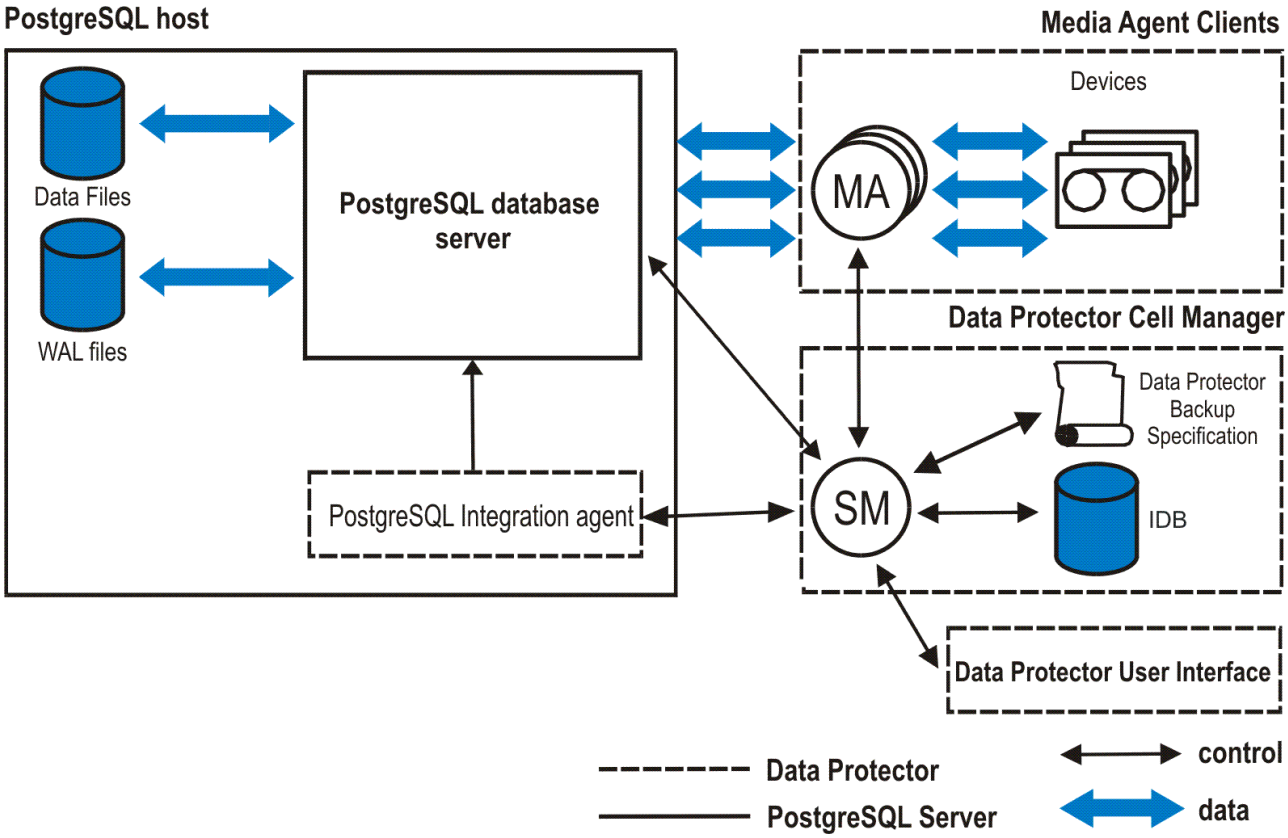
使用 Data Protector PostgreSQL 集成，您可以将 PostgreSQL 数据迁移到另一个位置。您可以使用标准还原过程迁移整个 PostgreSQL 实例。

集成概念

Data Protector PostgreSQL 集成利用 PostgreSQL 预写日志记录 (WAL) 方法来确保数据完整性并为 PostgreSQL 提供企业级备份和恢复。Data Protector 使用 PostgreSQL 集成代理与 PostgreSQL 集成。

PostgreSQL 集成体系结构显示了 Data Protector PostgreSQL 集成的体系结构。

PostgreSQL 集成体系结构



图例

SM	Data Protector 会话管理器；在备份会话期间为 Data Protector 备份会话管理器，在还原会话期间为 Data Protector 还原会话管理器。
IDB	Data Protector 内部数据库，在其中写入有关 Data Protector 会话的所有信息，包括会话消息、对象、数据以及使用的设备和介质。
PostgreSQL 集成代理	PostgreSQL 集成代理安装在需要使用 Data Protector 备份的 PostgreSQL 数据库所在的系统上。
MA	Data Protector 常规介质代理，用于在介质设备中读取和写入数据。

满足 PostgreSQL 的先决条件

以下是集成 PostgreSQL 的先决条件:

- 确保已正确安装和配置 PostgreSQL 数据库服务器。
- 确保已正确安装 Data Protector。
- 确保已根据 PostgreSQL 备份策略 (数据保护) 需求配置了 Data Protector 备份设备和备份介质。
- 确保为运行 PostgreSQL 备份和还原会话选择的 PostgreSQL 操作系统用户帐户在 Data Protector admin 或 operator 用户组中配置了相应的 Data Protector 用户。
- 在 PostgreSQL 主机上配置和运行 Data Protector 文件系统备份和还原会话，以此来测试 PostgreSQL 主机能否与 Cell Manager 正常通信。
- 确定 PostgreSQL 主机上 PostgreSQL 二进制文件目录的绝对路径。
- 配置 PostgreSQL 用户 (如果不存在)。
- 必须在将使用 Data Protector 备份数据的每个 PostgreSQL 实例上启用 WAL 存档。

备份考虑事项

- 定义备份策略范围时，还要考虑到同一数据库的表通常是相互关联的。

- 确保目标 PostgreSQL 实例处于脱机状态。
- 如果要将数据还原到非原始客户机 (PostgreSQL 主机) 上的 PostgreSQL 实例:
  - 确保目标 PostgreSQL 主机已安装 Data Protector PostgreSQL 集成组件，并且是 Data Protector 单元的成员。
  - 确保在 Data Protector 中配置了目标 PostgreSQL 实例。

配置集成

配置 Data Protector PostgreSQL 集成之前，请确认先决条件和限制条件。

要配置 PostgreSQL 实例，请在 Data Protector GUI 中执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“PostgreSQL”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。。
4. 在“结果区域”中，从“客户机”下拉列表中选择 PostgreSQL 主机。
5. 在“应用程序数据库”文本框中，键入 PostgreSQL 实例名称或从下拉列表中选择现有名称。下拉列表显示所有正在运行的数据库实例的列表，即 Data Protector 中配置的数据库实例以及 Data Protector 中未配置的数据库实例。该实例名称对于特定连接 (对于特定客户机和端口组合) 必须是唯一的。未配置的正在运行的数据库实例将以下列格式显示: 未配置 <端口> [状态] (例如，未配置: 3434 [正在运行])。
6. 如果已配置实例，则不会打开配置对话框。右键单击 PostgreSQL 实例，然后选择“配置”。在“配置 PostgreSQL 实例”对话框中，通过在输入文本框中指定 PostgreSQL 服务器用户帐户的“用户名”和“密码”、为 PostgreSQL 实例访问权限指定足够的特权 (至少为 SUPER) 以及指定实例使用的“端口”来配置连接参数。
7. 在“PostgreSQL 二进制文件目录”文本框中，输入 PostgreSQL 主机上 PostgreSQL 二进制文件目录的绝对路径。
8. 如果已经在 PostgreSQL 主机上创建了 WAL 存档目录 (archivedir) 并在 archive_command 配置参数中指定了该目录，请选中“PostgreSQL WAL 存档目录”选项并提供指向该目录的路径。第一次备份后，Data Protector 使用提供的 archive_dir 设置 archive_command 。

   > ⚠ **警告**仅当在 archive_command 配置参数中指定了 PostgreSQL archivedir 时才需要选中“PostgreSQL WAL 存档目录”选项。如果 WAL 存档目录不存在，Data Protector 会在备份期间创建并使用它，以便首先存档 WAL 文件，然后再备份这些文件。
   >
   > 但是，如果 WAL 存档目录在 PostgreSQL 主机上已存在并用于存档 WAL 文件，则必须选中“PostgreSQL WAL 存档目录”选项。否则会导致 Data Protector 无法成功备份和还原 PostgreSQL 数据。

   单击“确定”关闭对话框。

配置完成后，Data Protector 会将您指定的参数存储在 Cell Manager 上的相应配置文件中，并验证与该实例的连接。

安装 PostgreSQL 客户机

This feature is available in the Premium Edition

要将 Data Protector 与 PostgreSQL 数据库服务器系统集成并且希望能够备份 PostgreSQL 实例和数据，请在 PostgreSQL 主机上安装以下 Data Protector 组件：

- PostgreSQL Integration

  此组件可用于执行 PostgreSQL 数据库的集成备份和还原。

备份 PostgreSQL 集成

This feature is available in the Express Edition

Data Protector PostgreSQL 集成可以联机备份 PostgreSQL 数据库、数据库表和 PostgreSQL WAL 文件。您可以在创建备份规范时定义要备份的数据的范围。有关详细信息，请参阅创建备份规范。

在数据将由 Data Protector 备份的每个 PostgreSQL 实例上启用预写日志记录 (WAL) 存档。有关如何设置相应配置参数 (wal_level=archive (PostgreSQL 版本 9.4 和 9.5) 或 wal_level=replica (PostgreSQL 版本 9.6 和 10) 和 archive_mode=on) 的详细说明，请参阅 PostgreSQL 文档。

为了在大型 PostgreSQL 数据库中获得更好的备份性能，您可以同时将数据库备份到多个“备份到设备 (B2D)”设备中。

创建备份规范

要在 Data Protector GUI 中创建 PostgreSQL 备份规范，请继续执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“PostgreSQL”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择负载均衡和重复数据删除首选项。单击**确定**。
4. 在“结果区域”中，从“客户机”下拉列表中选择 PostgreSQL 主机。在“应用程序数据库”下拉列表中，选择要备份的 PostgreSQL 实例。

   选择“指定 OS 用户”选项。在“用户名”和“组/域名”文本框中，输入相应的 PostgreSQL 用户帐户。有关详细信息，请按 **F1**。

   单击“下一步”。
5. 查看已选择进行备份的 PostgreSQL 实例。单击“下一步”。
6. 选择用于备份会话的备份设备。如果需要，可更改它们的顺序并调整负载均衡和对象镜像。

   右键单击该设备，然后选择“属性”以设置介质池、预分配策略和其他备份设备选项。如需各选项的介绍信息，请按 F1。单击**确定**。

   要创建其他备份副本 (镜像)，请通过单击“添加镜像”或“删除镜像”指定所需的数量。为每个镜像选择单独的设备。镜像的最小设备数等于用于备份的设备数。有关对象镜像的详细信息，请参阅《*Data Protector 帮助*》。

   单击“下一步”。
7. 指定备份选项。

   单击“下一步”。
8. 单击“另存为”。
9. 在“将备份另存为”对话框的“名称”文本框中，输入备份规范的名称。在“组”下拉列表中，选择备份规范组。单击“确定”，保存备份规范。

   (可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。有关如何创建和编辑计划的详细信息，请参阅《*Data Protector 管理员指南*》中 Data Protector 中的“调度程序”。

> **提示**您可以创建一个专用的 Data Protector 备份规范组，然后将自己的备份规范都保存在该组中，从而将 Data Protector PostgreSQL 备份规范整理得井井有条。

多主数据库备份

进行群集备份的过程与在多主数据库节点设置中备份单个节点相同。任何多主数据库节点均可用于备份整个群集。

特定于应用程序的备份选项

该表列出了与 PostgreSQL 集成有关的选项。

选项	描述
常规选项	

Pre-exec、**Post-exec**	此选项用于指定在备份之前 (pre-exec) 或之后 (post-exec) 执行的命令行。 该命令行在启动了备份会话的 PostgreSQL 系统 (在该系统上还启动了 Data Protector PostgreSQL 集成代理) 上执行。 仅输入命令名称和所需参数，并确保该命令位于同一系统上的默认 Data Protector 命令目录中。不要使用双引号。
存档日志选项	
清除备份的归档日志文件	此选项指定从归档日志成功备份 WAL 文件后，Data Protector 是否应请求显式归档日志清理。清理归档日志后，已成功备份的 WAL 文件将从系统中删除，然后 PostgreSQL 会开始在新的归档日志（如果已在 archive_command 配置参数中指定）中记录数据库事务。选择此选项可有效地减小 WAL 文件的备份映像大小并限制归档日志占用的存储空间。 默认：未选择。

PostgreSQL 的规格选项:

util_postgredb.pl -version|-help

util_postgresqldb.pl -app

util_postgresqldb.pl -chkconf <INSTANCE NAME>

util_postgresqldb.pl -objs0 <INSTANCE NAME>

-objs1 <INSTANCE NAME><DATABASE NAME>

列出所有实例的输出片段:

C:\Program Files\OmniBack\bin>perl -I ..\lib\perl util_postgresqldb.pl -app

INS1 3306 [RUNNING]

Not-configured: 3434 [RUNNING]

*RETVAL*0

C:\Program Files\OmniBack\bin>

修改备份规范

有关修改 PostgreSQL 备份规范的信息，请参阅《Data Protector 帮助》索引: “备份规范, 修改”。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

有关如何创建和编辑计划的详细信息，请参阅调度程序。

启动备份会话

您可以按需运行交互式备份。交互式备份可用于在紧急情况下立即保护数据，还可用于重新启动失败的备份。

有关如何使用 Data Protector GUI 启动备份会话的说明，请参阅《Data Protector 帮助》索引: “启动, 备份会话”。

有关如何使用 Data Protector CLI 启动备份会话的说明，请参阅 omnib 命令页。

检查配置

您可以使用 Data Protector GUI 检查 Data Protector 中 PostgreSQL 实例的配置。请执行以下操作：

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，展开“备份规范”，接着展开“PostgreSQL”，然后选择属于 PostgreSQL 实例的备份规范。
3. 在“结果区域”中，右键单击“PostgreSQL 实例”，然后选择“检查配置”。配置检查成功完成后将显示以下消息: Integration is properly configured.

还原 PostgreSQL 集成

This feature is available in the Express Edition

Data Protector PostgreSQL 集成可以还原 PostgreSQL 数据库和 PostgreSQL WAL 文件。还原范围在启动还原会话时进行定义。只能从通过同一代理进行的备份执行还原和恢复。这意味着新代理将仅还原通过新代理进行的备份，而旧代理将仅还原通过旧代理进行的备份。

通过以下任何方式还原 PostgreSQL 对象:

- 使用 Data Protector GUI。请参阅使用 Data Protector GUI 还原。
- 使用 Data Protector CLI。请参阅使用 Data Protector CLI 还原。
- 使用 Data Protector REST API。请参阅使用 Data Protector REST API 还原。

要将 PostgreSQL 数据还原到另一个位置 (迁移 PostgreSQL 实例)，请参阅 PostgreSQL 数据迁移。

查找还原所需的信息

为了能够还原 PostgreSQL 数据，您应该从 Data Protector 内部数据库 (IDB) 检索有关 PostgreSQL 备份会话的信息，例如备份类型、使用的备份介质以及会话期间报告的消息。为此，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在 Data Protector GUI 中，执行以下步骤:

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开“对象”或“会话”。

   在“对象”树中，备份对象按照收集的备份数据来自的系统 (PostgreSQL 主机) 进行分组。PostgreSQL 主机按字母顺序排序。在会话树中，备份对象根据其创建会话进行分组，最新会话位于顶部。

   要查看某个备份对象的详细信息，请右键单击该备份对象，然后单击“属性”。要查看在会话期间报告的消息，请单击“消息”选项卡。

使用 Data Protector CLI

打开“命令提示符”窗口，然后运行 Data Protector `omnidb –integ PostgreSQL` 命令。该命令检索使用 Data Protector 备份的 PostgreSQL 对象列表。然后，可以通过指定其他命令选项列出相应的会话和备份介质。

使用 Data Protector GUI 进行还原

要使用 Data Protector GUI 还原 PostgreSQL 数据，请完成以下步骤:

1. 在“上下文列表”中，单击“还原”。
2. 在“范围窗格”中，依次展开“还原对象”、“PostgreSQL”以及要从中还原的 PostgreSQL 客户机。此时将在“结果区域”中显示备份对象的列表。
3. 选择要还原的备份版本和已备份的 PostgreSQL 实例。
4. 指定与还原有关的选项。如需了解与 PostgreSQL 有关的选项，请按 **F1**。**注意**: 在“选项”属性页中，“还原为实例”下拉列表显示所有实例的状态。如果选择任何正在运行的实例并单击“还原”，则会弹出消息，要求您确认是否要先停止所选实例，然后再继续还原。如果选择“是”，则数据库实例将停止并且还原将继续，否则还原过程将终止。停止的实例以下列格式显示: <实例名称> <端口><[已停止]> 暂存和导入表 (联机还原) 选项不会显示弹出窗口。如果所选实例未在运行，则还原将正常进行。
5. 查看还原所需的介质和设备并验证其可用性:
6. 单击**还原**。
7. 在“开始还原会话”对话框中，单击**下一步**。
8. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
9. 单击**完成**启动还原。

   会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

   成功还原数据库后，如果选中“还原后不启动服务”复选框，则服务不启动。

多主数据库还原

要还原到任何多主数据库框架的新群集，请完成以下步骤:

1. 识别构成新群集所需的所有节点。
2. 使用 Data Protector 的单节点还原功能仅还原到一个节点。然后，执行以下操作来创建新群集并显示群集。
3. 关闭 PostgreSQL 服务器。
4. 修改 **pg_hba.conf** 文件以仅接受来自选定节点的连接。
5. 将数据从已还原的节点复制到选定的所有其他节点。
6. 在所有节点上启动 PostgreSQL 服务。
7. 创建 PostgreSQL 多主数据库群集。
8. 再次修改 **pg_hba.conf** 文件以接受来自应用程序服务器的连接并重新启动 PostgreSQL 服务。

使用 Data Protector CLI 进行还原

要还原 PostgreSQL 实例，请在安装了 Data Protector“用户界面”组件的系统上运行以下命令:

omnir SESSION_OPTIONS [-noexpand] -integ PostgreSQL -barhost TargetPostgreSQLHostname -appname TargetInstanceName [-user Username:GroupName] -options -source_client SourcePostgreSQLHostname -source_instance SourceInstanceName -{session SessionID | -roll_forward [EndDateTime] } [GENERAL_OPTIONS]

有关选项说明和命令调用示例，请参阅 omnir 命令页。

使用 Data Protector REST API 还原

REST API 支持查看可用备份并通过可用备份之一进行还原。

GET

这用于查看可用的备份版本。

API 调用

https://win-6idthl5itko:7116/idb/restoretree/postgresql

Input Signature

{

End_time: “05/03/2019 16:55:00.0000”,

Mountpoint: “POSTGRES#8”,

Owner: “server.agent.test\ ADMINISTRATOR”,

Session_name: “2019/03/05-6”,

Start_time: “05/03/2019 16:50:00.0000”

}

参数说明:

End_time:	备份结束时间
Mountpoint:	源对象名称
Owner:	系统用户
Session_name:	备份会话 ID
Start_time:	备份开始时间

验证:

End_time:	字符串
Mountpoint:	字符串
Owner:	字符串
Session_name:	字符串
Start_time:	字符串

输出字段

Status:	“成功”或“失败”状态
Session_id:	备份会话名称

原始目标还原

此方法用于还原原始目标目录

Signature

{

"type": "PostgreSQL",

"barhost": "server1.agent.test",

"source_instance": "CM-BACKUP-5432",

"source_client": "server1.agent.test",

"session": "2019/03/05-4",

"appname": "CM-BACKUP-5432",

"username":"ADMINISTRATOR",

"groupname":"AGENT"

}

参数描述

Type:	代理类型
Barhost:	进行备份的系统的主机名
Source_instance:	备份实例名称
Source_client:	备份可用的系统名称
Session/Roll_forward:	会话 ID/还原/恢复时间
Appname:	备份实例名称
Username:	系统的用户名
Group:	域名

验证:

Type:	字符串
Barhost:	字符串
Source_instance:	字符串
Source_client:	字符串
Session/Roll_forward:	字符串
Appname:	字符串
Username:	字符串
Group:	字符串

输出字段

Status:	“成功”或“失败”状态
Session_id:	备份会话名称

非原始目标还原:

此方法用于还原非原始目标目录上的备份。

Signature

{

"type": "PostgreSQL",

"barhost": "server1.agent.test",

"source_instance": "CM-BACKUP-5432",

"source_client": "server1.agent.test",

"session": "2019/03/05-4",

"target_dir": "C:/rest_testing",

"appname": "CM-BACKUP-5432",

"username":"ADMINISTRATOR",

"groupname":"AGENT",

"port":"5432"

"pg_bin_dir": "C:/rest"

}

参数描述

Type:	代理类型
Barhost:	进行备份的系统的主机名
Source_instance:	备份实例名称
Source_client:	源系统名称
Session/Roll_forward:	会话 ID/还原/恢复时间
Target_dir:	必须进行备份的目标系统
Appname:	备份实例名称
Username:	系统的用户名
Group:	域名
Port:	端口号
Pg_bin_dir:	Bin 目录路径

验证

Type:	字符串
Barhost:	字符串
Source_instance:	字符串
Source_client:	字符串
Session/Roll_forward:	字符串
Target_dir:	字符串
Appname:	字符串
Username:	字符串
Group:	字符串
Port:	字符串
Pg_bin_dir:	字符串

输出字段:

Status:	“成功”或“失败”状态
Session_id:	备份会话名称

PostgreSQL 数据迁移

您可以将整个 PostgreSQL 实例迁移到同一个或不同客户机上的另一个 PostgreSQL 实例。按照标准还原过程执行操作，使用“恢复为实例”选项，并指定现有或新配置的实例。(您应该在开始还原之前配置新实例。单击“选项”属性页面中的“配置”。)如果实例尚不存在，Data Protector 将在还原后自动创建并启动它。使用“使用非原始目标目录”选项并指定目标目录的路径。要迁移 PostgreSQL 实例，目标 PostgreSQL 实例应在还原过程中处于脱机状态。

PostgreSQL 还原选项

以下是与 PostgreSQL 有关的还原选项:

要将选定的 PostgreSQL 对象还原到同一 PostgreSQL 实例，请保留以下选项的设置不变。请仅在迁移 PostgreSQL 时 (还原到与已备份实例不同的其他 PostgreSQL 实例) 使用这些选项。

恢复到客户机	此选项指定要将数据恢复到的 Data Protector 客户机。可以指定托管 PostgreSQL 数据库服务器且安装了 Data Protector“PostgreSQL 集成”组件的任何客户机。在此客户机上，Data Protector PostgreSQL 集成代理在还原会话开始时启动。 默认值：源客户机的完全限定域名。
恢复到实例	此选项指定要将数据恢复到其上的 PostgreSQL 实例的名称。如果实例尚不存在，则 Data Protector 将在恢复会话结束时自动创建并启动它。如果目标实例未启动，Data Protector 将在还原结束时自动配置并启动该实例。 默认值：源实例的名称。

用户名	此选项指定要用于恢复会话的操作系统用户帐户的用户名。必须比照 PostgreSQL 数据库管理员向所选帐户授予相应的特权，而且该所选帐户必须是在还原场景（Start restore 、 Restore from other users 、 Restore to other clients 等）中具有适当用户权限的 Data Protector 用户。如果未指定任何值，则将使用目标客户机上的 Data Protector Inet 帐户。 默认值：本地启动 Data Protector GUI 的用户帐户的用户名。
组/域	此选项指定要用于恢复会话的操作系统用户帐户的用户组或域。如果未指定任何值，则将使用目标客户机上 Data Protector Inet 帐户的用户组或域。 默认值：从本地启动 Data Protector GUI 的用户帐户的组/域。

恢复重定向

使用非原始目标目录	选择此选项可将数据库或 WAL 文件的还原重定向到不同于原始位置的位置 (执行迁移)。指定所选目录的完整路径。 对现有实例执行还原时，请确保提供到此实例上的数据库根目录（datadir）的有效路径。 默认：未选择。

数据库恢复

恢复到最新状态	选择此选项后，Data Protector 将应用存档的 WAL 文件，并将已还原的 PostgreSQL 实例置于最新的可用状态。 默认：选择。
恢复到	选择此选项后，Data Protector 将仅应用备份存档日志中的 WAL 文件，它们可将已还原的 PostgreSQL 实例置于其在所选时间点的状态。日期和时间解释为源客户机上的本地时间。 默认：未选择。
从备份版本恢复	选择此选项可从指定的备份版本恢复已还原的 PostgreSQL 实例。 默认：未选择。
不启动数据库实例	如果您不想在目标端口上启动数据库实例，请选中此复选框。仅当源实例和目标实例不同时，才启用此选项。 如果尚未选择“不启动数据库实例”，则还原将以旧样式进行。

监视和查看会话

可以在 Data Protector GUI 的监视器上下文中监视当前运行的 Data Protector 会话。“结果窗格”将显示选定会话的进度。关闭 GUI 不会影响会话。此外，也可以使用 GUI 的“内部数据库”上下文查看以前的 Data Protector 会话。

要监视正在 Data Protector 单元中或正在 Data Protector Manager-of-Managers 环境的所有单元中运行的会话，可以使用分别安装了 Data Protector“用户界面”或“Manager-of-Managers 用户界面” 组件的任何系统。

代理切换

代理切换有助于在新旧代理之间切换。仅 PostgreSQL 代理支持代理切换。

代理切换是通过编辑 global 文件完成的，因此会影响所有用户。备份规范和实例规范对这两个代理均通用。任何代理均可创建和使用规范。

global 文件中的切换标志 **EnableLegacyPostgreSqlAgent** 决定新旧代理是否用于备份和还原。

要切换代理，请完成以下步骤:

1. 打开任何文本编辑器。
2. 在文本编辑器中，打开位于以下路径中的 global 文件:
   - Windows： <PROGRAMDATA>\Config\Server\Options 。示例： C:\ProgramData\OmniBack\Config\Server\Options 。
   - Linux： /etc/opt/omni/server/options 。
3. 找到代理切换 EnableLegacyPostgreSqlAgent 的选项。如果未激活该选项，请删除选项名称前的 **#** 标记。
4. 设置代理切换的值。
   - EnableLegacyPostgreSqlAgent = 1 表示使用旧代理
   - EnableLegacyPostgreSqlAgent = 0 表示使用新代理

   默认情况下，新代理将处于活动状态。
5. 以 Unicode 格式保存文件。
6. 重新启动 Data Protector GUI 以应用新设置。

Postgres Professional 集成

Data Protector 提供了基于脚本的解决方案，以使用 pg_probackup 实用程序执行 Postgres Professional 数据库的备份和还原。本节介绍了执行备份和还原任务的步骤。

重要说明使用此脚本执行 Postgres Professional 数据库的备份和还原时，您将禁用或绕过安全功能，会使系统增加安全风险。使用此脚本即表示您了解并同意承担所有相关风险，同样使 Micro Focus 免受损失。

Micro Focus 鼓励您添加相关的保护措施以防范与用户信息相关的风险，Micro Focus 没有提供此保护措施。若未实施相应的保护措施，您的系统可能面临更多的安全风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

先决条件

以下先决条件适用:

- Data Protector Cell Manager 和磁盘代理版本 2020.05 或更高版本。
- Postgres Professional 版本 11.5.4。
- Postgres Professional 服务器必须在 RHEL 7.x 或 SLES 12.x 平台上运行。
- 在 Postgres Professional 服务器上安装 pg_probackup 实用程序，初始化该实用程序的备份编目并添加备份实例。

另外，建议:

- 采用专用的装载点来存储 pg_probackup 的备份编目。
- 仅将此备份编目用于 Data Protector 备份和还原操作。
- 设置适当的保留策略，以避免耗尽可用磁盘空间。

Postgres Professional 服务器与 Data Protector 的集成

Data Protector 使用名为 postgrespro.sh 的脚本来执行 Postgres Professional 数据库的备份和还原。该脚本在文件系统工作流中用作执行前或执行后脚本，并使用 pg_probackup 实用程序执行数据库备份和还原操作。

要将 Data Protector 与 Postgres Professional 服务器集成并配置 Data Protector，请按照以下步骤操作:

1. 从 ITOM Marketplace 下载 postgrespro.sh 脚本。如果您有任何问题，请联系客户支持。
2. 登录 Postgres Professional 备份主机，并将下载的脚本解压缩到以下位置:
   /opt/omni/lbin
   以下脚本是软件包的一部分: config.sh 和 postgrespro.sh
3. 将 postgrespro.sh 的文件权限更改为 500。
   例如： cd /opt/omni/lbin | chmod 500 postgrespro.sh
4. 将 config.sh 的文件权限更改为 700。
   例如： cd /opt/omni/lbin | chmod 700 config.sh
5. 使用任何文件编辑器打开 config.sh 文件，然后根据需要进行编辑。

备份 Postgres Professional 数据

Data Protector 使用文件系统备份功能支持 Postgres Professional 数据的完整和增量备份。Data Protector 增量模式对应于 Postgres Professional Delta 模式。

创建备份规范

要创建备份规范，请完成以下步骤:

1. 在 Data Protector UI 中，选择“备份”上下文。
2. 在“范围窗格”中，展开“备份规范”，右键单击“文件系统”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”，然后根据需要创建备份规范。创建备份规范后，它会在左窗格的“文件系统”类别下列出。
4. 在左窗格中选择备份规范。
5. 在“源”选项卡中，选择要备份的 pg_probackup 备份编目文件夹。
6. 在“选项”选项卡中，转到“文件系统选项”，然后单击“高级”。
7. 在“Pre-exec”字段中，指定 postgrespro.sh 。单击“确定”，然后单击“应用”。在备份期间，pre-exec 脚本使用通过 config.sh 和 Data Protector 备份代理传递的参数执行 pg_probackup 实用程序。 pg_probackup 实用程序在备份编目中备份 Postgres Professional 数据库。脚本成功运行后，Data Protector 会将数据从备份编目备份到配置的存储位置。

还原和恢复 Postgres Professional 数据

您可以将 Postgres Professional 数据还原到原始备份编目或其他位置。但是，只能对原始数据位置执行恢复。

注意: 在执行下列步骤之前，您必须重命名或删除 Postgres Professional 实例的原始数据文件夹。

要还原 Postgres Professional 数据库，请按照下列步骤操作:

1. 在 Data Protector UI 中，选择“还原”上下文。
2. 在“范围窗格”中，展开“文件系统”，使用要还原的数据展开客户端，然后仅选择用于 Postgres Professional 数据的备份文件夹，而不是整

个根级别。
3. 在“选项”选项卡中，转到“文件系统选项”，然后单击“高级”。
4. 在“Post-exec”字段中，指定 postgrespro.sh 。单击“确定”，然后单击“应用”。
如果要求您在“并行还原/单次还原”之间进行选择，请选择“单次还原”选项。Data Protector 会将所选数据还原到指定位置。然后， post-exec 脚本使用通过 config.sh 和 Data Protector 还原代理传递的参数来执行 pg_probackup 实用程序。之后， pg_probackup 将 Postgres Professional 实例恢复到其原始数据位置。

限制

以下限制适用：

- 不支持数据库级备份和还原。
- 仅支持完整备份和增量备份。
- 不支持恢复到原始位置以外的数据位置。
- 不支持介质副本。
- 不支持流备份。
- 不支持恢复到其他 Postgres Professional Server。
- 在备份期间，如果在执行 Postgres Professional 脚本后会话中止，则由 Data Protector 创建的大小为零字节的虚拟文件 (例如 postgres_1587411825_Q93SY) 不会被自动删除。
- 还原的目录不会自动清除。

故障排除

问题

增量备份会话可能因以下错误失败:

```
ERROR: Valid backup on current timeline 1 is not found. Create new FULL backup before an incremental one.
```

解决方案

触发完整备份而不是增量备份。

问题

备份会话显示以下错误消息:

```
ERROR: Switched WAL segment 0000000xxxxxxxxxxxxxxx could not be archived in 300 seconds
```

解决方案

要解决此问题，请尝试以下步骤:

1. 使用 --overwrite 选项设置正确的存档命令，然后重新启动 postgrespro-std-11 服务。
示例:
```
archive_command ='opt/pgpro/std-11/bin/pg_probackup archive-push -B /backup --instance dpbackup --wal-file-path %p --wal-file-name %f --overwrite'
```
2. 如果问题仍然存在，请检查 postgresql.conf 的 swp 文件是否存在:
示例：
```
/var/lib/pgpro/std-11/data
```

问题

备份会话失败并显示以下错误消息:

```
ERROR: required parameter not specified: PGDATA (-D, --pgdata)
```

解决方案

按如下所示设置 pg_probackup 配置:

```
pg_probackup set-config -B <backupCatalog> --instance=<InstanceName> --pgdata=<Path to PostgresPro server data folder>
```

示例:

```
pg_probackup set-config -B /backup --instance=dpbackup --pgdata=/var/lib/pgpro/std-11/data
```

SAP HANA 集成

本节提供特定于 Data Protector SAP HANA 集成的信息。它描述了概念以及成功备份和还原 SAP HANA 数据库和 SAP S/4 HANA 系统的过程，无论它们是否已作为 MDC (多租户数据库容器)、MCOD (一个数据库中的多个组件) 或 MCOS (一个系统中的多个组件) 部署在专用的物理或虚拟系统上。

除了保护 SAP HANA 数据库外，Data Protector 还提供文件系统备份和还原功能，以保护 SAP 基础架构的其他元素。

> 注意**:** SAP 继续为之前经过认证的第三方备份工具提供支持。但是，建议升级到该工具的最新认证版本以获得最佳体验。

Data Protector 在基于 IBM Power 和 Intel 的系统上使用 backint 与 SAP HANA 集成，以提供 SAP HANA 实例的联机备份和还原。使用 Data Protector SAP HANA 集成可以备份以下实体:

- SAP HANA 数据库
- SAP HANA 重做日志
- SAP HANA 编目

除了数据库备份外，还使用 Data Protector 文件系统备份功能配置 SAP HANA 配置文件的备份。

在备份期间，数据库保持联机状态，这意味着其他应用程序和用户可以主动使用该数据库。Data Protector 为 SAP HANA 数据库提供以下类型的备份:

完整	这将备份完整的 SAP HANA 数据库。相应的会话会备份整个数据库内容。 在 SAP HANA 术语中，此备份类型称为数据备份。
事务	这将备份 SAP HANA 重做日志。相应的会话会备份重做日志。 在 SAP HANA 术语中，此备份类型称为日志备份。
增量	此备份会存储上次修改过的数据备份。它会存储上次数据备份或上次增量备份 (增量或差异)。
差异	此备份会存储自上次完整数据备份以来发生更改的所有数据。

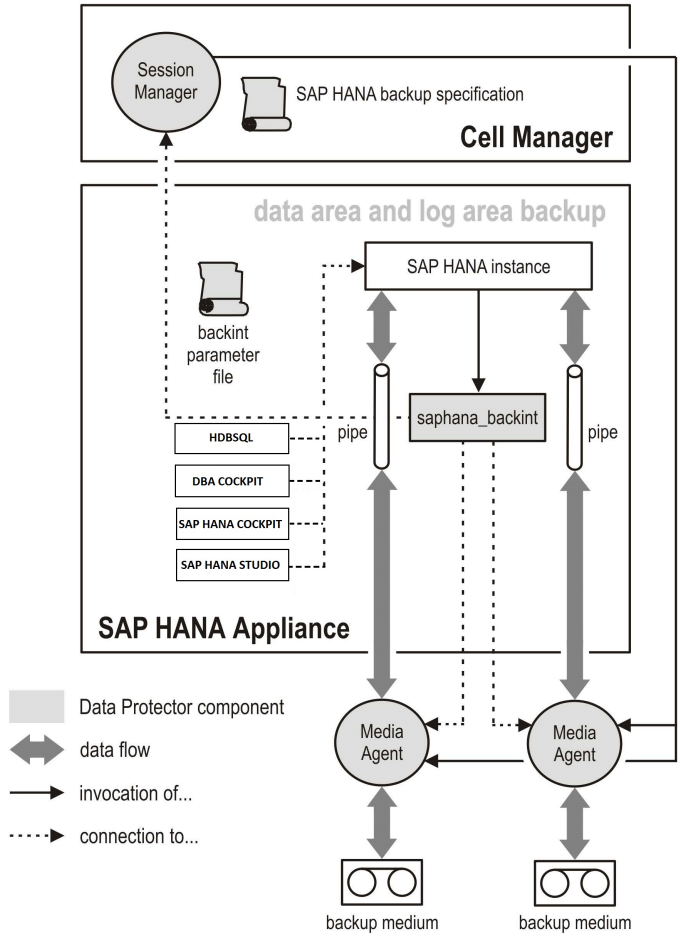
有关将 SAP HANA 对象还原到的可用目标位置 (原始位置与不同 Data Protector SAP HANA 客户机比较，原始位置与同一客户机上不同 SAP HANA 实例比较)，请参阅《SAP HANA 管理指南》以及 SAP HANA 文档集内的其他文档。

在还原过程中，还可将 SAP HANA 数据库恢复到特定时间点的状态或恢复到使用可用重做日志重新创建的最新状态。

> 重要说明**:** Data Protector SAP HANA 集成的当前实现不包括传统 Data Protector 应用程序集成代理。在该实现中，只能使用 Data Protector:
>
> - 定义需要备份的数据、这些数据的备份方式以及备份映像的存储位置，具体方式是在 Data Protector GUI 中配置 SAP HANA 备份规范。
> - 监视 Data Protector SAP HANA 备份和还原会话的进度。
> - 列出 Data Protector 备份的 SAP HANA 对象及其对应的会话。
>
> 备份和还原过程的执行时机 (例如备份会话何时启动、何时还原数据以及将数据还原到哪里) 以及数据库恢复选项由 SAP HANA 数据库本身控制。您只能从 SAP HANA Studio、 SAP HANA Cockpit、DBA Cockpit 或 CLI (SAP HANA `hdbsql` 命令行实用程序) 中定义和控制它们。

集成概念

Data Protector 使用“SAP HANA 集成” 组件与 SAP HANA 集成，而该组件的作用是提供 SAP HANA backint 代理的 Data Protector 实现。下图显示了 Data Protector SAP HANA 集成的体系结构。



Data Protector SAP HANA backint 代理由 saphana_backint 二进制文件组成，该文件充当 Data Protector 与 SAP HANA 备份和还原功能之间的接口。SAP HANA 数据库、重做日志和编目都作为流进行备份并还原。

多流数据备份

默认情况下，SAP HANA 使用一个通道进行数据备份。借助 SAP HANA 1.0 SPS 11 及更高版本，可以将备份数据并行分发到多个设备来显著缩短备份时间。使用多个通道时，SAP HANA 会在多个可用通道之间均匀地分发数据。多流备份的所有部分大致相同。为了提高性能，backint 代理可以使用多个并行流执行数据备份。如果已配置并行流，则各个服务备份将在所有可用流之间分发。不同的服务始终使用专用备份流。

对于旧版本的 SAP HANA，仅当备份大于 128 GB 时才会分发备份。较小的数据库将仅在单个备份流中备份。SAP HANA 2.0 SPS 05 及更高版本提供配置选项 parallel_data_backup_backint_data_threshold=n（以 GB 为单位）来配置多流的最小数据备份大小。

- 要配置并行流数量，请在 SAP HANA 数据库中配置参数 parallel_data_backup_backint_channels 。
- SAP HANA 1.0 SPS 11 及更高版本中提供了此功能。
- 每项服务允许的最大通道数为 32 个。
- 支持完整备份和增量备份。
- 启用多流备份时无需宕机时间。

> 注意**:** SAP HANA 重做日志的备份和还原始终是按顺序的，因为 SAP HANA 实例的重做日志是连续流，必须按时间顺序进行处理。处理日志备份的顺序由 backint 输入文件中列出管道的顺序指定。

满足 SAP HANA 集成的先决条件

满足以下要求:

- 确保 SAP HANA 数据库已正确安装和配置。有关安装、配置和使用 SAP HANA 数据库的信息，请参阅 SAP HANA 文档。
- 确保在 SAP HANA 服务器上正确安装 Data Protector 磁盘代理和 SAP HANA 集成代理。如果 SAP HANA 服务器直接访问备份设备，建议也安装介质代理。
- 根据 SAP HANA 备份策略需求配置 Data Protector 备份设备和 Data Protector 备份介质。
  - 由于 SAP HANA 数据库触发了 SAP HANA 重做日志备份的数量，因此强烈建议为重做日志备份配置“备份到磁盘”设备。
- 确保为运行 SAP HANA 备份和还原会话选择的 SAP HANA 操作系统用户帐户在 Data Protector admin 或 operator 用户组中配置了相应的 Data Protector 用户。
- 启用授权 BACKUP ADMIN 和 CATALOG READ 以备份 SAP HANA 单容器系统或 SAP HANA 多租户数据库容器中的系统数据库。
- 启用授权 DATABASE ADMIN 以备份 SAP HANA 多租户数据库容器中的租户数据库。
- 如果 Data Protector 备份旨在创建系统副本，请使用 Data Protector 将数据和日志备份到 backint。

- 如果 SAP HANA 编目备份未配置为 backint，请确保已使用其他方法正确备份了该备份。
- 为了进行备份，选定 SAP HANA 实例的数据库必须处于联机状态。
- 为了进行还原，目标 SAP HANA 实例的数据库必须处于脱机状态。

> 注意: 启动还原会话时， SAP HANA Studio可以自动使数据库脱机。但是，使用 hdbsql 命令行实用程序还原或恢复 SAP HANA 数据库之前，需要手动将该数据库置于脱机状态。

注意事项

以下限制适用:

- SAP HANA 实例的列表基于 /hana/shared 目录中的目录。如果它存储在任何其他非默认文件夹中，则必须在 omnirc 变量中添加路径 OB2_SAP_HANA_INSTALLATION_PATH.
- SQL 用户需要系统特权 **Backup Admin** 或 **Backup Operator** 来执行数据备份。如果使用 SAP HANA 接口执行数据备份，还需要 **Catalog Read** 特权。不建议使用 SYSTEM 用户进行正常的数据库操作。建议您创建一个仅具有备份和恢复所需特权的专用管理用户。
- 从 Data Protector 11.00 或更早版本升级后，您必须新建要从 Data Protector GUI 和 CLI 支持的 barlist。
- 如果在完整数据备份之前运行增量备份，它将回退到完整备份。
- 创建备份规范后，您必须从 SAP HANA Studio 执行日志备份。
- 升级到 Data Protector 11.01 后，必须创建新的备份规范才能从 Data Protector UI 或计划执行备份。

限制

以下限制适用:

- Data Protector GUI 仅支持完整和增量数据库备份。
- 不支持并行备份数据库。
- 如果 HDBSQL 查询需要更多时间来响应，则必须手动终止该进程。
- 不支持在多节点 (或横向扩展) 配置中备份数据库。
- 不支持从 Data Protector GUI 还原。
- 租户数据库备份完成后，租户数据库的 global.ini 文件中将不会重置以下键的值:
  - data_backup_parameter_file
  - parallel_data_backup_backint_channels
  - catalog_backup_parameter_file
  - catalog_backup_using_backint

配置集成

配置 SAP HANA 实例以执行 Data Protector 备份时，您需要:

- 将 Data Protector backint 代理与 SAP HANA 数据库链接起来。
- 为 SAP HANA 实例创建 Data Protector 备份规范。
- 创建 backint 参数文件作为 Data Protector 备份规范的参考。
- 调整数据库、重做日志和编目备份的 SAP HANA 备份设置，以使用 backint 接口而不是磁盘进行备份存储。

将 Data Protector backint 代理与 SAP HANA 数据库链接起来

请遵循以下步骤：

1. 以数据库系统管理员身份登录 SAP HANA 系统。这是为了确保创建的文件和目录具有正确的权限和所有权 (例如，如果 SAP HANA InstanceID 是 DB1，则管理员身份为 db1adm)。
2. 此步骤取决于您的 SAP HANA 环境。将工作目录更改为共享安装数据路径中的 global/hdb 文件夹。(例如，如果 SAP HANA 实例 ID 为 DB1， 则目录为 /hana/shared/DB1)执行以下命令:

   ```
   cd /hana/shared/<InstanceID>/global/hdb
   ```

3. 找到子目录 opt 。如果它不存在，请通过执行以下命令创建它:

   ```
   mkdir -m 750 opt
   ```

4. 创建指向 Data Protector backint 代理的符号链接。执行以下命令：

   ```
   cd opt
   ln -s /opt/omni/lbin/saphana_backint hdbbackint
   ```

5. 创建将包含稍后创建的 backint 参数文件的目录。操作系统用户 <sid>adm 和组 sapsys 必须具有特定于数据库的目录。

   ```
   mkdir -m 700 hdbconfig
   ```

要验证是否已在 SAP HANA Studio 中正确链接 backint 代理，可以在 SAP HANA Cockpit 中检查“备份”>“配置” >“Backint 设置” 上下文或“数据库管理” >“备份配置” >“目标类型” >“位置” 中的 backint 代理选项。

Cell Manager 配置

根据需要在 Cell Manager 上调整全局配置文件。

- MaxObjectsPerBackupSession 参数限制连接到同一备份会话的对象数。有效值为 1 到 223，默认值为 223。如果 MaxObjectsPerBackupSession 值达到 223，则备份将在新会话中继续。

- 使用 SmWaitForNewBackupClient 或 SmWaitForNewBackupClientSec 参数来增加最后一个备份客户机断开连接后的备份会话超时。在从同一 SAP HANA 数据库服务器启动大量重做日志备份的情况下，这可能很有用。在为备份会话超时设置的持续时间内，备份会话不会终止。如果它从同一数据库服务器接收其他备份对象，则将它们附加到同一备份介质。如果未收到任何信息，备份会话将结束并关闭备份介质。

安装 SAP HANA Appliance 客户机

This feature is available in the Premium Edition

要将 Data Protector 与 SAP HANA Appliance (SAP HANA) 集成，请在 SAP HANA 系统上安装以下Data Protector 软件组件:

- SAP HANA Integration

  该组件支持完整 SAP HANA 数据库和 SAP HANA 重做日志的集成备份。

- Disk Agent

  该组件支持使用 Data Protector 文件系统备份功能对 SAP HANA 配置文件进行非集成备份。发生灾难后，SAP HANA 配置文件的备份映像可以帮助您更轻松地识别和还原更改。

在分布式 SAP HANA 环境中，在组成该环境的每个 SAP HANA 系统上安装上述组件。

备份 SAP HANA 集成

Data Protector SAP HANA 集成提供 SAP HANA 数据库、重做日志和编目的联机备份。从 Data Protector GUI 或 SAP HANA 用户界面启动备份会话时会定义备份范围。有关需要在 SAP HANA 配置文件备份范围内备份的数据及其位置的信息，请参阅《SAP HANA 文档》。

> 注意**:** 使用数据或日志备份时，不会备份数据库配置文件 (.ini 文件)。您可以手动备份包含特定于客户的更改的配置文件，以便在恢复情况下识别并还原特定于客户的更改。您还可以从 Data Protector 配置文件系统备份以备份和还原数据库配置文件，或者在配置备份规范以备份数据库配置文件时使用 post-exec 脚本。

创建备份规范

要创建 SAP HANA 备份规范，请继续执行以下步骤:

1. 启动 Data Protector GUI。
2. 在上下文列表中，单击**备份**。
3. 在“范围窗格”中，展开“备份规范”，右键单击“SAP HANA 服务器”，然后选择“添加备份”。
4. 在“创建新备份”对话框中，选择“空白 SAP HANA 备份”模板。单击**确定**。
5. 从“客户机”下拉列表中选择:
   - SAP HANA 系统

     (如果您的 SAP HANA 数据库是单服务器环境)
   - 具有配置的名称服务器角色的 SAP HANA 主控主机 MASTER1

     (如果您的 SAP HANA 数据库是分布式环境；有关如何确定具有此角色的 SAP HANA 系统的说明，请参阅 SAP HANA 文档)

   “实例名称” 将列出属于所选客户机的所有实例。选择一个实例。
6. 在“用户名”和“组/域名”文本框中，输入相应的 SAP HANA 用户帐户。这是运行 SAP HANA 实例的操作系统用户和组。

   单击“下一步”。
7. 此时将显示配置对话框。输入创建配置文件所需的详细信息。单击 确定。有关每个字段的详细信息，请单击“帮助” 选项。
8. 选择要备份的对象。您可以选择备份“编目” 、“数据” 或“日志” 。展开对象以进行此选择。Data Protector GUI 仅支持“编目” 和“数据” 备份。要运行“日志” 备份，请创建单独的备份规范并从任何 SAP HANA 接口启用自动日志备份。有关创建日志备份的详细信息，请参阅配置 SAP HANA 以进行备份。单击“下一步”。
9. 选择用于备份会话的备份设备。如果需要，可更改它们的顺序并调整负载均衡和对象镜像。

   要指定设备选项，请右键单击该设备，然后选择“属性”打开“设备属性”对话框，从中可以修改与设备有关的选项。完成后，单击“确定”。

   > 注意**:** 为了以最佳性能还原 SAP HANA 重做日志，建议在用于日志备份的备份规范中将设备“并发”选项设置为 1 或“备份到磁盘”设备。

   单击“下一步”。
10. 在“备份规范选项”下，输入备份规范的可选描述，然后单击“高级”来调整常规备份规范选项。

    在“常见应用程序选项”下，单击“高级”以调整常见备份选项。
    在“应用程序特定选项”下，单击“高级” 以调整 SAP HANA 集成特定选项。您可以在此处为多流数据、自定义脚本执行 (pre-exec 和 post-exec 脚本) 设置并行性。有关这些选项的详细信息，请单击对话框底部的“帮助” 选项。
11. 单击“下一步”。
12. 单击“另存为”。
13. 在“将备份另存为”对话框的“名称”文本框中，输入备份规范的名称。在“组”下拉列表中，选择备份规范组。
14. 单击“确定”，保存备份规范。

    > 注意**:** 您可以创建一个专用的 Data Protector 备份规范组，然后将自己的备份规范都保存在该组中，从而将 Data Protector SAP HANA 备份规范整理得井井有条。
15. 为重做日志创建单独的备份规范。您可以再次使用“另存为” 按钮，也可以使用先前创建的 SAP HANA 备份规范的上下文菜单中的“复制为” 。

> 注意**:** 单独的备份规范允许为编目、数据和重做日志备份配置不同的设备。建议保留单独的日志备份规范。数据和编目备份可以是同一备份规范的一部分。根据设备类型，这将避免在备份或还原期间锁定设备。

启动 SAP HANA 备份

通过当前实施的 Data Protector SAP HANA 集成，您现在可以使用以下任一方式启动 SAP HANA 数据备份:

- Data Protector GUI，或
- 任何 SAP HANA 接口。

从 Data Protector GUI 启动 SAP HANA 备份

完成以下步骤：

1. 启动 Data Protector GUI。
2. 在上下文列表中，单击**备份**。
3. 在“范围窗格”中，展开“备份规范”，然后展开“SAP HANA 服务器”。右键单击要启动的备份规范，然后单击“启动备份...”。

从 Data Protector 高级调度程序计划备份

要从 Data Protector 高级调度程序计划备份，请完成以下步骤:

1. 启动 Data Protector GUI。
2. 在“上下文列表”中，单击“主页”。
3. 单击“调度程序”。
4. 单击“+ 新建” 选项创建新的计划。此时将显示“创建新计划”对话框。
5. 在“规范” 选项卡中，展开“备份规范” 并展开 **hana**。选择您要为其计划备份的备份规范，然后单击“下一步”。
6. 在“属性” 选项卡中，指定详细信息并单击“下一步”。
7. 在“重复” 选项卡中，指定详细信息并单击“下一步”。
8. 在“摘要” 选项卡中查看详细信息，然后单击“完成”。

从 SAP HANA 界面启动 SAP HANA 备份

要从 SAP HANA 界面启动 SAP HANA 备份，请执行以下操作:

为 SAP HANA 创建参数文件
要成功执行 SAP HANA 备份和从 SAP HANA 界面还原会话，您需要定义 Data Protector 参数，并使其可供 SAP HANA 实例使用。请执行以下操作:

1. 以数据库系统管理员身份登录 SAP HANA 系统。这是为了确保创建的文件和目录具有正确的权限和所有权。(例如，如果 SAP HANA 实例 ID 为 DB1， 则使用 db1adm 登录)
2. 此步骤取决于您的 SAP HANA 环境。将工作目录更改为共享安装数据路径中 backint 参数的特定于数据库的目录。(例如，如果 SAP HANA 实例 ID 为 DB1， 则目录为 /hana/shared/DB1)执行以下命令:

   ```
   cd /hana/shared/<InstanceID>/global/hdb/opt/hdbconfig
   ```

3. 在特定于数据库的目录中，为先前创建的备份规范创建 backint 参数文件。

   在 OB2BARLIST 参数中，提及特定于编目、数据或重做日志备份的备份规范的名称。 OB2BARHOSTNAME 它是在配置备份规范时从客户机下拉列表中选择的字符串。建议参数文件名称、备份规范和参数文件中的 OB2BARLIST 与备份保持一致。

4. 为数据备份规范创建参数文件。例如 DB1_DATA.par：

   ```
   OB2BARLIST='DB1_DATA';
   OB2BARHOSTNAME='HANA_System_FQDN';
   OB2_SAPHANA_DATABACKUP=1;
   OB2_SAPHANA_DBNAME='DATABASE_NAME'
   OB2_SAPHANA_BACKUP_PREFIX='BACKUP_PREFIX'
   ```

5. 为日志备份规范创建参数文件。例如 DB1_LOG.par：

   ```
   OB2BARLIST='DB1_LOG';
   OB2BARHOSTNAME='HANA_System_FQDN';
   OB2_SAPHANA_DBNAME='DATABASE_NAME'
   ```

6. 为编目备份规范创建 (可选) 参数文件。如果决定不为编目备份配置单独的参数文件，请对日志备份和编目备份使用相同的参数文件。例如 DB1_CATALOG.par：

   ```
   OB2BARLIST='DB1_CATALOG';
   OB2BARHOSTNAME='HANA_System_FQDN';
   ```

7. 参数文件必须由操作系统用户 <sid>adm 和组 sapsys 拥有。将访问权限 600 分配给参数文件。相应地使用 chown 和 chmod 命令。

配置 SAP HANA 进行备份

一旦创建了参数文件和备份规范，您必须在 SAP HANA 用户界面之一中进行配置。在 SAP HANA Cockpit 上执行以下步骤:

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理” >“备份配置” 。
2. 在“Backint 参数文件” 上选择“编辑”：
   - 禁用“对所有备份使用相同的参数文件” 。
   - 指定使用完整路径创建的参数文件。

     参数文件的完整路径名的示例为 /hana/shared/DB1/global/hdb/opt/hdbconfig/DB1_DATA.par 。
3. 在“编目设置” 上选择“编辑”：
   - 将“目标类型” 从“文件”更改为“Backint” 。
4. 确认在“日志设置日志” 中将“日志模式” 配置为“正常” 。
5. 在“日志备份” 上选择“编辑”：
   - 将“目标类型” 从“文件”更改为“Backint” 。
   - 使用选项根据您的还原要求配置备份日志。默认配置将导致每 15 分钟进行一次日志备份 。
     - “最晚在指定的时间限制后”，代表 log_backup_interval_mode = immediate ，位于以下文件: global.ini
     - “仅在指定的时间限制后”，代表 log_backup_interval_mode = service ，位于以下文件: global.ini

     重要说明**:** 虽然可以在 SAP HANA Cockpit 中配置该选项，但 SAP HANA Studio 不允许您配置“仅在指定的时间限制后” ，因此如果需要，请在 global.ini 中配置它。SAP HANA 2.0 SPS 00 及更高版本提供了选项 log_backup_interval_mode 。
6. 在“数据备份” 上选择“编辑”：
   - 将“目标类型” 从“文件”更改为“Backint” 。
   - 根据需要增加并行流 (Backint 备份)。这仅适用于大于 128 GB 的数据库。
7. 在“数据备份调度程序” 上选择“编辑”：
   - 为 SYSTEMDB 和租户数据库配置数据备份计划。
   - 对于租户数据库，无需创建单独的备份规范。它使用相同的系统数据库备份规范。

     注意**:** SAP HANA 多租户数据库容器中的默认隔离级别较低。您可以将隔离级别提高到较高水平，以确保一个租户数据库无法访问另一个租户数据库的数据备份或日志备份。在具有多个租户数据库的 SAP HANA 多租户数据库容器中，可能需要许多 backint 参数文件以确保高度隔离。这些 backint 参数文件由具有读写访问权限的操作系统用户 (<sid>adm) 管理。
8. 在 **SAP HANA Cockpit** 中，导航到“数据库管理” > 选择一个 **HANA** 数据库 >“数据加密” >“备份加密” 。
   - 确保仅对支持备份加密的备份设备启用了备份加密。

     重要说明**:** 如果在具有本地重复数据删除或压缩功能的备份设备上启用加密，将防止备份介质上任何类型的数据减少。在 SAP HANA 中使用备份加密时要格外小心。如果需要加密，请在备份设备级别或在 Data Protector 中进行配置。

启动 SAP HANA 备份

您可以使用 SAP HANA 用户界面之一启动 Data Protector SAP HANA 备份会话: SAP HANA Studio、SAP HANA Cockpit、DBA Cockpit 或 hdbsql 命令行实用程序。您还可以执行租户数据库备份。从 SAP HANA 1.0 SPS 9 开始，您可以执行增量备份和差异备份。

有关如何启动会话来备份 SAP HANA 数据库以及如何配置和调整来定期备份 SAP HANA 重做日志的说明，请参阅《SAP HANA 管理指南》以及 SAP HANA 文档集中的其他文档。

要使用 SAP HANA Cockpit 创建 SAP HANA 数据库的手动备份，请执行以下操作:

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理” > 选择 一个 HANA 数据库 >“数据库备份”。
2. 选择“创建备份”。
3. 选择“备份类型”(“完整”、“增量”或“差异”)，并选择 “Backint” 作为“目标类型”。
4. 选择“备份” 并从 SAP HANA Cockpit 或 Data Protector 监视器监视会话进度。

使用 SAP HANA 接口计划 SAP HANA 备份

要使用 SAP HANA Cockpit 计划 SAP HANA 数据库的备份，请执行以下操作:

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理” >“备份计划” 。
2. 选择“创建计划” 。
3. 选择“系列备份” 或 “单个备份” 和“要备份的数据库” 。
4. 分配“计划名称” 、“备份类型” (“完整”、“增量”或“差异”) 和“目标类型” (Backint)。
5. 选择“重复模式” 和“重复详细信息” 。
6. 选择“预览” 以查看更改，然后选择“保存计划” 。
7. 确保已为 SYSTEMDB 和租户数据库启用了调度程序。

> 注意**:** 如果需要从 Data Protector 计划，请配置文件系统备份作业，以使用 pre-exec 脚本备份 SAP HANA 系统的其他关键元素，并使用适当的 hdbsql 命令启动 SAP HANA 备份。您可能要使用 ITOM Marketplace 中的SAP HANA backint。

SAP HANA 日志备份

SAP HANA 实例触发 SAP HANA 重做日志备份到配置的备份目标 (backint 或文件)。默认情况下，日志备份将每 15 分钟执行一次，这会每天产生大量的备份会话，尤其是在具有多个实例和/或租户数据库的环境中。

SAP HANA 的最新版本提供了重做日志的细粒度配置。您可以配置备份重做日志的时间:“最晚在指定的时间限制后” 或“仅在指定的时间限制后” 。通过后一选项，可以选择根据服务级别主动减少重做日志备份的数量。

SAP HANA 编目备份

SAP HANA 备份编目中的内容更改后就执行 SAP HANA 编目备份。更改可能是数据的新备份、重做日志或对编目的手动更改。编目备份可以在单独的备份规范中配置，也可以配置到与重做日志备份相同的位置。

> 重要说明**:** global.ini 中的默认 catalog_backup_parameter_file 参数为空。因此，备份编目的备份将写入日志备份的默认目录。 global.ini 中的默认 catalog_backup_using_backint 参数为 false。因此，默认情况下，备份编目的备份将写入文件系统。

编目备份对象在 Data Protector 备份会话报告中显示为 log_backup_0_0_0_0 。

```
[Normal] From: OB2BAR_SAPHANA_BACKINT@hana.domain.tld "DB1"  Time: 16.03.2021 14:37:26    backint input information (/var/tmp/hdbbackint_DB1.0XVRVA):
#SOFTWAREID "backint 1.04" "HANA HDB server 2.00.045.00.1575639312"    #PIPE "/usr/sap/DB1/SYS/global/hdb/backint/SYSTEMDB/ log_backup_0_0_0_0"
```

从 Data Protector IDB 删除的 SAP HANA 对象的信息存储在 SAP HANA 系统上的 /var/opt/omni/log/saphana.log 文件中。

有关“SAP HANA 备份编目” 的详细信息，请参考《SAP HANA 管理指南》。

为 SAP HANA 配置多流数据备份

除非数据库大于 128 GB，否则将始终以一个流执行 SAP HANA 数据库的备份。如果数据库大于 128 GB，则可以配置 SAP HANA 数据备份的流数。请注意，附加备份流将消耗附加系统资源。

请遵循以下步骤：

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理” >“备份配置” 。
2. 在“数据备份” 上选择“编辑” :
   - 根据需要增加并行流 (Backint 备份)。这仅适用于大于 128 GB 的数据库。
3. 在 **SAP HANA Cockpit** 中，导航到“数据库管理” >“SYSTEMDB” >“管理系统配置”
   - 验证参数 parallel_data_backup_backint_channels 。它应当反映步骤 2 中所做的更改。
   - 根据步骤 2 中配置的流数更改参数 data_backup_buffer_size 。每个流消耗 512 MB。例如，对于 4 个流，将 2048 MB 配置为 data_backup_buffer_size 。
4. 监视接下来的几次备份及其备份时间，确认备份性能有无提升。您会发现备份时间缩短了 30-40%，但具体提升幅度取决于您的备份环境。

系统维护

为了在 Cell Manager、介质代理或备份设备上进行系统打补丁和其他日常维护活动，可能需要停止并阻止启动新会话。由于 SAP HANA 备份会话是从 SAP HANA 实例启动的，因此停止 Data Protector 调度程序不会阻止触发 SAP HANA 备份。根据情况，有几个选项可用。

Data Protector 维护模式

为了阻止来自所有客户机系统 (包括单元中的所有 SAP HANA 实例) 的备份会话，请使用 Data Protector 维护模式。使用命令 omnisv -maintenance 在 Cell Manager 上从“生产模式”转换为“维护模式”。

- 生产模式到阶段 **1:** 正在进行的会话将继续运行，新会话被 Cell Manager 拒绝。触发器将停止。
- 阶段 **1** 到阶段 **2:** 仍在进行的所有会话 (包括 GUI 连接) 将主动终止
- 阶段 **2** 到维护模式**:** 没有会话正在运行，新会话被 Cell Manager 拒绝。触发器保持停止。

Cell Manager 进入维护模式后，您可以根据需要使用 omnisv -stop 停止服务或重新启动 Cell Manager 系统。维护模式是永久性的，直到您使用 omnisv -maintenance -stop 离开该模式为止。

阻止从 SAP HANA Cockpit 进行 SAP HANA 备份

要仅阻止单个或一组 SAP HANA 实例执行备份，还有其他选项。在 **SAP HANA Cockpit** 中，您可以禁用自动日志备份，在以后的某个时间点再将其改回。确保在禁用日志备份时监视日志区域的可用空间。

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理” >“备份配置” 。
2. 在“日志备份” 上选择“编辑”：
    - 禁用 Backint 的自动日志备份。

阻止从 Cell Manager 进行 SAP HANA 备份

要仅阻止单个或一组 SAP HANA 实例执行备份，还有其他选项。在 **Cell Manager** 中，您可以重命名 SAP HANA 备份规范以使其不可用。

1. 登录 **Cell Manager** 系统。
2. 导航到 %DP_DATA_DIR%Config\Server\BarLists\hana (Windows) 或 /etc/opt/omni/server/barlists/hana (Linux)
    - 重命名 SAP HANA 备份的相应文件，以使参数文件无法找到备份规范。

      无效备份规范文件的示例为 DB1_DATA.disabled

> 警告**:** 如果使 Cell Manager 或单个备份配置再次可用，将导致立即并行执行可能大量的备份。备份数量取决于为备份配置的 SAP HANA 实例。

还原 SAP HANA 集成

Data Protector SAP HANA 集成可以还原 SAP HANA 数据库和 SAP HANA 重做日志。从 SAP HANA 用户界面启动恢复会话时会定义还原范围。Data Protector SAP HANA 集成可还原特定租户数据库，以及将 SAP HANA 数据库的副本提供给另一个 SAP HANA 数据库。

> 注意**:** 有关要在 SAP HANA 配置文件还原范围内还原的数据及其位置的信息，请参阅 SAP HANA 文档。

数据库恢复的先决条件

- 您必须在目标系统中以操作系统用户 <sid> adm 登录。
- 如果数据库从一台主机恢复到另一台主机，则 SAP HANA 数据库服务的数量和类型在源系统和目标系统中应相同。有关数据库服务的更多详细信息，请参考《SAP HANA 管理指南》。
- 以下备份或数据必须可用:
  - 完整备份 (完整的数据备份或存储快照)，该备份在恢复之前已存在。
  - 自从使用完整备份以来创建的增量备份 (如果需要)。
  - 自从使用完整备份以来创建的日志备份 (如果需要) (覆盖增量备份中尚未包含的更改)。
  - 日志区域 (如果需要)。
- 要恢复特定于客户的配置设置，建议您先配置特定于客户的设置，然后再恢复数据库和重播日志备份。
- 要恢复完整的 SAP HANA 多租户数据库容器系统，需要首先恢复系统数据库，然后再分别恢复所有租户数据库。

> 注意**:** 执行数据库恢复时，客户特定的配置文件并不是必需的。它们没有进行备份。有关备份客户特定配置文件的详细信息，请参阅《SAP HANA 管理指南》。

查找要还原的信息

要查找还原 SAP HANA 数据所需的信息，请使用 Data Protector omnidb –saphana [Client:Set] 命令。该命令会检索由 Data Protector 备份的 SAP HANA 对象列表及其对应的会话。有关详细信息，请参阅《Data Protector 命令行界面参考》中的 omnidb 参考页或 omnidb 手册页。

SAP HANA 数据库恢复

在当前的 Data Protector SAP HANA 集成实现中，只能使用以下 SAP HANA 用户界面之一来启动 Data Protector SAP HANA 还原或恢复会话: SAP HANA Studio、SAP HANA Cockpit 或 hdbsql 命令行实用程序。有关如何启动 Data Protector 会话来还原 SAP HANA 数据库、如何执行数据库恢复以及如何指定其他还原选项的说明，请参阅《SAP HANA 管理指南》和 SAP HANA 文档集中的其他文档。

> **注意:** 要在开始数据库恢复之前检查备份的完整性，请运行 hdbbackupcheck 命令。检查自使用 hdbbackupdiag 命令创建以来，各个数据备份和日志备份是否已更改。确定完成恢复所需的数据备份和日志备份，并检查这些备份是否可用并且可访问。

可以出于各种原因使用 SAP HANA 数据库恢复。如果数据和日志区域变得不可用，则需要快速将数据库恢复到最新的时间点。如果数据库中出现逻辑错误，则必须将其恢复到损坏发生之前的时间点。

数据库恢复也常用于将 SAP HANA 数据库复制到另一个系统或租户数据库。可以对同一台计算机和 SID 执行恢复，也可以对具有相同或不同 SID 的另一台计算机执行恢复。根据情况使用或不使用 SAP HANA 备份编目。如果不使用，用户必须相应地指定备份片。

租户数据库必须通过其系统数据库进行恢复。如果只是租户数据库损坏，则不需要先恢复系统数据库。仅在系统数据库已损坏时恢复系统数据库。如果使用 SAP HANA Cockpit 执行系统数据库的恢复，则只能还原最近的状态。使用 recoverSys.py 命令行实用程序进行时间点恢复。请记住，在该时间点之后注册的租户数据库将丢失，必须重新创建和还原。

在同一台计算机上恢复数据库

使用 SAP HANA Cockpit 在同一台计算机上恢复数据库时，请执行以下步骤。请执行以下操作：

1. 启动 **SAP HANA Cockpit**，然后导航到“数据库管理”。
2. 在需要恢复的数据库 上选择“恢复”。

   > 重要说明**:** SAP HANA Cockpit 将立即停止选择用于还原的数据库。在生产系统上测试还原操作时要加以小心。

3. 选择“恢复到最近状态”或“恢复到特定时间点”。恢复选项因 SAP HANA Cockpit 中的 SAP HANA 部署 (单容器系统或 MDC) 和数据库类型 (系统或租户数据库) 而异。
4. 当系统要求输入“最新备份编目的位置”时，选择“仅 Backint 位置”。将为数据库还原最后一个 SAP HANA 备份编目。您可以在 Data Protector 监视器中监视状态。

5. 选择要还原的数据备份之一。仅显示 SAP HANA 备份编目中记录的备份。
6. 在下一步中，选择除了完整数据备份之外，是否应使用增量备份进行还原。使用增量备份进行还原还需要在还原期间进行日志备份。如果它们不可用，则只能还原到完整数据备份。
7. 如果所有备份都已通过 Data Protector 使用 Backint 进行了备份，则“指定备用备份位置” 无利可图。
8. 在“检查备份可用性” 中，如果仅使用 Backint，建议不进行文件系统功能备份的检查。
9. 选择是否应初始化日志区域。
10. 如果不需要更改，请查看“摘要”并使用“启动恢复”按钮。您可以在 Data Protector 监视器和 SAP HANA Cockpit 中监视还原会话的状态。

数据库复制到相同或不同的计算机

数据库复制是设置克隆数据库的快速方法，例如用于培训、测试或开发。备份和恢复是将系统数据库或租户数据库复制到同一系统或不同系统的首选选项。复制数据库使用完整数据备份或使用数据和日志备份的时间点。数据库复制后，目标数据库配置有与原始数据库相同的备份计划。

> 注意**:** 编目、数据和日志的备份必须配置为使用 Backint (Data Protector) 或文件系统 (SAP HANA 系统)，否则复制数据库将失败。这是 SAP HANA 的限制。

在继续将 SAP HANA 数据库复制或还原到另一个系统之前，请确保已为 Data Protector 配置了目标计算机和数据库，并且已配置和测试目标数据库的备份。有关详细信息，请参阅 SAP HANA 集成和 SAP HANA 备份配置。使用 SAP HANA Cockpit 在具有相同或不同 SID 的另一台计算机上恢复数据库时，请执行以下步骤。请执行以下操作：

1. 以数据库系统管理员身份登录 SAP HANA 系统。这是为了确保创建的文件和目录具有正确的权限和所有权 (例如，如果 SAP HANA InstanceID 是 DB9，则管理员身份为 db9adm)。
2. 此步骤取决于您的 SAP HANA 环境。将工作目录更改为共享安装数据路径中 backint 参数文件的特定于数据库的目录。(例如，如果 SAP HANA 实例 ID 为 DB9， 则目录为 /hana/shared/DB9)执行以下命令:

   ```
   cd /hana/shared/<InstanceID>/global/hdb/opt/hdbconfig
   ```

3. 在特定于数据库的目录中，创建用于还原 的附加 backint 参数文件。它应当与 SAP HANA 源系统上使用的参数文件的内容相匹配。

   在 OB2BARLIST 参数中，使用用于源系统数据备份的备份规范的名称。 OB2BARHOSTNAME 是 Data Protector 中为源系统的备份对象列出的主机名。

4. 为数据备份规范创建参数文件。例如 DB1_RESTORE.par：

   ```
   OB2BARLIST='DB1_DATA';
   OB2BARHOSTNAME='HANA_System_FQDN';
   ```

5. 启动 **SAP HANA Cockpit**，然后导航到目标计算机的“数据库管理” 。这假设目标租户数据库已经存在 (例如 DBR)。
6. 选择目标数据库并打开“管理系统配置” 。
7. 选择 **data_backup_parameter_file** 旁边的“覆盖值” 并配置刚刚创建的参数文件的绝对路径 (例如: /hana/shared/DB9/global/hdb/opt/hdbconfig/DB1_RESTORE.par)。
8. 导航到“数据库管理” ，然后在需要复制的数据库 上选择“复制” 。

   > 重要说明**:** SAP HANA Cockpit 将立即停止选择用于复制的数据库。在生产系统上测试还原操作时要加以小心。

9. 选择“仅完整数据备份” 。这是必需的，因为目标数据库的备份编目不包含任何备份。
10. 在下一步中，如果系统询问是否应使用“备份编目” ，请选择“否” 。
11. 选择“Backint” 作为“备份位置” 。
12. 根据“源系统类型” ，选择“多容器” 或“单容器” 。
13. 输入“源系统的 SID” (例如: DB1) 和“源数据库名称” (例如: DB1)。
14. 由于未使用备份编目，用户必须指定要复制的备份。可以通过查看要复制的 SAP HANA 备份会话的会话消息来标识“备份前缀” (例如: /usr/sap/DB1/SYS/global/hdb/backint/DB_DB1/2021_05_10_18_00_00)。

    ```
    [Normal] From: OB2BAR_SAPHANA_BACKINT@lejlx15.mfdemo.local "DB1"  Time: 10.05.2021 18:00:00
      backint input information (/var/tmp/hdbbackint_DB1.SCUQIF):
      #SOFTWAREID "backint 1.04" "HANA HDB server 2.00.045.00.1575639312"
      #PIPE " /usr/sap/DB1/SYS/global/hdb/backint/DB_DB1/2021_05_10_18_00_00_databackup_0_1
    ```

15. 如果不需要更改，请查看“摘要” 并单击“启动复制” 按钮。您可以在 Data Protector 监视器和 SAP HANA Cockpit 中监视还原会话的状态。
16. 撤消在步骤 7 中添加的特定于数据库的配置更改，以允许数据备份使用系统范围的默认值并执行完整数据备份。
17. 如果不需要更多副本，则可以选择删除在步骤 3 中添加的特定于还原的 backint 参数文件。

使用其他设备进行还原

SAP HANA 正在使用 Data Protector 通过 backint 进行介质管理。这意味着整个介质管理对 SAP HANA 是透明的。使用对象复制、对象镜像或替换来复制备份对 backint 和 SAP HANA 是透明的。如果未找到原始介质，Data Protector 将在内部切换到可用的下一个副本。

如果需要更改备份设备或需要从副本执行还原，用户可以执行用于备份的还原设备以外的还原设备。在启动还原操作之前，针对每个对象相应地更新 Cell Manager 上的内部数据库。

> 注意**:** 根据还原操作，可能需要更改多个备份会话和对象。 RECOVER DATABASE 将数据库恢复到特定时间点或特定日志位置。因此，完整数据备份、增量备份和日志备份构成了还原链。 RECOVER DATA 仅将数据库恢复到特定的完整数据备份。

1. 标识 Data Protector 内部数据库 (IDB) 中的备份会话
2. 通过运行以下命令获取会话详细信息和首选备份设备:
   omnidb -session <SessionID> -detail
3. 通过运行以下命令更新首选备份设备:
   omnidbutil -changebdev <FromDevice><ToDevice> -session <SessionID>

监视会话

可以在 Data Protector GUI 的监视器上下文中监视当前运行的 Data Protector 会话。“结果”窗格将显示选定会话的进度。关闭 GUI 不会影响会话。

要监视正在 Data Protector 单元中或正在 Data Protector Manager-of-Managers 环境的所有单元中运行的会话，可以使用分别安装了 Data Protector 用户界面或 Manager-of-Managers 用户界面组件的任何系统。

Red Hat KVM 主机集成和 VM 备份

本主题提供有关 Red Hat KVM 主机与 Data Protector 的集成以及 Red Hat KVM 主机中联机虚拟机 (VM) 上的备份/还原的信息。

基于 Red Hat 内核的虚拟机

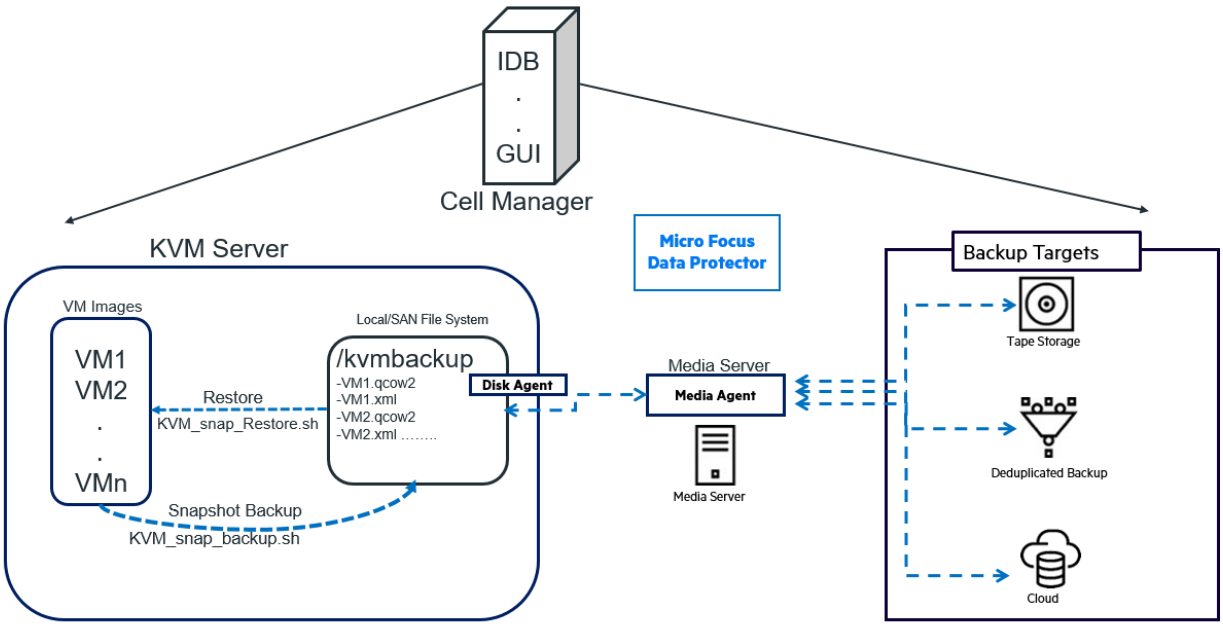
基于 Red Hat 内核的虚拟机 (KVM) 是一种内置到 Linux 的开源虚拟化技术。具体来说，KVM 可将 Linux 转变为虚拟机监控程序，而该虚拟机监控程序则允许主机运行多个称为来宾或虚拟机 (VM) 的隔离虚拟环境。

KVM 将 Linux 转变为 Type-1 (裸机) 虚拟机监控程序。所有虚拟机监控程序都需要一些操作系统级别的组件 (例如内存管理器、进程调度程序、输入/输出 (I/O) 堆栈、设备驱动程序、安全管理器、网络堆栈等) 才能运行 VM。KVM 具有所有这些组件，因为它是 Linux 内核的一部分。每个 VM 都以常规 Linux 进程的形式实现，由标准 Linux 调度程序计划，并具有专用的虚拟硬件，例如网卡、图形适配器、CPU、内存和磁盘。

Data Protector 和 Red Hat KVM 集成

Data Protector 使用脚本来备份 Red Hat KVM 主机中的实时、运行中或联机 VM。这些脚本保存在备份规范的 pre-exec 和 post-exec 区域中。pre-exec 脚本创建 VM 的实时外部快照，并将其保存在为备份脚本中的 $BACKUPDIR 变量配置的本地/SAN 存储装载点中。该脚本使用 Red Hat KVM 的所有特性和功能来执行操作。

VM 的还原基于用于还原的 post-exec 脚本。在 Data Protector 中，选择备份目录 (由 $BACKUPDIR 变量指定) 以选择要还原的 VM。这些选定的 VM 将复制到还原脚本 KVM_snap_Restore.sh 中定义的还原路径 $RESTORED_PATH 变量。从备份脚本中的 $BACKUPDIR 变量中选择 VM 目录，然后选择还原脚本中定义的还原路径 $RESTORED_PATH 变量。



使用案例

Data Protector 和 Red Hat KVM 集成支持以下使用案例:

- 单 VM 备份和还原
- 多 VM 备份和单 VM 还原
- 多 VM 备份和多 VM 还原

支持的磁盘类型

对支持的磁盘类型没有限制。Red Hat KVM 脚本使用 virsh 实用程序创建快照。

先决条件

- 确保 KVM 主机已导入到 Cell Manager 中。
- 确保已安装实用程序包 virt-manager 1.4.3 或更高版本以及 virsh 3.9.0 或更高版本。
- 确保有足够的可用存储 (SAN 或本地文件系统) 来备份 Red Hat KVM 主机中的所有联机 VM。

存储要求

1. 将备份文件系统装载为 /kvmbackup。
2. 创建具有的存储可以为任何给定的备份会话备份 Red Hat KVM 主机中所有联机 VM 的 SAN 或本地文件系统。例如，假设 Red Hat KVM 主机中有三个联机 VM，其大小分别为 10 GB、20 GB 和 30 GB。
   - 如果要备份所有三个 VM，请确保 /kvmbackup 目录具有至少 75-80 GB 的可用存储空间。
   - 如果要单独备份 VM，请确保 /kvmbackup 目录的可用存储空间超过最大的 VM。
   - 此处提及的存储空间只是标示的存储空间。实际存储空间可能会因环境而变。
3. 在计划存储时，还应考虑 Red Hat KVM 环境的增长。

安装 Red Hat KVM

使用 qemu-kvm-rhev 包安装 KVM，以利用联机 VM 快照功能。

备份 Red Hat KVM 主机中的联机 VM

要将 Red Hat KVM 主机与 Data Protector 集成，然后在其中备份联机 VM，请完成以下步骤：

1. 从 ITOM Marketplace 下载 KVM 脚本 zip 包。如果您有任何问题，请联系客户支持。
2. 登录 Red Hat KVM 主机，并在 /opt/omni/lbin 路径中提取下载的脚本。将提取以下脚本:
   - KVM_snap_backup.sh
   - KVM_cleanup_post_backup.sh
   - KVM_snap_Restore.sh
3. 更改脚本的文件权限以读取、写入和执行:
   - chmod 755 KVM_snap_backup.sh
   - chmod 755 KVM_cleanup_post_backup.sh
   - chmod 755 KVM_snap_Restore.sh
4. 编辑 KVM_snap_backup.sh 脚本文件。示例: vi KVM_snap_backup.sh。
   - 如果您不想备份所有联机 VM，请编辑 $VMS 变量以手动输入要备份的 VM。默认情况下，将备份所有联机 VM。
   - 定义您的 SAN/本地存储文件系统装载点。使用存储装载点路径更新 $BACKUPDIR 变量。
     示例：BACKUPDIR=/kvmbackup/$VM/$(date +'%d-%m-%Y%H%M%S')
5. 编辑 KVM_post_cleanup_backup.sh 脚本文件。示例: vi KVM_post_cleanup_backup.sh。
   使用存储装载点路径更新 $BACKUPDIR 变量。
   示例：BACKUPDIR=/kvmbackup。
6. 登录到 Cell Manager。
7. 如果尚未将 Red Hat KVM 主机导入到 Cell Manager 中，则将其导入。
8. 在 Cell Manager 上创建磁带或磁盘设备，以存储 Red Hat KVM 主机备份。有关创建磁带或磁盘设备的信息，请参阅 Data Protector 文档，网址为 https://docs.microfocus.com/?DP。
9. 启动 Data Protector，然后转到“备份”上下文。
10. 在左侧导航栏中选择“文件系统”，然后转到“选项”选项卡。
11. 在“备份规范选项”区域的“说明”字段中输入说明。
12. 单击“备份规范选项”区域中的“高级”'。指定以下内容:
    - Pre-exec 区域:
      - 在 Pre-exec 脚本字段中指定 KVM_snap_backup.sh (浏览并从 /opt/omni/lbin 路径中选择脚本文件)。
      - 在“在客户机上”字段中指定 Red Hat KVM 主机名。
    - Post-exec 区域:
      - 在 Pre-exec 脚本字段中指定 Post_backup_cleanup_KVMsnapshot.sh (浏览并从 /opt/omni/lbin 路径中选择脚本文件)。
      - 在“在客户机上”字段中指定 Red Hat KVM 主机名。
13. 在“备份选项”窗口中单击“确定”。
14. 在“文件系统选项”区域为所有已备份的文件和目录选择默认保护期限。
15. 在“磁盘映像选项”区域中为所有已备份的磁盘映像选择默认保护期限。
16. 单击“备份”上下文中的“应用”以保存备份规范。
17. 开始完整备份并监控进度。

还原 VM

要还原已备份的 VM，请完成以下步骤：

1. 启动 Data Protector，然后选择“还原”上下文。
2. 从左侧导航栏的文件系统树中选择 Red Hat KVM 主机备份会话。
   或者，选择要还原的对象。对象层次结构为 /kvmbackup/<VM_Name>/<Date&Time>/。
3. 选择 VM 和基础文件以还原 VM。
4. 在“目标”选项卡中选择默认还原位置。如果 $RESTORE_PATH 值与 $BACKUPDIR 值不同，则在“目标”选项卡中选择 $RESTORE_PATH 值。
5. 转到“选项”选项卡，然后单击“高级”。
6. 在 Post-exec 脚本字段中指定 KVM_snap_Restore.sh (浏览并选择 /opt/omni/lbin 路径中的脚本文件)。
7. 单击“还原”。
8. 还原完成后，检查 Red Hat KVM 主机中的 VM 状态。

SAP MaxDB 集成

This feature is available in the Premium Edition

本主题介绍如何配置和使用 Data Protector SAP MaxDB 集成 (SAP MaxDB 集成)。它说明了备份和还原 SAP MaxDB 数据库对象 (SAP MaxDB 对象) 需要理解的概念和方法。

Data Protector 与 SAP MaxDB 服务器集成后可联机备份 SAP MaxDB 服务器实例 (SAP MaxDB 实例)。您可以使用 Data Protector SAP MaxDB 集成来备份以下 SAP MaxDB 对象:

- SAP MaxDB 数据
- SAP MaxDB 配置
- SAP MaxDB 存档日志

备份期间，数据库为联机并可正常使用。它可以处于“管理”或“联机”模式下。

SAP MaxDB 不支持对相同实例进行并行备份，并且同一时间数据库中只能有一个备份操作处于活动状态。Data Protector 也不支持数据库和日志的并行备份。

Data Protector 提供以下类型的交互式备份和安排的备份：

备份类型

完整	SAP MaxDB 完整备份。备份所选的所有对象。
差异	SAP MaxDB 增量备份。备份从上次完整备份以来对数据库所做的更改。
事务	SAP MaxDB 日志备份。备份存档的日志。

您可以将 SAP MaxDB 对象:

- 还原到原始位置
- 还原到另一个 SAP MaxDB 客户机
- 还原到另一个 SAP MaxDB 实例

在还原会话中，还可以将数据库恢复到特定时间点或恢复到上次存档日志。

您还可以使用 SAP MaxDB 实用程序备份和还原 SAP MaxDB 对象。

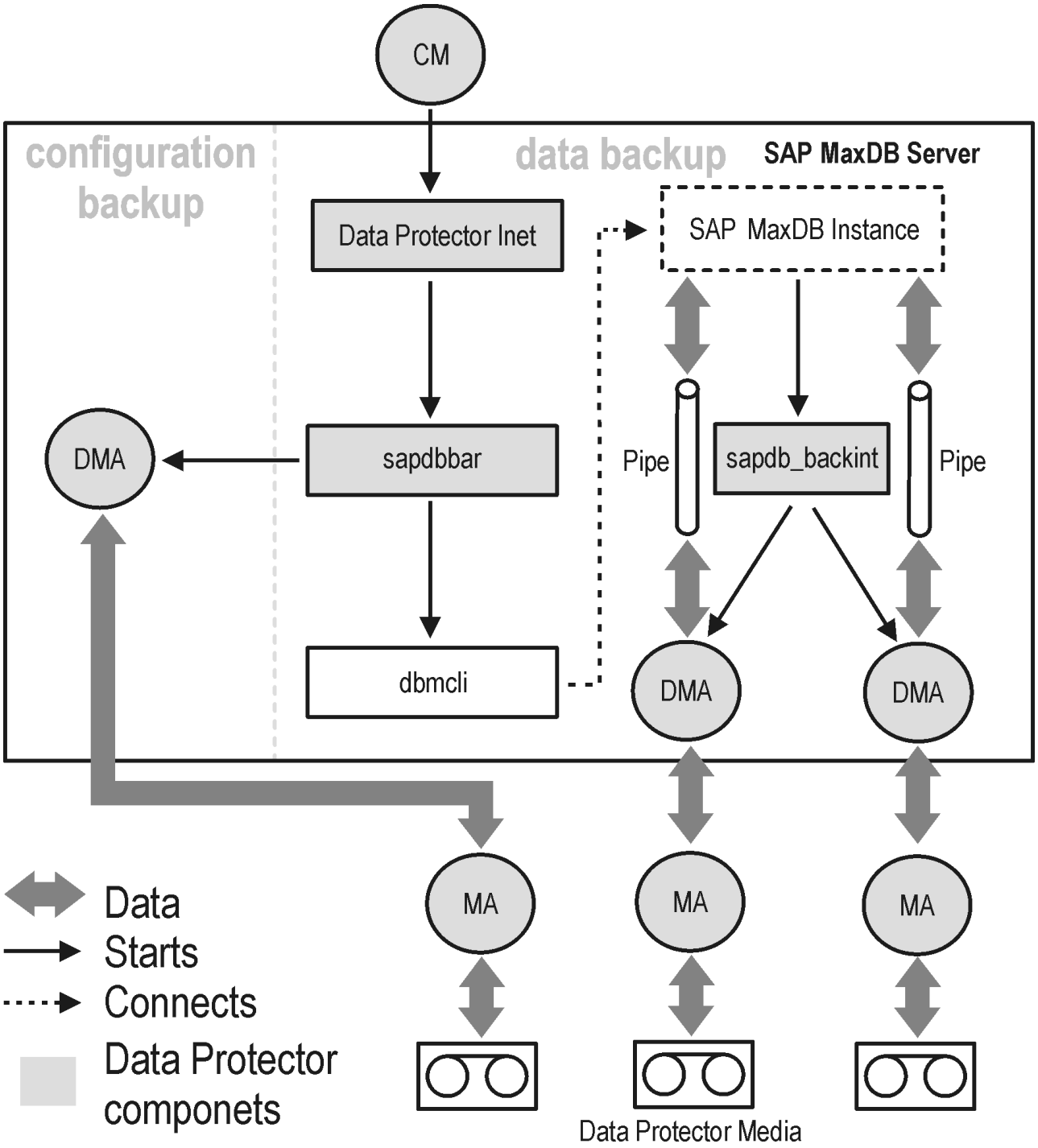
本节提供 Data Protector SAP MaxDB 集成的相关信息。

集成概念

Data Protector 使用 SAP MaxDB 数据库管理服务器和 backint 接口通过 SAP MaxDB 集成组件与 SAP MaxDB 服务器集成。

SAP MaxDB 集成体系结构显示了 Data Protector SAP MaxDB 集成的体系结构。

SAP MaxDB 集成体系结构



Data Protector 集成软件由以下组件组成：

- sapdbbar 模块，它安装在 SAP MaxDB 服务器系统上，负责控制 SAP MaxDB 服务器与 Data Protector 备份和还原进程之间的活动。
- sapdb_backint 组件，它安装在 SAP MaxDB 服务器系统上，而且是 Data Protector 与 SAP MaxDB 备份和还原功能之间的二进制接口。
- DMA（数据移除器代理）组件，安装在 SAP MaxDB Server 系统上，它是实际数据传输模块，由 sapdb_backint 调用。
- util_sapdb 实用程序，Data Protector 使用它来配置 SAP MaxDB 实例，以便与 Data Protector 结合使用以及检查实例配置。

SAP MaxDB 数据和存档日志在流中备份或还原，而 SAP MaxDB 配置作为普通文件备份或还原。备份完成后，可以删除存档日志或将其保留在 SAP MaxDB 服务器上，具体取决于所选选项。

该集成还利用了“SAP MaxDB 介质”和“介质组”的概念，从而同时备份和还原 SAP MaxDB 对象。若干 SAP MaxDB 介质组成一个 SAP MaxDB 介质组，然后在流中备份或还原介质组。这称为 SAP MaxDB **并行性**。有关 Data Protector“并行性”选项的详细信息，请参阅 SAP MaxDB 备份选项。

注意使用 SAP MaxDB 实用程序运行备份时，必须手动配置 SAP MaxDB 介质和管道。

备份流

启动备份会话时，Cell Manager 将使用备份规范中的所选备份参数启动 sapdbbar。 sapdbbar 模块随后使用 SAP MaxDB dbmcli 启动 SAP MaxDB 会话。 sapdbbar 模块会发出 dbmcli 命令来配置 SAP MaxDB 备份介质 (并行性)，配置 sapdb_backint ，然后再使用 SAP MaxDB dbmcli 启动备份。接着，SAP MaxDB 启动已配置的 sapdb_backint 组件。对于每个 SAP MaxDB 介质 (管道)，sapdb_backint 会启动 DMA，由后者将数据从 SAP MaxDB 介质 (管道) 传输到 Data Protector 介质。对于完整备份、差异备份和事务备份来说，此过程相同。此外，如果选择了备份配置 (包括介质规范和备份历史记录)，则由 sapdbbar 模块和 DMA 直接备份。要备份的配置文件列表通过 dbmcli 检索。

备份历史记录文件 (dbm.ebf 和 dbm.knl) 仅用于备份。不支持还原这些文件。

还原流

启动还原会话时，Cell Manager 启动 sapdbbar 模块，后者再启动 SAP MaxDB dbmcli。 sapdbbar 模块向 SAP MaxDB dbmcli 发出命令以配置 sapdb_backint 和 SAP MaxDB 备份介质 (并行性)。然后，SAP MaxDB 启动已配置的 sapdb_backint ，由后者将数据流式传输到 SAP MaxDB 创建的介质 (管道)。对于每个 SAP MaxDB 介质 (管道)， sapdb_backint 会启动 DMA，由后者将数据从 Data Protector 介质传输到 SAP MaxDB 介质 (管道)。如果正在还原 SAP MaxDB 配置，则执行还原的是 sapdbbar 模块和 DMA。

满足 SAP MaxDB 的先决条件

以下是 SAP MaxDB 集成的先决条件:

- 确保已正确安装和配置 SAP MaxDB 系统。
  - 有关安装、配置和使用 SAP MaxDB 服务器的信息，请参阅 SAP MaxDB 文档。

  要启用事务备份 (日志备份)，需要激活 SAP MaxDB 自动日志备份。
- 确保已正确安装 Data Protector。有关如何在各种体系结构中安装 Data Protector 的信息，请参阅《Data Protector 安装指南》。

  要对其执行备份或还原的每个 SAP MaxDB 系统都必须安装 Data Protector“SAP MaxDB 集成”组件。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 SAP MaxDB 系统和 Cell Manager 是否正常通信，请在 SAP MaxDB 系统上配置并运行 Data Protector 文件系统备份和还原。
- 确保 SAP MaxDB 实例处于联机状态。
- 为了能够备份 MaxDB 历史文件，请确保这些文件所在的路径名不含空格。如果路径名含空格，请调整历史记录文件的位置。

如果要还原到另一个 SAP MaxDB 实例:

- 在要还原到的 SAP Max DB Server 系统上安装 Data Protector SAP MaxDB 集成。
- 将 SAP MaxDB 客户机添加到 Data Protector 单元。
- 配置 SAP MaxDB 用户。
- 配置要还原到的实例。

群集感知客户机

仅在一个群集节点上配置 SAP MaxDB 实例，因为配置文件驻留在 Cell Manager 上。

如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称，如下所示:

Windows 系统： set OB2BARHOSTNAME=virtual_server_name

UNIX 系统： export OB2BARHOSTNAME=virtual_server_name

配置集成

您需要配置 SAP MaxDB 用户以及要对其执行备份或还原的每个 SAP MaxDB 实例。

配置 SAP MaxDB 用户

创建或找到至少具有以下 SAP MaxDB 权限的“SAP MaxDB 数据库用户”:

- Saving backups (Backup)
- Restoring backups (Recovery)
- Installation management (InstallMgm)
- Parameter access (ParamCheckWrite)

最后两个权限对 Data Protector 配置是必需的。

*UNIX 系统：*添加正在其帐户下运行 SAP MaxDB 的操作系统用户 (“SAP MaxDB 操作系统用户”) 或属于 Data Protector admin 或 operator 组下 sapdb admin 组的用户。有关详细信息，请参阅《Data Protector 帮助》索引: “添加用户”。例如，默认情况下，SAP MaxDB OS 用户是 sapsys 组中的 sapdb 用户。

配置 SAP MaxDB 实例

您需要为 Data Protector 提供 SAP MaxDB 实例的以下配置参数:

- SAP MaxDB 数据库用户的用户名。
- SAP MaxDB 数据库用户的密码。
- (可选) SAP MaxDB 独立程序路径参数

要配置 SAP MaxDB 实例，请使用 Data Protector GUI 或 CLI。

然后，Data Protector 在 Cell Manager 上创建 SAP MaxDB 实例配置文件，并验证与该实例的连接。

提示创建配置文件后，可以使用 Data Protector util_cmd 命令设置、检索和列出配置文件参数。有关详细信息，请参阅 util_cmd 手册页。

要配置 SAP MaxDB 实例，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP MaxDB Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 SAP MaxDB 备份”模板。单击**确定**。
4. 在“客户机”中，选择 SAP MaxDB 服务器系统。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，键入 SAP MaxDB 实例名称。

   有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 在“配置 SAP MaxDB”对话框中，指定“SAP MaxDB 独立程序路径”参数。此参数是在安装 SAP MaxDB 应用程序期间指定的独立程序路径目录。要自动检测该目录，请保持“自动检测”选项处于选中状态。

   在“连接”下，键入 SAP MaxDB 数据库用户的用户名和密码，如配置 SAP MaxDB 用户中所述。

   单击**确定**。
6. 此时便配置了 SAP MaxDB 实例。退出 GUI 或继续创建备份规范。

使用 Data Protector CLI

以 SAP MaxDB OS 用户身份登录 SAP MaxDB 服务器系统并执行:

```
util_sapdb \[-homedir SAPMaxDB_independent_program_directory] \-config Instance Nameusernamepassword
```

参数描述

SAPMaxDB_independent_program_directory	SAP MaxDB 独立程序路径参数。此参数是在 SAP MaxDB Server 上安装 SAP MaxDB 应用程序期间指定的独立程序路径目录。 此参数为可选。如果未指定，则自动检测该目录。
Instance_Name	要配置的 SAP MaxDB 实例的名称。
username	按配置 SAP MaxDB 用户中所述，创建或标识 SAP MaxDB 数据库用户的用户名。
password	按配置 SAP MaxDB 用户中所述，创建或标识 SAP MaxDB 数据库用户的密码。

注意用户名和 SAP Max DB 独立程序路径参数不得包含单引号字符 (')。

消息 *RETVAL*0 表示配置成功。

示例

要通过指定数据库用户 sapmaxdb_user、密码 sapmaxdb_pass 以及 SAP MaxDB 独立程序路径 /opt/sapdb/indep_prog (UNIX) 或 c:\program files\sapdb\indep_prog (Windows) 来配置实例 sapmaxdb_inst，请执行:

Windows 系统：

```
util_sapdb -homedir "SAP_MaxDB_independent_program_directory" -config sapdb_inst sapdb_user sapdb_pass
```

UNIX 系统：

```
util_sapdb -homedir SAP_MaxDB_independent_program_directory/indep_prog -config sapdb_inst sapdb_user sapdb_pass
```

提示要更改配置参数，请使用新值执行相同的命令。

处理错误

If an error occurs, the error number is displayed in the form *RETVAL*error_number.

*UNIX 系统：*要获取错误描述，请将目录更改为 /opt/omni/lbin 并执行:

```
omnigetmsg 12 Error_number
```

安装 SAP MaxDB 客户机

This feature is available in the Premium Edition

假设 SAP MaxDB 服务器已启动并正在运行。

为了能够备份 SAP MaxDB 数据库，您需要在安装期间选择以下 Data Protector 组件：

- SAP MaxDB Integration - 为了能够运行 SAP MaxDB 数据库的集成联机备份
- Disk Agent - 为了能够运行 SAP MaxDB 数据库的文件系统备份

备份 SAP MaxDB 集成

This feature is available in the Premium Edition

该集成可提供不同类型的数据库联机备份。具体备份内容取决于所选的对象和备份类型。

备份内容

SAP MaxDB 备份模式。

		SAP MaxDB 备份模式		
		完整	差异	事务
GUI 选择	**数据**	数据	差异数据	存档日志
	配置	配置	配置	配置
	实例	数据与配置	差异数据与配置	存档日志与配置

限制

SAP MaxDB 不支持对相同实例进行并行备份，并且同一时间数据库中只能有一个备份操作处于活动状态。Data Protector 也不支持数据库和日志的并行备份。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP MaxDB Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择“空白 SAP MaxDB 备份”模板。单击**确定**。
4. 在“客户机”中，选择 SAP MaxDB 服务器系统。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，键入 SAP MaxDB 实例名称。

   有关“用户和组/域”选项的信息，请按 **F1**。

   单击“下一步”。
5. 如果尚未将 SAP MaxDB 实例配置为与 Data Protector 配合使用，则会显示“配置 SAP MaxDB”对话框。按照配置 SAP MaxDB 实例中的描述进行配置。
6. 选择要备份的 SAP MaxDB 对象。

   重要说明要备份 SAP MaxDB 存档日志，请选择“数据”项。随后在计划备份或以交互方式运行备份时，选择“事务”备份类型即可触发存档日志备份。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。指定设备“并发”、介质池和预分配策略。

单击“下一步”。

8. 设置备份选项。

   单击“下一步”。

9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。有关如何创建和编辑计划的详细信息，请参阅《*Data Protector 管理员指南*》中 Data Protector 中的“调度程序”。

提示将备份规范保存在“SAP MaxDB 集成”组中。

提示请在实际使用之前先预览备份规范。

SAP MaxDB 备份选项

选项	描述
更改数据库状态	指定备份期间的 SAP MaxDB 数据库模式 (“管理”或“联机”)。如果此选项为“关”，数据库会一直处于当前模式。
保留归档日志	指定备份完成后在 SAP MaxDB 服务器上保留 (ON) 还是删除 (OFF) 存档日志。
并行性	指定在 SAP MaxDB 服务器上创建的 SAP MaxDB 介质数，随后指定 SAP MaxDB 备份数据流数。 该值必须等于或小于: • SAP MaxDB MAXBACKUPDEVS 参数。 • 备份规范中选择的所有备份设备的并发值总和。 有关 Data Protector Concurrency 选项的详细信息，请参阅《Data Protector 帮助》索引: “并发”。 默认值: 1. 最大值: 32。 建议值: 要备份的 SAP MaxDB 数据卷的数量。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

预览备份会话

使用 Data Protector GUI 或 CLI 预览备份会话以对其进行测试。

此交互式测试不会备份任何数据。但是，作为此测试的结果， Backup_Specification_Name_TEST_FILE 文件将在 SAP MaxDB 服务器系统的默认 Data Protector 临时文件目录中创建。测试后请删除该文件。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“SAP MaxDB 服务器”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

请执行以下命令：

```
omnib -sapdb_list backup_specification_name -test_bar
```

预览期间会发生什么?

1. 启动 sapdbbar 程序，然后启动 Data Protector testbar2 命令。
2. Data Protector 测试配置的 Data Protector 部分。测试以下内容:
   - SAP MaxDB 实例与 Data Protector 之间的通信
   - 备份规范的语法
   - 如果正确指定设备
   - 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

> **注意**如果要执行的备份是还原后的第一个备份，则必须选择完整备份类型。

备份方法

通过以下任一方式开始备份在备份规范中选择的 SAP MaxDB 对象:

- 使用 Data Protector GUI。
- 使用 Data Protector CLI。
- 使用 SAP MaxDB 实用程序。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“SAP MaxDB 集成”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 选择“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI 以 SAP MaxDB OS 用户身份登录 SAP MaxDB 服务器系统并执行以下命令:

```
omnib -sapdb_list ListName [-barmode sapdbmode] [ list_options ] [-preview]
```

ListName 是备份规范的名称。

sapdbmode 指定备份类型。您可以选择完整、差异或事务。

有关 List_options ，请参阅 omnib 手册页。

示例

要使用名为 TEST 的现有 SAP MaxDB 备份规范启动完整备份并将数据保护设置为 10 周，请执行:

```
omnib -sapdb_list TEST -barmode full -protect weeks 10
```

使用 SAP MaxDB 实用程序

有关下面列出的变量的说明，请参阅参数说明。

1. 在 SAP MaxDB 服务器系统上创建 bsi_env 文件。

   *UNIX 系统：*授予 SAP MaxDB OS 用户对此文件的读取权限。

   此文件必须包含以下两行:

   Windows 系统：

   ```
   BACKINT Data_Protector_home\bin\sapdb_backint INPUT Data_Protector_program_data\tmp\inst_name.bsi_in OUTPUT
   Data_Protector_program_data\tmp\inst_name.bsi_out ERROROUTPUT Data_Protector_program_data\tmp\inst_name.bsi_err PARAMETERFILE
   name_of_backup_spec TIMEOUT_SUCCESS 900 TIMEOUT_FAILURE 30
   ```

   UNIX 系统：

   ```
   BACKINT /opt/omni/bin/sapdb_backint INPUT /var/opt/omni/tmp/inst_name.bsi_in OUTPUT /var/opt/omni/tmp/inst_name.bsi_out
   ERROROUTPUT /var/opt/omni/tmp/inst_name.bsi_err PARAMETERFILE SAPDB_PARAMETER TIMEOUT_SUCCESS 900 TIMEOUT_FAILURE 30
   ```

   SAPDB_PARAMETER 文件应包含以下几行:

   ```
   OB2BARLIST=name_of_backup_spec OB2APPNAME=inst_name OB2BARHOSTNAME=FQDN
   ```

2. 通过执行以下命令，以 SAP MaxDB 数据库用户身份登录 SAP MaxDB 数据库管理器:

   ```
   dbmcli -d inst_name -u username,password
   ```

3. 在 SAP MaxDB 数据库管理器中，执行以下命令，注册在 SAP MaxDB 服务器系统上创建 bsi_env 文件一节中创建的 bsi_env 文件的位置:

   Windows 系统：

   ```
   dbm_configset -raw BSI_ENV location\inst_name.bsi_env
   ```

   UNIX 系统：

   ```
   dbm_configset -raw BSI_ENV location/inst_name.bsi_env
   ```

4. 创建 SAP MaxDB 介质，并将它们分组在同一个名称下 (*media_group_name*)。创建的介质数应该等于备份打算使用的并行性。要创建介质 *medium_name*，请执行以下命令，具体取决于 SAP MaxDB 版本:

   - 对于 SAP MaxDB 7.6 版本:

     ```
     medium_put media_group_name/medium_namepipe_nametypebackup_type [size [block_size [overwrite [autoloader [os_command [tool_t
     ype]]]]]]
     ```

   - 对于其他 SAP MaxDB 版本:

     ```
     medium_put media_group_name/medium_namepipe_namemedium_typebackup_type
     ```

   backup_type 可以执行下列操作之一:

   - DATA 对于完整备份
   - PAGES 对于差异备份
   - LOG 对于日志备份

   tool_type 必须如下:

   - "BACK" 用于使用 Backint for SAP MaxDB 进行备份

重要说明为 Data Protector 备份和还原创建 SAP MaxDB 介质时，介质组名称必须以 "BACK" 字符串开头。

示例

以下命令会在介质组中创建两个介质和两个管道 (并行性 = 2) BACKDP-Data[2].

Windows 系统，SAP MaxDB 7.6 版本:

```
medium_put BACKDP-Data[2]/1 \ \\.\Pipe\inst_name.BACKDP_Data[2].1 PIPE DATA 0 8 \ NO NO \" \" "BACK"
```

```
medium_put BACKDP-Data[2]/2 \ \\.\Pipe\inst_name.BACKDP_Data[2].2 PIPE DATA 0 8 \ NO NO \" \" "BACK"
```

UNIX 系统，SAP MaxDB 7.6 版本:

```
medium_put BACKDP-Data[2]/1 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].1 PIPE \ DATA 0 8 NO NO \" \" "BACK"
```

```
medium_put BACKDP-Data[2]/2 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].2 PIPE \ DATA 0 8 NO NO \" \" "BACK"
```

Windows 系统，其他 SAP MaxDB 版本:

```
medium_put BACKDP-Data[2]/1 \ \\.\Pipe\inst_name.BACKDP_Data[2].1 PIPE DATA
```

```
medium_put BACKDP-Data[2]/2 \ \\.\Pipe\inst_name.BACKDP_Data[2].2 PIPE DATA
```

UNIX 系统，其他 SAP MaxDB 版本:

```
medium_put BACKDP-Data[2]/1 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].1 PIPE DATA
```

```
medium_put BACKDP-Data[2]/2 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].2 PIPE DATA
```

5. 通过执行以下命令启动 SAP MaxDB 实用程序会话:

   ```
   util_connect
   ```

6. 开始备份。以下命令示例将为在此过程的步骤 4 中创建的介质启动完整备份:

   ```
   backup_start BACKDP-Data[2] DATA
   ```

7. 会话进度会显示在 Data Protector“监视器”上下文中。有关详细信息，请参见。

参数描述

inst_name	要备份的实例的名称。
name_of_backup_spec	要用于备份的 Data Protector 备份规范的名称。
username, password	SAP MaxDB 数据库用户的连接字符串。
location	bsi_env file 的位置。
media_group_name	SAP MaxDB 介质组的名称。
medium_name	SAP MaxDB 介质的名称。
pipe_name	SAP MaxDB 管道的名称。
medium_type	SAP MaxDB 介质的类型。

检查配置

为 SAP MaxDB 实例创建至少一个备份规范后，请检查 SAP MaxDB 实例的配置。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，展开“备份规范”，然后展开“SAP MaxDB 服务器”。单击备份规范可显示要检查的 SAP MaxDB 实例。
3. 右键单击 SAP MaxDB 实例，然后单击“检查配置”。

使用 Data Protector CLI

*UNIX 系统：*以 SAP MaxDB OS 用户身份登录 SAP MaxDB 服务器系统。

请执行以下命令：

```
util_sapdb -chkconf Instance_Name
```

其中 Instance_Name 是 SAP MaxDB 实例的名称。

成功的配置检查将显示消息 *RETVAL*0 。

还原 SAP MaxDB 集成

This feature is available in the Premium Edition

使用以下任一方法还原 SAP MaxDB 对象:

- 使用 Data Protector GUI。
- 使用 Data Protector CLI。
- 使用 SAP MaxDB 实用程序。

还原和恢复概述

本节提供选择 Data Protector 还原和恢复选项时要执行的还原和恢复过程概述。
有关这些选项的详细说明，请参阅 SAP MaxDB 还原选项。

还原会话开始执行时，Data Protector 会将 SAP MaxDB 数据库切换到“管理”模式。如果无法将数据库切换到“管理”模式，Data Protector 监视器中会显示错误。

根据还原类型以及所选的还原和恢复选项，还原后，SAP MaxDB 数据库可以切换到以下模式:

- 如果选择了 Data Protector“恢复”选项，则在还原后数据库将切换到“联机”模式。
- 如果未选择 Data Protector“恢复” 选项并且尚未还原存档日志 (如果执行了从完整备份或差异备份会话进行还原)，则数据库还原后仍保留在“管理”模式。
- 如果未选择 Data Protector“恢复”选项并且已还原存档日志，则数据库 (如果已还原的存档日志允许) 将切换到“联机”模式。但是，如果数据库无法切换到“联机”模式 (因为还原的存档日志不允许该操作)，则它将保留在“管理”模式中。

重要说明SAP MaxDB 数据库可以切换到的状态存在几种情况，具体取决于备份选项“保留存档日志” 和恢复选项“使用现有存档日志” ，其中 SAP MaxDB 服务器上的重做日志序列可能会与已还原的卷存在事务差异。执行还原时 (当数据库切换到“联机” 模式时)，SAP MaxDB 会始终检查是否存在该差异，而不管为恢复选择的时间点。如果存在差异，则不执行恢复，并且数据库仍处于“管理” 模式，除非在开始还原之前手动删除了现有重做日志。

如果还原了完整备份或差异备份会话，则只会还原所选备份会话中的数据 (无存档日志)。SAP MaxDB 服务器上的数据将被覆盖。

如果还原了事务备份会话，则仅还原所选备份会话中的存档日志 (无数据)。

还原期间不会删除还原之前存在于 SAP MaxDB 服务器上的重做日志。

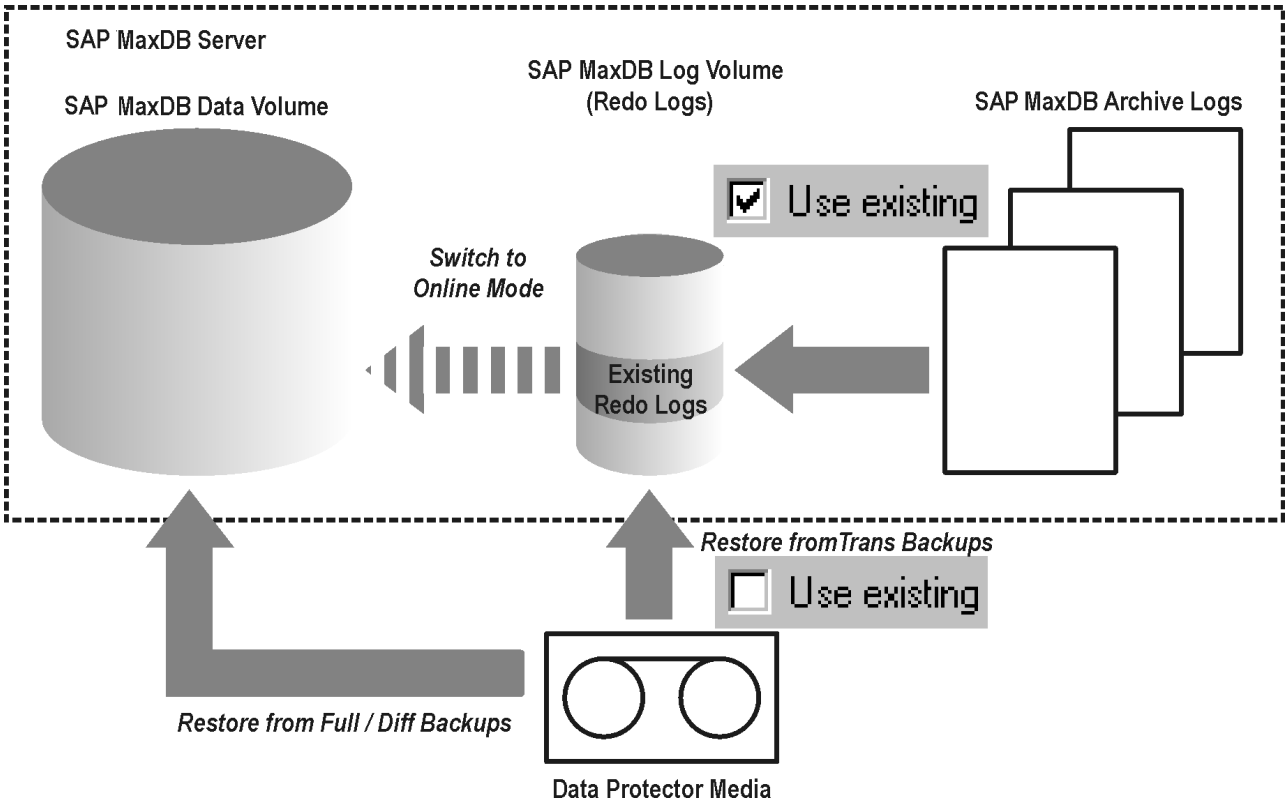
还原时，SAP MaxDB 服务器上的现有重做日志可以按如下方式处理，具体取决于所选的 Data Protector“使用现有存档日志”选项 (该选项仅在选择了“恢复”选项时才能选择):

- 如果选择了“使用现有存档日志”选项，SAP MaxDB 服务器上的现有存档日志将应用于重做日志。

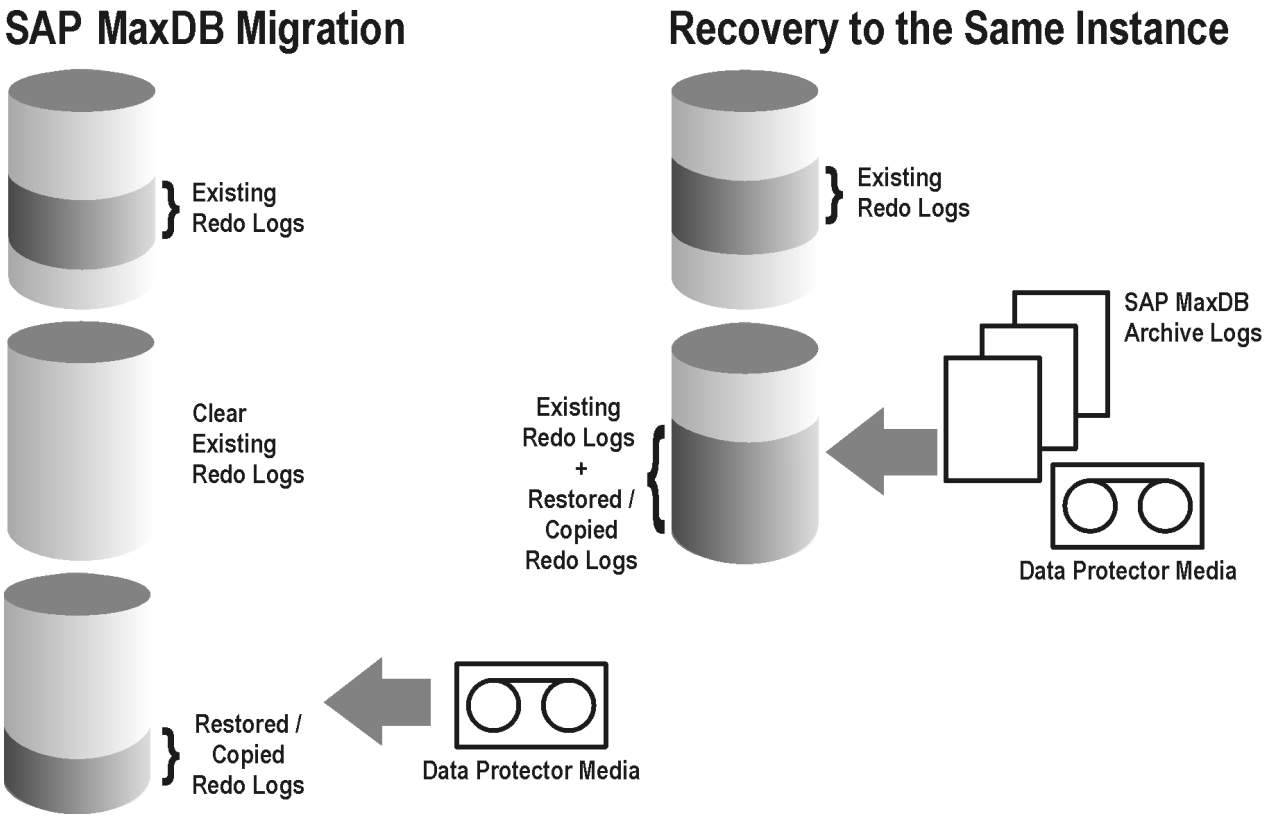
  为还原选择了事务备份会话时或者还原是所需还原链的一部分时，如果同时选择了“使用现有存档日志”选项，来自 Data Protector 介质的存档日志将应用于重做日志。然后，SAP MaxDB 服务器上的存档日志将应用于重做日志。
- 如果未选择“使用现有存档日志”选项，备份介质上的已备份存档日志将应用于重做日志 (如果还原了事务备份会话)，或者重做日志会与现有存档日志一起完好保留在 SAP MaxDB 服务器上 (如果还原了完整或差异备份会话)。

  注意在 SAP MaxDB 迁移时将禁用“使用现有存档日志”选项，因此仅允许从备份介质上的已备份存档日志还原重做日志 (如果还原了事务备份会话)。

SAP MaxDB 还原过程



SAP MaxDB 存档日志还原进程 - 重做日志详细信息



如果选择还原差异备份或事务备份会话，则可以将集成设置为:

- 执行完整数据库还原。在这种情况下，集成将自动确定执行还原时所需的完整、差异或事务备份会话链。还原完成后，如果选择了“恢复”选项，数据库将切换到“联机”模式。

- 仅还原选定的差异备份会话或选定的事务备份会话。如果数据库在此类还原保持一致性，并且如果选择了“恢复”选项，则会将数据库切换到“联机”模式。否则，让它保留在“管理”模式下。

  如果从完整备份会话还原之后数据库保持脱机或处于“管理”模式下，而且随后又通过差异或事务备份会话执行还原，则只还原所选的事务或差异备份会话很有用。

注意还原或迁移期间，SAP MaxDB 服务器上的存档日志永远不会被删除。

注意执行还原或恢复后，您将执行的第一个备份必须是完整备份。

注意如果使用的是 Data Protector GUI，则可以在还原过程中配置实例。

还原到另一个 SAP MaxDB 实例期间，将覆盖现有数据并删除现有重做日志。

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击“还原”。
2. 在“范围窗格”中，展开“SAP MaxDB 服务器”，展开此前曾从中备份过要还原的数据的客户机，然后单击要还原的 SAP MaxDB 实例。
3. 在“源”页中，选择要还原的对象。
4. 要从特定备份会话还原 SAP MaxDB 对象，请右键单击“数据”项，单击“属性”，然后在“数据属性”对话框中指定“备份版本”。
5. 选择“事务”或“差异”备份会话后，您可以:
   - 对数据库执行完整还原 (“完整还原数据库”)。在这种情况下，集成将自动确定所需的完整、差异或事务备份会话链。
   - 仅还原选定的备份会话 (“仅还原此备份”)。

     如果从完整备份会话还原后数据库保持脱机状态或处于“管理”模式，则仅还原所选的“事务”或“差异”备份会话非常有用。

   要还原 SAP MaxDB 存档日志，请选择“数据”项以及要从中还原的“事务”备份会话。

   重要说明无论为“配置”项选择了什么，“配置”项都将从为“数据”项选择的同一个备份会话中还原。

6. 在“选项”页面中，设置还原和恢复选项。
7. 在“设备”页中，选择要用于还原的设备。
8. 在“介质”页面中，查看还原所需的介质并验证其可用性。
9. 单击**还原**。
10. 在“启动还原会话”对话框中，单击“下一步”。
11. 指定“报告级别”和“网络负载”。

    注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。

12. 单击**完成**启动还原。

会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

以 SAP MaxDB OS 用户身份登录 SAP MaxDB 服务器系统并执行以下命令:

```
omnir -sapdb -barhost ClientName -instance InstanceName

[-destination ClientName]

[-newinstance DestinationInstanceName]

[-session BackupID]

[-recover [-endlogs | -time: YYYY-MM-DD.hh.mm.ss] [-from_disk]]

[-nochain]
```

-barhost 选项会设置此前备份的 SAP MaxDB 服务器的名称。

-instance 选项会设置此前备份的 SAP MaxDB 实例的名称。

-session 指定要从中进行还原的备份数据 (BackupID)。备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是对象*复制*会话的会话 ID。

如果同一个对象有多个副本，则 omnir 语法不允许指定要从哪个对象副本进行还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

如果未指定此选项，则使用具有最新备份 ID 的备份数据，而不管所选的 -endlogs 或 -time 选项。

-nochain 选项会指示集成仅还原选定或上次备份会话；集成不会还原整个完整备份、差异备份和事务备份还原链。

有关所有其他选项的说明，请参阅 SAP MaxDB 还原选项。另请参阅 omnir 手册页。

示例

要从上次备份会话中还原名为 "inst1" 且此前在名为 "srv1.company.com" 的 SAP MaxDB 服务器上备份的实例 (及配置)，接着再执行恢复直到日志结束，请执行以下命令:

```
omnir -sapdb -barhost srv1.company.com -instance inst1 -recover -endlogs
```

有关如何查找有关要从中进行还原的备份对象的信息，请参阅查找还原信息。

使用 SAP MaxDB 实用程序还原

使用此集成，还可以从 SAP MaxDB 实用程序运行集成的 Data Protector，并利用它来还原 SAP MaxDB 服务器。

要对现有 SAP MaxDB 服务器实例执行还原，请参阅 SAP MaxDB 还原和恢复。

要迁移 SAP MaxDB 实例，请参阅 SAP MaxDB 迁移。

有关如何查找有关要从中进行还原的备份对象的信息，请参阅查找还原信息。

SAP MaxDB 还原和恢复

按照接下来几页中的步骤，使用 SAP MaxDB 实用程序从现有 Data Protector SAP MaxDB 备份会话中还原和恢复数据库。该过程中使用了以下约定:

inst_name 是要还原的实例的名称

name_of_backup_spec 是备份时使用的 Data Protector 备份规范的名称。

username ，password 是如配置 SAP MaxDB 用户中所述，所创建或标识的 SAP MaxDB 数据库用户的连接字符串。

location 是 bsi_env 文件的位置

media_group_name 是 SAP MaxDB 介质组的名称

medium_name 是 SAP MaxDB 介质的名称

pipe_name 是 SAP MaxDB 管道的名称

medium_type 是 SAP MaxDB 介质的类型

SessionID 是要还原的会话的 Data Protector 会话 ID

还原

1. 如果 bsi_env 文件已存在，而且已在 SAP MaxDB 服务器上配置，请跳过此步骤。

   在 SAP MaxDB 服务器上，在所选的目录中创建 bsi_env 文件。它必须包含以下几行:

   Windows 系统：

   ```
   BACKINT Data_Protector_home\bin\sapdb_backint INPUT Data_Protector_program_data\tmp\inst_name.bsi_in OUTPUT Data_Protector_program_data\tmp\inst_name.bsi_out ERROROUTPUT Data_Protector_program_data\tmp\inst_name.bsi_err PARAMETERFILE SAPDB_PARAMETER TIMEOUT_SUCCESS 900 TIMEOUT_FAILURE 30
   ```

   UNIX 系统：

   ```
   BACKINT /opt/omni/bin/sapdb_backint INPUT /var/opt/omni/tmp/inst_name.bsi_in OUTPUT /var/opt/omni/tmp/inst_name.bsi_out ERROROUTPUT /var/opt/omni/tmp/inst_name.bsi_err PARAMETERFILE SAPDB_PARAMETER TIMEOUT_SUCCESS 900 TIMEOUT_FAILURE 30
   ```

   SAPDB_PARAMETER 文件应包含以下几行:

   ```
   OB2BARLIST=name_of_backup_spec OB2APPNAME=inst_name OB2BARHOSTNAME=FQDN
   ```

2. 以配置 SAP MaxDB 用户一节中创建或标识的 SAP MaxDB 数据库用户的身份，登录 SAP MaxDB 数据库管理器。在 SAP MaxDB 服务器上，执行以下命令进行登录:

   ```
   dbmcli -d inst_name -u username,password
   ```

3. 在 SAP MaxDB 数据库管理器中，通过执行以下命令将数据库切换到“管理”模式:

   ```
   db_admin
   ```

4. 如果 bsi_env 文件的位置已在 SAP MaxDB 服务器上注册，请跳过此步骤。

   如下所述，注册 bsi_env 文件的位置:

   Windows 系统：

   ```
   dbm_configset -raw BSI_ENV location\inst_name.bsi_env
   ```

   UNIX 系统：

   ```
   dbm_configset -raw BSI_ENV location/inst_name.bsi_env
   ```

5. 如果 SAP MaxDB 服务器上已存在要与 Data Protector 一起使用的 SAP MaxDB 介质和管道，请跳过此步骤。

   请注意，要还原 Data Protector SAP MaxDB 备份会话，所需的 SAP MaxDB 介质和管道数等于备份会话期间使用的并行性值。

   在 SAP MaxDB 介质组中创建 SAP MaxDB 介质。根据 SAP MaxDB 版本，为要创建的每个介质执行以下命令:

   - 对于 SAP MaxDB 7.6 版本:

     ```
     medium_put media_group_name/medium_namepipe_namemedia_typetypebackup_type [size [block_size [overwrite [autoloader [os_command [tool_type]]]]]]
     ```

- 对于其他 SAP MaxDB 版本:

  medium_put media_group_name/medium_namepipe_namemedia_typebackup_type

backup_type 可以执行下列操作之一:

- DATA 对于完整备份
- PAGES 用于差异 (diff) 备份
- LOG 用于事务 (trans) 备份

tool_type 必须如下:

- "BACK" 用于使用 Backint for SAP MaxDB 进行备份

> **重要说明**为 Data Protector 备份和还原创建 SAP MaxDB 介质和管道时，介质组名称必须以 "BACK" 字符串开头。以下命令会在介质组中创建两个介质和两个管道 (并行性 = 2):

Windows 系统，SAP MaxDB 7.6 版本:

```
medium_put BACKDP-Data[2]/1 \ \\.\Pipe\inst_name.BACKDP_Data[2].1 PIPE DATA 0 8 \ NO NO \"\" "BACK"
```

```
medium_put BACKDP-Data[2]/2 \ \\.\Pipe\inst_name.BACKDP_Data[2].2 PIPE DATA 0 8 \ NO NO \"\" "BACK"
```

UNIX 系统，SAP MaxDB 7.6 版本:

```
medium_put BACKDP-Data[2]/1 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].1 PIPE \ DATA 0 8 NO NO \"\" "BACK"
```

```
medium_put BACKDP-Data[2]/2 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].2 PIPE \ DATA 0 8 NO NO \"\" "BACK"
```

Windows 系统，其他 SAP MaxDB 版本:

```
medium_put BACKDP-Data[2]/1 \ \\.\Pipe\inst_name.BACKDP_Data[2].1 PIPE DATA
```

```
medium_put BACKDP-Data[2]/2 \ \\.\Pipe\inst_name.BACKDP_Data[2].2 PIPE DATA
```

UNIX 系统，其他 SAP MaxDB 版本:

```
medium_put BACKDP-Data[2]/1 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].1 PIPE DATA
```

```
medium_put BACKDP-Data[2]/2 \ /var/opt/omni/tmp/inst_name.BACKDP_Data[2].2 PIPE DATA
```

6. 通过执行以下命令，启动 SAP MaxDB 实用程序会话:

   util_connect

7. 通过执行以下命令，开始从 Data Protector 备份会话进行还原。

   recover_start media_group_namebackup_type EBID "inst_nameSessionID:1 pipe_name1,inst_nameSessionID:2 pipe_name2[, ...]"

   Windows 系统：

   recover_start BACKDP-Data[2] DATA EBID "inst_nameSessionID:1 \\.\Pipe\inst_name.BACKDP-Data[2].1,TEST SessionID:2 \\.\Pipe\inst_name.BACKDP-Data[2].2"

   UNIX 系统：

   recover_start BACKDP-Data[2] DATA EBID "inst_nameSessionID:1 /var/opt/omni/tmp/inst_name.BACKDP-Data[2].1,inst_nameSessionID:2 /var/opt/omni/tmp/inst_name.BACKDP-Data[2].2"

   针对所需备份会话链中的每个会话重复此步骤。

   a. 要将数据库一直恢复到指定的时间点，请使用 recover_start 命令及 UNTIL 子句:

      recover_start BACKDP-Archive LOG EBID "inst_name SessionID:1 pipe_name1,inst_name SessionID:2 pipe_name2[, ...]" UNTIL yyyymmdd

hhmmss

其中 yyyymmdd 和 hhmmss 参数指定最后该应用哪个重做日志。

8. 根据上一次执行 recover_start 或 recover_replace 时的退出代码，相应地使用 recover_start 或 recover_replace 命令。

   有关详细信息，请参阅 SAP MaxDB 文档。

9. 如果上一步中的命令 recover_start 或 recover_replace 返回退出代码 -8020 ，并且您已经还原了所有相关数据，请执行以下命令:

   recover_ignore

   有关详细信息，请参阅 SAP MaxDB 文档。

SAP MaxDB 集成

执行 SAP MaxDB 迁移时，必须首先执行一些其他任务以便准备 SAP MaxDB 服务器或实例。

按照 SAP MaxDB 还原和恢复一节中的步骤，使用 SAP MaxDB 实用程序从现有 Data Protector SAP MaxDB 备份会话迁移 SAP MaxDB 数据库。执行所述的步骤时，请在执行 recover_start 命令“之前”，通过在 SAP MaxDB 数据库管理器中执行以下命令来删除 SAP MaxDB 服务器上的现有重做日志:

```
util_execute clear log
```

查找要还原的信息

要查找还原所需的信息，请按照以下步骤操作:

执行以下 Data Protector 命令:

- omnidb -sapdb

  获取 SAP MaxDB 对象列表。

- omnidb -sapdb object_name

  获取特定对象的详细信息，包括 SessionID。

SAP MaxDB 还原选项

SAP MaxDB 还原和恢复选项介绍了 SAP MaxDB GUI 还原和恢复选项。

以下是与 SAP MaxDB 有关的备份选项:

迁移选项

要将选定的 SAP MaxDB 对象还原到同一 SAP MaxDB 服务器和实例，请保留迁移选项不变。仅在执行 SAP MaxDB 迁移 (即还原到其他 SAP MaxDB 服务器或其他实例，而不是还原到备份的实例) 时才使用迁移选项。

以下是迁移选项的说明。首先列出 GUI 选项，接着是斜杠 (/)，后面是同等 CLI，最后是描述。

还原到客户机/ -destination ClientName	使用 GUI 时，请在下拉列表中，选择要将数据库还原到的 SAP MaxDB 服务器。 使用 CLI 时，请将 -destination 选项和 SAP MaxDB 服务器的名称指定为 ClientName 参数。 所选的 SAP MaxDB 服务器必须是 Data Protector 单元的一部分，并且必须安装有 Data Protector SAP MaxDB Integration 软件组件。

还原到实例/ -newinstance DestinationInstanceName	使用 GUI 时，您可以: • 在“还原到实例”下拉列表中选择一个实例。该下拉列表仅显示已配置为与此集成一起使用的实例。有关如何配置 SAP MaxDB 服务器以使其与此集成一起使用的信息，请参阅配置 SAP MaxDB 实例。 • 输入尚未配置为与此集成一起使用的现有实例的名称。在这种情况下，单击“设置”按钮以配置指定的实例。 使用 CLI 时，以 DestinationInstanceName 参数的形式指定给 -newinstance 选项的实例必须已配置为与此集成一起使用。有关如何配置 SAP MaxDB 服务器以使其与此集成一起使用的信息，请参阅配置 SAP MaxDB 实例。
“用户名”和“用户组”/不可用	在 UNIX 上，您可以更改 SAP MaxDB 应用程序在 SAP MaxDB 服务器上运行时所使用的 OS 系统用户的用户名和组名 (例如 sapsys 组下的 sapdb 用户)。默认情况下，为启动了 Data Protector GUI 的用户设置此选项。 使用 CLI 时，无法更改用户名和组名。使用与备份会话期间使用的用户相同的用户。
数据库联机时强制恢复	选择此选项可还原数据库 (即便该数据库处于联机状态)。 未选择此选项且数据库 (实例) 处于联机状态时，还原将终止并显示警告消息，而数据库则保持原样。
设置/不可用	如果要还原到的实例尚未配置为与此集成一起使用，请单击此按钮。有关必须输入的参数的信息，请参阅配置 SAP MaxDB 实例。 使用 CLI 时，此选项不可用。要配置实例，请按配置 SAP MaxDB 实例所述使用 util_sapdb 实用程序。

恢复选项

使用还原选项，并通过将重做日志一直应用到最新版本或应用到指定日期和时间来恢复数据库。

重要说明SAP MaxDB 数据库可以切换到的状态存在几种情况，具体取决于备份选项“保留存档日志” 和恢复选项“使用现有存档日志”，其中 SAP MaxDB 服务器上的重做日志序列可能会与已还原的卷存在事务差异。执行还原时 (当数据库切换到“联机” 模式时)，SAP MaxDB 会始终检查是否存在该差异，而不管为恢复选择的时间点。如果存在差异，则不执行恢复，并且数据库仍处于“管理” 模式，除非在开始还原之前手动删除了现有重做日志。

以下是各恢复选项的说明。首先列出 GUI 选项，接着是斜杠 (/)，后面是同等 CLI，最后是描述。

恢复/ -recover	选择此选项时，数据库在还原后恢复 (并切换到 “联机”模式)，具体恢复方式是将重做日志一直应用到最新版本 (如果选择了“最新版本”选项) 或一直应用到指定的日期和时间 (如果选择了“截止时间”选项)。 **重要说明** 使用此选项时，请确保在“数据属性”对话框中选择的备份 ID (使用 GUI 时) 或 -session 选项指定的备份 ID (使用 CLI 时) 能为此集成还原足够数据，从而将重做日志一直应用到最新版本或一直应用到指定日期和时间。 如果不选择此选项，将禁用所有其他恢复选项，并在还原之后发生以下情况： • 如果没有还原存档日志 (如果从完整备份会话执行还原)，则数据库在还原后仍保持在“管理”模式下。 • 如果还原了存档日志，则数据库 (如果还原的存档日志允许) 将切换到“联机”模式。但是，如果数据库无法切换到“联机”模式 (因为还原的存档日志不允许)，则它将仍旧处于“管理”模式下。
最新版本/ -endlogs	选择此选项可将数据库恢复到最新日志。 使用 CLI 时，这是默认选项。
截止日期/ -time: YYYY-MM-DD.hh.mm.ss	使用 GUI 时，选择此选项可将数据库恢复到您在“截止日期”下拉菜单中选择的时间点。 使用 CLI 时，如果要将数据库恢复到 YYYY-MM-DD.hh.mm.ss 参数指定的时间点，请指定 -time: 选项。 **注意** 所选时间是运行 Data Protector GUI 或 CLI 的系统上的系统时间。如果要恢复的系统与运行 Data Protector GUI 的系统不在同一时区，则还原点调整为要还原的系统上设置的本地时间。
“使用现有存档日志”/ -from_disk	选择此选项可以将 SAP MaxDB 服务器上的现有存档日志复制到 SAP MaxDB 服务器重做日志。 如果未选择此选项，备份介质上的已备份存档日志将应用于重做日志 (如果还原了事务备份会话)，或者重做日志会与现有存档日志一起完好保留在 SAP MaxDB 服务器上 (如果还原了完整或差异备份会话)。 为还原选择了事务备份会话时或者还原是所需还原链的一部分时，如果同时选择了“使用现有存档日志”选项，来自 Data Protector 介质的存档日志将应用于重做日志。然后，SAP MaxDB 服务器上的存档日志将应用于重做日志。 **注意** 在 SAP MaxDB 迁移时将禁用“使用现有存档日志”选项，因此仅允许从备份介质上的已备份存档日志还原重做日志 (如果还原了事务备份会话)。

使用其他设备进行还原

您可以使用与备份不同的设备执行还原。

使用 Data Protector GUI

有关如何使用 Data Protector GUI 为还原选择其他设备的信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

使用 Data Protector CLI 或 SAP 命令

如果要使用 Data Protector CLI 或 SAP MaxDB 命令进行还原，请在文件中指定新设备:

Windows 系统： Data_Protector_program_data\Config\Server\cell\restoredev

UNIX 系统： /etc/opt/omni/server/cell/restoredev

使用以下格式:

" DEV 1 " " DEV 2 "

其中， DEV 1 是原始设备，而 DEV 2 是新设备。

> **重要说明**使用后删除此文件。

在 Windows 系统上，请为该文件使用 Unicode 格式。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

有关如何监视会话，请参阅《Data Protector 帮助》索引: “查看当前正在运行的会话”。

SAP R/3 集成

This feature is available in the Premium Edition

本主题介绍如何配置和使用 Data Protector SAP R/3 集成。它说明了备份和还原 SAP R/3 数据库环境的以下文件 (**SAP R/3 对象**) 时需要了解的概念和方法:

- 数据文件
- 控制文件
- 联机重做日志
- 脱机 (存档) 重做日志
- SAP R/3 日志和参数文件

Data Protector 支持脱机和联机备份。联机备份期间，仍可主动使用 SAP R/3 应用程序。

Data Protector 提供以下类型的交互式备份和安排的备份：

备份类型

完整	备份全部所选的 SAP R/3 对象。
增量	Oracle RMAN 备份增量级别 1 (仅在使用 Oracle RMAN 时可用)。备份从上一次完整备份以来对 Oracle 数据文件所做的更改。

您可以使用以下方法启动备份和还原备份:

- Data Protector 用户界面
- SAP BRTOOLS 界面

Data Protector 仅支持文件系统还原。您可以将 SAP R/3 文件:

- 还原到原始位置
- 还原到另一个客户机
- 到其他目录

即时恢复完成后，可以使用 SAP BRTOOLS 界面将数据库还原到特定时间点。

本主题提供特定于 Data Protector SAP R/3 集成的信息。有关 Data Protector 的常规过程和选项，请参阅《Data Protector 帮助》。

集成概念

此集成将 SAP 备份和还原工具 (BR*Tools) 与 Data Protector 相关联。由于 SAP R/3 应用程序基于 Oracle 数据库运行，因此 SAP R/3 备份对象与 Oracle 对象非常类似。主要区别是 SAP 备份实用程序对 Data Protector 隐藏了数据库，这使得 Data Protector 将这些对象视为普通文件。

SAP 工具可以使用 Data Protector 界面或 SAP BRTOOLS 界面启动。

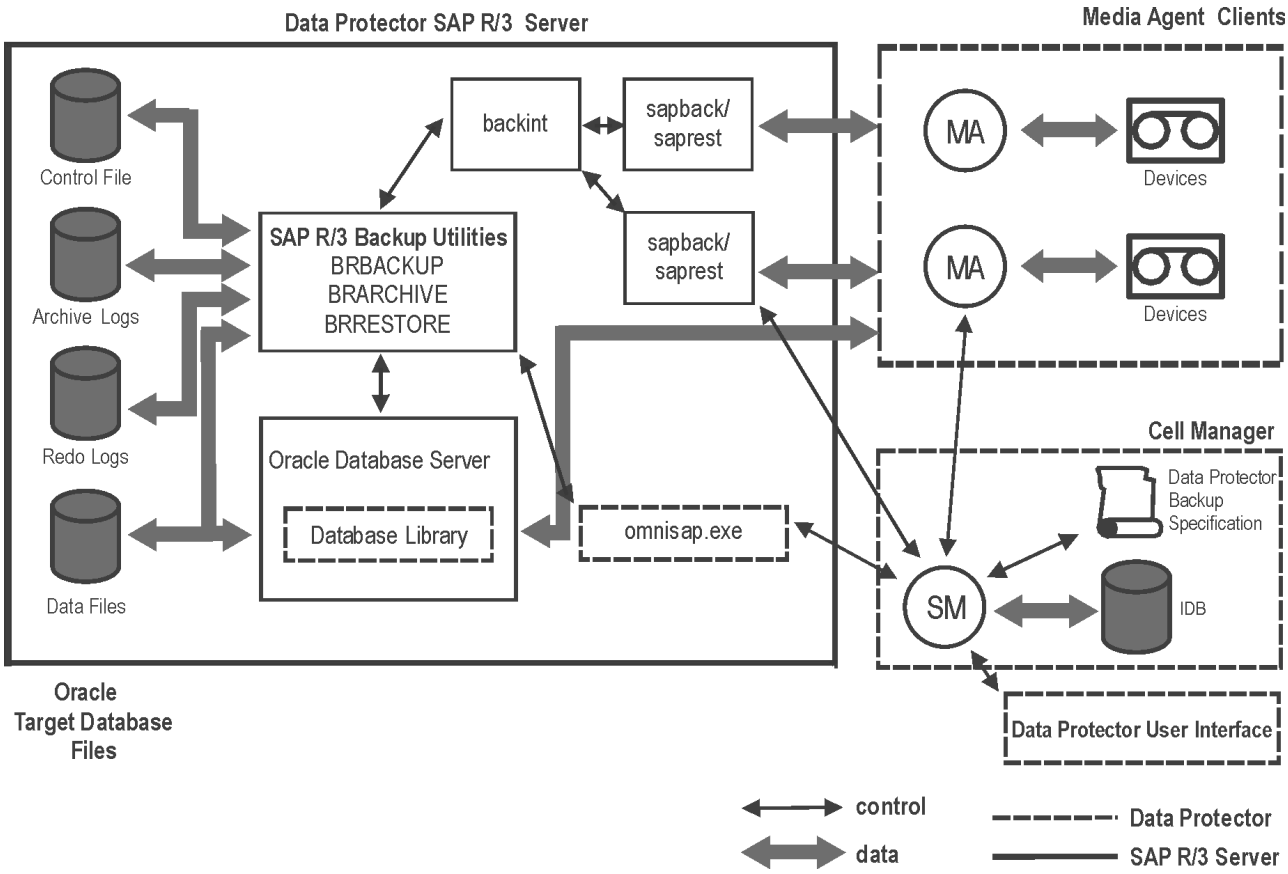
SAP 备份和还原实用程序

BRBACKUP	备份控制文件、数据文件和联机重做日志文件。此外，还保存与特定备份会话相关的配置文件和日志。
BRARCHIVE	备份由 Oracle 写入到存档目录的脱机 (存档) 重做日志。
BRRESTORE	还原使用 BRBACKUP 和 BRARCHIVE 备份的数据。

您可以在两种不同的模式下备份 Oracle 数据文件:

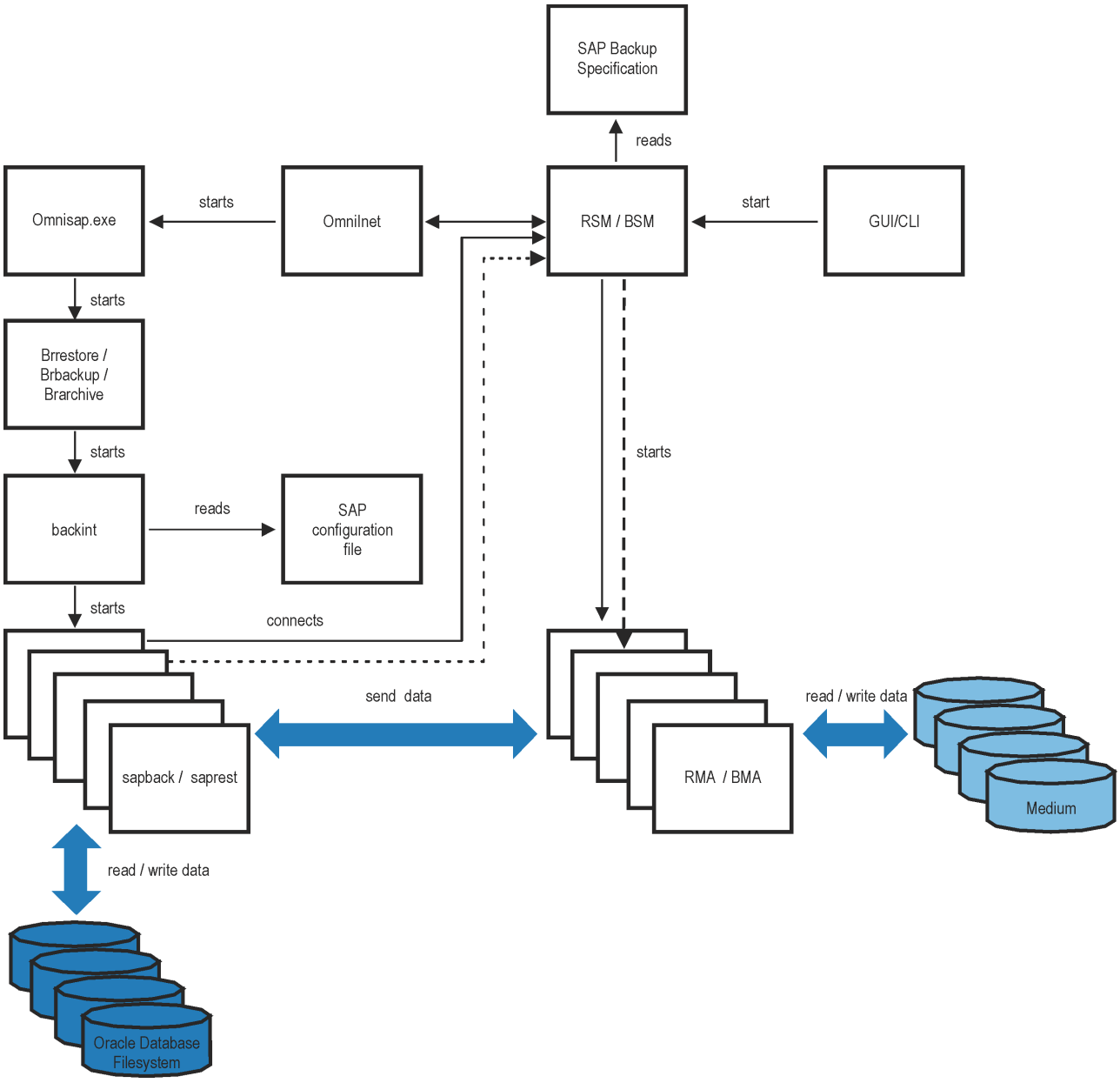
backint	使用 Data Protector SAP R/3 集成备份数据。
RMAN	使用 Oracle Recovery Manager (RMAN) 备份数据。RMAN 模式的主要优点是允许增量备份 Oracle 数据库。

SAP R/3 体系结构



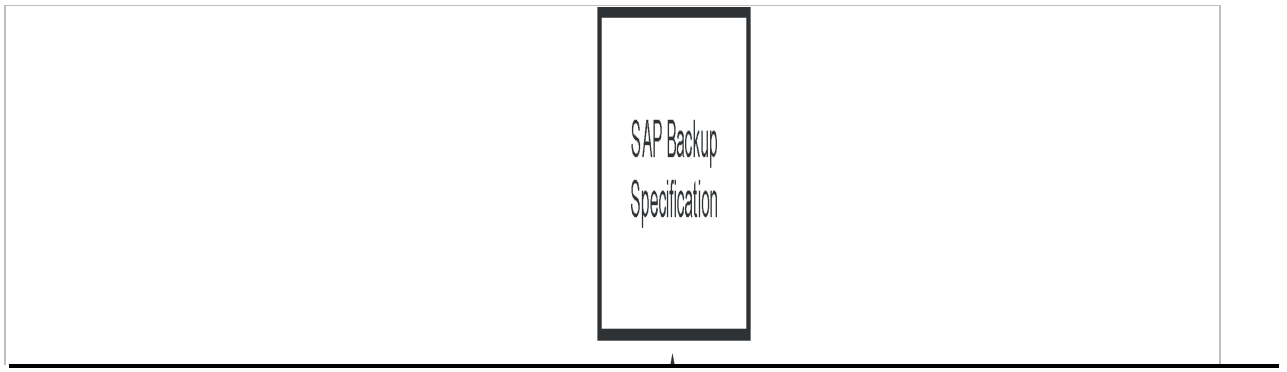
图例	
SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
数据库例程库	一组 Data Protector 可执行文件，用于在 Oracle Server 和 Data Protector 之间传输数据。仅当 Oracle 数据文件以 RMAN 模式备份时才需要。
MA	Data Protector 常规介质代理。
备份规范	要备份的对象列表、备份设备和要使用的选项。
IDB	Data Protector 内部数据库。
backint	Data Protector 与 SAP R/3 应用程序之间的备份接口。它由 SAP 工具启动: BRBACKUP 或 BRARCHIVE 使用 BACKINT 将备份请求传递给 Data Protector。BRRESTORE 使用 BACKINT 触发 Data Protector 来还原请求的文件。
sapback/saprest	实际备份/还原文件的程序。
omnisap.exe	启动 SAP 备份工具的 Data Protector 程序。

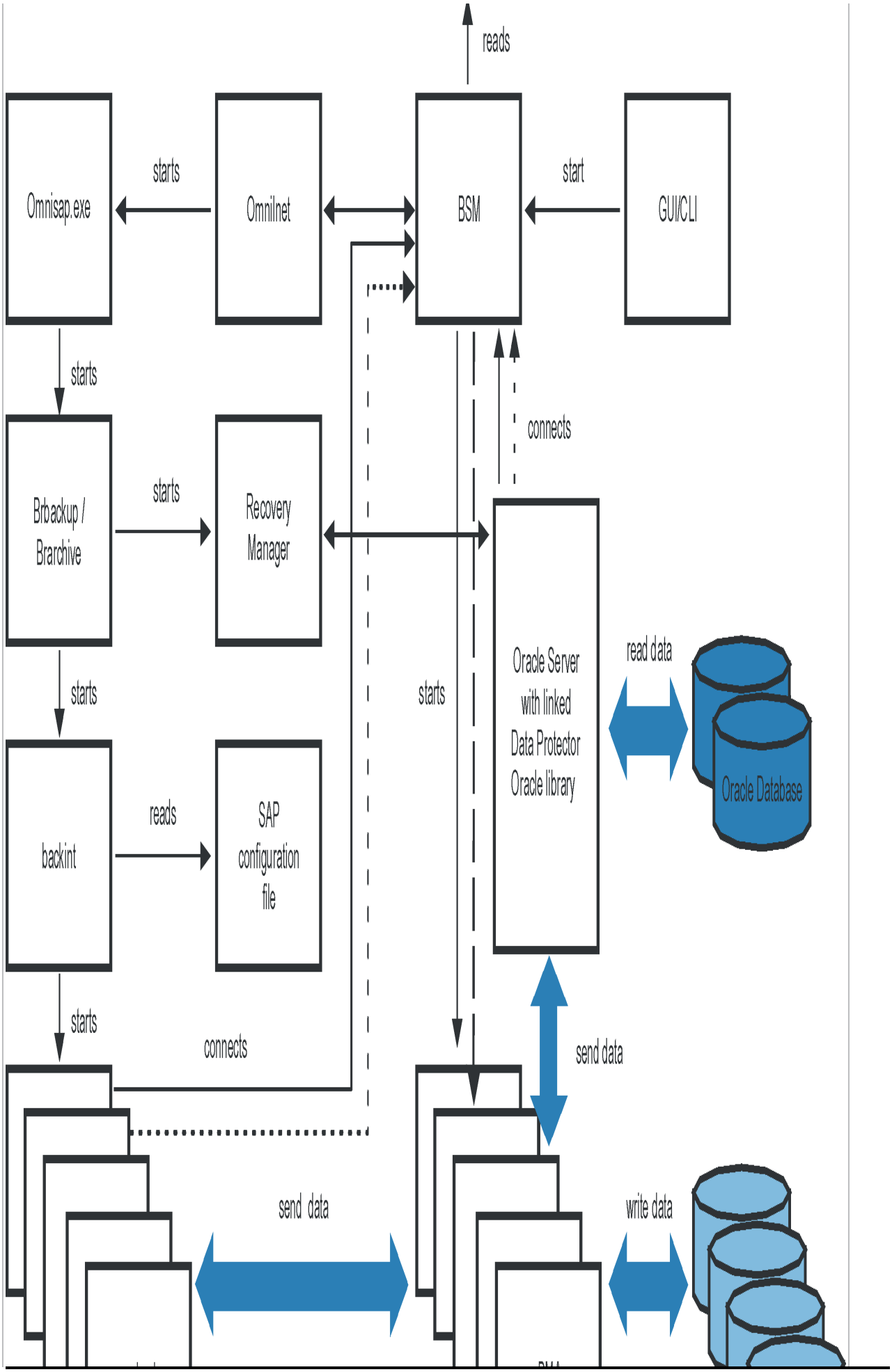
SAP R/3 体系结构: backint 模式

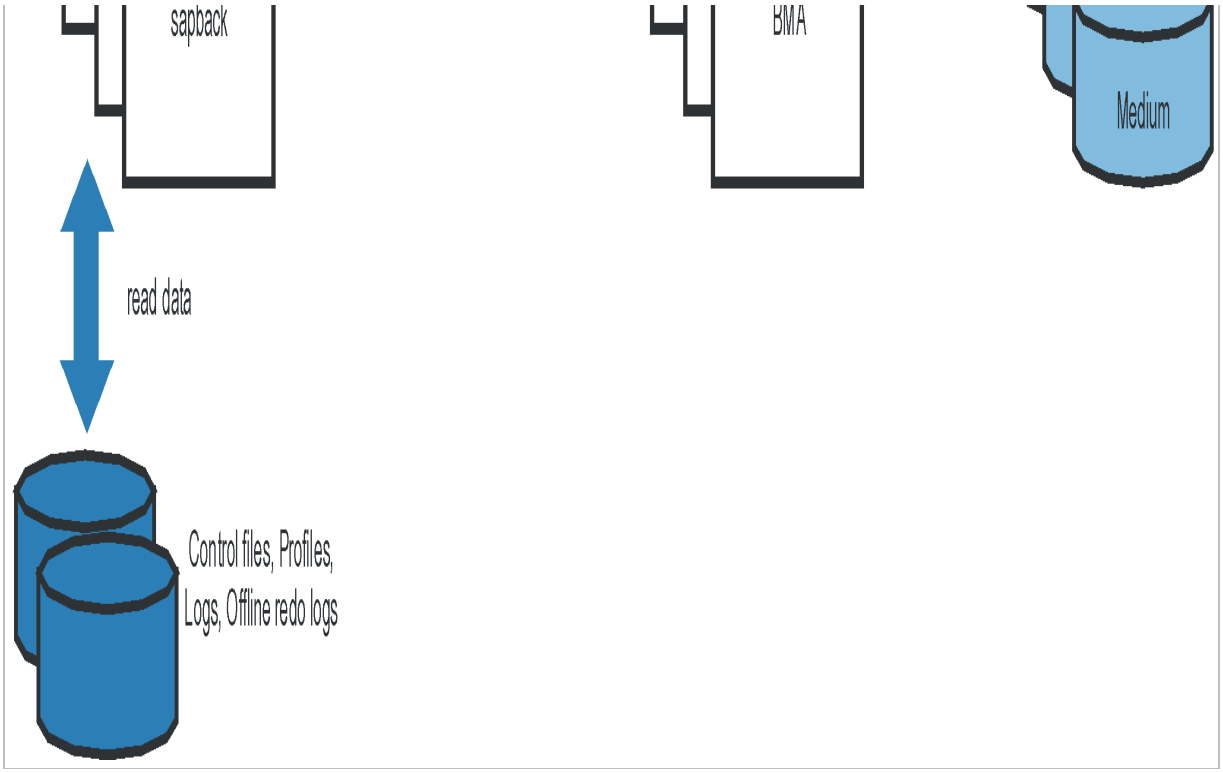


图例	
BSM/RSM	Data Protector 备份会话管理器/还原会话管理器
BMA/RMA	Data Protector 备份/还原介质代理
GUI/CLI	Data Protector 图形用户界面/命令行界面

SAP R/3 体系结构: RMAN 模式




reads
Omnisap.exe
starts
Omniinet
BSM
start
GUI/CLI
starts
Brbackup /
Brarchive
starts
Recovery
Manager
connects
starts
Oracle Server
with linked
Data Protector
Oracle library
read data
Oracle Database
starts
backint
reads
SAP
configuration
file
starts
connects
send data
send data
write data



备份流

1. 如果备份会话已启动:
   - **使用 Data Protector 接口 (或调度程序):** BSM 已启动，接着它会读取相应的 Data Protector 备份规范，检查设备是否可用，并在 SAP R/3 客户机上启动 omnisap.exe 。 omnisap.exe 代理导出适当的环境变量并启动 BRBACKUP 或 BRARCHIVE。
   - **使用 SAP BRTOOLS 界面:** BRBACKUP 或 BRARCHIVE 直接启动。
2. BRBACKUP 执行以下操作:
   - 根据备份类型 (联机或脱机) 来更改 Oracle 目标数据库的状态 (已打开或已关闭)。
   - 将 Oracle 目标数据库切换到 ARCHIVELOG 模式。

     存档的重做日志文件由 Oracle 写入存档目录，然后使用 BRARCHIVE 进行备份。
   - 在备份会话期间创建 BRBACKUP 日志，其中包含有关已备份文件和备份 ID 的信息。还原期间需要此信息来确定数据库文件和存档重做日志文件的位置。
   - 使用 backint 进行联机备份时设置表空间模式 (BEGIN/END BACKUP)。通过这种方式，SAP R/3 应用程序在备份前一刻将表空间置于备份模式，并在备份完成后立即将其恢复到正常模式。
3. - 如果 BRBACKUP 已启动:
     1. BRBACKUP 启动 backint 命令 (backint 模式) 或 RMAN (RMAN模式)，然后由后者备份 Oracle 数据文件和控制文件。
     2. BRBACKUP 启动 backint 命令 (在 backint 和 RMAN 模式下)，然后由后者备份在备份 Oracle 数据文件和控制文件期间创建的 SAP 参数文件和 SAP R/3 历史记录文件。
   - 如果启动了 BRARCHIVE (在 backint 或 RMAN 模式下)，BRARCHIVE 将启动 backint 命令，然后由后者备份存档的重做日志文件。此外还会创建控制文件的一份副本，且该副本也会进行备份。

   注意 Backint 根据所选的均衡类型，将为备份指定的文件分为若干子集，并为每个子集启动 sapback 进程 (前提是指定的并发数足够大)。 sapback 进程从磁盘读取数据并将其发送到通用介质代理。
4. 当所有通用介质代理完成数据传输后，BSM 等待超时 (smWaitForNewBackupClient 全局选项) 并在此时间期限内未启动 backint 命令时完成备份会话。

还原流

您可以使用 Data Protector 用户界面或 SAP BRTOOLS 用户界面启动还原。但是，使用 Data Protector 只能执行标准文件系统还原。

1. 选择要还原的对象并使用 SAP BRTOOLS 开始还原时会发生以下情况 (具体取决于使用的模式):
   - **Backint 模式:** BRRESTORE 会检查是否有足够的可用磁盘空间，然后启动 backint 命令还原 Oracle 数据文件。

     如果要还原的文件的备份驻留在不同的介质上，backint 会为每个介质启动单独的 saprest 进程，以便并行还原文件 (前提是指定的并发数足够大)。第一个 saprest 进程会启动 RSM，而后续的 saprest 进程会连接到同一个 RSM。RSM 检查还原设备是否可用并启动数据流。

- **RMAN 模式:** BRRESTORE 启动 RMAN，后者通过 Data Protector 数据库例程库和 Oracle Server 进程连接到 Data Protector，并支持传输 Oracle 数据文件的数据。

2. 当所有通用介质代理完成数据传输后，RSM 等待超时 (smWaitForNewRestoreClient 全局选项) 并在此时间期限内未启动 backint 命令时完成还原会话。

手动均衡

手动均衡意味着手动将文件分为若干子集，然后并行备份这些子集。要将文件分为若干子集，请将 manual_balance 部分添加到 Data Protector SAP R/3 配置文件，如以下示例所述。

示例

假设有一个名为 SAP-R3 的备份规范，并且需要备份以下文件: fileA 、 fileB 、 fileC 、 fileD 。要将这些文件分为三个子集 (0={fileA, fileC} 、 1={fileB} 、 2={fileD})，请将以下几行添加到 Data Protector SAP R/3 配置文件:

```
manual_balance={ SAP-R3={ fileA=0; fileB=1; fileC=0;fileD=2;}}
```

将文件分成若干子集时，请考虑以下事项:

- 一次只能使用同一硬盘中的一个文件。
- 子集中的文件数必须等于小于为备份指定的所有设备的并发数之和。
- 如果备份规范包含并未分配给任何子集的文件，Data Protector 会基于负载均衡原则，自动将这些文件添加到要备份的文件列表中。在备份之前，此列表已记录到:

  Windows 系统： SAPDATA_HOME\sapbackup*.lst

  UNIX 系统： ORACLE_HOME/sapbackup/.*.lst

本地化 SAP R/3 对象

Oracle Server 使用自有的编码，这可能与文件系统使用的编码不同。在备份上下文中，Data Protector 会显示 Oracle 数据库的逻辑结构 (使用 Oracle 名称)；在还原上下文中，则显示 Oracle 数据库的文件系统结构。因此，要正确显示非 ASCII 字符，请确保 Data Protector 编码在备份期间与 Oracle Server 编码匹配，在还原期间与文件系统编码匹配。但是，显示不正确并不会影响还原。

Windows 系统： 如果 DBCS 的当前值与非 Unicode 程序的默认 Windows 字符集不匹配，则会出现问题。请参阅 SAP R/3 故障诊断

UNIX 系统： 为了能够在不同的 Data Protector 编码之间切换，请在 UTF-8 语言环境下启动 GUI。

如果要使用 Data Protector CLI 还原文件，而且已备份对象的名称包含当前语言组 (Windows) 或代码页 (UNIX) 无法正确显示的字符:

1. 将环境变量 OB2_CLI_UTF8 设置为 1 。
2. *Windows 系统：* 将终端使用的编码设置为 UTF-8。

否则，某些命令的输出无法正确显示 (例如 omnidb 返回的备份对象)，并且不能用作其他命令的输入 (例如 omnir)。

稀疏文件

您可以通过设置 sparse 选项来提高稀疏文件还原的性能。通过以下任意一种方式设置该选项:

- 使用 Data Protector GUI: 在“选项”页面中选择“还原稀疏文件”选项。
- 使用 Data Protector CLI: 执行 omnir 命令时，添加 -sparse 选项。
- 使用 SAP 命令: 执行 BRRESTORE 命令之前，设置 Data Protector OB2SPARSE 变量:

  Windows 系统： set OB2SPARSE=sparse

  UNIX 系统： export OB2SPARSE=sparse

灾难恢复

有关一般信息，请参阅灾难恢复。

还原控制文件

控制文件包含有关数据库结构的所有信息。如果控制文件丢失，请在还原数据库的任何其他部分之前先还原控制文件:

1. 使用标准 Data Protector 还原过程还原控制文件。

   控制文件 (ctrlORACLE_SID.dbf) 将还原到 SAPBACKUP 变量定义的目录中。如果未设置该变量，控制文件将还原到默认的 Data Protector 临时文件目录。

2. 执行：

   ```
   run { allocate channnel 'dev0' type disk; replicate controlfile from 'TMP_FILENAME'; release channel 'dev0'; }
   ```

   其中 TMP_FILENAME 是将控制文件还原到的文件夹。

Data Protector SAP R/3 配置文件

Data Protector 在 Cell Manager 上的以下文件中存储每个已配置的 SAP R/3 数据库的集成参数:

Windows 系统： Data_Protector_program_data\Config\Server\Integ\Config\Sap\ClientName%ORACLE_SID

UNIX 系统： /etc/opt/omni/server/integ/config/SAP/ClientName%ORACLE_SID

存储的参数包括:

- Oracle 主目录
- 连接到目标数据库的已编码连接字符串
- BRTOOLS 主目录
- 启动备份前需要导出的变量
- SAPDATA 主目录
- 用户名和用户组
- 用于控制文件或重做日志副本的临时目录
- 将复制到安全位置的控制文件和重做日志列表
- 字符集 (ORA_NLS_CHARACTERSET)
- 每个备份规范的并发数和均衡，以及 RMAN 备份的通道数
- 速度参数 (备份特定文件所需的时间 - 以秒为单位)
- 手动均衡参数

这些配置参数会写入到 Data Protector SAP R/3 配置文件:

- 在配置集成期间
- 在创建备份规范期间
- 更改配置参数时

重要说明 为避免备份问题，请特别注意确保配置文件的语法和标点与示例一致。

注意: 您可以通过以下方式引用其他环境变量，从而设置配置文件 Environment 部分 (子列表) 中的参数:

```
SAPDATA_HOME=${ORACLE_HOME}/data
```

语法

Data Protector SAP R/3 配置文件的语法如下:

```
ORACLE_HOME='ORACLE_HOME'; ConnStr='ENCODED_CONNECTION_STRING_TO_THE_TARGET_DATABASE'; BR_directory='BRTOOLS_HOME';
SAPDATA_HOME='SAPDATA_HOME'; ORA_NLS_CHARACTERSET='CHARACTER_SET'; OSUSER='USER_NAME'; OSGROUP='USER_GROUP';
Environment={ [ENV_var1='value1';] [ENV_var2='value2'; ...] } SAP_Parameters={backup_spec_name=('-concurrency #_of_concurrency ' | '-
time_balance' | '-load_balance' | '-manual_balance' | '-channels #_of_RMAN_channels'); } speed={ AVERAGE=1;
'filename'=#_of_seconds_needed_to_back_up_this_file; } compression={'filename'=size_of_the_file_in_bytes_after_the _compression; }
manual_balance={backup_specification_name={ 'filename'=device_number; } }
```

在 SAP R/3 数据库配置期间，Data Protector 会自动设置 ORA_NLS_CHARACTERSET 参数。有关如何配置 SAP R/3 数据库以与 Data Protector 一起使用的详细信息，请参阅配置 SAP R/3 数据库。

示例

这是该文件的一个示例:

```
ORACLE_HOME='/app/oracle805/product'; ConnStr='EIBBKIBBEIBBFIBBGHBBOHBB
QDBBOFBBCFBBPFBBCFBBIFBBGFBBDGBBBFBBCFBBDFBBCFBB'; BR_directory='/usr/sap/ABA/SYS/exe/run'; SAPDATA_HOME='/sap';
ORA_NLS_CHARACTERSET='USASCII7'; OSUSER='orasid'; OSGROUP='dba'; Environment={ } SAP_Parameters={ sap_weekly_offline=('-
concurrency 1','-no_balance'); sap_daily_online=('-concurrency 3','-load_balance'); sap_daily_manual=('-concurrency 3','-manual_balance'); }
speed={ AVERAGE=203971; '/file1'=138186; '/file2'=269756; } compression={ '/file1'=1234; '/file2'=5678; } manual_balance={
sap_daily_manual={ '/file1'=1; /* file 1 is backed up by the first sapback */ '/file2'=2; /* file 2 is backed up by the second sapback */ '/file3'=1; /*
file 3 is backed up by the first sapback */ '/file4'=1; } }
```

使用 CLI 设置、检索、列出和删除 Data Protector SAP R/3 配置文件参数

Data Protector SAP R/3 配置文件参数通常在以下情况后写入到 Data Protector SAP R/3 配置文件:

- Data Protector 配置完 SAP R/3 运行的 Oracle 实例。
- 创建了新的备份规范。
- 完成了使用按时间均衡算法的备份。

util_cmd 命令

您可以在 Data Protector SAP R/3 客户机上，使用 util_cmd -putopt（设置参数）、 util_cmd -getopt（检索参数）或 util_cmd -getconf（列出所有参数）命令来设置、检索、列出或删除 Data Protector SAP R/3 配置文件参数。

必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。

设置 OB2BARHOSTNAME=client_name（Windows）或 OB2BARHOSTNAME=client_name（Linux）

群集感知客户机

在群集环境中，必须先将环境变量 OB2BARHOSTNAME 定义为虚拟主机名，然后才能 (在客户机上) 从命令行执行 util_cmd 命令。 OB2BARHOSTNAME 变量设置如下:

Windows 系统： set OB2BARHOSTNAME=virtual_hostname

UNIX 系统： export OB2BARHOSTNAME=virtual_hostname

util_cmd 概要

util_cmd 命令的语法如下:

util_cmd -getconf[ig] SAP oracle_instance [-local filename]

util_cmd -getopt[ion] [SAP oracle_instance] option_name [-sub[list] sublist_name] [-local filename]

util_cmd -putopt[ion] [SAP oracle_instance] option_name [option_value] [-sub[list] sublist_name] [-local filename]

其中：

option_name 是参数的名称

option_value 是参数的值

[-sub[list] sublist_name] 指定配置文件中用来写入或读取参数的子列表。

[-local filename] 指定以下内容之一:

- 将它与 -getconf[ig] 选项一起使用时，它会指定命令输出要写入到的文件名。如果未指定 -local 选项，则输出将写入标准输出。
- 将它与 -getopt[ion] 一起使用时，它会指定要从中获取参数及参数值的文件的文件名，随后读取的参数及参数值将写入到标准输出。如果未指定 -local 选项，则从 Data Protector SAP R/3 配置文件中获取参数及参数值，然后将它们写入标准输出。
- 将它与 -putopt[ion] 选项一起使用时，它会指定命令输出要写入到的文件名。如果未指定 -local 选项，则输出将写入 Data Protector SAP R/3 配置文件。

注意: 如果要将 option_value 参数设置为数字，则必须将该数字放在单引号中，并用双引号括起来。

返回值

util_cmd 命令在每次操作后显示一条短状态消息 (将其写入标准错误):

- Configuration read/write operation successful.

  成功完成所有请求的操作后，将显示此消息。

- Configuration option/file not found.

  如果配置中不存在具有指定名称的选项，或者指定为 -local 参数的文件不存在，则会显示此消息。

- Configuration read/write operation failed.

如果发生任何致命错误，则会显示此消息；例如 Cell Manager 不可用、Cell Manager 上缺少 Data Protector SAP R/3 配置文件，等等。

设置参数

要为 SAP R/3 运行的 Oracle 实例 ICE 设置 Data Protector OB2OPTS 和 Oracle BR_TRACE 参数，请在 Data Protector SAP R/3 客户机上使用以下命令:

Windows、HP-UX、Solaris 和 Linux 系统

```
util_cmd -putopt SAP ICE OB2OPTS '-debug 1-200 debug.txt' -sublist Environment
```

```
util_cmd -putopt SAP ICE BR_TRACE "'10'" -sublist Environment
```

其他 UNIX 系统

```
util_cmd -putopt SAP ICE NLS_LANG 'US7ASCII' -sublist Environment
```

```
util_cmd -putopt SAP TOR BR_TRACE "'10'" -sublist Environment
```

检索参数

要检索 Oracle 实例 ICE 的 OB2OPTS 参数的值，请在 Data Protector SAP R/3 客户机上使用以下命令:

```
util_cmd -getopt SAP ICE OB2OPTS -sublist Environment
```

列出参数

要列出 Oracle 实例 ICE 的所有 Data Protector SAP R/3 配置文件参数，请在 Data Protector SAP R/3 客户机上使用以下命令:

```
util_cmd -getconf SAP ICE
```

删除参数

要删除 Oracle 实例 ICE 的 OB2OPTS 参数的值，请在 Data Protector SAP R/3 客户机上使用以下命令:

```
util_cmd -putopt SAP ICE OB2OPTS "" -sublist Environment
```

满足 SAP R/3 集成的先决条件

以下是 SAP R/3 集成的先决条件:

- 确保已正确安装和配置 SAP R/3 应用程序。SAP R/3 应用程序使用的数据库必须是 Oracle 数据库。如果使用任何其他数据库，可以使用相应的 Data Protector 集成 (例如 Informix) 进行备份。假设您熟悉 SAP R/3 应用程序和 Oracle 数据库管理。
  - 有关安装、配置和使用 SAP R/3 应用程序以及 SAP 备份和还原工具 (BRBACKUP、BRRESTORE 和 BRARCHIVE) 的信息，请参阅 SAP R/3 应用程序文档。
- 确保拥有使用 Data Protector SAP R/3 集成的许可证。有关信息，请参阅《Data Protector 安装指南》。
- 确保已正确安装 Data Protector。
  - 有关如何在各种体系结构中安装 Data Protector SAP R/3 集成磁盘阵列 (P9000 XP 阵列、EMC 或非 HPE 存储阵列) 与 SAP R/3 集成的信息，请参阅“Data Protector 安装”一节。
  - 有关如何配置 Data Protector 集成 (EMC、P9000 XP 阵列或 NetApp Storage) 的信息，请参阅《Data Protector 零宕机时间备份管理员指南》。
  - 有关 SG 群集中 Data Protector Cell Manager 包配置的信息，请参阅《Data Protector 帮助》索引: “Serviceguard 集成”。

  要对其执行备份或还原的每个 SAP R/3 应用程序系统都必须安装 Data Protector“SAP R/3 集成”组件。
- SAP R/3 目录 SAPBACKUP、SAPARCH、SAPREORG、SAPCHECK 和 SAPTRACE 不得与数据文件驻留在相同的磁盘阵列源卷上。否则，在即时恢复期间将覆盖完整恢复数据库所需的 BRTOOLS 数据。您可以在 initDBSID.sap 文件中设置这些目录的位置。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 SAP R/3 系统和 Cell Manager 是否正常通信，请配置并运行一次 Data Protector 文件系统备份和还原。
- Windows 系统：

  在支持的 Windows 操作系统上，为具有运行备份和还原所需的 SAP R/3 权限的用户配置 Data Protector Inet 服务用户模拟。

  有关详细信息，请参阅 Data Protector 帮助索引: “Inet 用户模拟”。

  如果在同一系统上运行多个 SAP R/3 实例，并为每个实例配置了不同的 SAP 管理员帐户，请创建一个额外的通用 SAP 管理员帐户。配置 Data Protector Inet 服务以将此帐户用作服务启动帐户。
- 开始备份前，请确保 SAP R/3 数据库处于“打开”或“关闭”模式。

- 开始备份前，请确保将 SAP R/3 参数文件中的 primary_db 参数设置为 LOCAL。有关设置 SAP R/3 参数文件的详细信息，请参阅配置集成。
- *P9000 XP 阵列:* 如果使用 LVM 镜像配置，Data Protector 会在备份期间显示警告，因为应用程序系统上的卷组源卷并未分配到相应的 BC 对。该消息可忽略。
- 备份同一个 Oracle 实例的多个备份会话无法同时运行。
- 仅当使用模板时支持可配置的备份模式。
- 默认情况下，Data Protector 支持除 -a 和 -b 以外的所有 BRTOOL 选项。要启用对 -a 和 -b 的支持，请将 OB2BRTNOSECU omnirc 选项设置为 1。有关如何设置 omnirc 选项的信息，请参阅《Data Protector 帮助》索引: “omnirc 选项”。
- 一般来说，还原操作的耗时比备份更长。如果文件是使用许多个流备份的，还原操作的耗时还会显著延长。请注意，如果在 Oracle RMAN 脚本选项 FILESPERSET 设为 1 的情况下在 RMAN 模式下启动备份，RMAN 会为每个数据库文件创建单独的备份流 (对象)。

- Oracle RMAN 创建的备份只能使用 SAP 还原实用程序还原。
- 原始分区上的 SAP R/3 表空间无法使用 Data Protector GUI 还原。变通方法：使用 SAP 还原命令 (例如 brrestore)。
- 如果要还原稀疏文件，可以通过设置稀疏选项来提高性能。请参见稀疏文件。
- 如果 Oracle 数据库已本地化，则可能需要在开始还原前设置适当的 Data Protector 编码。有关详细信息，请参阅本地化 SAP R/3 对象。
- 不支持还原预览。

群集感知客户机

- 仅在一个群集节点上配置 SAP R/3 数据库，因为配置文件驻留在 Cell Manager 上。

  *Windows 系统：*配置期间，Data Protector 会将 Data Protector backint 和 ob2smbsplit.exe 程序 (BRTOOLS 支持 splitint 时仅复制后者) 从 Data_Protector_home\bin 复制到存储着 SAP 备份工具的目录，而且会将 ob2smbsplit.exe 重命名为 splitint.exe。此操作仅在当前活动节点上执行。在其他节点上须手动执行此操作。

  UNIX 系统：配置期间，Data Protector 会创建链接，指向当前活动节点上的 Data Protector backint 和 splitint 程序。在所有其他节点上，请手动执行此操作。执行：

  ```
  ln -s /opt/omni/lbin/backint \ /usr/sap/ORACLE_SID/sys/exe/run
  ```

  如果 BRTOOLS 支持 splitint ，还要执行:

  ```
  ln -s /opt/omni/lbin/ob2smbsplit \ /usr/sap/ORACLE_SID/sys/exe/run/splitint
  ```

- 如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称，如下所示:

  Windows 系统： set OB2BARHOSTNAME=virtual_server_name

  UNIX 系统： export OB2BARHOSTNAME=virtual_server_name

安装 SAP R/3 客户机

This feature is available in the Premium Edition

为了能够备份 SAP R/3 数据库，在安装过程中请选择以下组件：

- SAP R/3 Integration
- Disk Agent

  Data Protector 要求在 Backup Server（具有需要备份的文件系统数据的客户机）上安装磁带客户机。

配置 SAP R/3 集成

要配置 SAP R/3 集成，请完成以下步骤:

1. 配置所需的用户帐户。请参阅配置用户帐户。
2. 检查从应用程序系统到 Oracle 数据库的连接。请参阅检查连接。
3. 启用身份验证密码文件。请参阅身份验证密码文件。
4. (可选) 设置存档日志记录模式以启用联机备份。请参阅启用存档日志记录。
5. 共享应用程序系统上的目录。请参阅共享应用程序系统上的目录。
6. 配置要对其执行备份或还原的每个 SAP R/3 数据库。请参阅配置 SAP R/3 数据库。
7. 配置 SAP R/3 参数文件。请参阅配置集成。

注意: SAP 建议在所有群集节点上安装 SAP 备份实用程序。

配置用户帐户

要启用对 SAP R/3 数据库文件的备份和还原，您需要配置或创建多个用户帐户。

Oracle 操作系统用户帐户	添加到以下用户组的操作系统用户帐户: *Windows 系统：* ORA_DBA 和 ORA_SID_DBA 本地组 *UNIX 系统：* dba 和 sapsys 例如用户 oraSID 。 *UNIX 系统：*确保此用户是文件系统的所有者或安装了数据库的原始逻辑卷的所有者。最低权限应为 740。
用户帐户 root（仅限 UNIX 系统）	添加到 dba 用户组的默认操作系统管理员的用户帐户。
Oracle 数据库用户帐户	至少被授予以下 Oracle 角色的数据库用户帐户: • sysdba • sysoper 例如用户 system 。 不要将 Oracle SYS 用户配置为用于备份 SAP R/3 对象。使用 SYS 用户帐户进行备份时，SAP 备份将失败并显示错误 ORA-28009: connection as SYS should be as SYSDBA or SYSOPER.

将以下用户帐户添加到 Data Protector admin 或 operator 用户组:

- Oracle 操作系统用户帐户

  (如果使用备份集方法，请同时在应用程序和备份系统上添加此用户)

- *UNIX 系统：*用户帐户 root（应用程序系统和备份系统）

在群集环境中，请将这些用户帐户添加到以下客户机的 Data Protector admin 或 operator 用户组:

- 虚拟服务器
- 群集中的每个节点

有关添加 Data Protector 用户的信息，请参阅《Data Protector 帮助》索引: “添加用户”。

检查连接

要检查从应用程序系统到 Oracle 实例的连接，请执行以下操作:

1. 以 Oracle OS 用户身份登录应用程序系统 SAP R/3 客户机。
2. 导出/设置 ORACLE_HOME 和 ORACLE_SID 变量。
3. 启动 sqlplus 。
4. 以 Oracle 数据库用户身份 (首先使用 sysdba 角色，然后使用 sysoper 角色) 连接到 Oracle 目标数据库。

示例

对于以下配置:

Oracle 实例：PRO ORACLE_HOME：/app/oracle816/product

执行:

```
id uid=102(oraprod) gid=101(dba) export ORACLE_SID=PRO export ORACLE_HOME=/app/oracle816/product export SHLIB_PATH=/app/oracle816/product/lib:/opt/omni/lbin sqlplus /nolog SQLPLUS> connect system/manager@PRO as sysdba; 已连接。 SQLPLUS> connect system/manager@PRO as sysoper; 已连接。
```

身份验证密码文件

为数据库管理员启用身份验证密码文件:

1. 关闭应用程序系统上的 Oracle 目标数据库。
2. 在 init ORACLE_SID .ora 文件中，指定:

   remote_login_passwordfile = exclusive

有关如何设置密码文件的说明，请参阅 Oracle 文档。

启用存档日志记录

将数据库设置为存档日志记录模式时，可以防止未保存的联机重做日志被覆盖。缺少相关的重做日志时，数据文件的联机备份毫无用处，因为这时无法将数据库恢复到一致状态。

提示: 在 BRBACKUP 完成后立即存档联机备份期间生成的重做日志文件。

要保护存档目录不会溢出，请定期清除该目录。

要启用存档日志记录，请执行以下操作:

1. 在 init ORACLE_SID. ora 文件中，设置

   log_archive_start = true

   并指定 log_archive_dest 选项。

   示例

   这是 Oracle 实例 PRO 的 initORACLE_SID.ora 文件的示例:

   ```
   # @(#)initSID.ora 20.4.6.1 SAP 13/03/30 ############################################################ # (c)Copyright SAP AG, Walldorf ############################################################ .。。。 。。。。。。。。。。 。。。。。。。。。 。。。。。。。。。 ### ORACLE Authentication Password File remote_login_passwordfile = exclusive ### ORACLE archiving log_archive_dest = /oracle/PRO/saparch/PROarch log_archive_start = true .。。。
   ```

2. 装载 Oracle 数据库并使用 Oracle Server Manager 启动存档日志记录模式。执行：

   ```
   startup mount alter database archivelog; archive log start; alter database open;
   ```

   示例

   对于 Oracle 实例 PRO ，执行:

   Windows 系统： set ORACLE_SID=PRO

   UNIX 系统： export ORACLE_SID=PRO

   任何操作系统:

   ```
   sqlplus /nolog SQLPLUS> connect user/passwd@PRO; 已连接。 SQLPLUS> startup mount ORACLE 实例已启动。 总体系统全局区域 6060224 字节 固定大小 47296 字节 可变大小 4292608 字节 数据库缓冲区 1638400 字节 重做缓冲区 81920 字节 数据库已装载。 SQLPLUS> alter database archivelog; 语句已处理。 SQLPLUS> archive log start; 语句已处理。 SQLPLUS> alter database open;
   ```

将 Oracle Server 与 Data Protector MML 链接在一起

要在 RMAN 模式下使用 Data Protector SAP R/3 集成，Oracle Server 软件需要与运行 Oracle 实例的每个客户机上的 Data Protector Oracle 集成介质管理库 (MML) 链接起来:

- 使用 Data Protector GUI 或 CLI 启动备份或还原时，Data Protector 会自动将 Oracle Server 与特定于平台的相应 Data Protector MML 链接在一起。

  注意: 出于测试目的，可以覆盖此自动选择的项。您可以通过设置 Data Protector SBT_LIBRARY 参数，手动指定应使用哪个 Data Protector MML。该参数保存在 Data Protector SAP R/3 实例配置文件中。有关如何设置参数的信息，请参阅 util_cmd 手册页。

- 要直接使用 Oracle Recovery Manager 或 BRBACKUP 实用程序启动备份，您需要如使用 Oracle Recovery Manager 备份中所述，手动将 Oracle Server 软件和正确的特定于平台的 Data Protector MML 链接起来。

选择身份验证模式

Data Protector SAP R/3 集成支持通过两种身份验证模式来访问 SAP R/3 使用的 Oracle 数据库:

- 数据库身份验证模式
- 操作系统身份验证模式

使用数据库身份验证模式时，对应的 Oracle 数据库用户帐户每次发生更改时，都需要使用新的 Oracle 登录信息重新配置 SAP R/3 集成使用的 SAP R/3 数据库。如果使用操作系统身份验证模式，则无需执行此类重新配置。

请在配置特定的 SAP R/3 数据库时选择首选身份验证模式。

配置 SAP R/3 数据库

您需要为 Data Protector 提供以下配置参数:

- Oracle Server 主目录
- SAP R/3 数据主目录
- (可选) 如果选择数据库身份验证模式，则为 Oracle 数据库用户帐户。备份期间 BRBACKUP 和 BRARCHIVE 会使用该用户帐户。
- 存储 SAP 备份实用程序的目录

Data Protector 随后在 Cell Manager 上为 SAP R/3 数据库创建配置文件，并验证与数据库的连接。在 UNIX 系统上，Data Protector 还会为 backint 程序创建从存储 SAP 备份实用程序的目录到以下位置的软链接:

HP-UX、Solaris 和 Linux 系统: /opt/omni/lbin

其他 UNIX 系统: /usr/omni/bin

在 Windows 系统上，Data Protector 会将 backint 程序从 Data_Protector_home\bin 复制到 SAP 备份工具所在的目录。

重要说明: 如果计划使用 RMAN 执行脱机备份，请不要使用 Oracle 数据库用户 Internal 配置数据库，因为备份将失败。请使用用户 System 配置数据库。

要配置 SAP R/3 数据库，请使用 Data Protector GUI 或 CLI。确保 SAP R/3 数据库已打开。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP R/3”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择模板。

   单击**确定**。
4. 在“备份系统”中，选择备份系统。
5. 在“应用程序数据库”中，键入 Oracle 实例名称 (ORACLE_SID)。

   指定 UNIX 和 Windows Server 2008 客户机上可用的“用户和组/域”选项，如下所示:

   Windows Server 2008 : 在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator 、域 DP)。

   UNIX 系统 : 在“用户名”中，键入配置用户帐户中所述的 Oracle OS 用户。在“组/域名”中，键入 dba 。

   请确保此用户已添加到 Data Protector admin 或 operator 用户组，具有 SAP R/3 备份权限，以及已设置为用于 Data Protector Inet 服务用户模拟。此用户成为备份所有者。

   单击“下一步”。
6. 在“配置 SAP”对话框中，指定 Oracle Server 主目录和 SAP R/3 数据主目录的路径名。如果将这些字段留空，系统会使用默认的 ORACLE_HOME 目录。

   在“目标数据库的 Oracle 登录信息”下，指定以下内容:

   - 对于数据库身份验证模式，请指定“用户名”、“密码”和“服务”。
   - 对于本地操作系统身份验证模式，请将“用户名”、“密码”和“服务”留空。
   - 对于远程操作系统身份验证模式，请仅指定“服务”(将“用户名”和“密码”留空)。

   以下是各选项的说明:

- **用户名**和**密码**: 指定配置用户帐户中所述的 Oracle 数据库用户帐户的用户名和密码。
- **服务**: 指定 Oracle 服务名称。

在“备份和还原可执行文件目录”中，指定 SAP 备份实用程序所在目录的路径名。默认情况下，这些实用程序位于:

Windows 系统： \\SAP_system\sapmnt\ORACLE_SID\sys\exe\run

UNIX 系统： /usr/sap/ORACLE_SID/SYS/exe/run

单击**确定**。

7. SAP R/3 数据库已配置。退出 GUI，或按选择要备份的 SAP R/3 对象中所述继续创建备份规范。

使用 Data Protector CLI

1. 使用 Oracle 操作系统用户帐户登录 SAP R/3 系统。
2. 在命令提示符下，将当前目录更改为以下目录:

   Windows 系统： Data_Protector_home\bin

   HP-UX、Solaris 和 Linux 系统: /opt/omni/lbin

   其他 UNIX 系统: /usr/omni/bin/
3. 执行：

   util_sap.exe -CONFIG ORACLE_SIDORACLE_HOMEtargetdb_connection_stringSAPTOOLS_DIR [SAPDATA_HOME][SQL_PATH]

参数描述

ORACLE_SID	Oracle 实例名称。
ORACLE_HOME	Oracle Server 主目录的路径名。
targetdb_connection_string	此参数值决定用于访问 Oracle 数据库的身份验证模式: • 要选择数据库身份验证模式，请以 .user_name/password@Oracle_service 格式指定目标数据库的登录信息。 • 要选择本地操作系统身份验证模式，请仅指定字符 /。 • 要选择远程操作系统身份验证模式，请以 /@Oracle_service 格式指定目标数据库的登录信息。
SAPTOOLS_DIR	存储 SAP 备份实用程序的目录的路径名。
SAPDATA_HOME	安装 SAP R/3 数据文件的目录的路径名。默认情况下，此选项设置为 ORACLE_HOME 。

消息 *RETVAL*0 表示配置成功。

处理错误

如果收到 *RETVAL*error_number 消息 (其中 error_number 不为零)，则表示发生错误。

要获取错误描述，请执行:

Windows 系统：

Data_Protector_home\bin\omnigetmsg 12 error_number

HP-UX 和 Linux 系统:

/opt/omni/lbin/omnigetmsg 12 error_number

其他 UNIX 系统:

/usr/omni/bin/omnigetmsg 12 error_number

提示: 要获取 SAP R/3 应用程序使用的 Oracle 实例列表，请执行:

```
util_sap.exe -APP
```

要获取 Oracle 实例的表空间列表，请执行:

```
util_sap.exe -OBJS0  ORACLE_SID
```

要获取表空间的数据库文件列表，请执行:

```
util_sap.exe -OBJS1  ORACLE_SID TABLESPACE
```

检查配置

为此数据库创建至少一个备份规范后，可以检查 SAP R/3 数据库的配置。使用 Data Protector GUI 或 CLI。

使用 **Data Protector GUI**

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。单击备份规范以显示要检查的 Oracle 实例。
3. 右键单击 Oracle 实例，然后单击“检查配置”。

使用 **Data Protector CLI**

以 Oracle OS 用户身份登录 SAP R/3 系统并执行:

```
util_sap.exe -CHKCONF ORACLE_SID
```

其中， `ORACLE_SID` 是 Oracle 实例的名称。成功的配置检查将显示消息 `*RETVAL*0` 。

如果收到 `*RETVAL*error_number` 消息 (其中 error_number 不为零)，则表示发生错误。有关如何获取错误说明的信息，请参阅备份 SAP R/3。

备份 SAP R/3 集成

This feature is available in the Premium Edition

此集成可执行以下类型的联机和脱机数据库备份:

备份类型

完整	备份全部所选的 SAP R/3 对象。
增量	Oracle RMAN 备份增量级别 1 (仅在使用 Oracle RMAN 时可用)。备份从上一次完整备份以来对 SAP R/3 数据文件所做的更改。 运行增量备份之前，请确保存在完整备份。

有关这些备份类型的详细信息，请参阅 Oracle SAP R/3 文档。

要配置备份，请创建 ZDB 备份规范。

备份的内容取决于您在备份规范中的选择。

备份内容

选定的项	已备份的文件
存档日志	• 脱机（归档）重做日志 • 控制文件
数据库或单个表空间	• 数据文件 • 控制文件 • SAP R/3 日志和参数文件 • 联机重做日志 (仅在脱机备份期间)

您可以通过两种不同的方式指定 SAP R/3 备份选项:

- 使用 BRBACKUP 选项。
- 使用 SAP 参数文件。

注意: BRBACKUP 选项会覆盖 SAP 参数文件中的设置。

您可以在创建备份规范时指定 BRBACKUP 选项。如果未指定任何选项，SAP R/3 应用程序将引用 SAP 参数文件中的当前设置。在这种情况下，请在运行备份前，请确保已正确配置 SAP 参数文件。请参阅指定备份选项的两种方法中的示例。

指定备份选项的两种方法

备份类型	1. BRBACKUP 选项 2. SAP 参数文件设置
使用 backint 进行脱机备份	1. -t offline -d util_file 2. backup_type = offline backup_dev_type = util_file
使用 backint 进行联机备份 (表空间在整个备份会话期间处于备份模式)	1. -t online -d util_file 2. backup_dev_type = util_file backup_type = online

使用 backint 进行联机备份 (表空间仅在备份时处于备份模式)	1. -t online -d util_file_online 2. backup_dev_type = util_file_online backup_type = online
完整备份	1. -m full 2. backup_mode = full
使用 RMAN 进行备份	1. -d rman_util 2. backup_dev_type = rman_util rman_channels = number_of_channels rman_parms = "ENV=(OB2BARTYPE=SAP,OB2APPNAME=DB_Name, OB2BARLIST=Backup_Specification_Name)"

提示: 创建备份规范时，请选择已包含所需 BRBACKUP 选项的备份模板。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP R/3”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择模板，然后单击“确定”。

   可用于标准备份的备份模板

空白 SAP 备份	无预定义选项。
Brarchive_Save	备份脱机重做日志。
Brarchive_SaveDelete	备份脱机重做日志并在备份后删除它们。
Brarchive_SecondCopyDelete	创建已存档的脱机重做日志的第二个副本，并在备份后删除它们。
Brbackup_Offline	使用 backint 备份已关闭的数据库。
Brbackup_Online	备份活动数据库。util_file 设备类型用于备份。在整个备份会话期间，表空间处于备份模式 (已锁定)。您可以备份整个数据库，也可以仅备份单个表空间或数据文件。
Brbackup_RMAN_Offline	使用 Oracle RMAN 备份已关闭的数据库。
Brbackup_RMAN_Online	使用 Oracle RMAN 备份活动数据库。表空间在整个备份会话期间处于备份模式。
Brbackup_Util_File_Online	备份活动数据库。表空间仅在备份时处于备份模式。因此，与使用 util_file 设备类型的备份相比，存档日志文件的增加幅度更小。但是，如果数据库包含大量小文件，则此备份可能需要更长时间。

单击“下一步”。

4. 在“客户机”中，选择应在其上启动备份的 SAP R/3 系统。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，选择要备份的 Oracle 实例 (ORACLE_SID)。

   指定 UNIX 和 Windows Server 2008 客户机上可用的“用户和组/域”选项，如下所示:

   Windows Server 2008 : 在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator 、域 DP)。

   UNIX 系统 : 在“用户名”中，键入配置用户帐户中所述的 Oracle OS 用户。在“组/域名”中，键入 dba 。

请确保此用户已添加到 Data Protector admin 或 operator 用户组，具有 SAP R/3 备份权限，以及已设置为用于 Data Protector Inet 服务用户模拟。此用户成为备份所有者。

单击“下一步”。

5. 如果尚未将 SAP R/3 数据库配置为与 Data Protector 配合使用，则会显示“配置 SAP”对话框。按照配置 SAP R/3 数据库中所述进行配置。
6. 选择要备份的 SAP R/3 对象。您可以选择单个表空间、数据文件或存档日志。

   单击“下一步”。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。在“并发”选项卡中指定并行备份流的数量并指定介质池。

   注意: 并行性 (备份 SAP R/3 数据库时使用的备份流的数量) 会自动设置。如果使用负载均衡，则备份流的数量等于所选设备的并发性总和。

   单击“下一步”。
8. 设置备份选项。有关特定于应用程序的选项的信息，请参阅 SAP R/3 备份选项。

   单击“下一步”。
9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 单击“保存并计划”进行保存，然后计划备份规范。

提示: 请在实际使用之前先预览备份规范。请参阅预览备份会话。

SAP R/3 备份选项

选项	描述
日志文件	如果要在备份期间创建 backint 日志文件，请指定该文件的路径名。默认情况下不会创建该文件，因为 Data Protector 会将与备份会话有关的所有相关信息存储在数据库中。
BR 备份	指定 BRBACKUP 选项。 要在与配置期间指定的用户不同的 Oracle 数据库用户下运行 BRBACKUP，请键入 -u user_name。
备份对象	列出 omnisap.exe 传递的 BRBACKUP 选项。保存备份规范后将显示该列表。
BR 归档	指定 BRARCHIVE 选项。
均衡: 按负载	将文件分成大小大致相等的若干子集。然后，Data Protector sapback 程序将同时备份这些子集。 如果备份设备使用硬件压缩，则原始文件和备份文件的大小会有所不同。要将此情况通知 Data Protector，请在 Data Protector SAP R/3 配置文件的 compression 部分指定已备份文件的原始大小。
均衡: 按时间	将文件按大致相同的备份时间段分成若干子集。该时间段取决于文件类型、备份设备的速度和外部影响因素 (例如装载提示)。此选项最适合具有相同质量的大型库的环境。这些子集将由 Data Protector sapback 程序同时备份。Data Protector 会自动将备份速度信息存储在 Data Protector SAP R/3 配置文件的 speed 部分中。它会使用此信息来优化备份时间。 联机备份时或备份设备的速度差异很大时，此类型均衡有可能会导致文件分组并非最佳。
均衡: 手动	将文件按 Data Protector SAP R/3 配置文件的手动均衡部分中的指定分成若干子集。有关详细信息，请参阅备份 SAP R/3。
均衡: 无	没有使用均衡。文件按照它们在内部 Oracle 数据库结构中列出的顺序进行备份。要检查该顺序，请使用 Oracle Server Manager SQL 命令: select * from dba_data_files
Pre-exec、Post-exec	此处指定的命令由 SAP R/3 系统上的 omnisap.exe 在备份之前 (pre-exec) 或之后 (post-exec) 启动。不要使用双引号。只提供名称。命令必须位于以下目录中： *Windows 系统：* Data_Protector_home\bin *HP-UX、Solaris 和 Linux 系统:* /opt/omni/bin *其他 UNIX 系统：* /usr/omni/bin

备份模式	指定要使用的 RMAN 备份类型。仅当选择了整个数据库进行备份时可用 如果指定了 All ，RMAN 将备份整个数据库。 如果指定了 Full ，RMAN 将执行完整备份 (级别 0)，随后 RMAN 增量备份即会启用。
使用默认 RMAN 通道数	指定备份的并发值。仅在 RMAN 用于备份时适用。此选项会覆盖 SAP 参数文件中的设置。
数据库外部的对象	指定要保存的 Oracle SAP R/3 环境的非数据库文件。 将这些文件保存在单独的备份会话中。

注意: 使用 Data Protector 在一个会话中启动的 sapback 进程总数限制为 256 个。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。有关如何创建和编辑计划的详细信息，请参阅管理中的“调度程序”。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行：

```
omnib -sap_list backup_specification_name -test_bar
```

预览期间会发生什么?

omnisap.exe 命令启动，进而启动 Data Protector testbar 命令来测试:

- Oracle 实例与 Data Protector 之间的通信 (仅当使用 RMAN 时)
- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

备份方法

通过以下任一方式启动 SAP R/3 对象的备份:

- 使用 Data Protector GUI.
- 使用 Data Protector CLI.
- 使用 SAP BR*Tools。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。

2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行：

```
omnib -sap_list backup_specification_name [-barmode SAP_mode][List_options]
```

其中， SAP_mode 为下列项之一:

```
full|incr
```

示例

要使用 SAP R/3 备份规范 RONA 启动完整备份，请执行:

```
omnib -sap_list RONA -barmode full
```

使用 SAP BRTOOLS

1. 以 Oracle OS 用户身份登录 SAP R/3 备份系统或 SAP R/3 应用程序系统。
2. 导出/设置以下环境变量:

ORACLE_SID=*SAP_instance_name*	
ORACLE_HOME=*Oracle_software_home_directory*	
$ORACLE_HOME/dbs/init<Instance_ID>.sap	应由 Oracle 用户拥有，权限应为 644。同一用户用于 SAP R/3 备份。
[SAPBACKUP_TYPE=OFFLINE]	默认值为 ONLINE 。
SAPDATA_HOME=*database_files_directory*	
SAPBACKUP=*BRTOOLS_logs_and_control_file_copy_directory*	
SAPREORG=*BRSPACE_logs_directory*	
OB2BARLIST=*backup_specification_name*	仅需要用备份规范来指定应该使用哪些 Data Protector 设备进行备份。备份规范中的其他信息 (如要备份的 SAP R/3 对象或 BRBACKUP 选项) 将被忽略，必须在运行时手动指定。
[OB2_3RD_PARTY_BACKINT=1]	
[OB2BARHOSTNAME=*application_system_name*]	如果要在群集环境中指定虚拟服务器名称，则是可选的。

这些变量也可以在 backint 参数文件中指定。如果需要，则必须使用 *util_par_file* 参数在 SAP 配置文件中指定该文件的位置:

```
util_par_file = path\filename
```

如果未提供路径，系统将在目录中搜索该参数文件:

Windows 系统： SAPDATA_HOME\database

UNIX 系统： ORACLE_HOME/dbs

3. 如果计划在 RMAN 模式下备份，请确保 initSAP_instance.sap 文件中的 SBT_LIBRARY 参数指向正确的特定于平台的 Data Protector

MML。

4. 执行 BRBACKUP 命令。

```
brbackup -t {online_split | offline_split | online_mirror | \ offline_mirror} [–q split] -d \ util_file -m all -c -u user/password
```

使用 Oracle Recovery Manager 执行备份

如果直接使用 RMAN，请考虑以下事项:

- RMAN 将有关备份的信息存储在恢复编目中。出于安全考虑，请将该编目保存在单独的数据库中。这需要执行更多的管理工作。
- 发生灾难时 (例如丢失生产数据库和恢复编目)，数据的还原和恢复会非常复杂。如果这时没有 Oracle 支持人员的的帮助，恢复和还原几乎是不可能的。如果 Recovery Manager 没有将管理数据存储在恢复编目中，就无法只凭借已创建的备份来恢复数据库。
- 对于每个 RMAN 通道，将 SBT_LIBRARY 参数设置为指向正确的特定于平台的 Data Protector MML。

如果通过 BRBACKUP 实用程序使用 RMAN，请考虑以下事项:

- 这时不会使用恢复编目。有关备份的信息保存在控制文件和 SAP R /3 日志文件中。每次备份后，都会保存控制文件和 SAP R /3 日志文件。还原数据后，首先复制回控制文件，然后再复制回数据文件。如果发生灾难，则先还原 SAP R /3 日志文件，然后再还原所有数据文件。
- 其他重要文件仍将使用 backint 程序自动备份。
- 所有以前的 SAP R/3 备份策略仍可与 RMAN 一起使用。但是，RMAN 不能与 BRARCHIVE 一起执行脱机重做日志备份，也不能用于备用数据库备份。
- 确保 initSAP_instance.sap 文件中的 SBT_LIBRARY 参数指向正确的特定于平台的 Data Protector MML。有关 Data Protector MML 位置的详细信息，请参阅指定 parms 操作数。。

还原 SAP R/3 集成

This feature is available in the Premium Edition

您可以通过以下任意方式使用以下任意方法还原 SAP R/3 对象:

- 使用 Data Protector GUI。请参见标准还原。
- 使用 Data Protector CLI。请参阅使用 Data Protector CLI 进行还原。
- 使用 SAP 还原命令。请参阅使用 SAP 命令进行还原。

还原后，可以使用 SAP BRTOOLS 接口将数据库恢复到特定时间点。

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“SAP R/3”，展开此前从中备份过数据的客户机 (备份系统)，然后单击要还原的 Oracle 实例。
3. 在“源”页面中，选择要还原的 SAP R/3 文件。

   要以不同的名称还原文件或将文件还原到不同的目录，请右键单击该文件，然后单击“还原为/还原至”。

   要从特定备份会话还原文件，请右键单击该文件，然后单击“还原版本”。
4. 在“目标”选项卡中，选择要还原到的客户机 (“目标客户机”)。默认情况下，这是应用程序系统。

   有关各选项的详细信息，请按 **F1**。
5. 在“选项”页面中，设置还原选项。有关信息，请按 **F1**。
6. 在“设备”页中，选择要用于还原的设备。
7. 单击**还原**。
8. 在“启动还原会话”对话框中，单击“下一步”。
9. 指定“报告级别”和“网络负载”。

   注意: 选择“显示统计信息”可查看会话输出中的还原配置文件消息。
10. 单击**完成**启动还原。

会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

使用 Data Protector CLI 进行还原

请执行以下命令：

```
omnir -sap Client:Set -session SessionID -tree FileName
```

其中， FileName 是要还原的 SAP R/3 文件的路径名。

*Windows 系统：*以 UNIX 格式指定路径名 (使用斜杠分隔驱动器号、目录和文件名。驱动器号前面必须带有一个斜杠)。

示例 (Windows)

要将 SAP R/3 文件 btabd_1.dat 从备份会话 2011/01/23-1 还原到 Windows 系统 computer1.company.com 上的原始位置 C:\oracle\ABA\sapdata1\btabd_1 ，请执行:

```
omnir -sap computer1.company.com:ABA.0 -session 2011/01/23-1 -tree /C:/oracle/ABA/sapdata1/btabd_1/btabd_1.dat
```

示例 (UNIX)

要将 SAP R/3 文件 btabd_1.dat 从备份会话 2011/01/23-1 还原到 UNIX 系统 computer2.company.com 上的原始位置 /app/oracle/ABA/sapdata1/btabd_1 ，请执行:

omnir -sap computer2.company.com:ABA.0 -session 2011/01/23-1 -tree /app/oracle/ABA/sapdata1/btabd_1/btabd_1.dat

提示: 要获取已备份的 SAP R/3 对象列表，请执行:

omnidb -sap

要获取特定对象的详细信息 (包括 SessionID)，请执行:

omnidb -sap object_name

使用 SAP 命令进行还原

您可以使用 SAP BRRESTORE 命令启动 SAP R/3 数据库还原。该命令使用 Data Protector backint 接口来还原使用 Data Protector 备份的文件。

1. 以 Oracle OS 用户身份登录 SAP R/3 客户机。
2. 确保有足够的磁盘空间。BRRESTORE 需要额外的磁盘空间来还原控制文件和存档的重做日志文件。
3. 通过设置 OB2APPNAME 环境变量指定要还原的 Oracle 数据库:

   Windows 系统： set OB2APPNAME=ORACLE_SID

   UNIX 系统： export OB2APPNAME=ORACLE_SID

   注意: 如果同一个 ORACLE_SID 名称对应着多个数据库，请同时指定客户机:

   Windows 系统： set OB2HOSTNAME=client_name

   UNIX 系统： export OB2HOSTNAME=client_name
4. 如果计划在 RMAN 模式下执行还原，请确保 initSAP_instance.sap 文件中的 SBT_LIBRARY 参数指向正确的特定于平台的 Data Protector MML。
5. 执行 SAP 还原命令。

使用其他设备进行还原

您可以使用与备份不同的设备执行还原。

使用 **Data Protector GUI**

有关如何使用 Data Protector GUI 为还原选择其他设备的信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

使用 **Data Protector CLI** 或 **SAP** 命令

如果要使用 Data Protector CLI 或 SAP R/3 命令进行还原，请在文件中指定新设备:

Windows 系统： Data_Protector_program_data\Config\Server\cell\restoredev

UNIX 系统： /etc/opt/omni/server/cell/restoredev

使用以下格式:

" DEV 1 " " DEV 2 "

其中， DEV 1 是原始设备，而 DEV 2 是新设备。

重要说明: 使用后删除此文件。

在 Windows 系统上，请为该文件使用 Unicode 格式。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

有关如何监视会话，请参阅《Data Protector 帮助》索引：“查看当前正在运行的会话”。

备份期间生成的系统消息将发送到 SAP R/3 和 Data Protector 监视器。但是，装载请求仅发送到 Data Protector 监视器。

SAP R/3 ZDB 集成

本主题介绍如何配置和使用 Data Protector SAP R/3 ZDB 集成 (SAP R/3 ZDB 集成。它说明了备份和还原 SAP R/3 数据库环境的以下文件 (**SAP R/3 对象**) 时需要了解的概念和方法:

- 数据文件
- 控制文件
- 联机重做日志
- 脱机 (存档) 重做日志
- SAP R/3 日志和参数文件

Data Protector 支持脱机和联机备份。联机备份期间，仍可主动使用 SAP R/3 应用程序。

Data Protector 提供以下类型的交互式备份和安排的备份:

- ZDB 到磁盘
- ZDB 到磁带
- ZDB 到磁盘 + 磁带

Data Protector 仅支持文件系统还原。您可以将 SAP R/3 文件:

- 还原到原始位置
- 还原到另一个客户机
- 到其他目录

下表显示了可用的还原方法，具体取决于从中执行还原的 ZDB 会话。

备份和还原会话

ZDB 类型	还原方法
ZDB 到磁带	标准还原
ZDB 到磁盘	即时恢复
ZDB 到磁盘 + 磁带	标准还原、即时恢复

即时恢复完成后，可以使用 SAP BRTOOLS 界面将数据库还原到特定时间点。

支持的磁盘阵列和阵列配置

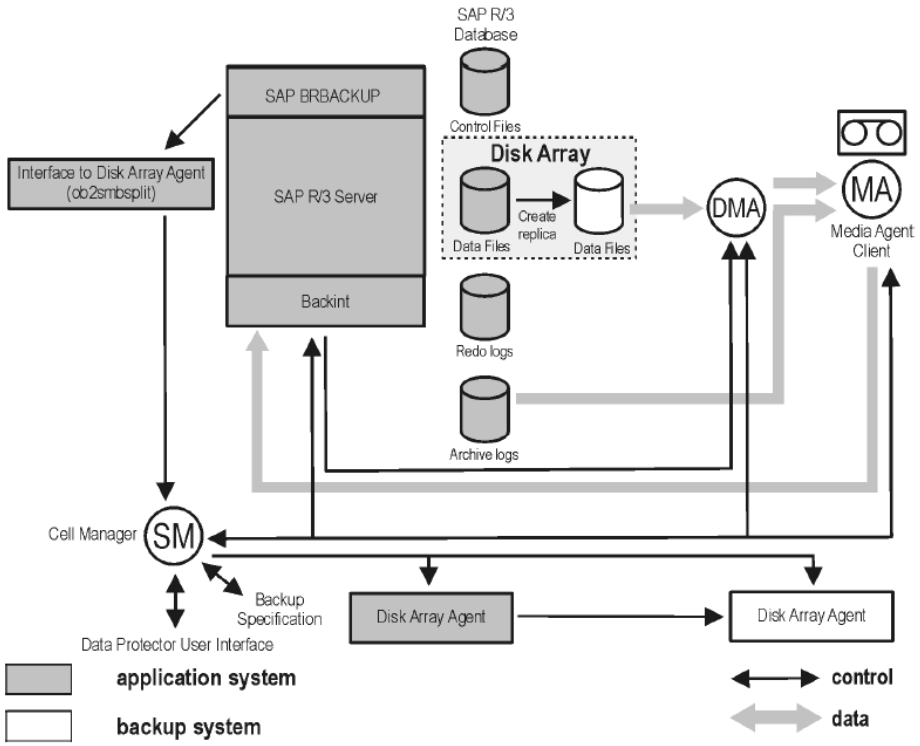
支持的阵列	支持的配置
P9000 XP 磁盘阵列系列 (P9000 XP 阵列)	BC P9000 XP、CA P9000 XP、组合 CA+BC P9000 XP
存储阵列 (NetApp Storage)	本地复制

本主题专门介绍与 Data Protector SAP R/3 ZDB 集成有关的信息。有关 Data Protector 的常规过程和选项，请参阅《Data Protector 帮助》。有关 ZDB 术语、ZDB 类型、脱机和联机备份的优势以及即时恢复概念的详细信息，请参阅《Data Protector 概念指南》。

集成概念

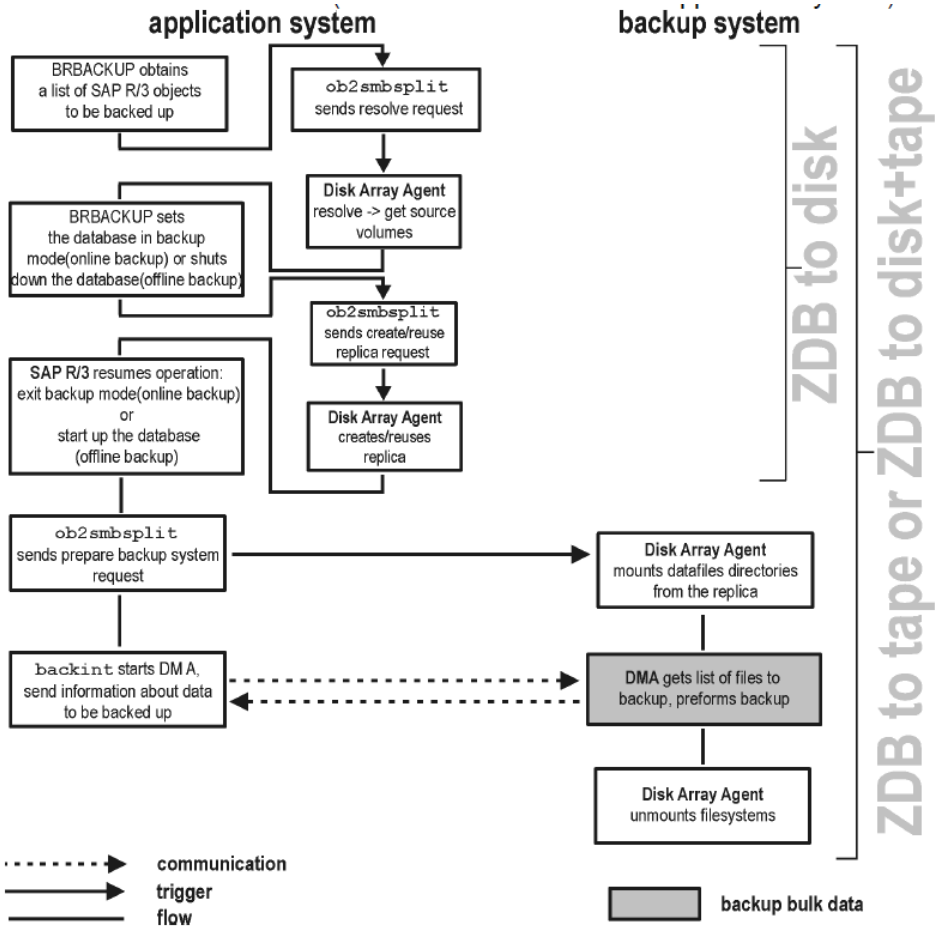
下面的 SAP R/3 集成体系结构显示了 Data Protector SAP R/3 ZDB 集成的体系结构。该图说明了首选配置，其中 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 驻留在与 Oracle 数据文件不同的卷组中。

SAP R/3 集成体系结构



ZDB 流

SAP R/3 ZDB 会话流 (在应用程序系统上启动 BRBACKUP)。



1. 读取 SAP R/3 备份规范并在应用程序系统上启动 Data Protector omnisap.exe 程序。
2. omnisap.exe 准备排除列表 (Oracle 控制文件和联机重做日志文件)
3. omnisap.exe 启动 BRBACKUP (它将数据库切换到备份模式 (联机备份) 或关闭数据库 (脱机备份))，并在应用程序系统上启动 split 命令

(仅含将要包含在复本创建中的文件列表)。
创建复本后，数据库退出备份模式 (联机备份) 或重新启动 (脱机备份) 。

> 注意: Data Protector 可以使用 splitint 接口 (如果 BRTOOLS 支持) 来减少数据库处于备份模式的时间。

4. Data Protector ob2smbsplit 命令解析备份配置，创建复本，并准备复本进行备份。
   备份对象的装载点是在备份系统上创建的。
   备份卷/磁盘组被激活，文件系统装载在备份系统上。
5. **ZDB** 到磁盘: 处理剩余的 ZDB 选项，并将会话的详细信息写入 ZDB 数据库。会话完成。
6. ZDB 到磁带、ZDB 到磁盘 + 磁带: BRBACKUP 启动 Data Protector backint 程序，该程序开始在备份系统上的 Data Protector 数据移动代理 (DMA) 和常规介质代理 (MA) 之间建立连接。该过程由 Data Protector 备份会话管理器 (BSM) 协调。建立连接后，指定用于备份的数据将流式传输到磁带。

> 注意: 您可以将 SAP 配置为使用第三方 backint 工具来执行 ZDB 到磁盘和磁带的备份会话。要启用此功能，请将 OB2_3RD_PARTY_BACKINT 环境变量设置为 1 并将要使用的 backint 复制到 SAP BRTOOLS 目录。如果是 ZDB 到磁盘和磁带的备份会话，则会在 Data Protector IDB 中创建一个 disk_only 备份对象。第三方 backint 在 split 之后启动，负责备份需要的文件。

7. 数据传输完成后，将禁用备份系统 (卸除所有平台的文件系统并停用 UNIX 系统的卷/磁盘组)。
8. EMC 和 P9000 XP 阵列: 重新建立链接，具体取决于指定 ZDB 选项的方式。

手动均衡

手动均衡意味着手动将文件分为若干子集，然后并行备份这些子集。要将文件分为若干子集，请将 manual_balance 部分添加到 Data Protector SAP R/3 配置文件，如以下示例所述。

示例

假设有一个名为 SAP-R3 的备份规范，并且需要备份以下文件: fileA 、 fileB 、 fileC 、 fileD 。要将这些文件分为三个子集 (0={fileA, fileC} 、 1={fileB} 、 2={fileD})，请将以下几行添加到 Data Protector SAP R/3 配置文件:

```
manual_balance={ SAP-R3={ fileA=0; fileB=1; fileC=0;fileD=2;}}
```

将文件分成若干子集时，请考虑以下事项:

- 一次只能使用同一硬盘中的一个文件。
- 子集中的文件数必须等于小于为备份指定的所有设备的并发数之和。
- 如果备份规范包含并未分配给任何子集的文件，Data Protector 会基于负载均衡原则，自动将这些文件添加到要备份的文件列表中。在备份之前，此列表已记录到:

  Windows 系统: SAPDATA_HOME\sapbackup*.lst

  UNIX 系统: ORACLE_HOME/sapbackup/.*.lst

本地化 SAP R/3 对象

Oracle Server 使用自有的编码，这可能与文件系统使用的编码不同。在备份上下文中，Data Protector 会显示 Oracle 数据库的逻辑结构 (使用 Oracle 名称)；在还原上下文中，则显示 Oracle 数据库的文件系统结构。因此，要正确显示非 ASCII 字符，请确保 Data Protector 编码在备份期间与 Oracle Server 编码匹配，在还原期间与文件系统编码匹配。但是，显示不正确并不会影响还原。

Windows 系统: 如果 DBCS 的当前值与非 Unicode 程序的默认 Windows 字符集不匹配，则会出现问题。请参阅 SAP R/3 故障诊断

UNIX 系统: 为了能够在不同的 Data Protector 编码之间切换，请在 UTF-8 语言环境下启动 GUI。

如果要使用 Data Protector CLI 还原文件，而且已备份对象的名称包含当前语言组 (Windows) 或代码页 (UNIX) 无法正确显示的字符:

1. 将环境变量 OB2_CLI_UTF8 设置为 1 。
2. *Windows 系统:* 将终端使用的编码设置为 UTF-8。

否则，某些命令的输出无法正确显示 (例如 omnidb 返回的备份对象)，并且不能用作其他命令的输入 (例如 omnir)。

稀疏文件

您可以通过设置 sparse 选项来提高稀疏文件还原的性能。通过以下任意一种方式设置该选项:

- 使用 Data Protector GUI: 在“选项”页面中选择“还原稀疏文件”选项。
- 使用 Data Protector CLI: 执行 omnir 命令时，添加 -sparse 选项。
- 使用 SAP 命令: 执行 BRRESTORE 命令之前，设置 Data Protector OB2SPARSE 变量:

  Windows 系统: set OB2SPARSE=sparse

  UNIX 系统: export OB2SPARSE=sparse

灾难恢复

有关一般信息，请参阅灾难恢复。

还原控制文件

控制文件包含有关数据库结构的所有信息。如果控制文件丢失，请在还原数据库的任何其他部分之前先还原控制文件:

1. 使用标准 Data Protector 还原过程还原控制文件。

   控制文件 (ctrlORACLE_SID.dbf) 将还原到 SAPBACKUP 变量定义的目录中。如果未设置该变量，控制文件将还原到默认的 Data Protector 临时文件目录。

2. 执行:

   ```
   run { allocate channnel 'dev0' type disk; replicate controlfile from 'TMP_FILENAME'; release channel 'dev0'; }
   ```

   其中 TMP_FILENAME 是将控制文件还原到的文件夹。

满足 SAP R/3 集成的先决条件

以下是 SAP R/3 集成的先决条件:

- 确保已正确安装和配置 SAP R/3 应用程序。SAP R/3 应用程序使用的数据库必须是 Oracle 数据库。如果使用任何其他数据库，可以使用相应的 Data Protector 集成 (例如 Informix) 进行备份。假设您熟悉 SAP R/3 应用程序和 Oracle 数据库管理。
  - 有关安装、配置和使用 SAP R/3 应用程序以及 SAP 备份和还原工具 (BRBACKUP、BRRESTORE 和 BRARCHIVE) 的信息，请参阅 SAP R/3 应用程序文档。
- 确保拥有使用 Data Protector SAP R/3 ZDB 集成的许可证。有关信息，请参阅《Data Protector 安装指南》。
- 确保已正确安装 Data Protector。
  - 有关如何在各种体系结构中安装 Data Protector SAP R/3 集成磁盘阵列 (P9000 XP 阵列、EMC 或非 HPE 存储阵列) 与 SAP R/3 集成的信息，请参阅“Data Protector 安装”一节。
  - 有关如何配置 Data Protector ZDB 集成 (EMC、P9000 XP 阵列或 NetApp Storage) 的信息，请参阅《Data Protector 零宕机时间备份管理员指南》。
  - 有关 SG 群集中 Data Protector Cell Manager 包配置的信息，请参阅《Data Protector 帮助》索引: “Serviceguard 集成”。

  要对其执行备份或还原的每个 SAP R/3 应用程序系统都必须安装 Data Protector“SAP R/3 集成”组件。

  注意: 无法在 RMAN 模式下运行 ZDB 会话。
- SAP R/3 目录 SAPBACKUP 、 SAPARCH 、 SAPREORG 、 SAPCHECK 和 SAPTRACE 不得与数据文件驻留在相同的磁盘阵列源卷上。否则，在即时恢复期间将覆盖完整恢复数据库所需的 BRTOOLS 数据。您可以在 initDBSID.sap 文件中设置这些目录的位置。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 SAP R/3 系统和 Cell Manager 是否正常通信，请配置并运行一次 Data Protector 文件系统备份和还原。
- Windows 系统:

  在支持的 Windows 操作系统上，为具有运行备份和还原所需的 SAP R/3 权限的用户配置 Data Protector Inet 服务用户模拟。

  有关详细信息，请参阅 Data Protector 帮助索引: “Inet 用户模拟”。

  如果在同一系统上运行多个 SAP R/3 实例，并为每个实例配置了不同的 SAP 管理员帐户，请创建一个额外的通用 SAP 管理员帐户。配置 Data Protector Inet 服务以将此帐户用作服务启动帐户。
- 开始备份前，请确保 SAP R/3 数据库处于“打开”或“关闭”模式。
- 开始备份前，请确保将 SAP R/3 参数文件中的 primary_db 参数设置为 LOCAL 。有关设置 SAP R/3 参数文件的详细信息，请参阅配置集成。
- 在应用程序系统上使用相同源卷的 ZDB、还原和即时恢复会话无法同时运行。
- 如果另一个会话正在备份存档日志，则无法启动 ZDB 到磁盘会话，即使 Oracle 数据文件和存档日志驻留在不同的源卷上也是如此。
- *P9000 XP 阵列:* 如果使用 LVM 镜像配置，Data Protector 会在备份期间显示警告，因为应用程序系统上的卷组源卷并未分配到相应的 BC 对。该消息可忽略。
- *ZDB 到磁盘:* 无法备份存档日志。要备份存档日志，请创建非 ZDB (标准) SAP R/3 备份规范。有关详细信息，请参阅《Data Protector

集成指南》。
- 备份同一个 Oracle 实例的多个备份会话无法同时运行。
- 仅当使用模板时支持可配置的备份模式。
- 默认情况下，Data Protector 支持除 -a 和 -b 以外的所有 BRTOOL 选项。要启用对 -a 和 -b 的支持，请将 OB2BRTNOSECU omnirc 选项设置为 1。有关如何设置 omnirc 选项的信息，请参阅《Data Protector 帮助》索引: “omnirc 选项”。
- 一般来说，还原操作的耗时比备份更长。如果文件是使用许多个流备份的，还原操作的耗时还会显著延长。请注意，如果在 Oracle RMAN 脚本选项 FILESPERSET 设为 1 的情况下在 RMAN 模式下启动备份，RMAN 会为每个数据库文件创建单独的备份流 (对象)。

- Oracle RMAN 创建的备份只能使用 SAP 还原实用程序还原。
- 原始分区上的 SAP R/3 表空间无法使用 Data Protector GUI 还原。变通方法: 使用 SAP 还原命令 (例如 brrestore)。
- 如果要还原稀疏文件，可以通过设置稀疏选项来提高性能。请参见稀疏文件。
- 如果 Oracle 数据库已本地化，则可能需要在开始还原前设置适当的 Data Protector 编码。有关详细信息，请参阅本地化 SAP R/3 对象。
- 不支持还原预览。

- 数据库恢复操作在即时恢复过程完成后执行。数据库恢复期间，SAP BR*Tools 实用程序会从磁带还原在 ZDB 之后执行的存档日志备份。如果选中，则重置日志并打开数据库。
- 如果要用于即时恢复的复本包含控制文件，请首先参阅 SAP R/3 ZDB 集成。

群集感知客户机

- 仅在一个群集节点上配置 SAP R/3 数据库，因为配置文件驻留在 Cell Manager 上。

  Windows 系统: 配置期间，Data Protector 会将 Data Protector backint 和 ob2smbsplit.exe 程序 (BRTOOLS 支持 splitint 时仅复制后者) 从 Data_Protector_home\bin 复制到存储着 SAP 备份工具的目录，而且会将 ob2smbsplit.exe 重命名为 splitint.exe。此操作仅在当前活动节点上执行。在其他节点上须手动执行此操作。

  UNIX 系统: 配置期间，Data Protector 会创建链接，指向当前活动节点上的 Data Protector backint 和 splitint 程序。在所有其他节点上，请手动执行此操作。执行:

  ln -s /opt/omni/lbin/backint \ /usr/sap/ORACLE_SID/sys/exe/run

  如果 BRTOOLS 支持 splitint ，还要执行:

  ln -s /opt/omni/lbin/ob2smbsplit \ /usr/sap/ORACLE_SID/sys/exe/run/splitint

- 如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称，如下所示:

  Windows 系统: set OB2BARHOSTNAME=virtual_server_name

  UNIX 系统: export OB2BARHOSTNAME=virtual_server_name

以下限制适用:

- 如果在 Windows 系统上的 ZDB 环境中使用“ZDB 到磁带”备份表空间，且 ZDB_ORA_INCLUDE_CF_OLF

omnirc 选项未设置为 1，则当要备份的镜像磁盘或快照中没有控制文件时，备份将失败。

- 在备份系统上使用 Data Protector GUI 进行的 SAP R/3 数据拆分镜像还原是作为常规文件系统还原执行的，在此期间 ZDB 代理 (SYMA、SSEA) 将把磁盘安装到 /var/opt/omni/tmp (默认装载点) 上。由于这是应用程序数据的还原，VRDA 将把文件还原到原始装载点。因此，数据未还原到 P9000 XP 阵列磁盘上，而是还原到根分区。

Data Protector SAP R/3 配置文件

Data Protector 在 Cell Manager 上的以下文件中存储每个已配置的 SAP R/3 数据库的集成参数:

Windows 系统: Data_Protector_program_data\Config\Server\Integ\Config\Sap\ClientName%ORACLE_SID

UNIX 系统: /etc/opt/omni/server/integ/config/SAP/ClientName%ORACLE_SID

存储的参数包括:

- Oracle 主目录
- 连接到目标数据库的已编码连接字符串
- BRTOOLS 主目录
- 启动备份前需要导出的变量
- SAPDATA 主目录
- 用户名和用户组
- 用于控制文件或重做日志副本的临时目录
- 将复制到安全位置的控制文件和重做日志列表
- 每个备份规范的并发数和均衡，以及 RMAN 备份的通道数
- 速度参数 (备份特定文件所需的时间 - 以秒为单位)
- 手动均衡参数

这些配置参数会写入到 Data Protector SAP R/3 配置文件:

- 在配置集成期间
- 在创建备份规范期间
- 更改配置参数时

重要说明 为避免备份问题，请特别注意确保配置文件的语法和标点与示例一致。

注意: 您可以通过以下方式引用其他环境变量，从而设置配置文件 Environment 部分 (子列表) 中的参数:
SAPDATA_HOME=${ORACLE_HOME}/data

语法

Data Protector SAP R/3 配置文件的语法如下:

```
ORACLE_HOME='ORACLE_HOME'; ConnStr='ENCODED_CONNECTION_STRING_TO_THE_TARGET_DATABASE'; BR_directory='BRTOOLS_HOME';
SAPDATA_HOME='SAPDATA_HOME'; ORA_NLS_CHARACTERSET='CHARACTER_SET'; OSUSER='USER_NAME'; OSGROUP='USER_GROUP';
Environment={ [ENV_var1='value1';] [ENV_var2='value2'; ...] } SAP_Parameters={backup_spec_name=('-concurrency #_of_concurrency ' | '-
time_balance' | '-load_balance' | '-manual_balance') } speed={ AVERAGE=1; 'filename'=#_of_seconds_needed_to_back_up_this_file; }
compression={'filename'=size_of_the_file_in_bytes_after_the _compression; } manual_balance={backup_specification_name={
'filename'=device_number; } }
```

在 SAP R/3 数据库配置期间，Data Protector 会自动设置 ORA_NLS_CHARACTERSET 参数。有关如何配置 SAP R/3 数据库以与 Data Protector 一起使用的详细信息，请参阅配置 SAP R/3 数据库。

示例

这是该文件的一个示例:

```
ORACLE_HOME='/app/oracle805/product'; ConnStr='EIBBKIBBEIBBFIBBGHBBOHBB
QDBBOFBBCFBBPFBBCFBBIFBBGFBBDGBBBFBBCFBBDFBBCFBB'; BR_directory='/usr/sap/ABA/SYS/exe/run'; SAPDATA_HOME='/sap';
ORA_NLS_CHARACTERSET='USASCII7'; OSUSER='orasid'; OSGROUP='dba'; Environment={ } SAP_Parameters={ sap_weekly_offline=('-
concurrency 1','-no_balance'); sap_daily_online=('-concurrency 3','-load_balance'); sap_daily_manual=('-concurrency 3','-manual_balance'); }
speed={ AVERAGE=203971; '/file1'=138186; '/file2'=269756; } compression={ '/file1'=1234; '/file2'=5678; } manual_balance={
sap_daily_manual={ '/file1'=1; /* file 1 is backed up by the first sapback */ '/file2'=2; /* file 2 is backed up by the second sapback */ '/file3'=1; /*
file 3 is backed up by the first sapback */ '/file4'=1; } }
```

使用 CLI 设置、检索、列出和删除 Data Protector SAP R/3 配置文件参数

Data Protector SAP R/3 配置文件参数通常在以下情况后写入到 Data Protector SAP R/3 配置文件:

- Data Protector 配置完 SAP R/3 运行的 Oracle 实例。
- 创建了新的备份规范。
- 完成了使用按时间均衡算法的备份。

util_cmd 命令

您可以在 Data Protector SAP R/3 客户机上，使用 util_cmd -putopt (设置参数)、 util_cmd -getopt (检索参数) 或 util_cmd -getconf (列出所有参数) 命令来设置、检索、列出或删除 Data Protector SAP R/3 配置文件参数。

必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。

设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

群集感知客户机

在群集环境中，必须先将环境变量 OB2BARHOSTNAME 定义为虚拟主机名，然后才能 (在客户机上) 从命令行执行 util_cmd 命令。 OB2BARHOSTNAME 变量设置如下:

Windows 系统: set OB2BARHOSTNAME=virtual_hostname

UNIX 系统: export OB2BARHOSTNAME=virtual_hostname

util_cmd 概要

util_cmd 命令的语法如下:

util_cmd -getconf[ig] SAP oracle_instance [-local filename]

util_cmd -getopt[ion] [SAP oracle_instance] option_name [-sub[list] sublist_name] [-local filename]

util_cmd -putopt[ion] [SAP oracle_instance] option_name [option_value] [-sub[list] sublist_name] [-local filename]

其中:

option_name 是参数的名称

option_value 是参数的值

[-sub[list] sublist_name] 指定配置文件中用来写入或读取参数的子列表。

[-local filename] 指定以下内容之一:

- 将它与 -getconf[ig] 选项一起使用时，它会指定命令输出要写入到的文件名。如果未指定 -local 选项，则输出将写入标准输出。
- 将它与 -getopt[ion] 一起使用时，它会指定要从中获取参数及参数值的文件的文件名，随后读取的参数及参数值将写入到标准输出。如果未指定 -local 选项，则从 Data Protector SAP R/3 配置文件中获取参数及参数值，然后将它们写入标准输出。
- 将它与 -putopt[ion] 选项一起使用时，它会指定命令输出要写入到的文件名。如果未指定 -local 选项，则输出将写入 Data Protector SAP R/3 配置文件。

> 注意: 如果要将 option_value 参数设置为数字，则必须将该数字放在单引号中，并用双引号括起来。

返回值

util_cmd 命令在每次操作后显示一条短状态消息 (将其写入标准错误):

- Configuration read/write operation successful.

  成功完成所有请求的操作后，将显示此消息。

- Configuration option/file not found.

  如果配置中不存在具有指定名称的选项，或者指定为 -local 参数的文件不存在，则会显示此消息。

- Configuration read/write operation failed.

  如果发生任何致命错误，则会显示此消息；例如 Cell Manager 不可用、Cell Manager 上缺少 Data Protector SAP R/3 配置文件，等等。

设置参数

要为 SAP R/3 运行的 Oracle 实例 ICE 设置 Data Protector OB2OPTS 和 Oracle BR_TRACE 参数，请在 Data Protector SAP R/3 客户机上使用以下命令:

Windows、HP-UX、Solaris 和 Linux 系统

util_cmd -putopt SAP ICE OB2OPTS '-debug 1-200 debug.txt' -sublist Environment

util_cmd -putopt SAP ICE BR_TRACE "'10'" -sublist Environment

检索参数

要检索 Oracle 实例 ICE 的 OB2OPTS 参数的值，请在 Data Protector SAP R/3 客户机上使用以下命令:

util_cmd -getopt SAP ICE OB2OPTS -sublist Environment

列出参数

要列出 Oracle 实例 ICE 的所有 Data Protector SAP R/3 配置文件参数，请在 Data Protector SAP R/3 客户机上使用以下命令:

util_cmd -getconf SAP ICE

删除参数

要删除 Oracle 实例 ICE 的 OB2OPTS 参数的值，请在 Data Protector SAP R/3 客户机上使用以下命令:

util_cmd -putopt SAP ICE OB2OPTS "" -sublist Environment

安装 SAP R/3 ZDB 客户机

P9000 XP 与 SAP R/3 的集成

完成以下步骤：

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：
   - P9000 XP Agent
   - SAP R/3 Integration
   - Disk Agent

注意: 只有计划运行 SAP 兼容 ZDB 会话 (在该会话中，BRBACKUP 在备份系统上启动) 时，才需要在备份系统上安装 SAP R/3 Integration。
在 Windows 系统上，必须使用 SAP R/3 管理员用户帐户安装 Data Protector 软件组件，并且该帐户必须包含在运行 SAP R/3 实例的系统的 ORA_DBA 或 ORA_SID_DBA 本地组中。

与 SAP R/3 的存储阵列集成

完成以下步骤：

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：
   - 存储阵列的存储提供程序 (NetApp Storage Provider)
   - SAP R/3 Integration
   - Disk Agent

以下限制适用：

- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

注意

- 只有计划运行 SAP 兼容 ZDB 会话（在该会话中，BRBACKUP 在备份系统上启动）时，才需要在备份系统上安装 SAP R/3 Integration。
- 在 Windows 系统上，必须使用 SAP R/3 管理员用户帐户安装 Data Protector 软件组件，并且该帐户必须包含在运行 SAP R/3 实例的系统的 ORA_DBA 或 ORA_SID_DBA 本地组中。

配置 SAP R/3 ZDB 集成

要配置 SAP R/3 集成，请完成以下步骤:

1. 配置所需的用户帐户。请参阅配置用户帐户。
2. 配置 SQL*Net V2 或 Net8 TNS 侦听程序。请参阅配置 SQL*Net V2 或 Net8 TNS 侦听程序。
3. 检查从应用程序系统到 Oracle 数据库的连接。请参阅检查连接。
4. 启用身份验证密码文件。请参阅身份验证密码文件。
5. (可选) 设置存档日志记录模式以启用联机备份。请参阅启用存档日志记录。
6. 共享应用程序系统上的目录。请参阅共享应用程序系统上的目录。
7. 配置要对其执行备份或还原的每个 SAP R/3 数据库。请参阅配置 SAP R/3 数据库。
8. 配置 SAP R/3 参数文件。请参阅配置集成。

群集感知客户机

- 仅在一个群集节点上配置 SAP R/3 数据库，因为配置文件驻留在 Cell Manager 上。
  ***Windows** 系统*:
  配置期间，Data Protector 会将 Data Protector backint 和 ob2smbsplit.exe 程序 (BRTOOLS 支持 splitint 时仅复制后者) 从 Data_Protector_home\bin 复制到存储着 SAP 备份工具的目录，而且会将 ob2smbsplit.exe 重命名为 splitint.exe 。此操作仅在当前活动节点上执行。在其他节点上须手动执行此操作。
  ***UNIX** 系统*:
  配置期间，Data Protector 会创建链接，指向当前活动节点上的 Data Protector backint 和 splitint 程序。在所有其他节点上，请手动执行此操作。执行:
  ln -s /opt/omni/lbin/backint \ /usr/sap/ORACLE_SID/sys/exe/run
  如果 BRTOOLS 支持 splitint ，还要执行:
  ln -s /opt/omni/lbin/ob2smbsplit \ /usr/sap/ORACLE_SID/sys/exe/run/splitint
- 如果要使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称，如下所示:
  ***Windows** 系统*: set OB2BARHOSTNAME=virtual_server_name
  ***UNIX** 系统*: export OB2BARHOSTNAME=virtual_server_name

SAP 建议在所有群集节点上安装 SAP 备份实用程序。

配置用户帐户

要启用对 SAP R/3 数据库文件的备份和还原，您需要配置或创建多个用户帐户。

Oracle 操作系统用户帐户	添加到以下用户组的操作系统用户帐户: ***Windows** 系统:* ORA_DBA 和 ORA_SID_DBA 本地组 ***UNIX** 系统:* dba 和 sapsys 例如用户 oraSID 。 ***UNIX** 系统:* 确保此用户是文件系统的所有者或安装了数据库的原始逻辑卷的所有者。最低权限应为 740。
用户帐户 root (仅限 UNIX 系统)	添加到 dba 用户组的默认操作系统管理员的用户帐户。
Oracle 数据库用户帐户	至少被授予以下 Oracle 角色的数据库用户帐户: • sysdba • sysoper 例如用户 system 。 不要将 Oracle SYS 用户配置为用于备份 SAP R/3 对象。使用 SYS 用户帐户进行备份时，SAP 备份将失败并显示错误 ORA-28009: connection as SYS should be as SYSDBA or SYSOPER.

将以下用户帐户添加到 Data Protector admin 或 operator 用户组:

- Oracle 操作系统用户帐户

  (如果使用备份集方法，请同时在应用程序和备份系统上添加此用户)
- ***UNIX** 系统:* 用户帐户 root (应用程序系统和备份系统)

在群集环境中，请将这些用户帐户添加到以下客户机的 Data Protector admin 或 operator 用户组:

- 虚拟服务器

- 群集中的每个节点

有关添加 Data Protector 用户的信息，请参阅《Data Protector 帮助》索引：“添加用户”。

配置 SQL*Net V2 或 Net8 TNS 侦听程序

1. 确保已按以下示例所示配置了应用程序系统上的 listener.ora 和 tnsnames.ora 文件。这些文件位于:

   ***UNIX** 系统:* ORACLE_HOME/network/admin

   ***Windows** 系统:* ORACLE_HOME\network\admin

   示例

   Oracle 实例: PRO

   应用程序系统: alpha.hp.com

listener.ora	LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = alpha.hp.com) (PORT = 1522)))) SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (GLOBAL_DBNAME = PRO) (SID_NAME = PRO) (ORACLE_HOME = /app/oracle815/product)))
tnsnames.ora	PRO = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = alpha.hp.com) (PORT = 1522))) (CONNECT_DATA = (SERVICE_NAME = PRO)))

2. 通过在 Oracle Server 系统上执行以下命令来启动 SQL*Net V2 或 Net8 TNS 侦听程序:

   UNIX 系统: ORACLE_HOME/bin/lsnrctl start

   Windows 系统: ORACLE_HOME\bin\lsnrctl start

检查连接

要检查从应用程序系统到 Oracle 实例的连接，请执行以下操作:

1. 以 Oracle OS 用户身份登录应用程序系统 SAP R/3 客户机。
2. 导出/设置 ORACLE_HOME 和 ORACLE_SID 变量。
3. 启动 sqlplus 。
4. 以 Oracle 数据库用户身份 (首先使用 sysdba 角色，然后使用 sysoper 角色) 连接到 Oracle 目标数据库。

示例

对于以下配置:

Oracle 实例: PRO ORACLE_HOME： /app/oracle816/product

执行:

```
id uid=102(oraprod) gid=101(dba) export ORACLE_SID=PRO export ORACLE_HOME=/app/oracle816/product export SHLIB_PATH=/app/oracle816/product/lib:/opt/omni/lbin sqlplus /nolog SQLPLUS> connect system/manager@PRO as sysdba; 已连接。 SQLPLUS> connect system/manager@PRO as sysoper; 已连接。
```

身份验证密码文件

为数据库管理员启用身份验证密码文件:

1. 关闭应用程序系统上的 Oracle 目标数据库。
2. 在 init ORACLE_SID .ora 文件中，指定:

   remote_login_passwordfile = exclusive

有关如何设置密码文件的说明，请参阅 Oracle 文档。

启用存档日志记录

将数据库设置为存档日志记录模式时，可以防止未保存的联机重做日志被覆盖。缺少相关的重做日志时，数据文件的联机备份毫无用处，因为这时无法将数据库恢复到一致状态。

> 提示: 在 BRBACKUP 完成后立即存档联机备份期间生成的重做日志文件。
> 要保护存档目录不会溢出，请定期清除该目录。

要启用存档日志记录，请执行以下操作:

1. 在 init ORACLE_SID. ora 文件中，设置

   log_archive_start = true

   并指定 log_archive_dest 选项。

   示例

   这是 Oracle 实例 PRO 的 initORACLE_SID.ora 文件的示例:

   ```
   # @(#)initSID.ora 20.4.6.1 SAP 13/03/30 ############################################################ # (c)Copyright SAP AG, Walldorf ############################################################ .。。。 。。。。。。 。。。。 。。。。。。。。 。。。。。。。。 ### ORACLE Authentication Password File remote_login_passwordfile = exclusive ### ORACLE archiving log_archive_dest = /oracle/PRO/saparch/PROarch log_archive_start = true .。。。
   ```

2. 装载 Oracle 数据库并使用 Oracle Server Manager 启动存档日志记录模式。执行:

   ```
   startup mount alter database archivelog; archive log start; alter database open;
   ```

   示例

   对于 Oracle 实例 PRO ，执行:

   Windows 系统: set ORACLE_SID=PRO

   UNIX 系统: export ORACLE_SID=PRO

   任何操作系统:

   ```
   sqlplus /nolog SQLPLUS> connect user/passwd@PRO; 已连接。 SQLPLUS> startup mount ORACLE 实例已启动。 总体系统全局区域 6060224 字节 固定大小 47296 字节 可变大小 4292608 字节 数据库缓冲区 1638400 字节 重做缓冲区 81920 字节 数据库已装载。 SQLPLUS> alter database archivelog; 语句已处理。 SQLPLUS> archive log start; 语句已处理。 SQLPLUS> alter database open;
   ```

共享应用程序系统上的目录

应用程序系统上的以下目录必须可以访问:

- sapbackup
- sapreorg
- Oracle 主目录
- BR*Tools 主目录

> 注意 仅当要运行符合 SAP 标准的 ZDB 会话时，sapreorg 和 BR*Tools 主目录才必须可以访问 (BRBACKUP 在备份系统上启动，而不是在应用程序系统上启动)。

UNIX 应用程序系统

1. 使用 root 权限并通过 NFS 共享应用程序系统上的目录。

   例如，假设应用程序系统上的 sapbackup 目录指向 /oracle/SID/sapbackup ，而备份系统是 backup.company.com 。要共享 sapbackup 目录，请执行以下操作:

   ***HP-UX 系统*:** 在应用程序系统上的文件 /etc/exports 中，添加以下行:

   /oracle/SID/sapbackup -root=backup.company.com

   Solaris *系统:* 在应用程序系统上的文件 /etc/dfs/dfstab 中，添加以下行:

   share -F nfs -o root=backup.company.com /oracle/SID/sapbackup

2. 在备份系统上装载目录。确保应用程序和备份系统上具有相同的目录结构。

例如，假设您有一个 HP-UX 应用程序系统 app.company.com 。要在备份系统上装载 /oracle/SID/sapbackup 目录，请将下面一行添加到备份系统上的 /etc/fstab 文件:

```
app.company.com:/oracle/SID/sapbackup /oracle/SID/sapbackup nfs defaults 0 0
```

Windows 应用程序系统

- 在应用程序系统上，找到 sapbackup 和 sapreorg 目录的位置。如果它们位于 SAP 数据主目录内，请共享此目录并以所需的名称命名它。然后，在备份系统上，创建 HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ ORACLE_SID\Environment\SAPDATA_HOME Windows 注册表项，指定从备份系统中看到的 SAP 数据主目录路径。

  例如，假设您的应用程序系统是 mycomputer.company.com ，SAP 数据主目录是 K:\oracle\my_instance ，而且您使用名称 my_SAPinstance 共享它。那么，备份系统上的 SAPDATA_HOME Windows 注册表项必须具有值 \\mycomputer.company.com\my_SAPinstance 。

  如果 sapbackup 和 sapreorg 目录不在一起，请分别共享每个目录，并在备份系统上创建单独的 Windows 注册表项 (SAPBACKUP 、 SAPREORG)。

- 在应用程序系统上共享 Oracle 主目录，并在备份系统上的 ORACLE_HOME Windows 注册表项中指定其路径，具体方式类似于上面所述。
- 确保可以从备份系统访问应用程序系统上的 BR*Tools 主目录，具体方式如下:

  \\application_system\sapmnt\SAP_SID\SYS\exe\run

> 提示**:** 您也可以设置 Data Protector SAP R/3 集成环境变量 (ORACLE_HOME 、 SAPDATA_HOME 、 SAPBACKUP 、 SAPREORG)，而不是创建注册表项。

选择身份验证模式

Data Protector SAP R/3 ZDB 集成支持通过两种身份验证模式来访问 SAP R/3 使用的 Oracle 数据库:

- 数据库身份验证模式
- 操作系统身份验证模式

使用数据库身份验证模式时，对应的 Oracle 数据库用户帐户每次发生更改时，都需要使用新的 Oracle 登录信息重新配置 SAP R/3 集成使用的 SAP R/3 数据库。如果使用操作系统身份验证模式，则无需执行此类重新配置。

请在配置特定的 SAP R/3 数据库时选择首选身份验证模式。

配置 SAP R/3 数据库

您需要为 Data Protector 提供以下配置参数:

- Oracle Server 主目录
- SAP R/3 数据主目录
- (可选) 如果选择数据库身份验证模式，则为 Oracle 数据库用户帐户。备份期间 BRBACKUP 和 BRARCHIVE 会使用该用户帐户。
- 存储 SAP 备份实用程序的目录

Data Protector 随后在 Cell Manager 上为 SAP R/3 数据库创建配置文件，并验证与数据库的连接。在 UNIX 系统上，Data Protector 还会为 backint 程序创建从存储 SAP 备份实用程序的目录到 /opt/omni/lbin 的软链接。

在 Windows 系统上，Data Protector 会将 backint 程序 (后者仅在 BR*Tools 支持 splitint 时复制) 从 Data_Protector_home\bin 复制到存储 SAP 备份工具的目录，并将 ob2smbsplit.exe 重命名为 splitint.exe.

要配置 SAP R/3 数据库，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP R/3”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择模板。

   从“备份类型”下拉列表中，选择“快照或拆分镜像备份”选项，然后从“子类型”下拉列表中选择适当的磁盘阵列代理。代理必须安装在应用程序系统和备份系统上。

单击**确定**。

4. 在“应用程序系统”中，选择要备份的 SAP R/3 客户机。在群集环境中，选择虚拟服务器。

   在“备份系统”中，选择备份系统。

   指定其他与磁盘阵列有关的备份选项。有关各选项的详细信息，请按 **F1**。

   > 注意 *P9000 XP 阵列:* 要启用即时恢复，请选择“跟踪复本以用于即时恢复”。

5. 在“应用程序数据库”中，键入 Oracle 实例名称 (ORACLE_SID)。

   在 UNIX 和 Windows 客户机上，指定下列“用户和组/域”选项:

   ***Windows** 系统：*在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator 、域 DP)。

   ***UNIX** 系统:* 在“用户名”中，键入配置用户帐户中所述的 Oracle OS 用户。在“组/域名”中，键入 dba 。

   请确保此用户已添加到 Data Protector admin 或 operator 用户组，具有 SAP R/3 备份权限，以及已设置为用于 Data Protector Inet 服务用户模拟。此用户成为备份所有者。

   单击“下一步”。

6. 在“配置 SAP”对话框中，指定 Oracle Server 主目录和 SAP R/3 数据主目录的路径名。如果将这些字段留空，系统会使用默认的 ORACLE_HOME 目录。

   在“目标数据库的 Oracle 登录信息”下，指定以下内容:

   - 对于数据库身份验证模式，请指定“用户名”、“密码”和“服务”。
   - 对于本地操作系统身份验证模式，请将“用户名”、“密码”和“服务”留空。
   - 对于远程操作系统身份验证模式，请仅指定“服务”(将“用户名”和“密码”留空)。

   以下是各选项的说明:

   - **用户名**和**密码**: 指定配置用户帐户中所述的 Oracle 数据库用户帐户的用户名和密码。
   - **服务**: 指定 Oracle 服务名称。

   在“备份和还原可执行文件目录”中，指定 SAP 备份实用程序所在目录的路径名。默认情况下，这些实用程序位于:

   ***Windows** 系统:* \\SAP_system\sapmnt\ORACLE_SID\sys\exe\run

   ***UNIX** 系统:* /usr/sap/ORACLE_SID/SYS/exe/run

   单击**确定**。

7. SAP R/3 数据库已配置。退出 GUI，或按选择要备份的 SAP R/3 对象中所述继续创建备份规范。

使用 Data Protector CLI

1. 使用 Oracle 操作系统用户帐户登录 SAP R/3 系统。
2. 在命令提示符下，将当前目录更改为以下目录:

   ***Windows** 系统:* Data_Protector_home\bin

   ***HP-UX**、**Solaris** 和 **Linux** 系统:* /opt/omni/lbin

3. 执行:

   util_sap.exe -CONFIG ORACLE_SIDORACLE_HOMEtargetdb_connection_stringSAPTOOLS_DIR [SAPDATA_HOME][SQL_PATH]

参数描述

ORACLE_SID	Oracle 实例名称。
ORACLE_HOME	Oracle Server 主目录的路径名。
targetdb_connection_string	此参数值决定用于访问 Oracle 数据库的身份验证模式: • 要选择数据库身份验证模式，请以 .user_name/password@Oracle_service 格式指定目标数据库的登录信息。 • 要选择本地操作系统身份验证模式，请仅指定字符 /。 • 要选择远程操作系统身份验证模式，请以 /@Oracle_service 格式指定目标数据库的登录信息。

SAPTOOLS_DIR	存储 SAP 备份实用程序的目录的路径名。
SAPDATA_HOME	安装 SAP R/3 数据文件的目录的路径名。默认情况下，此选项设置为 ORACLE_HOME 。

消息 *RETVAL*0 表示配置成功。

处理错误

如果收到 *RETVAL*error_number 消息 (其中 error_number 不为零)，则表示发生错误。

要获取错误描述，请执行:

***Windows** 系统:*

Data_Protector_home\bin\omnigetmsg 12 error_number

***HP-UX** 和 **Linux** 系统:*

/opt/omni/lbin/omnigetmsg 12 error_number

> 提示
> 要获取 SAP R/3 应用程序使用的 Oracle 实例列表，请执行:
> util_sap.exe -APP
>
> 要获取 Oracle 实例的表空间列表，请执行:
> util_sap.exe -OBJS0ORACLE_SID
>
> 要获取表空间的数据库文件列表，请执行:
> util_sap.exe -OBJS1ORACLE_SID TABLESPACE

检查配置

为此数据库创建至少一个备份规范后，可以检查 SAP R/3 数据库的配置。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。单击备份规范以显示要检查的 Oracle 实例。
3. 右键单击 Oracle 实例，然后单击“检查配置”。

使用 Data Protector CLI

以 Oracle OS 用户身份登录 SAP R/3 系统并执行:

util_sap.exe -CHKCONF ORACLE_SID

其中， ORACLE_SID 是 Oracle 实例的名称。

成功的配置检查将显示消息 *RETVAL*0 。

如果收到 *RETVAL*error_number 消息 (其中 error_number 不为零)，则表示发生错误。有关如何获取错误说明的信息，请参阅备份 SAP R/3。

要检查 SAP R/3 配置是否适合即时恢复，请执行:

util_sap.exe -CHKCONF_IR ORACLE_SID [-verbose]

-verbose 选项会创建一个文件，其中包含与数据库文件位于相同源卷上的控制文件和重做日志文件列表。如果此列表不为空，则会显示警告，指出无法执行即时恢复。

配置 SAP R/3 参数文件

要配置集成，需要在应用程序系统和备份系统上的 SAP R/3 参数文件中设置一些参数。文件模板位于此处:

UNIX 系统： ORACLE_HOME/dbs/initORACLE_SID.sap

Windows 系统: ORACLE_HOME\database\initORACLE_SID.sap

如果您具有 Oracle RAC 或 ASM 配置，则文件模板位于此处:

UNIX 系统： SAPDATA_HOME/sapprof/initORACLE_SID.sap

Windows 系统： SAPDATA_HOME\sapprof\initORACLE_SID.sap

在这种情况下，必须将文件模板从 SAPDATA_HOME 复制到 ORACLE_HOME ，或者创建指向 SAPDATA_HOME 的符号链接。

SAP 参数文件设置

参数	值/说明
split_cmd	在应用程序系统上: *UNIX 系统：* "/opt/omni/lbin/ob2smbsplit $" *Windows 系统:* "Data_Protector_home\bin\ob2smbsplit $" 在备份系统上，无需设置该参数。 BRBACKUP 使用此参数来触发复本创建操作。在运行时，包含要备份的文件名称的文本文件的名称会替换可选符号“ $ ”。 *Windows 系统：*如果路径名包含空格，请改用 Windows 短名称。
primary_db	在应用程序系统上: LOCAL 在备份系统上: 用于连接 Oracle 数据库的服务的名称。 此参数定义 Oracle 数据库的服务名称，以将备份系统链接到应用程序系统。

配置符合 SAP 标准的 ZDB 会话

SAP R/3 标准建议，在使用 splitint 备份接口的 ZDB 会话中，BRBACKUP 应在备份系统上启动，而不是在应用程序系统上启动。您可以通过配置 Data Protector 来符合这些标准，具体方式是将 Data Protector OB2_MIRROR_COMP 环境变量设置为 1 。该变量保存在 Data Protector SAP R/3 实例配置文件中。因此，在此 SAP R/3 实例的所有 splitint ZDB 会话中，BRBACKUP 都将在备份系统上启动。默认情况下，BRBACKUP 在应用程序系统上启动。

使用 Data Protector GUI 或 CLI 设置 OB2_MIRROR_COMP 环境变量。

> 注意: 如果不存在相关 SAP R/3 实例的备份规范，则无法使用 Data Protector CLI 设置 OB2_MIRROR_COMP 变量。

使用 Data Protector GUI

您可以在创建备份规范或修改现有规范时设置 OB2_MIRROR_COMP 变量:

1. 前往备份规范的“源”页面。

> 注意: 在控制文件和数据文件驻留在同一源磁盘的环境中，如果选择“跟踪复本以用于即时恢复”选项，Data Protector 将不允许访问“源”页面。具体来说，Data Protector 即时恢复检查将失败。在这种情况下，请先清除该选项。如果已设置 OB2_MIRROR_COMP 变量，则可以在以后需要时选择该选项，这时就不会再执行即时恢复检查。

右键单击顶部的 SAP R/3 实例，然后单击“设置环境变量”。

2. 在“高级”对话框中，将 OB2_MIRROR_COMP 设置为 1 。

   单击**确定**。

使用 Data Protector CLI

请执行以下命令:

必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。

设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

```
util_cmd –putopt SAP instance_name OB2_MIRROR_COMP 1 –sublist Environment
```

备份 SAP R/3 ZDB 集成

此集成可执行以下类型的联机和脱机数据库备份:

备份类型

- ZDB 到磁盘
- ZDB 到磁带
- ZDB 到磁盘 + 磁带

要配置备份，请创建 ZDB 备份规范。

存档日志只能与数据库一起在“ZDB 到磁盘 + 磁带”、“ZDB 到磁带”或非 ZDB (标准备份) 会话中备份。如果尝试在“ZDB 到磁盘”会话中备份存档日志或尝试在 ZDB 会话中只备份存档日志，则会话将失败。

备份的内容取决于您在备份规范中的选择。

备份内容

选定的项	已备份的文件
存档日志	• 脱机（归档）重做日志 • 控制文件
数据库或单个表空间	• 数据文件 • 控制文件 • SAP R/3 日志和参数文件 • 联机重做日志 (仅在脱机备份期间)

您可以通过两种不同的方式指定 SAP R/3 备份选项:

- 使用 BRBACKUP 选项。
- 使用 SAP 参数文件。

> 注意: BRBACKUP 选项会覆盖 SAP 参数文件中的设置。

您可以在创建备份规范时指定 BRBACKUP 选项。如果未指定任何选项，SAP R/3 应用程序将引用 SAP 参数文件中的当前设置。在这种情况下，请在运行备份前，请确保已正确配置 SAP 参数文件。

> 提示: 创建备份规范时，请选择已包含所需 BRBACKUP 选项的备份模板。

创建备份规范

使用 Data Protector Manager 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“SAP R/3”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择模板，然后单击“确定”。

   可用于标准零宕机时间备份的备份模板

空白 **SAP** 备份	无预定义选项。
Brbackup_offline_mirror	用于使用 splitint 执行脱机 ZDB (拆分镜像或快照备份)。数据库在创建复本期间停止。与使用 Brbackup_SMB_Offline 相比，数据库脱机的时间更短，但 BRTOOLS 必须支持 splitint 。
Brbackup_online_mirror	用于使用 splitint 执行联机 ZDB (拆分镜像或快照备份)。数据库在创建复本期间处于活动状态。与使用 Brbackup_SMB_Online 相比，数据库处于备份模式的时间更短，但 BRTOOLS 必须支持 splitint 。

Brbackup_SMB_Offline	用于脱机 ZDB (拆分镜像或快照备份)。数据库在创建复本期间停止。
Brbackup_SMB_Online	用于联机 ZDB (拆分镜像或快照备份)。数据库在创建复本期间处于活动状态。

在“备份类型”下拉列表中，选择“快照或拆分镜像备份”。

从“子类型”下拉列表中，选择相应的磁盘阵列代理。代理必须安装在应用程序系统和备份系统上。

4. 在“应用程序系统”中，选择要备份的 SAP R/3 客户机。在群集环境中，选择虚拟服务器。

   在“备份系统”中，选择备份系统。

   选择其他特定于磁盘阵列的备份选项。有关备份选项的详细信息，请按 **F1**。

   P9000 XP 阵列详情

   要启用即时恢复，请将“跟踪复本以用于即时恢复”选项保持选中状态。如果清除此选项，则无法使用 Data Protector 运行即时恢复。

   单击“下一步”。

5. 在“应用程序数据库”中，选择要备份的 Oracle 实例 (ORACLE_SID)。

   指定 UNIX 和 Windows 客户机上可用的下列“用户和组/域”选项:

   Windows 系统 : 在“用户名”和“组/域名”中，指定要用于运行备份会话的操作系统用户帐户 (例如，用户名 Administrator 、域 DP)。

   UNIX 系统: 在“用户名”中，键入配置用户帐户中所述的 Oracle OS 用户。在“组/域名”中，键入 dba 。

   请确保此用户已添加到 Data Protector admin 或 operator 用户组，具有 SAP R/3 备份权限，以及已设置为用于 Data Protector Inet 服务用户模拟。此用户成为备份所有者。

   单击“下一步”。

6. 如果尚未将 SAP R/3 数据库配置为与 Data Protector 配合使用，则会显示“配置 SAP”对话框。按照配置 SAP R/3 数据库中所述进行配置。

7. 选择要备份的 SAP R/3 对象。您可以选择单个表空间、数据文件或存档日志。

   > 注意: 如果打算执行即时恢复，请选择整个“数据库”项。

   单击“下一步”。

8. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。在“并发”选项卡中指定并行备份流的数量并指定介质池。

   > 注意: 并行性 (备份 SAP R/3 数据库时使用的备份流的数量) 会自动设置。如果使用负载均衡，则备份流的数量等于所选设备的并发性总和。

   单击“下一步”。

9. 设置备份选项。有关特定于应用程序的选项的信息，请参阅 SAP R/3 备份选项。

   单击“下一步”。

10. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 单击“保存并计划”进行保存，然后计划备份规范。有关如何创建和编辑计划的详细信息，请参阅《Data Protector 管理员指南》中的“Data Protector 中的调度程序”。

> 提示: 请在实际使用之前先预览备份规范。请参阅预览备份会话。

SAP R/3 备份选项

选项	描述
日志文件	如果要在备份期间创建 backint 日志文件，请指定该文件的路径名。默认情况下不会创建该文件，因为 Data Protector 会将与备份会话有关的所有相关信息存储在数据库中。

BR 备份	指定 BRBACKUP 选项。 例如，对于使用 splitint 接口的联机备份，请键入 -t online_mirror。如果 BRTOOLS 不支持 splitint，请键入 -t online_split。 要在与配置期间指定的用户不同的 Oracle 数据库用户下运行 BRBACKUP，请键入 -u user_name。
备份对象	列出 omnisap.exe 传递的 BRBACKUP 选项。保存备份规范后将显示该列表。
BR 归档	指定 BRARCHIVE 选项。 对“ZDB 到磁盘”不适用
均衡: 按负载	将文件分成大小大致相等的若干子集。然后，Data Protector sapback 程序将同时备份这些子集。 如果备份设备使用硬件压缩，则原始文件和备份文件的大小会有所不同。要将此情况通知 Data Protector，请在 Data Protector SAP R/3 配置文件的 compression 部分指定已备份文件的原始大小。
均衡: 按时间	将文件按大致相同的备份时间段分成若干子集。该时间段取决于文件类型、备份设备的速度和外部影响因素 (例如装载提示)。此选项最适合具有相同质量的大型库的环境。这些子集将由 Data Protector sapback 程序同时备份。Data Protector 会自动将备份速度信息存储在 Data Protector SAP R/3 配置文件的 speed 部分中。它会使用此信息来优化备份时间。 联机备份时或备份设备的速度差异很大时，此类型均衡有可能会导致文件分组并非最佳。
均衡: 手动	将文件按 Data Protector SAP R/3 配置文件的手动均衡部分中的指定分成若干子集。有关详细信息，请参阅备份 SAP R/3。 对“ZDB 到磁盘”不适用
均衡: 无	没有使用均衡。文件按照它们在内部 Oracle 数据库结构中列出的顺序进行备份。要检查该顺序，请使用 Oracle Server Manager SQL 命令: select * from dba_data_files
Pre-exec、Post-exec	此处指定的命令由 SAP R/3 系统上的 omnisap.exe 在备份之前 (pre-exec) 或之后 (post-exec) 启动。不要使用双引号。只提供名称。命令必须位于以下目录中: *Windows 系统:* Data_Protector_home\bin *HP-UX、Solaris 和 Linux 系统:* /opt/omni/bin *其他 UNIX 系统:* /usr/omni/bin
备份模式	不适用于 ZDB。
使用默认 RMAN 通道数	不适用于 ZDB。
数据库外部的对象	指定要保存的 Oracle SAP R/3 环境的非数据库文件。 将这些文件保存在单独的备份会话中。

> 注意: 使用 Data Protector 在一个会话中启动的 sapback 进程总数限制为 256 个。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。有关如何创建和编辑计划的详细信息，请参阅管理中的“调度程序”。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行:

```
omnib -sap_list backup_specification_name -test_bar
```

预览期间会发生什么?

omnisap.exe 命令启动，进而启动 Data Protector testbar 命令来测试:

- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

备份方法

通过以下任一方式启动 SAP R/3 对象的备份:

- 使用 Data Protector GUI.
- 使用 Data Protector CLI.
- 使用 SAP BR*Tools。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，依次展开“备份规范”和“SAP R/3”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

> 注意: 仅支持完整 备份类型。

“ZDB 到磁盘”、*“ZDB 到磁盘 + 磁带”:* 指定“拆分镜像/快照备份”选项。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行:

ZDB 到磁带、*ZDB 到磁盘 + 磁带:*

```
omnib -sap_list backup_specification_name
```

ZDB 到磁盘:

omnib -sap_list backup_specification_name -disk_only

示例

要使用 SAP R/3 备份规范 RONA 启动完整备份，请执行:

omnib -sap_list RONA -barmode full

使用 SAP BRTOOLS

1. 以 Oracle OS 用户身份登录 SAP R/3 备份系统或 SAP R/3 应用程序系统。
2. 导出/设置以下环境变量:

ORACLE_SID=*SAP_instance_name*	
ORACLE_HOME=*Oracle_software_home_directory*	
[SAPBACKUP_TYPE=OFFLINE]	默认值为 ONLINE 。
SAPDATA_HOME=*database_files_directory*	
SAPBACKUP=*BRTOOLS_logs_and_control_file_copy_directory*	
SAPREORG=*BRSPACE_logs_directory*	
OB2BARLIST=*backup_specification_name*	仅需要用备份规范来指定应该使用哪些 Data Protector 设备进行备份。备份规范中的其他信息 (如要备份的 SAP R/3 对象或 BRBACKUP 选项) 将被忽略，必须在运行时手动指定。
[OB2_3RD_PARTY_BACKINT=1]	指定使用第三方 backint 工具来执行“ZDB 到磁盘 + 磁带”备份会话。设置变量后，将要使用的 backint 复制到 SAP BRTOOLS 目录。
[OB2BARHOSTNAME=*application_system_name*]	如果已登录备份系统，这是必需的。如果要在群集环境中指定虚拟服务器名称，则是可选的。
[OB2BACKUPHOSTNAME=*backup_system_name*]	如果已登录到应用程序系统，这是必需的。
OB2SMB=1	指定一个 ZDB 会话。
[OB2SMBIR=1]	指定即时恢复的跟踪复本。
[ZDB_ORA_INCLUDE_CF_OLF=1]	如果已登录备份系统，这是必需的。
[OB2DISKONLY=1]	指定一个“ZDB 到磁盘”会话。

如果登录到备份系统，请确保将 NLS_LANG 环境变量设置为与应用程序系统上的 NLS_LANG 环境变量相同的值。

这些变量也可以在 backint 参数文件中指定。如果需要，则必须使用 *util_par_file* 参数在 SAP 配置文件中指定该文件的位置:

util_par_file = path\filename

如果未提供路径，系统将在目录中搜索该参数文件:

Windows 系统: SAPDATA_HOME\database

UNIX 系统: ORACLE_HOME/dbs

3. 如果计划在 RMAN 模式下备份，请确保 initSAP_instance.sap 文件中的 SBT_LIBRARY 参数指向正确的特定于平台的 Data Protector MML。

4. 执行 BRBACKUP 命令。该命令语法取决于您是登录到应用程序系统还是备份系统:

   应用程序系统:

   ```
   brbackup -t {online_split | offline_split | online_mirror | \ offline_mirror} [–q split] -d \ util_file -m all -c -u user/password
   ```

   备份系统:

   ```
   brbackup -t {online_mirror | offline_mirror} [–q split] -d util_file -m all -c -u user/password
   ```

   如果 `OB2DISKONLY` 设置为 `1` ，则需要 `-q split` 选项。

使用 Oracle Recovery Manager 执行备份

如果直接使用 RMAN，请考虑以下事项:

- RMAN 将有关备份的信息存储在恢复编目中。出于安全考虑，请将该编目保存在单独的数据库中。这需要执行更多的管理工作。
- 发生灾难时 (例如丢失生产数据库和恢复编目)，数据的还原和恢复会非常复杂。如果这时没有 Oracle 支持人员的的帮助，恢复和还原几乎是不可能的。如果 Recovery Manager 没有将管理数据存储在恢复编目中，就无法只凭借已创建的备份来恢复数据库。
- 对于每个 RMAN 通道，将 `SBT_LIBRARY` 参数设置为指向正确的特定于平台的 Data Protector MML。

如果通过 BRBACKUP 实用程序使用 RMAN，请考虑以下事项:

- 这时不会使用恢复编目。有关备份的信息保存在控制文件和 SAP R /3 日志文件中。每次备份后，都会保存控制文件和 SAP R /3 日志文件。还原数据后，首先复制回控制文件，然后再复制回数据文件。如果发生灾难，则先还原 SAP R /3 日志文件，然后再还原所有数据文件。
- 其他重要文件仍将使用 backint 程序自动备份。
- 所有以前的 SAP R/3 备份策略仍可与 RMAN 一起使用。但是，RMAN 不能与 BRARCHIVE 一起执行脱机重做日志备份，也不能用于备用数据库备份。
- 确保 `initSAP_instance.sap` 文件中的 `SBT_LIBRARY` 参数指向正确的特定于平台的 Data Protector MML。有关 Data Protector MML 位置的详细信息，请参阅指定 parms 操作数。。

还原 SAP R/3 ZDB 集成

您可以通过以下任意方式使用以下任意方法还原 SAP R/3 对象:

- **标准还原:** 数据从在“ZDB 到磁带”、“ZDB 到磁盘 + 磁带”和非 ZDB (标准备份) 会话中创建的备份介质进行还原。请参见标准还原。
- **即时恢复:** 数据从在联机“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话中创建的复本进行还原。请参见即时恢复。

还原后，可以使用 SAP BRTOOLS 接口将数据库恢复到特定时间点。使用即时恢复方法可以在同一会话中还原和恢复数据库。但是，您只能还原 (和恢复) 整个数据库。要仅还原一部分数据库或存档日志，请使用标准还原方法。

下表显示了可用的还原方法，具体取决于从中执行还原的备份会话。

SAP 恢复方法

磁盘阵列	备份类型	恢复整个数据库		恢复一部分数据库
		恢复到现在	恢复到某个时间点、日志序列号/线程或 SCN 编号	
P9000 XP、EMC、NetApp Storage	**ZDB 到磁带 - 联机**	还原	还原	还原
	ZDB 到磁带 - 脱机	还原	还原	还原
P9000 XP	**ZDB 到磁盘 - 联机**	即时恢复 + 数据库恢复	即时恢复 + 数据库恢复	不适用
	ZDB 到磁盘 - 脱机	不适用	不适用	不适用
	ZDB 到磁盘 + 磁带 - 联机	• 即时恢复 + 数据库恢复 或 • 还原	• 即时恢复 + 数据库恢复 或 • 还原	还原
	ZDB 到磁盘 + 磁带 - 脱机	还原	还原	还原

图例

还原	您可以使用 Data Protector GUI 或 SAP BRTOOLS 从 Data Protector 介质执行标准还原。还原后，可以使用 SAP BRTOOLS 恢复数据库。
即时恢复 + 数据库恢复	您可以执行即时恢复。通过使用 BRTOOLS，您可以将数据库恢复包含在即时恢复中，也可以稍后执行数据库恢复。
不适用	不可用。

标准还原

使用 Data Protector GUI 进行还原

1. 在“上下文列表”中，单击“还原”。
2. 在“范围窗格”中，展开“SAP R/3”，展开此前从中备份过数据的客户机 (备份系统)，然后单击要还原的 Oracle 实例。
3. 在“源”页面中，选择要还原的 SAP R/3 文件。

   要以不同的名称还原文件或将文件还原到不同的目录，请右键单击该文件，然后单击“还原为/还原至”。

   要从特定备份会话还原文件，请右键单击该文件，然后单击“还原版本”。
4. 在“目标”选项卡中，选择要还原到的客户机 (“目标客户机”)。默认情况下，这是应用程序系统。

   有关各选项的详细信息，请按 **F1**。
5. 在“选项”页面中，设置还原选项。有关信息，请按 **F1**。
6. 在“设备”页中，选择要用于还原的设备。
7. 单击**还原**。

8. 在“启动还原会话”对话框中，单击“下一步”。
9. 指定“报告级别”和“网络负载”。

   > 注意: 选择“显示统计信息”可查看会话输出中的还原配置文件消息。

10. *P9000 XP 阵列:* 从 Mirror mode 下拉列表中，选择“已禁用”。这会将还原设置为直接从备份介质还原到应用程序系统。
11. 单击**完成**启动还原。

会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

即时恢复

可以使用 Data Protector GUI 或 CLI 启动即时恢复。

使用 Data Protector GUI 即时恢复

要执行即时恢复，请执行以下操作:

1. 使用 sqlplus 关闭 Oracle 数据库:

   例如:

   ```
   sqlplus sqlplus> shutdown immediate sqlplus> exit
   ```

2. 在 Data Protector Manager 的上下文列表中，选择“即时恢复”。
3. 展开“SAP R/3”，并选择要从中执行还原的“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话。
4. 在“源”选项卡中，选择要恢复的对象。只能选择整个数据库。

   对于 P9000 XP 磁盘阵列系列，建议保持“在还原完成之后保留复本”选项处于选中状态，以便能重新启动即时恢复会话。该选项在默认情况下处于选中状态，但备份期间数据库处于 NOARCHIVELOG 模式的脱机备份除外。

   设置其他 P9000 XP 磁盘阵列系列选项。有关详细信息，请按 **F1**。
5. 此时，您可以决定是否在即时恢复后立即执行数据库恢复:
   - 要仅执行即时恢复，请单击“还原”。
   - 要在即时恢复后自动执行数据库恢复，请选择恢复选项。

     单击**还原**。

     Data Protector 会在执行即时恢复后还原数据库，具体方式是将数据库切换到装载状态、从磁带还原必要的存档重做日志并应用重做日志。

数据库恢复选项

用户名 (仅限 UNIX 系统)	指定在其名下执行即时恢复的用户名。用户需要是 DBA 组的成员。
用户组 (仅限 UNIX 系统)	指定“用户名”字段中的用户所属的用户组。 注意 “用户名”和“用户组”必须与备份所有权中定义的相同。
恢复	在即时恢复后启用数据库恢复。

在此前恢复	使用此下拉列表中的选项可以指定要恢复到的时间点。 可用的选项如下: **现在**: 将应用所有现有存档日志。 **所选时间**: 仅应用指定时间前的存档日志。 **选定的日志序列号/线程编号**: 指定未完成的恢复。仅应用编号小于或等于指定日志序列号或线程编号的存档日志。 **选定的 SCN 编号**: 仅应用指定 SCN 编号前的存档日志。
恢复之后打开数据库	执行恢复后打开数据库。
重置日志	在打开数据库之后，重置存档日志。如果“在此前恢复”选项设置为“现在”，则默认情况下不会选择此选项。 以下是 Oracle 关于何时重置日志的建议: *始终*重置日志: • 执行不完整的恢复之后，即如果并没有应用所有存档重做日志。 • 如果使用控制文件的备份进行恢复。 在以下情况下，请勿重置日志: • 执行完整恢复之后，未使用控制文件时。 • 如果存档日志用于备用数据库。但是，如果必须重置存档日志，则将需要重新创建备用数据库。

使用 Data Protector CLI 执行即时恢复

执行:

omnir

–host ClientName

-session SessionID

-instant_restore

[P9000_DISK_ARRAY_XP_OPTIONS | P6000_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS]

-sap

-user UserName -group GroupName

-recover {now | time MM/DD/YY hh:mm:ss | logseq LogSeqNumber thread ThreadNumber | SCN Number} [-open [-resetlogs]]

-appname ApplicationDatabaseName

各选项的顺序很重要。在 Windows 客户机上，不需要用户名和组名选项。有关各选项的详细说明，请参阅《Data Protector 命令行界面参考》。

从包含控制文件的复本执行即时恢复

从包含控制文件的复本执行即时恢复期间，当前控制文件乃至联机重做日志将被覆盖。因此，在启动会话之前，请将当前控制文件和联机重做日志复制到安全位置，以便以后能够执行数据库恢复。

如果在以下任一会话中创建了复本，该复本将包含控制文件:

- 联机 ZDB 会话，同时 omnirc 选项 ZDB_ORA_INCLUDE_CF_OLF 设置为 1
- 符合 SAP 标准的联机 ZDB 会话
- 脱机 ZDB 会话 (任何配置)

> 注意: 脱机 ZDB 会话还包含联机重做日志。您可以使用此类会话将 SAP R/3 数据库还原到执行备份的时间点。在这种情况下，您无需执行以下步骤。

要还原和恢复数据库，请执行以下操作:

1. 将当前的控制文件和联机重做日志复制到安全位置。
2. 执行即时恢复 (无数据库恢复)。使用 Data Protector GUI 或 CLI。
3. 将当前的控制文件和联机重做日志复制到各自的原始位置。
4. 装载目标数据库。
5. 还原数据库恢复所需的缺失存档重做日志。

   示例:

   ```
   # sqlplus user/password@net_service_name SQL> select SEQUENCE#, NAME from V$ARCHIVED_LOG where (NEXT_TIME>to_date('2010/10/03','YYY/MM/DD') and (FIRST_CHANGE#<='1000'); # brrestore -a log_no,...-d util_file -c force -u user/password
   ```

6. 恢复目标数据库。

   示例:

   ```
   # rman target user/password@net_service_name RMAN> run{ 2> allocate channel dbrec type disk; 3> recover database until scn 1000; 4> release channel dbrec; 5> }
   ```

使用其他设备进行还原

您可以使用与备份不同的设备执行还原。

使用 Data Protector GUI

有关如何使用 Data Protector GUI 为还原选择其他设备的信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

使用 Data Protector CLI 或 SAP 命令

如果要使用 Data Protector CLI 或 SAP R/3 命令进行还原，请在文件中指定新设备:

Windows 系统: Data_Protector_program_data\Config\Server\cell\restoredev

UNIX 系统: /etc/opt/omni/server/cell/restoredev

使用以下格式:

" DEV 1 " " DEV 2 "

其中， DEV 1 是原始设备，而 DEV 2 是新设备。

> 重要说明: 使用后删除此文件。

在 Windows 系统上，请为该文件使用 Unicode 格式。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面 组件的任何 Data Protector 客户机中监视会话。

有关如何监视会话，请参阅《Data Protector 帮助》索引: “查看当前正在运行的会话”。

备份期间生成的系统消息将发送到 SAP R/3 和 Data Protector 监视器。但是，装载请求仅发送到 Data Protector 监视器。

Sybase IQ 集成

本主题说明如何使用 Data Protector 文件系统备份与用户定义的 pre-exec 和 post-exec 脚本 (包含 Sybase IQ 备份或还原命令) 的组合来执行 SAP Sybase IQ 备份。

> **注意:** 支持 Data Protector 文件系统备份和还原的平台都支持 Sybase IQ。本主题中提供的命令适用于 Sybase IQ 版本 16。

本主题介绍与 Data Protector Sybase IQ 集成有关的信息。有关 Data Protector 的常规过程和选项，请参阅《Data Protector 帮助》。

备份 Sybase IQ

Sybase IQ 支持以下备份类型: 完整、完整后的增量、增量、系统级别和虚拟。在新数据库上运行完整备份来提供一个基准点，然后按固定计划执行完整备份和增量备份。

考虑时间和存储要求。备份前始终要检查数据库的大小。运行 SQL 语句将有助于确定当前已使用的空间量 (%)。建议在已使用空间总量的基础上增加 10% 的空间量以确保有足够空间。平衡创建备份的耗时与还原数据的耗时。建议做好以下工作:

- 备份前验证数据库。
- 每周执行一次完整数据库备份。
- 根据需要执行“完整后的增量”备份。
- 一天中每隔几个小时执行一次“增量”备份。
- 每次备份后，都可以运行 post-exec 脚本来删除用于备份的转储数据库的备份文件。
- 将数据库写入存档设备。

> **注意:** BACKUP DATABASE 语句将覆盖同名的现有磁盘文件。要保留以前的备份，请为存档设备使用不同的文件或路径名，或将旧备份转移到其他位置。

要备份 Sybase IQ，请继续执行以下步骤:

1. 在将创建数据库备份的 Sybase Server 上创建目录 (例如 /BackupFull_Sybase)。
2. 创建连接到 Sybase IQ 数据库的脚本以执行以下操作:
    1. 执行备份 (脚本可以作为 pre-exec 命令运行)。
    2. 清理旧备份文件 (使用 post-exec 命令) 以回收磁盘空间。
3. 创建 Data Protector 文件系统备份规范，其中包含在步骤 1 中创建的 Sybase 备份目录。
4. 在“备份选项 - 常规”选项卡中，选择将在其上执行 pre-exec 备份脚本和 post-exec 还原脚本的 Sybase Server。有关详细信息，请参阅“Pre-Exec Sybase IQ 备份命令示例”和“Post-Exec Sybase IQ 还原命令示例”小节。
5. 为此 Sybase Server 计划定期备份。

Pre-Exec Sybase IQ 备份命令

有关详细信息，请参阅 SAP Sybase Infocenter。

完整备份

```
BACKUP DATABASE
FULL
TO 'Backup_DataProtector_Sybase/Full/file1'
TO 'Backup_DataProtector_Sybase/Full/file2'
WITH COMMENT 'Full backup database'
```

增量备份

```
BACKUP DATABASE
INCREMENTAL
TO 'Backup_DataProtector_Sybase/Incr/file1'
TO 'Backup_DataProtector_Sybase/Incr/file2'
WITH COMMENT 'Incremental backup'
```

差异备份

```
BACKUP DATABASE
INCREMENTAL SINCE FULL
TO 'Backup_DataProtector_Sybase/IncrSF/file1'
TO 'Backup_DataProtector_Sybase/IncrSF/file2'
WITH COMMENT 'IncrementalSinceFull backup'
```

还原 Sybase IQ

您可以按以下顺序还原备份文件:

1. 从 Data Protector 还原每周完整备份。
2. 从 Data Protector 还原自完整备份以来的最后一次增量备份。

3. 按时间递增的顺序还原自上次使用 Incremental since full backup 选项以来的所有增量备份。
4. 还原后，连接到数据库并执行 SQL 命令以还原和恢复 Sybase 数据库。

> 注意**:** 以下步骤可以是 DP post-exec 还原脚本的一部分。

5. 关闭 Sybase Server:
   stop_iq
6. 启动具有数据库独占访问权限的服务器:
   start_iq -su mypwd -gd DBA -gm 1 -n my_server
7. 按照如下方式，启动 dbisql 并连接到实用程序数据库:
   dbisql -c "UID=DBA;PWD=mypwd;DBN=utility_db"

> 注意**:** RESTORE DATABASE 语句是从实用程序数据库 (utility_db) 执行的，需要对该数据库具有独占访问权限。有关 RESTORE 命令的详细信息，请参阅 Post-Exec Sybase IQ 还原命令示例。

根据计划还原的备份类型，您可能需要删除一些对象并验证其他对象，具体如下所示:
- 对于完整还原，要将数据还原到的位置不得存在存储文件 (默认情况下为 .iq 文件)、编目存储 (默认情况下为 .db 文件) 和事务日志 (默认情况下为 .log 文件)。如果存在上述任何一种文件，则必须先删除它们或将它们转移到其他目录，然后再执行完整还原。完整还原开始后，它会销毁所有旧数据库文件，然后重新创建它们。如果手动删除存储、编目存储和事务日志文件，则可以防止意外执行完整还原。
- 对于任何增量还原，必须存在编目存储 (.db)。如果它存在，但位于与要还原到的位置不同的位置，请移动数据库文件。如果它不存在，则只能执行完整还原。如果在任何增量还原之前先执行完整还原，则会将正确的文件放置到位。
- 按照下文所述还原备份:
  - 如果数据库不一致，或者要将任何文件移动到新位置，则必须还原 FULL 备份。
  - 如果最近的备份是 FULL 备份，或者如果需要将数据库还原到创建任何现有增量之前的状态，请仅还原完整备份。
  - 如果在数据库发生故障之前有 INCREMENTAL_SINCE_FULL 备份，请先从最后一个 FULL 备份进行还原，然后再还原 INCREMENTAL_SINCE_FULL 备份。
  - 如果没有 INCREMENTAL_SINCE_FULL 备份，但自上次 FULL 备份以来已执行了一次或多次 INCREMENTAL 备份，请先还原 FULL 备份，然后按照创建顺序还原各个 INCREMENTAL 备份。
  - 请勿启动数据库，直至还原了最近一次备份。否则，您将无法进一步还原。

8. 从 dbisql 运行所有 RESTORE DATABASE 命令。
9. 对于数据库验证，请在还原后运行 sp_iqcheckdb 存储过程。
10. 使用 stop_iq 来停止实用程序数据库和关联的引擎。
11. 使用 start_iq 启动已还原的数据库。

Post-Exec Sybase IQ 还原命令

有关详细信息，请参阅 SAP Sybase Infocenter。

从最后一次增量备份还原数据库

```
 RESTORE DATABASE ‘newdata.db’
FROM ' Backup_DataProtector_Sybase/Full/file1'
FROM ' Backup_DataProtector_Sybase/Full/file2'

 RESTORE DATABASE ‘newdata.db’
FROM ' Backup_DataProtector_Sybase/IncrSF/file1'
FROM ' Backup_DataProtector_Sybase/IncrSF/file2'

 RESTORE DATABASE ‘newdata.db’
FROM ' Backup_DataProtector_Sybase/Incr/file1'
FROM ' Backup_DataProtector_Sybase/Incr/file2'
```

Sybase Server 集成

This feature is available in the Premium Edition

本主题说明如何配置和使用 Data Protector Sybase Adaptive Server (Sybase Server) 集成。其中描述了备份和还原 Sybase 数据库需要了解的概念和方法。

Data Protector 提供以下类型的交互式备份和安排的备份：

备份类型

完整	备份所选的全部 Sybase 数据库和事务日志。
事务	备份从任何类型的上一次备份以来对事务日志所做的更改。 请注意，对于 此备份类型，必须将事务日志放置在单独的 Sybase 数据库设备上。否则，备份失败。有关如何将事务日志放置在单独的 Sybase 数据库设备上的详细信息，请参阅 Sybase 文档。

备份期间，数据库为联机并可正常使用。

使用 isql 实用程序还原 Sybase 数据库。您可以将数据库:

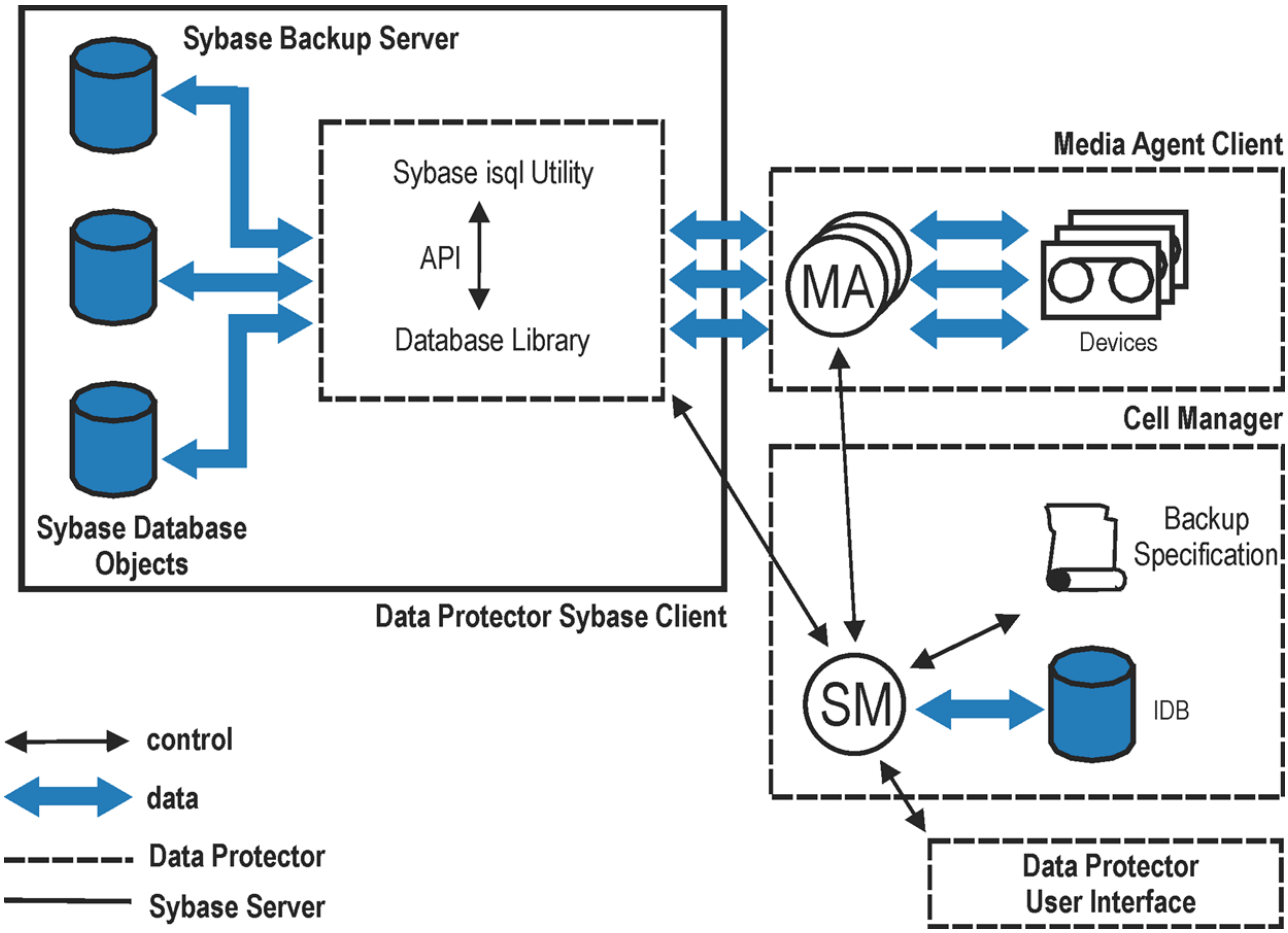
- 还原到特定时间点
- 还原到一个新的数据库
- 还原到另一个 Sybase 实例

本主题提供特定于 Data Protector Sybase Server 集成的信息。有关 Data Protector 的常规过程和选项，请参阅《Data Protector 帮助》。

集成概念

Data Protector 通过基于名为 Data Protector **BAR** (备份和还原) 的公共库的 Data Protector 数据库例程库与 Sybase Backup Server 集成。Data Protector 数据库例程库通道在 Data Protector 会话管理器与 Sybase **ISQL** 实用程序 (通过 **Sybase Backup Server API**) 之间进行通信。Sybase 集成体系结构显示了 Data Protector Sybase 集成的体系结构。

Sybase 集成体系结构



图例

SM	Data Protector 会话管理器: 备份会话管理器 (备份期间) 和还原会话管理器 (还原期间)。
API	Sybase Backup Server 应用程序编程接口。
数据库例程库	一组 Data Protector 可执行文件，可用于在 Sybase Backup Server 和 Data Protector 之间传输数据。
MA	Data Protector 常规介质代理。
备份规范	要备份的对象列表、备份设备和要使用的选项。
IDB	Data Protector 内部数据库。

符合 Sybase Server 的先决条件

下面是 Sybase Server 集成的先决条件:

- 确保已正确安装和配置 Sybase Server。
  - 有关 Sybase Server 的信息，请参阅《Adaptive Server Enterprise System 管理指南》和《Adaptive Server Enterprise 安装和配置指南》。

  每个 Sybase 实例及其默认 Sybase Backup Server 必须在同一系统上配置。
- 确保已正确安装 Data Protector。有关如何在各种体系结构中安装 Data Protector Sybase 集成的信息，请参阅《Data Protector 安装指南》。

  您要备份或还原到的每个 Sybase Server 系统都必须安装 Data Protector“Sybase 集成”组件。
- 配置要与 Data Protector 配合使用的设备和介质。
- 要测试 Sybase Server 系统和 Cell Manager 是否正常通信，请在 Sybase Server 系统上配置并运行 Data Protector 文件系统备份和还原。
- 确保 Sybase 实例的默认 Sybase Backup Server 处于联机状态。
- 在 Windows 操作系统上，为具有相应 Sybase Server 权限的用户配置 Data Protector Inet 服务用户模拟，以便运行备份和还原。
- 在 Windows 操作系统上，升级到 Data Protector 2020.05 或更高版本后，手动更新 Sybase 库路径中的 libob2syb 库。为此，请停止实例，然后将 libob2syb.dll 从 Data Protector bin 路径 (C:\Program Files\OmniBack\bin) 复制到 Sybase 库路径 (C:\..\ASE-16_0\lib)。现在重新启动实例。

群集感知客户机

仅在一个群集节点上配置 Sybase 实例，因为配置文件驻留在 Cell Manager 上。

如果您打算使用 Data Protector CLI，请将 Data Protector 环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称。

配置集成

您需要配置 Sybase 用户以及要备份或还原到的每个 Sybase Adaptive Server 实例 (**Sybase 实例**)。

配置 Sybase 用户

在 UNIX 系统上，将用户 root 和 Sybase Server 管理员 (isql 实用程序的所有者) 添加到 Data Protector admin 或 operator 用户组。有关信息，请参阅《Data Protector 帮助》索引: “添加用户”。

本节假定 Sybase Server 管理员是组 sybase 中的用户 sybase 。

配置 Sybase 实例

为 Data Protector 提供 Sybase 实例配置参数:

- Sybase Server 主目录的路径名
- Sybase isql 实用程序的路径名
- Sybase 实例名称
- Sybase 实例用户
- Sybase 实例用户的密码
- Sybase SYBASE_ASE 目录的名称
- Sybase SYBASE_OCS 目录的名称

然后，Data Protector 会在 Cell Manager 上创建 Sybase 实例配置文件，并验证与 Sybase Backup Server 的连接。

要配置 Sybase 实例，请使用 Data Protector GUI 或 Data Protector CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Sybase Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。
4. 在“客户机”中，选择 Sybase Server 系统。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，键入 Sybase 实例名称。

   *UNIX 系统：*在“用户名”和“组/域名”中键入 sybase 。此用户成为备份所有者。

   单击“下一步”。
5. 在“配置 Sybase”对话框中，查看并在必要时更正自动填写的配置参数。在 Windows 上，会自动确定所有配置参数。在 UNIX 系统上，您需要设置 Sybase Server 主目录，以及具有备份和还原数据库的 Sybase 权限的 Sybase 实例用户的用户名和密码。

   单击**确定**。
6. Sybase 实例已配置。退出 GUI 或继续创建备份规范。

使用 Data Protector CLI

执行：

Windows 系统： perl -I..\lib\perl util_sybase.pl -CONFIG \

Sybase_instanceSybase_homeisql_pathSybase_userSybase_password \

Sybase_ASESybase_OCS

UNIX 系统： util_sybase.pl -CONFIG Sybase_instanceSybase_home \

isql_pathSybase_userSybase_password Sybase_ASESybase_OCS

参数描述

Sybase_instance	Sybase 实例的名称。

Sybase_home	Sybase Server 主目录的路径名。
isql_path	Sybase isql 命令的路径名。
Sybase_user	具有备份和还原数据库的 Sybase 权限的 Sybase 实例用户。
Sybase_password	Sybase 实例用户的密码。
Sybase_ASE	Sybase Sybase_ASE 目录的名称。
Sybase_OCS	Sybase Sybase_OCS 目录的名称。

消息 *RETVAL*0 表示配置成功。否则，您会收到 *RETVAL*error_number 。要获取错误描述，请执行:

omnigetmsg 12 error_number 。

示例 1

要配置 Sybase 实例 mysybase ，请执行:

util_sybase.pl -CONFIG mysybase /applications/sybase.15/ \ /applications/sybase.15/OCS-15_0/bin/isql sa " " ASE-15_0 OCS-15_0

安装 **Sybase Server** 客户机

This feature is available in the Premium Edition

假设 Sybase Backup Server 正在运行。要备份 Sybase 数据库，需要在安装期间选择以下 Data Protector 组件:

- Sybase Integration - 为了能够备份 Sybase 数据库
- Disk Agent - 出于两个原因而安装磁带客户机：
  - 运行 Sybase Backup Server 的文件系统备份。请在配置 Data Protector Sybase 集成“之前”执行该备份，并解决与 Sybase Backup Server 和 Data Protector 有关的所有问题。
  - 对“无法”使用 Sybase Backup Server 备份的重要数据运行文件系统备份。

备份 Sybase Server 集成

This feature is available in the Premium Edition

Data Protector Sybase 集成提供以下类型的联机备份:

备份类型

完整	备份所选的全部 Sybase 数据库和事务日志。
事务	备份从任何类型的上一次备份以来对事务日志所做的更改。 请注意，对于 此备份类型，必须将事务日志放置在单独的 Sybase 数据库设备上。否则，备份失败。有关如何将事务日志放置在单独的 Sybase 数据库设备上的详细信息，请参阅 Sybase 文档。

为系统上的硬件或软件故障做好准备:

- 定期备份 Sybase 系统数据库。

  每次创建、更改或删除设备或数据库时，备份 master 数据库。每次更改时，备份 model 数据库和 system procedure 数据库。
- 保留以下系统表的副本:
  - sysusages
  - sysdatabases
  - sysdevices
  - sysloginroles
  - syslogins

创建备份规范

使用 Data Protector GUI 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“Sybase Server”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，单击“确定”。
4. 在“客户机”中，选择 Sybase Server 系统。在群集环境中，选择虚拟服务器。

   在“应用程序数据库”中，键入 Sybase 实例名称。

   *UNIX 系统：*在“用户名”和“组/域名”中键入 sybase 。此用户成为备份所有者。

   单击“下一步”。
5. 如果未将 Sybase 实例配置为使用 Data Protector，则会显示“配置 Sybase”对话框。按照配置 Sybase 实例中所述进行配置。
6. 选择要备份的数据库。

   单击“下一步”。
7. 选择要用于备份的设备。

   要指定设备选项，请右键单击该设备，然后单击“属性”。

   单击“下一步”。
8. 设置备份选项。

   单击“下一步”。
9. 查看选择用于备份的对象的属性。如果仅选择了特定数据库，而不是整个实例，则可以指定用于备份特定数据库的并发数据流数: 右键单击数据库，然后单击“属性”。

   此选项等同于 Sybase *dump striping*。

   Sybase Backup Server 将数据库拆分为大致相等的部分，并根据设备并发值将各个部分同时发送到设备。

   如果设备并发总和足够大，则可以同时备份两个或更多数据库。

   单击“下一步”。

10. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。有关如何创建和编辑计划的详细信息，请参阅《*Data Protector 管理员指南*》中 Data Protector 中的“调度程序”。

> **提示**请在实际使用之前先预览备份规范。

Sybase 备份选项

Pre-exec，Post-exec	指定在备份每个选定数据库之前 (pre-exec) 或之后 (post-exec)，将由 Sybase Server 系统上的 ob2sybase.exe (Windows 系统) 或 ob2sybase.pl (UNIX 系统) 启动的命令。不要使用双引号。 *Windows 系统：*仅提供命令的名称。命令必须位于默认的 Data Protector 命令目录中。*UNIX 系统：*提供命令的路径名。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。有关如何创建和编辑计划的详细信息，请参阅管理中的“调度程序”。

预览备份会话

预览备份会话以对其进行测试。使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Sybase Server”。右键单击要预览的备份规范，然后单击“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行：

```
omnib -sybase_list backup_specification_name -test_bar
```

预览期间会发生什么?

测试以下内容:

- Sybase 实例与 Data Protector 之间的通信
- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中
- 配置 Sybase 实例

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份十分有用。

通过以下任一方式启动备份:

- 使用 Data Protector GUI。
- 使用 Data Protector CLI。
- 使用 Sybase isql 实用程序。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Sybase Server”。右键单击要使用的备份规范，然后单击“启动备份”。
3. 选择“备份类型”和“网络负载”。单击**确定**。

成功备份会显示消息 Session completed successfully 。

使用 Data Protector CLI

执行：

```
omnib -sybase_list backup_specification [-barmode sybase_mode] [options ]
```

参数描述

backup_specification	Data Protector Sybase 备份规范的名称。
sybase_mode	备份类型。在 full 和 trans 之间选择。
options	有关信息，请参阅 omnib 手册页。

示例

要使用备份规范 FullSybase 执行完整备份，请执行:

```
omnib -sybase_list FullSybase -barmode full
```

使用 Sybase 命令

要从数据库所在的客户机启动数据库备份，请使用 Sybase isql 实用程序:

1. 检查要使用的设备是否包含具有足够可用空间的格式化 (初始化) 介质。
2. 验证 Data Protector Sybase 备份规范中的备份选项。
3. 以用户 sybase 身份登录 Sybase Server 系统。
4. 执行 Sybase isql 命令:

```
isql -SSybase_instance -USybase_user -PSybase_password dump \
database database to "ob2syb::backup_specification"
```

参数描述

Sybase_instance	Sybase 实例名称。
Sybase_user	Sybase 实例用户。
Sybase_password	Sybase 实例用户的密码。
database	要备份的数据库的名称。
backup_specification	Data Protector Sybase 备份规范的名称。

检查配置

在已为 Sybase 实例创建至少一个备份规范后，可以检查 Sybase 实例的配置。使用 Data Protector GUI 或 Data Protector CLI。

使用 Data Protector GUI

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，展开“备份规范”，然后展开“Sybase Server”。单击备份规范以显示要检查的 Sybase 实例。
3. 右键单击该实例，然后单击“检查配置”。

使用 Data Protector CLI

执行：

Windows 系统： perl -I..\lib\perl util_sybase.pl -CHKCONF \

Sybase_instance_name

UNIX 系统： util_sybase.pl -CHKCONF Sybase_instance_name

还原 Sybase Server 集成

This feature is available in the Premium Edition

使用 Sybase isql 实用程序还原 Sybase 数据库。

要还原 Sybase 数据库，请执行以下步骤:

1. 还原 Sybase 数据库的完整备份。
2. 还原后续事务备份 (如果存在)。

要在升级 Data Protector 后还原 Sybase 数据库，请执行以下步骤:

1. 重新配置 Sybase 数据库集成。
2. 还原 Sybase 数据库。

本地化的数据库名称

如果备份对象的名称包含无法使用当前语言组 (Windows 系统上) 或代码页 (UNIX 系统上) 显示的字符:

1. 将终端上使用的编码设置为 UTF-8。
2. *Windows 系统：*将环境变量 OB2_CLI_UTF8 设置为 1。
3. 收集信息以进行还原时，将 syb_tool 或 omnidb 命令的输出重定向到文本文件。

   如果需要编辑包含加载命令的文件，请使用不设置第一个字节 ("BOM") 的 UTF-8 感知编辑器，因为 isql 不支持此类文件。请注意，无法使用 Windows 记事本编辑器。

   有关详细信息，请参阅查找信息以进行还原。
4. 还原对象时，将 -i file_name –J utf8 选项添加到 isql 命令，其中 file_name 是具有加载命令的文件。

   有关详细信息，请参阅使用 Sybase isql 命令还原。

查找要还原的信息

要还原损坏的数据库，请首先查找必要的介质以及上次完整备份的会话 ID。如果使用了多个流备份数据库，还要确定流的数量。

使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在内部数据库上下文中，展开“对象”或“会话”。要查看有关会话的详细信息，请右键单击该会话，然后单击“属性”。

使用 Data Protector CLI

使用 Data Protector syb_tool 命令或标准 Data Protector CLI 命令。

使用 Data Protector syb_tool 命令

Data Protector syb_tool 命令会返回还原所需的确切 Sybase load 命令。

syb_tool 命令的语法是：

```
syb_tool databaseSybase_instance -date YYYY/MM/DD.hh:mm:ss [ -new_db new_database ] [ -new_server new_Sybase_instance ] [ -file file ] [ -media ]
```

参数描述

database	要还原的数据库。
Sybase_instance	备份要从中还原数据库的 Sybase 实例。
date	时间点。还原此时间点之后创建的第一个备份版本。使用 0-24h 时间格式。
new_database	要还原到的目标数据库。
new_Sybase_instance	要还原到的目标 Sybase 实例。
file	记录加载命令或命令序列的文件的路径名。
-media	列出还原所需的介质。

要定义事务日志关闭和备份会话开始之间的时间间隔，请设置全局选项 OB2SybaseTransLogDelay 。默认值为 20 秒。

示例 1

要获取从 1999 年 6 月 1 日中午 12.00 之后执行的第一个备份还原 Sybase 实例 audi 的 database1 的 load 命令，并获取必要的介质，请执行:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -media
```

示例 2

要获取从 1999 年 6 月 1 日中午 12.00 之后执行的第一个备份还原 Sybase 实例 sherlock 的 database1 的 load 命令，获取必要的介质，以及将 load 命令记录到文件 c:/tmp/isqlfile (Windows)，请执行:

```
syb_tool database1 sherlock -date 1999/06/01.12:00:00 -file \ c:\tmp\isqlfile -media
```

示例 3

要获取将 database1 从 1999 年 6 月 1 日中午 12.00 之后执行的第一个备份还原到 database2 的 load 命令，请执行:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -new_db database2 \ -media
```

示例 4

要获取将 Sybase 实例 audi 的 database1 还原到 Sybase 实例 toplarna 的 load 命令，请执行:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -new_server toplarna \
-file /tmp/isql -media
```

示例 5

要获取从 1999 年 7 月 7 日下午 14:28 之后执行的第一个备份还原 Sybase 实例 audi 的 database1 的 load 命令，并将 load 命令记录到文件 /tmp/dudule ，请执行:

```
syb_tool database1 audi -date 1999/07/07.14:28:00 -file /tmp/dudule
```

在从多个备份加载事务日志中，您会看到需要还原一个完整备份和四个事务日志备份，最后一个使用并发 3 备份。

使用标准 Data Protector CLI 命令

1. 获取备份的 Sybase 数据库列表:

   omnidb -sybase

2. 获取特定对象的备份会话列表，包括会话 ID:

   omnidb -sybase "object_name"

   > **重要说明**对于对象副本，请使用对象的备份 ID (等于对象的备份会话 ID)。不要使用对象的复制会话 ID。

3. 获取还原所需的介质列表:

   omnidb -session session_id -media

使用 Sybase isql 命令还原

1. 在 UNIX 系统上，以用户 sybase 身份登录 Sybase Server 系统。
2. 运行 Sybase isql 实用程序:

   isql -SSybase_instance -USybase_user -PSybase_password [-i \

   input_file -J utf8]

参数描述

Sybase_instance	Sybase 实例名称。
Sybase_user	Sybase 实例用户。
Sybase_password	Sybase 实例用户的密码。
input_file	保存加载参数的文件。另请参阅本地化的数据库名称。

3. 如果未在文件中提供加载命令，请在第一行中键入所需 load 命令。要执行命令，请在最后一行中键入 go，然后按 **Enter**。

   Sybase load 命令的语法是:

```
load {database|transaction} new_database from "ob2syb::version[::database[::Sybase_instance]]" stripe on
"ob2syb::version[::database[::Sybase_instance]]"
```

参数描述

transaction}	定义是否要还原数据库或事务日志。
version	要从中还原的备份版本的会话 ID。您还可以键入 latest version 以从最新备份还原。
new_database	要还原到的目标数据库。
database	要还原的数据库。
Sybase_instance	备份要从中还原数据库的 Sybase 实例。

仅当还原使用多个流备份的数据库时，才需要 stripe 部分。用于备份的流数量在备份会话期间在 Data Protector Monitor 中显示。

重要说明要将数据库还原到新数据库，请首先创建一个新数据库。新数据库应与要还原的数据库具有相同的结构。

要将数据库还原到另一个客户机系统上的其他 Sybase 实例，请在目标客户机上设置要将数据库还原到另一个客户机系统上的其他 Sybase 实例，请在目标客户机上设置 OB2HOSTNAME 变量: 将 OB2HOSTNAME=BackupClient.company.com 变量条目添加到位于默认 Data Protector 临时文件目录中的 Sybase_TargetInstance.cfg 配置文件。

有关 Sybase load 命令的详细信息，请参阅管理。

提示要列出特定 Sybase 实例的所有 Sybase 数据库，请执行:

Windows 系统： perl -I..\lib\perl util_sybase.pl -OBJS0 \

Sybase_instance_name

UNIX 系统： util_sybase.pl -OBJS0 Sybase_instance_name

还原示例

示例 1

要从备份会话 1999/06/09-2 还原数据库 database2 ，请执行:

```
1>load database database2 from "ob2syb::1999/06/09-2" 2>go
```

示例 2

将最新版本的数据库 Sybdata 还原到名为 Sybdata1 的新数据库:

1. 创建数据库设备。
2. 创建一个名为 Sybdata1 的空数据库。
3. 通过执行以下命令将 Sybdata 还原到 Sybdata1 :

   ```
   1>load database Sybdata1 from "ob2syb::latest version::Sybdata" 2>go
   ```

示例 3

要还原使用三个流备份的最新版本的数据库 database3 ，请执行:

```
1>load database database3 from "ob2syb::latest version" 2>stripe on "ob2syb::latest version" 3>stripe on "ob2syb::latest version" 4>go
```

示例 4

要从实例 "instance1" 开始还原数据库，该实例名称包含 Cyrillic 和 Latin 字符，并且已为其在文件 restore_20100609-2.txt 中保存加载命令，请执行:

```
isql -S instance1 -U admin -PSybase_password -J utf8 -i restore_20100609-2.txt
```

使用其他设备进行还原

您可以使用与用于备份的设备不同的设备进行还原。

在文件中指定新设备:

Windows 系统： Data_Protector_program_data\Config\server\Cell\restoredev

UNIX 系统： /etc/opt/omni/server/cell/restoredev

使用以下格式:

" DEV 1 " " DEV 2 "

其中， DEV 1 是原始设备，而 DEV 2 是新设备。

重要说明使用后删除此文件。

在 Windows 系统上，对此文件使用 Unicode 格式。

isql 实用程序将备份和还原命令 (通过 Data Protector GUI 或 CLI 发出，或者通过 Sybase isql 命令行界面发出) 发送到 Sybase Backup Server，从而在 Sybase 数据库和 Data Protector 介质之间启动数据传输。

虽然 Sybase Backup Server 负责磁盘的读/写操作，但 Data Protector 管理用于备份和还原的设备和介质。

Data Protector CLI 命令

从以下目录执行 Data Protector CLI 命令:

Windows 系统： Data_Protector_home\bin

UNIX 系统：

命令	目录
testbar	opt/omni/bin
omnigetmsg	opt/omni/lbin
util_sybase.pl	

有关其他命令位置，请参阅《Data Protector 命令行界面参考》中的 omniintro 参考页或 omniintro 手册页。

要执行这些命令，您必须具有相应的 Data Protector 用户权限。有关信息，请参阅《Data Protector 帮助》索引: “用户组”和“添加用户”。

如果数据库或数据库实例的名称采用非 ASCII 编码，请将 OB2_CLI_UTF8 环境变量设置为 1 ，以启用 Data Protector Sybase CLI 实用程序的 Unicode 输出。终端应用程序也必须使用 UTF-8 区域设置。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行交互式备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

有关如何监视会话，请参阅《Data Protector 帮助》索引：“查看当前正在运行的会话”。

适用于 H3C CAS 的虚拟环境集成

本主题介绍如何配置和使用适用于 H3C CAS 的 Data Protector 虚拟环境集成。Data Protector 与 H3C CAS 系统集成，以备份和还原虚拟机。

备份

可以使用以下备份方法：

- **H3C CAS 非缓存备份**

在关闭电源 (脱机备份) 或正常使用 (联机备份) 时，此方法使用 H3C CAS REST API 备份虚拟机。它是一种暂存备份方法，其中备份主机充当执行备份的暂存区域。

- **H3C CAS 缓存备份方法**

此方法还使用 H3C CAS REST API 和 CVD-SDK 进行磁盘操作。使用此方法，磁盘可以直接备份到目标设备，而无需暂存路径或备份主机。此方法目前仅在 Linux 平台上受支持。

还原

虚拟机可以还原:

- **到原始 H3C CAS 管理服务器**
  使用此选项可将虚拟机直接还原到 CAS 管理服务器。
- **到指定的 H3C CAS 服务器**
  使用此选项可将虚拟机还原到其他 CAS 服务器。
- **到目录**
  使用此选项可将备份的文件还原到安装了 VEPA 组件的所需暂存目录。

建议

Micro Focus 建议不要在 H3C CAS 管理服务器或 H3C CAS 服务器上安装任何 Data Protector 组件。

先决条件:

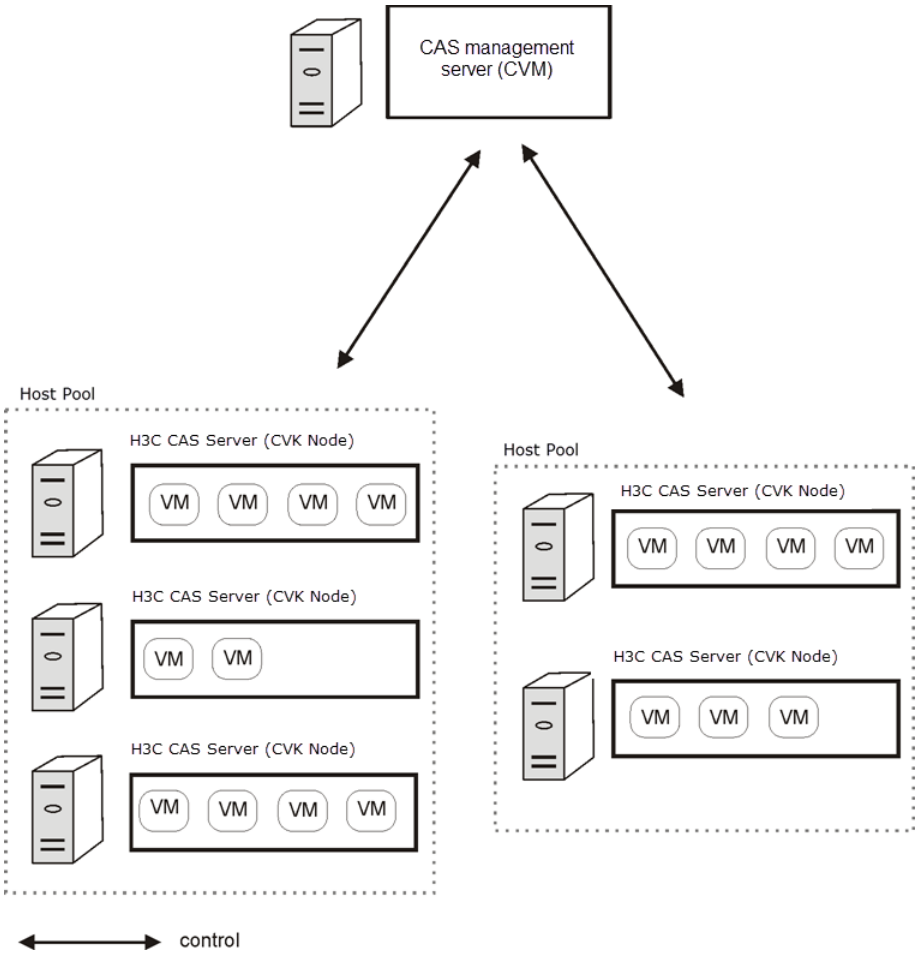
- 在 Windows 操作系统上，为具有相应 H3C CAS 的用户配置 Data Protector Inet 服务用户模拟，以便运行备份和还原。应将该用户添加到 Data Protector 用户列表中。
- 对于非缓存备份，应创建暂存区 (FTP/SCP)。

集成概念

Data Protector 支持 H3C CAS 环境，其他 CAS 服务器由 CAS 管理服务器进行管理。CAS 管理服务器是运行 Tomcat Web 服务器的物理机。

在 H3C CAS 环境中，Data Protector 通过 REST API 与 CAS 管理服务器通信。所有备份和还原请求均在此处发送。

H3C CAS 环境



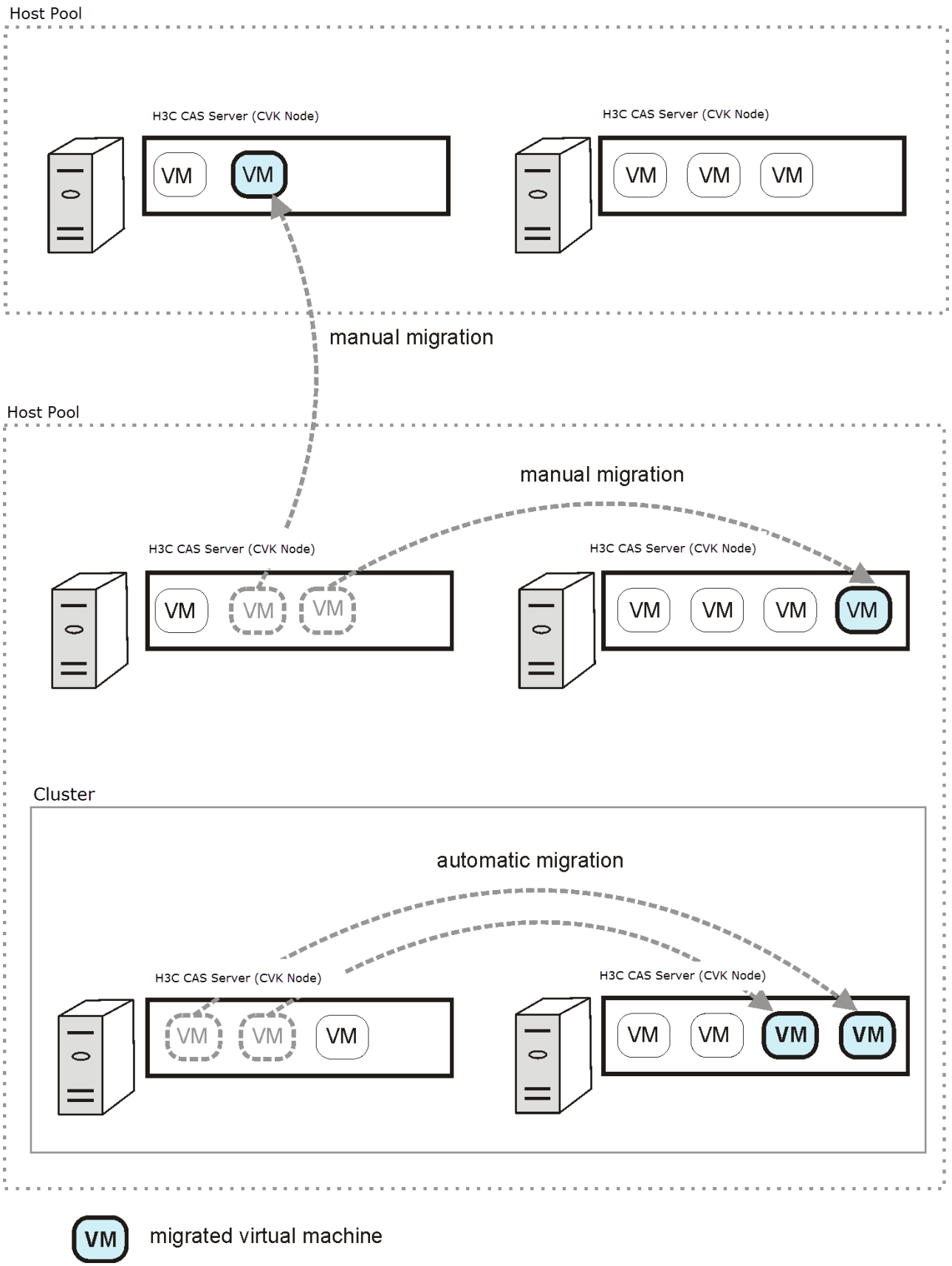
H3C CAS 环境

H3C CAS 环境	描述
H3C CAS 管理服务器	它是一个云管理平台。也被称为 CVM 节点。
CAS 服务器	CAS 平台能够托管多个虚拟机。它被称为 CVK 节点。
VM	虚拟机。虚拟化 x86 或 x64 PC 环境，在其中可以运行来宾操作系统和相关的应用程序软件。
主机池	对一个或多个托管虚拟机的 CVK 服务器进行分组的逻辑容器。

迁移虚拟机

在 H3C CAS 环境中，Data Protector 支持:

- 在主机池之间迁移虚拟机
- 在主机池的不同服务器之间迁移虚拟机。



如果将虚拟机迁移到不同的主机池，则必须创建新的备份规范才能成功备份。Data Protector 将自动查找迁移的虚拟机并进行备份 (如果在同一主机池中迁移)。

安装 H3C CAS 客户机

应在备份主机上安装以下 Data Protector 组件，以启用适用于 H3C CAS 环境的虚拟环境集成:

- Data Protector Virtual Environment Integration (VEAgent)
- Data Protector Disk Agent

配置 H3C CAS 集成

按如下所示配置集成:

- 将 H3C CAS 客户机导入 Data Protector 单元。
- 配置要备份的虚拟机。

以下先决条件适用:

- 确保已正确安装和配置 H3C CAS 环境。
- 确保已为用于连接到 H3C CAS 服务器的用户帐户授予必要的特权。
- 确保已正确安装 Data Protector。
- 确保环境中至少有一个客户机安装了“虚拟环境集成”组件 (备份系统)。
- 确保已正确配置 FTP 或 SCP，使其对暂存路径具有适当的读写特权。

开始之前:

- 配置要与 Data Protector 配合使用的设备和介质。

> **注意**在 *Data Protector Express* 中，按每个单元计算套接字许可证。可以将客户机 (vCenter/ESX/H3C CAS 服务器) 同时导入多个单元，并为每个单元中的每个客户机导入计算套接字许可证。

将客户机导入 Data Protector 单元:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“Data Protector 单元”，右键单击“客户机”，然后选择“导入客户机”。
3. 在“导入客户机”页中，在“名称”选项中输入客户机名称或 IP 地址。
4. 从“类型”下拉列表中选择适当的客户机类型 (**H3C CAS**)，然后单击“下一步”。
5. 选择“标准安全”以手动指定 Data Protector 应用于连接到 H3C CAS 管理服务器的登录凭据:

   端口: 指定 H3C CAS 正在使用的端口。默认情况下，H3C CAS 使用端口 8443。

   用户名：指定具有执行虚拟机备份和还原的适当权限的 CAS 管理服务器用户帐户。

   密码: 指定用户的密码。
6. 选择“下一步”。仅当使用的许可证类型为 *Data Protector Express* 时，此选项才可用。否则，该选项将灰显。

   如果是 **Data Protector Express**，则会列出选定 H3C CAS 管理中的 H3C CAS 服务器，以及主机名、主机套接字和主机 UUID 信息。
7. 选择要许可的 H3C CAS 服务器，然后选择“完成”。

   选定服务器将获得许可。

   要添加或回收许可证，请重新导入 vCenter 客户机。在这种情况下，未获得许可的 H3C CAS 服务器与已获得许可的 H3C CAS 服务器一起列出。

   - 要回收，请取消选择 H3C CAS 服务器并选择“完成”以取消许可 H3C CAS 服务器。
   - 要添加，请选择新服务器，然后选择“完成”以许可 H3C CAS 服务器。

更改 H3C CAS 客户机的配置

当您更新用于连接到 H3C CAS 客户机的凭据时，您实际上会更新驻留在 Data Protector Cell Manager 上的 cell_info 文件。因此，仅当您拥有 Data Protector“客户机配置” 用户权限时，才能更改登录凭据。

要更新凭据，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

您可以在两个不同的位置更新凭据: 在客户机中或备份上下文中。

客户机上下文

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“客户机”，然后选择要更改其登录凭据的客户机。
3. 在“结果区域”中，单击“登录”选项卡。
4. 更新凭据，然后单击“应用”。

备份上下文

假定要更改其登录凭据的 H3C CAS 客户机的备份规范已存在。

1. 在上下文列表中，单击**备份**。
2. 打开要更改其登录凭据的 H3C CAS 客户机的备份规范。
3. 在“源”页面中，右键单击顶部的客户机，然后选择“配置”。
4. 在“配置虚拟环境”对话框中，更新值并单击“确定”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   H3C CAS 服务器客户机

   ```
   vepa_util.exe command --config --virtual-environment h3ccas --host h3ccasClient --security-model 0 --username Username --password Password | --encoded-password Password} --port 8443
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

检查 H3C CAS 客户机的配置

在配置检查期间，Data Protector 尝试使用 Data Protector Cell Manager 上的 cell_info 文件中的登录凭据连接到 H3C CAS 客户机。

要验证连接，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在为 H3C CAS 客户机创建至少一个备份规范后，您可以验证与此客户机的连接。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。单击要检查的 H3C CAS 客户机的备份规范。
3. 在“源”页面中，右键单击 H3C CAS 客户机，然后选择“检查配置”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。

2. 执行：

   H3C CAS 客户机

   ```
   vepa_util.exe command --check-config --virtual-environment h3ccas --host h3ccasClient
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

配置虚拟机

配置虚拟机意味着指定应如何备份虚拟机。

您可以指定以下内容:

- 应用于主机池中的所有虚拟机的*常用设置*。

所有这些设置都保存在 Cell Manager 上的特定于主机池的文件 H3CCAS_Management_Server%HostPoolPath 中。该文件用于使用此主机池的任何备份规范的所有备份会话。

当您分别为特定主机池或所有主机池创建或更新备份规范时，将创建或更新文件 H3CCAS_Management_Server%HostPoolPath 。

要配置虚拟机，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在创建或修改备份规范时，您可以配置虚拟机。在备份规范的“源”页面中，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。

在“设置”页面的“配置虚拟机”对话框中，指定以下设置:

虚拟机设置

可用选项	描述/操作
选择是否要指定常用虚拟机设置 (“常用 VM 设置”) 或特定虚拟机的设置。特定于虚拟机的设置会覆盖常用虚拟机设置。	
配置虚拟机	
使用所选 VM 的常用设置	仅当选择虚拟机时可用。 如果希望常用设置应用于所选虚拟机，请选择此选项。 默认：选择
使用默认设置	仅在选择“常用 VM 设置”时可用。选择此选项可设置常用虚拟机设置的默认值。默认：选择
启用更改后的块跟踪	为选定的虚拟机启用 H3C CAS 更改后的块跟踪功能。如果 CAS 版本支持 CBT 备份，此操作将触发 CBT 备份。 默认: 选定并灰显
isCompress	REST API 可使用此值启用或禁用压缩下载的虚拟机。
备份模式	**SCP:** Linux 系统上的默认备份模式。它在 Windows 系统上不受支持。 **FTP:** Windows 系统上的默认备份模式。在 Linux 系统上也受支持。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

```
vepa_util.exe command --configvm --host h3ccasClient --virtual-environment h3ccas --instance /HostpoolInstance --vm-list vm=
({path='/cluster1/cvknode116/linux_vm(GUID:523650a0-8bb7-4a64-97e0-ab82792351fb)';uuid='523650a0-8bb7-4a64-97e0-
ab82792351fb';useCt=1;mode='SCP';useCompression=1;}) ...
```

通过使用 --vm-list vm 选项列出虚拟机，可以配置多个虚拟机。

使用 omnirc 选项自定义 Data Protector 行为

omnirc 选项可用于对影响 Data Protector 客户机行为的其他设置进行故障诊断或覆盖。适用于虚拟环境集成的选项带有前缀 OB2_H3CCAS 。有关如何使用 Data Protector omnirc 选项的详细信息，请参阅 CLI 参考。

备份 H3C CAS 集成

本节包含备份虚拟机所需的过程。

备份概念

通过使用适用于 H3C CAS 的 Data Protector 虚拟环境集成，可以采用以下两种备份方法备份虚拟机：

- H3C CAS 非缓存备份方法
- H3C CAS 缓存备份方法

H3C CAS 非缓存备份方法

Data Protector 虚拟环境集成提供的 H3C CAS 非缓存备份方法基于 CAS 提供的 REST API。在此方法中，使用单个中央备份主机备份 Data Protector 单元中的 CAS 服务器系统托管的所有虚拟机。此备份主机可以是专用物理主机、虚拟机或 Cell Manager。它安装了 Data Protector 虚拟环境集成组件 (VEAgent)。

在 H3C 映像的非缓存备份期间，VEAgent 首先在备份主机和虚拟化主机 (CAS 管理服务器) 之间建立连接。

然后请求使用 REST API 进行备份，以便将虚拟机文件下载到暂存路径 (FTP/SCP 根目录)。在创建备份规范时指定暂存路径。VEAgent 打开从暂存路径下载的虚拟机文件，初始化介质代理客户机并控制虚拟机及其所有关联数据的传输。

H3C CAS 缓存备份方法

此方法还使用 H3C CAS REST API，但与 CVD-SDK 一起用于磁盘操作，从而使备份性能更快。使用此方法，磁盘可以直接备份到目标设备，而无需暂存路径或备份主机。

备份类型

要执行的备份类型在备份规范级别，在“调度程序”页面中或在“启动备份”对话框中 (对于交互式备份) 指定。

备份类型	功能
完整	备份完整虚拟机。
增量	备份自上一次完整备份、增量备份或差异备份以来对虚拟机所做的更改。对于非缓存备份，第一次增量备份包含完整数据。
差异	备份自上一次完整备份以来对虚拟机所做的更改。对于非缓存备份，第一次差异备份包含完整数据。

对于增量备份或差异备份会话，还必须指定 Data Protector 应如何识别磁盘块级别的更改。H3C CAS 提供三种备份更改方式。

1. **更改后的块跟踪 (CBT)**: 使用此方法，H3C CAS 可以在指定的时间点后跟踪虚拟机磁盘的更改，并使磁盘增量备份变得简单高效。它可以缩短备份时间并降低系统计算资源消耗。CBT 备份仅在以下虚拟机上受支持: 装有在 CAS E0525 及更高版本中以智能 (qcow2) 格式创建的单级镜像磁盘。
2. **非更改块跟踪 (非 CBT)**: 使用此方法，H3C CAS 不会利用 CBT 技术跟踪修改后的块。这是默认行为。要更改为 CBT，请参考 VM 配置。有关详细信息，请参阅配置虚拟机。
3. **CBT 跟踪器 (CBTer)**: CAS 平台使用 CBTer 来跟踪虚拟磁盘数据块中的更改。此功能仅用于缓存备份方法。它使您能够获取增量或差异块信息。

> **注意**对于非缓存备份 (暂存备份)，如果使用 CBT 方法，则仅支持“完整”和“增量”备份 (CAS 版本 V5.0 (E0526))。如果使用非 CBT 方法，则支持所有备份类型 (“完整”、“增量”、“差异”)。
>
> 在缓存备份方法中，支持所有上述备份类型。

备份注意事项

- 要将文件下载到暂存区域，H3C CAS API 支持 **SCP** 或 **FTP** 传输协议。
- 在 Linux 上，**SCP** 和 **FTP** 均受支持。
  默认值：SCP。
- 在 Windows 上，仅 **FTP** 受支持。
- 在 Linux 上，使用 OB2_H3CCAS_TRANSFER_MODE=0 (ftp), 1(SCP) 更改为 FTP 模式。也可以从 UI 中选择“VM 配置”来更改此模式。有关详细信息，请参阅配置虚拟机。
- 无法备份处于 '未知状态' 的虚拟机。
- 要备份虚拟机，下载虚拟机文件所在的备份主机上的暂存区域中必须有足够的磁盘空间。
- 并发备份会话:
  - 使用相同设备的备份会话无法并行运行。
  - 备份 REST API 由 H3C CAS 服务器按顺序执行。如果在单个备份会话中考虑多个虚拟机，可能会出现 BSM 或 MA 超时。
    默认情况下，MA 空闲超时时间设置为 1 小时。这可以使用 Data Protector 全局变量 BackupDeviceIdle 来更改。
- H3C CAS 备份 API 需要使用 IPv4 作为远程或备份主机地址。不支持 IPv6。
- 对于非缓存备份，建议不要在备份主机上使用多个 FTP 配置。在这种情况下，使用第一个 FTP 配置。
- 缓存备份仅支持格式化的 qcow2 磁盘格式。
- 使用 H3C CAS 缓存备份方法，您可以为每个 VM 一次备份多达 16 个单独的磁盘。

- 使用 H3C CAS 缓存备份方法，您可以选择一个 VM 并排除您不想备份的单个磁盘。您还可以展开 VM，并仅选择要备份的单个磁盘。
- 确保磁盘名称是唯一的，因为单个磁盘不使用唯一 UUID 进行标识，而是使用磁盘名称来标识。

以下限制适用：

1. 在任何主机池或虚拟机的名称中只能使用受支持的字符。
   - 中文字符
   - 字母
   - 数字
   - 连字符 (-)
   - 下划线 (_)
   - 句点
   - 空格
2. 主机池和虚拟机的名称不能只包含空格或只包含数字。
3. 不支持重新启动失败的备份对象。

创建备份规范

使用 Data Protector GUI 创建备份规范。

单击“下一步”。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择“本地或网络备份”作为备份类型。有关选项的说明，请按 **F1**。单击**确定**。
4. 指定要备份的应用程序:
   - 在“客户机”下拉列表中，选择 H3C CAS 客户机。

     > **注意**下拉列表包含作为 H3C CAS 客户机导入 Data Protector 的所有客户机。这些客户机名称的末尾附加了相应的标签，例如 *(H3C CAS)*。

     如果未正确配置所选 H3C CAS 客户机，则会显示一条警告。单击“确定”打开“配置虚拟环境”对话框，并提供连接参数。
   - 在“备份主机”下拉列表中，选择要用于控制备份的 H3C CAS 系统。该列表包含安装了“虚拟环境集成”组件的所有客户机。
   - 在“备份方法”中，选择“H3C CAS 非缓存”来执行非缓存备份，或者选择“H3C CAS 缓存”来执行缓存备份。
   - 在“主机池”中，选择要从中进行备份的主机池。
   - 如果使用非缓存备份方法，请指定备份主机暂存详细信息。支持的协议为 SCP 或 FTP。
     - 用户名: 指定在备份主机上配置的 SCP 或 FTP 用户名。指定的用户应具有执行虚拟机备份和还原的适当权限。
     - 密码：指定用户的密码。
     - 暂存路径: 暂存路径是指备份主机上配置的 FTP 或 SCP 绝对路径。

     单击“下一步”。

     > **注意**对于非缓存备份，暂存用户名和密码保存在 cell_info 文件中。运行 vepa_util 命令可更新暂存用户名和密码。重新创建新的备份规范，以便对暂存路径进行更改。可以为每个备份规范配置暂存路径。可以为每个备份规范配置暂存路径。

     单击**确定**。
5. 选择要备份的对象。虚拟机按“主机和群集”视图列出。可以将视图模式更改为“VM 和模板”以查看整个“虚拟机”列表，您可从中选择多个虚拟机进行备份。

   对于缓存备份，您可以选择备份单个磁盘。您可以展开每个 VM 并直接选择要备份的磁盘，也可以选择一个 VM，展开它，然后排除该 VM 下不需要备份的磁盘。对于后者，所选 VM 中任何新添加的磁盘也将包含在备份中。
6. 如果您的虚拟机尚未配置，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。有关详细信息，请参见配置虚拟机。

   单击“下一步”。
7. 选择用于备份的设备。

   要指定设备选项，请右键单击设备，然后选择“属性”。在“并发”选项卡中指定并行备份流的数量以及要使用的介质池。

   单击“下一步”。
8. 设置备份选项。

9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后计划备份规范。
10. 单击“启动备份”以启动备份会话。

视图模式选项

Data Protector 有两个呈现虚拟机详细信息的视图模式选项。

主机和群集

在此视图模式下，可以查看整个主机和群集树结构，您可从中选择多个磁盘 (缓存备份)、虚拟机、整个主机或整个群集进行备份。它根据所选主机池显示所有结构化详细信息。

使用 Data Protector CLI

使用 CLI 执行以下 vepa_util 命令，获取主机池对象的视图模式数据，其中包含类型、路径、名称和 UUID 格式:

```
vepa_util.exe browse --virtual-environment h3ccas --host <CAS_server_IP> --root-node <Host_Pool_name> --inventory-view hosts_and_clusters
```

VM 和模板

在此视图模式下，可以查看整个“虚拟机”列表，您可从中选择多个虚拟机进行备份。在此视图模式下，不会列出模板。

使用 Data Protector CLI

使用 CLI 执行以下 vepa_util 命令，获取主机池对象的视图模式数据，其中包含类型、路径、名称和 UUID 格式:

```
vepa_util.exe browse --virtual-environment h3ccas --host <CAS_server_IP> --root-node <Host_Pool_name> --inventory-view vms_and_templates
```

在设置备份规范后，可以使用这些视图模式选项修改现有规范中的虚拟机条目。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

> **注意**一段时间不活动后，防火墙会关闭 BSM 和 Inet 之间的连接。因此，建议在客户机上的 omnirc 文件中进行以下设置，以启用 keepalive 包，保持连接处于活动状态:
>
> - OB2IPCKEEPALIVE = 1
> - OB2IPCKEEPALIVETIME = 600
> - OB2IPCKEEPALIVEINTERVAL = 600
>
> 虽然在所有系统上都遵守 OB2IPCKEEPALIVE ，但某些系统可能不支持由 OB2IPCKEEPALIVETIME 和 OB2IPCKEEPALIVEINTERVAL 定义的按套接字的保持活动设置。
>
> Windows、Linux 系统: 支持 OB2IPCKEEPALIVE 和 OB2IPCKEEPALIVEINTERVAL 。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

执行以下步骤以使用 Data Protector GUI 预览备份会话:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要预览的备份规范，然后选择“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

执行以下命令以使用 Data Protector CLI 预览备份:

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。

2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   omnib -veagent_list BackupSpecificationName -test_bar

预览期间会发生什么?

在预览期间执行以下测试：

- 备份主机与 Data Protector 之间的通信
- 备份规范的语法
- 设备的规范
- 设备中的介质
- 如果是缓存备份，它将检查可用体系结构是否支持缓存备份
- 检查添加的 DP 精简版许可证是否有效

启动备份会话

交互式备份按需运行。它们对于执行紧急备份或重新启动失败的备份非常有用。

要以交互方式启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要使用的备份规范，然后选择“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   omnib -veagent_list BackupSpecificationName [-barmode VirtualEnvironmentMode][ListOptions]

   其中， VirtualEnvironmentMode 是以下备份类型之一:

   full | diff | incr 默认为 full 。

   有关 ListOptions ，请参阅 omnib 手册页或《Data Protector 命令行界面参考》。

   示例

   要使用备份规范 MyVirtualMachines 启动完整备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode full

   要使用同一备份规范启动差异备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode diff

更改后的块跟踪

更改后的块跟踪 (CBT) 是 H3C CAS 版本 5.0 (E0526H02) 及更高版本的一项功能，可用于提高备份效率和速度。首次启用更改后的块跟踪时，虚拟机的下一个备份将始终为完整备份，以便为跟踪提供参考点。即，启动一个新的备份链。您可以将此功能用于非缓存备份。

执行还原会话时，CBT 备份链 (完整、差异、增量) 会被破坏。还原会话完成后，再次运行完整备份以启动新的备份链，否则后续增量备份和差异备份会话都将回退到完整备份。

> **注意**使用更改后的块跟踪时，请注意以下几点:
>
> - 使用 CBT 备份时，请确保符合 H3C CAS 的先决条件。
> - 仅格式化的 QCOW (智能磁盘) 磁盘格式支持更改后的块跟踪。如果磁盘不受支持，则虚拟机备份将失败。即使使用 CBT 跟踪器备份也是如此。
> - CBT 不支持非缓存差异备份。

非更改块跟踪（非 CBT）备份

非更改块跟踪 (非 CBT) 备份是一种不依赖于要备份的块级更改的功能。此功能不使用 CBT 功能来识别要备份的修改后的块。

CBT 跟踪器

CAS 平台使用已更改的块跟踪器 (CBTer) 来跟踪虚拟磁盘数据块中的更改。此功能仅用于缓存备份方法。它使您能够获取增量或差异块信息。

备份链

按顺序执行的一系列备份 (完整、增量、差异) 被称为备份链。备份链的概念适用于 VM 级别和单个磁盘级别的备份 (缓存备份)。

使用非缓存方法，出现以下情况时，备份链会断开:

- 备份方法发生更改 (CBT 或非 CBT)
- 备份主机发生更改
- 同一备份主机上的 FTP 目录或会话目录发生更改
- 与之前的备份相比，虚拟机的磁盘数发生更改

当备份链断开时，将回退到完整备份。

下表汇总了一些备份链方案:

备份类型	备份主机	备份模式	结果
完整	-	CBT	完整 CBT 备份
完整	-	非 CBT	完整非 CBT 备份
增量	备份主机 1	CBT	完整 CBT 备份
增量	备份主机 1	CBT	后续增量 CBT 备份
增量	备份主机 2	CBT	由于备份主机已从上次备份进行更改，因此将回退到完整备份。
增量	备份主机 2	非 CBT	即使备份主机相同，备份模式也会从 CBT 更改为非 CBT。回退到完整备份。
差异	-	CBT	不受支持
差异	备份主机 1	非 CBT	第一次差异非 CBT 备份
差异	备份主机 1	非 CBT	后续差异非 CBT 备份
差异	备份主机 2	非 CBT	由于备份主机已从上次备份进行更改，因此将回退到完整备份。

下表汇总了单个磁盘的一些备份链方案:

Barlist	磁盘	备份类型	结果
Barlist 1	磁盘 1	完整	完整备份
Barlist 2	磁盘 2	完整	完整备份
Barlist 3	磁盘 1、磁盘 3	增量	增量备份回退到完整备份，因为磁盘 3 的第一次备份不是完整备份。
Barlist 3 (已修改)	磁盘 1、 磁盘 2	增量	增量备份，因为您已经执行了磁盘 1 和磁盘 2 的完整备份。
Barlist 4	磁盘 5	增量	增量备份回退到完整备份，因为磁盘 5 的第一次备份不是完整备份。

单个磁盘备份

通过单个磁盘备份，您可以选择仅选择和备份 VM 下所需的磁盘。此选项仅用于缓存备份方法。您可以展开每个 VM 并直接选择要备份的磁盘，也可以选择一个 VM，展开它，然后排除该 VM 下不需要备份的磁盘。对于后者，所选 VM 中任何新添加的磁盘也将包含在备份中。

还原 H3C CAS 集成

本节包含还原虚拟机所需的过程。

还原概念

还原期间，在备份主机上运行的 VEAgent 与 CAS 管理服务器建立连接并执行还原 REST API，以便将虚拟机相应地还原到 CAS 服务器。

请考虑以下限制和注意事项:

非缓存方法:

对于早于 V5.0 (E0526H02) 的 H3C CAS 版本:

1. 由于 API 限制，无法从不同的备份主机进行还原。还原需要备份期间使用的备份主机。
2. 如果虚拟机磁盘配置在备份完成之后发生了更改 (例如，删除备份磁盘)，则无法进行还原。
3. 还原期间，虚拟机应该在 CAS 服务器中可用和可访问。
4. 还原期间，不得拥有两个或更多同名虚拟机。

对于 H3C CAS V5.0 (E0526H02) 及更高版本:

1. 要还原到其他 CAS 服务器，两个 CAS 服务器都应该运行 V5.0 (E0526H02) 或更高版本。
2. 在 V5.0 (E0526H02) 及更高版本中进行的虚拟机 CBT 备份无法还原到版本低于 V5.0 (E0526H02) 的 CAS 服务器，因为 CBT 备份在低于 V5.0 (E0526H02) 的版本中不受支持。
3. 在低于 V5.0 (E0526H02) 的版本中备份的虚拟机无法还原到高于 V5.0 (E0526H02) 的 CAS 服务器。新的 H3C CAS 还原 API 需要更多在 Data Protector (2018.11、2019.02) 的早期版本中不可用的信息。
4. H3C CAS 版本 E550 不支持非缓存备份。

缓存方法:

1. 只有 H3C CAS E550 和更高版本支持 CBTer。
2. 将单个磁盘还原到原始 VM 时，VM 在还原过程中会关闭电源。如果您要还原到另一个 VM，则情况并非如此。
3. 如果您在“源”选项卡中选择 VM 级别和磁盘级别的对象，则只会显示磁盘级别对象的“选项”选项卡。
4. 如果您选择单个磁盘对象进行还原，则“目标” 选项卡中的“虚拟机” 下拉列表将仅显示与所选对象的操作系统兼容的 VM。但是，如果您选择多个对象，则此下拉列表不会根据对象的操作系统进行过滤，而是列出所有可用的 VM。
5. “还原为” 选项在单个磁盘还原的情况下不可用。
6. 基于 Windows 的 VM 磁盘无法还原到基于 Linux 的 VM。
7. VM 还原的还原链和单个磁盘还原的还原链是相互独立的。它们不能组合以创建单个还原链。
8. 对于单个磁盘还原，“还原前删除” 和“跳过” 选项仅适用于还原到原始位置。
9. 单个磁盘的还原会清理现有快照。
10. “还原后删除” 选项仅适用于单个磁盘还原，不适用于 VM 级还原。
11. 对于单个磁盘备份和还原，磁盘没有用于标识的 UUID。磁盘路径将用于备份和还原。确保磁盘名称唯一。
12. 还原后，磁盘名称会随时间戳更改。例如，您还原名为 "disk1" 的磁盘。还原后，磁盘名称修改为 "disk1_timestamp"。 您必须修改备份规范以包含新磁盘名称。如果未修改，下次运行备份规范时，将不会备份该磁盘。
13. 每次还原时，磁盘名称的长度都会不断增加。例如，您还原名为 "disk1" 的磁盘。还原后，磁盘名称修改为 "disk1_timestamp"。每次还原该磁盘时，都会在其名称中添加一个新的时间戳 (disk1_timestamp_timestamp1..)。

查找要还原的信息

您可以在 Data Protector IDB 中找到有关备份对象的信息，如所使用的备份类型和介质，以及备份期间显示的消息。要检索此信息，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在“内部数据库”上下文中，展开“对象”或“会话”。

如果展开“对象”，则会根据为其创建备份对象的虚拟机对这些对象进行排序。例如：

- 在 H3C CAS 管理服务器环境中，虚拟机 vm_mach1 的备份对象在 /10/CAS_management_server%2FvmInstanceUUID 下列出。

  其中，

  H3C_management_server 是 H3C CAS 管理服务器的名称。

  vmInstanceUUID 是 H3C CAS 服务器上的虚拟机 vm_mach1 的唯一标识符。

  要在 H3C CAS 环境中查看会话，请双击 /object1/CAS_management_server%2FvmInstanceUUID 。

如果展开“会话”，则会根据在其中创建备份对象的会话对这些对象进行排序。

要查看有关备份对象的详细信息，请右键单击备份对象，然后选择“属性”。

提示要查看会话期间显示的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnidb 命令所在的目录。
3. 获取在备份会话中创建的会话 ID 为 *SessionID* 的 H3C CAS 备份对象列表:

   ```
   omnidb -session SessionID
   ```

4. 获取有关备份对象名称为 *BackupObjectName* 的备份对象的详细信息:

   ```
   omnidb -veagent BackupObjectName -session SessionID -catalog
   ```

使用 Data Protector GUI 进行还原

使用此过程还原、启动和实时迁移虚拟机。

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“虚拟环境”，展开相关客户机，然后单击从中备份的主机池。
3. 在“源”页面中，指定以下项:
   1. 从“备份方法”下拉列表中，选择以下任一备份方法:
      - **H3C CAS 非缓存** - 显示使用非缓存方法备份的对象
      - **H3C CAS 缓存** - 显示使用缓存方法备份的对象。
   2. 通过“从”和“到”下拉列表，您可以将显示的虚拟机范围缩小到在指定时间间隔内备份的虚拟机。
   3. 在“VM 过滤器”文本框中，输入 VM 的过滤器文本，然后按 Enter 键，或单击“应用过滤器”。过滤器会隐藏与过滤器模式不匹配的 VM，使您能够轻松找到所需对象。
   4. 选择 H3C CAS 对象后，您可以选择“还原”它们。

      选择要还原的对象。您可以选择多个要并行还原的虚拟机。在缓存备份的情况下，您可以选择多个单个磁盘进行还原。展开 VM，选择要还原的磁盘。如果您选择 VM，则该 VM 下的所有磁盘也将被选择。您可以展开 VM，排除不想还原的磁盘。

      还原所选备份版本

      右键单击所选虚拟机，然后单击“还原版本”以选择要还原的备份版本。

      将打开一个新的对话框以选择备份版本。在“备份版本”下拉列表中，选择要还原的备份版本。默认情况下，将选择最新备份版本。单击**确定**。

      单个磁盘还原不支持此选项。
   5. **还原为新虚拟机**

      右键单击所选虚拟机，然后单击“还原为/还原至”，以将其还原为新虚拟机。此时将打开一个新对话框以指定虚拟机的新名称。

   注意
   - Data Protector 会还原每个选定 H3C CAS 对象的完整还原链，以上一个完整备份会话开头 (即使该完整备份超出指定时间间隔)，并以在指定时间间隔内执行的上一个备份会话结尾。
   - 对于单个磁盘还原，还原到原始或其他 VM 后，可能会出现以下问题。完成以下步骤以继续:
     - 还原的磁盘脱机
       对于 Windows VM，连接到来宾操作系统，转到“磁盘管理” ，然后使磁盘重新联机。
       对于 Linux VM，由于分区编号更改，VM 必须断电再通电。在 VM 通电后尝试装载分区，使用 fdisk -ll 检查设备分区，然后使用 mount 命令将磁盘装载到本地文件夹。
     - 还原的 VM 无法引导
       还原操作系统磁盘时，如果 Linux 来宾 VM 无法引导，则引导顺序可能发生了变化。从 CAS 控制台连接到 VM 并更改引导顺序。将 VM 断电，转到“修改” ->“更多” ->“引导设备” 。将操作系统设备移至顺序顶部，然后为 VM 通电。
4. 在“目标”页中，根据单元配置中的信息选择备份主机。还原过程应该使用相同的备份主机。

   有关此页中各选项的更多详细信息，请参阅下面的“还原目标”表。
5. 在“选项”页中，指定 H3C CAS 还原选项。

   有关此页中各选项的更多详细信息，请参阅下面的“还原选项”表。
6. 在“设备”页中，选择要用于还原的设备。

7. 单击**还原**。
8. 在“启动还原会话”对话框中，单击“下一步”。
9. 指定“报告级别”和“网络负载”。

   注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
10. 单击**完成**启动还原。

    会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

还原目标

GUI/CLI 选项	描述
备份主机/ -barhost	根据单元配置中的信息选择备份主机。还原过程应该使用相同的备份主机。
还原客户机/ -apphost	指定所选虚拟机应还原到的客户机。默认情况下，会选择从中备份虚拟机的客户机。 您可以从下拉列表中选择新的还原客户机，以还原到新的 CAS 服务器。
还原到主机池/ –instance –newinstance	选择此选项可将虚拟机还原到主机池。默认情况下，将虚拟机还原到原始主机池。
主机/群集/ -host_cluster	选择应将虚拟机还原到的主机或群集。您可以选择不属于群集的主机。您可以选择还原到原始 CAS 服务器中的其他主机，或者还原到其他 CAS 服务器。
特定主机/ -specificHost	选择应将虚拟机还原到的群集中的特定主机。如果已从“主机/群集”下拉列表中选择不属于群集的主机，则该主机将被填充到“特定主机”下拉列表中。
数据存储/存储池/ -store	选择应将虚拟机还原到的存储池。您可以从可从所选还原目标主机访问的所有存储池中进行选择。如果将此选项保留为空，则会将虚拟机还原到原始存储池。
虚拟机/ -vm	此选项仅适用于使用缓存方法的单个磁盘还原。仅在 Data Protector 11.0 版及更高版本中支持此选项。 选择要将所选对象还原到的虚拟机。此选项在缓存还原的情况下可用。此下拉列表中列出的 VM 由您要还原的对象的操作系统确定。如果对象是 Windows 操作系统，则此处仅列出 Windows VM。 如果您选择多个对象进行还原，则情况并非如此。在这种情况下，此下拉列表中将显示所有 VM，而不仅仅显示与所选对象的操作系统兼容的 VM。
还原到目录/ –directory	选择此选项可将虚拟机文件还原到备份主机上的目录中 (主机池外部)。可以使用“浏览”按钮查找目标目录。

还原选项

GUI/CLI 选项	描述	
现有虚拟机处理	指定 Data Protector 在还原现有虚拟机时的行为。	
	还原前删除/ -deletebefore	选择此选项可在还原之前删除现有虚拟机，然后从新虚拟机将其还原。即使现有虚拟机驻留在目标主机池之外的主机池，也依然会被删除。此选项对 H3C CAS 的更高版本 (E0526) 有效。 这是提高空间利用率的选项，但是并不安全，因为如果还原失败，旧虚拟机便无法使用，因此请谨慎选择。
	还原后删除/ -deleteafter	选择此选项以在还原之后删除现有虚拟机，即使虚拟机驻留在除您的目标数据中心之外的其他数据中心。如果恢复失败，现有虚拟机不会被删除。H3C CAS VM 还原不支持此功能，但使用缓存方法的 H3C CAS 单个磁盘还原支持此功能。
	跳过还原/ -skip	选择此选项可跳过对现有虚拟机的还原。这样可以还原缺少的虚拟机而不会影响现有的虚拟机。

使用 Data Protector CLI 进行还原

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnir 命令所在的目录。
   1. 执行：

H3C CAS 服务器客户机上的 H3C CAS 管理服务器

```
omnir -veagent -virtual–environment h3ccas -barhost BackupHost -apphost Originalh3ccasClient
```

```
-instance OriginalHostPool -method [h3ccasImage -non-cached | h3ccasImage -cached] [-session BackupID] VirtualMachine [VirtualMachine...] VirtualMachine -vm VMPath -instanceUUID vmInstanceUUID -disk DiskName H3C CAS Client [- newinstance TargetHostpool] [- store TargetStoragePool]  [- targetVM TargetVM ] [- destination TargetH3CCASClient] [- host_cluster HostCluster] [- specificHost SpecificHost] [- new_name NewVMName] [- register] [- poweron] [- deletebefore |- deleteafter |- skip] Directory -directory RestoreDirectory [-overwrite | -skip ]
```

有关所有选项的说明，请参阅 omnir 手册页或《Data Protector 命令行界面参考》。

重要说明备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是*对象复制*会话的会话 ID。

如果存在同一对象的多个副本，则 omnir 语法不允许您指定要从哪个对象副本还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

示例 (将虚拟机还原到原始 CAS 服务器)

假定您要还原虚拟机 vm_machineA 。在备份时，虚拟机在属于由 CAS 管理服务器系统 casmanagementserver.company.com 管理的主机池 /MyHostPool 的 H3C CAS 服务器系统上运行。这些虚拟机采用 h3ccasImage -non-cached 备份方法进行备份。

要使用备份会话 2018/10/06-6 将它们还原到原始位置，并确保在会话完成时将新还原的虚拟机置于联机状态，请执行:

```
omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost casmanagementserver.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -session 2018/10/06-6 -vm vm_machineA -instanceUUID 503eeaac-6fae-7898-73e1-93b722a0517c -register -poweron
```

示例 (将虚拟机还原为新虚拟机) 假设虚拟机 /MyVirtualMachines/machineA 是使用 H3CCAS 缓存备份方法在会话 2020/02/10-18 中从 H3C CAS 管理服务器系统 h3ccas.company.com 所管理的主机池 /MyHostpool 备份的。要还原为新虚拟机，请执行:

```
omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -method h3ccasImage-cached -session 2020/02/10-18 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -new_name NewVMName -register
```

示例 (将虚拟机还原到目录) - 非缓存备份方法

假设使用 h3ccasImage -non-cached 备份方法，在会话 2018/10/06-6 中从由 CAS 管理服务器系统 cvm.company.com 管理的主机池 /MyHostPool 备份了虚拟机 /MyVirtualMachines/machineA 和 /MyVirtualMachines/machineB 。要将主机池以外的虚拟机还原到备份主机 backuphost.company.com 上的目录 C:\tmp ，请执行:

```
omnir -veagent -virtual–environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -session 2018/10/06-6 -vm /MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB -directory c:\tmp
```

示例 (将虚拟机还原到另一 CAS 服务器) 假设用户想要将虚拟机 /vm/machineA 还原到另一 CAS 服务器，该虚拟机运行于属于 H3C CAS 管理服务器系统 h3ccas.company.com .所管理的主机池 /MyHostpool 的 CAS 服务器系统上。这些虚拟机采用 H3CCAS 非缓存方法进行备份。

示例：要使用备份会话 2019/03/11–1 还原到新位置，并确保在会话完成时将新还原的虚拟机置于联机状态，请执行:

```
omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -destination h3ccasNew.company.com -newinstance /MyNewHostpool -host_cluster new_cluster1 -specificHost new_cvknode1 -store /vms/images -method h3ccasImage-noncached -session 2019/03/11-1 -vm /cvknode2/VM1 -instanceUUID fa62b2fa-4be7-44e4-8ba1-621d6a3adda2 -register -deletebefore
```

示例 (从单个会话还原多个虚拟机)

假设使用 H3C CAS 备份方法在会话 2018/12/14-13 期间从由 CAS 管理服务器系统 cvm.company.com 管理的主机池 /MyHostPool 备份了虚拟机 /MyVirtualMachines/machineA 、 /MyVirtualMachines/machineB 和 /MyVirtualMachines/machineC 。要在单个会话中还原所有三个虚拟机，请执行:

```
omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost casmanagementserver.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -session 2018/12/14-13 -vm /MyVirtualMachines/machineA -instanceUUID 893a8e41-015c-47df-8d9f-a70b3d12fdf6 -vm /MyVirtualMachines/machineB -instanceUUID e41021aa-2447-4cf3-8336-084b2eb46c8e -vm /MyVirtualMachines/machineC -instanceUUID 37f164cc-ade7-4544-af61-5674fe04ea8c -register -debug 1-500 C:\logs\test\Debug.txt
```

示例 (从多个会话还原多个虚拟机)

假设使用 h3ccasImage -non-cached 备份方法在会话 ID 2018/12/14-7 到会话 ID 2018/12/14-13 之间从由 CAS 管理服务器系统 casmanagementserver.company.com 管理的主机池 /MyHostPool 备份了虚拟机 /MyVirtualMachines/machineA 、 /MyVirtualMachines/machineB 和 /MyVirtualMachines/machineC 。要在多个会话中还原所有三个虚拟机，请执行:

omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost casmanagementserver.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -fromsession 2018/12/14-7 untilsession 2018/12/14-13 -vm /MyVirtualMachines/machineA -instanceUUID 893a8e41-015c-47df-8d9f-a70b3d12fdf6 -vm /MyVirtualMachines/machineB -instanceUUID e41021aa-2447-4cf3-8336-084b2eb46c8e -vm /MyVirtualMachines/machineC -instanceUUID 37f164cc-ade7-4544-af61-5674fe04ea8c -register -debug 1-500 C:\logs\test\Debug.txt

示例 **(**将虚拟机磁盘还原到同一 **H3C CAS** 服务器内的其他虚拟机**)**

假设在会话 2021/07/07-13 中备份了虚拟机 /vm/machineA 中的单个磁盘 /vms/images/DiskA 。要将磁盘还原到存储 /vm/images 中同一 H3C CAS 服务器内的其他虚拟机 /vm/machine1，请执行:

omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /vm/images/DiskA -targetVM /vm/machine1 -store /vm/images -specificHost cas1 -poweron -deletebefore

示例 **(**将虚拟机磁盘还原到同一 **H3C CAS** 服务器内其他存储池中的同一虚拟机**)**

假设在会话 2021/07/07-13 中备份了虚拟机 /vm/machineA 中的单个磁盘 /vms/images/DiskA 。要将磁盘还原到同一 H3C CAS 服务器内其他存储池中的同一虚拟机，请执行:

omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /vm/images/DiskA -store /vm/images -specificHost cas1 -poweron -deletebefore

示例 (将虚拟机磁盘还原到其他 H3C CAS 服务器中的虚拟机)

假设在会话 2021/07/07-13 中备份了虚拟机 /vm/machineA 中的单个磁盘 /vms/images/DiskA 。要将磁盘还原到其他 H3C CAS 服务器 h3ccas2.company.com 中的虚拟机 /vm/machine1 ，请执行:

omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /vm/images/DiskA -targetVM /vm/machine1 -store /vm/images -specificHost cas1 -destination h3ccas2.company.com -newinstance /Host_Pool1 -deletebefore

使用其他设备进行还原

您可以使用与用于备份的设备不同的设备进行还原。有关详细信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

并行还原

通过此功能，您可以从主机并行还原多个虚拟机。

使用非缓存方法，每个虚拟机还原都将创建一个内部路径，以将文件从“备份目标”复制到“暂存目录”，再进一步复制到“H3C CAS 管理服务器”。完成还原后，系统将自动清理暂存目录中的所有文件。

使用缓存方法，虚拟机直接还原到 H3C CAS 服务器。

还原到目录

使用“还原到目录”选项可将备份的文件还原到所需的暂存目录。此选项在“还原”上下文的“目标”页中可用。只有非缓存备份方法支持它。

文件冲突处理

使用“还原”上下文的“选项”页中的“文件冲突处理”选项可处理文件冲突。“文件冲突处理”下提供了以下选项:

- **覆盖**: 选择此选项时，即使备份文件已存在于所选目录中，也会将其还原到暂存目录。默认情况下选择此选项。
- **跳过**: 选择此选项时，如果备份文件已存在于所选目录中，则会跳过还原。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

要监视会话，请参阅《Data Protector 帮助》索引: “查看当前正在运行的会话”。

还原链

从在增量或差异会话中创建的非缓存备份或缓存备份还原虚拟机时，Data Protector 会自动还原整个备份链，从上次完整备份开始，然后是差异备份或增量备份。还原链概念也适用于缓存备份情况下的单个磁盘还原，

> **注意**使用 H3C CAS 非缓存方法 (CBT 或非 CBT 备份) 时，第一次增量或差异备份将包含完整数据。

注意事项

以下注意事项适用于非缓存方法:

- 如果选择增量备份，则将还原从最新完整备份开始到所选增量备份的所有会话。
- 如果选择差异备份，则将还原最新的完整备份、第一次差异备份和所选差异备份。
- 选定要还原的所有会话都必须具有在备份期间使用的相同备份方法 (CBT 或非 CBT)。备份方法发生更改将导致备份链断开。

以下注意事项适用于缓存方法:

- VM 还原的还原链和单个磁盘还原的还原链是相互独立的。它们不能组合以创建单个还原链。

有关备份链方案的详细信息，请参阅备份链。

下面是备份会话的列表以及使用非缓存方法创建的对应还原链:

备份方案	还原链	描述
完整、增量 1 (CBT)、增量 2 (CBT)	1.完整 (CBT)、增量 1 (CBT)	如果完整备份为 CBT 并选择增量 1 (CBT) 进行还原。
	2. 完整 (CBT)、增量 1 (CBT)、增量 2 (CBT)	如果完整备份为 CBT 并选择增量 2 (CBT) 进行还原。
	3.完整 (增量 1 (CBT))、增量 2 (CBT)	如果完整备份为非 CBT 并选择增量 2 (CBT) 进行还原。由于还原链在增量 1 (CBT) 处断开，因此将变成完整备份。
完整、增量 1 (CBT)、增量 2 (非 CBT)	1.完整、增量 2 (非 CBT)	如果完整备份为非 CBT 并选择增量 2 (非 CBT) 进行还原。
	2.完整 (增量 2 (非 CBT))	如果完整备份为 CBT 并选择增量 2 (非 CBT)。由于还原链在增量 2 (非 CBT) 处断开，因此将变成完整备份。
完整、增量 1 (CBT)、增量 2 (非 CBT)、增量 3 (非 CBT)	1.完整、增量 2 (非 CBT)、增量 3 (非 CBT)	如果完整备份为非 CBT 并选择增量 3 (非 CBT) 进行还原。
	2.完整 (增量 2 (非 CBT))、增量 3 (非 CBT)	如果完整备份为 CBT 并选择增量 3 (非 CBT) 进行还原。由于还原链在增量 2 (非 CBT) 处断开，因此将变成完整备份。
完整、增量 1 (非 CBT)、增量 2 (非 CBT)、增量 3 (非 CBT)	1.完整、增量 1 (非 CBT)、增量 2 (非 CBT)、增量 3 (非 CBT)	如果完整备份为非 CBT 并选择增量 3 (非 CBT) 进行还原。
	2.完整 (增量 1 (非 CBT))、增量 2 (非 CBT)、增量 3 (非 CBT)	如果完整备份为 CBT 并选择增量 3 (非 CBT) 进行还原。由于还原链在增量 1 (非 CBT) 处断开，因此将变成完整备份。
完整、增量 1 (CBT)、差异 (非 CBT)	1.完整、差异 (非 CBT)	如果完整备份为非 CBT 并选择差异 (非 CBT) 进行还原。
	2.完整 (差异 (非 CBT))	如果完整备份为 CBT 并选择差异 (非 CBT) 进行还原。由于还原链在差异 (非 CBT) 处断开，因此将变成完整备份。
完整、差异 1 (非 CBT)、差异 2 (非 CBT)	1.完整、差异 1 (非 CBT)、差异 2 (非 CBT)	如果完整备份为非 CBT 并选择差异 2 (非 CBT) 进行还原。
	2.完整 (差异 1 (非 CBT))、差异 2 (非 CBT)	如果完整备份为 CBT 并选择差异 2 (非 CBT) 进行还原。由于还原链在差异 1 (非 CBT) 处断开，因此将变成完整备份。

下面是备份会话的列表以及使用单个磁盘的缓存还原创建的对应还原链:

备份方案	还原链	描述
Full1(disk1)、Full2(disk2)、Incr1(disk1,disk2)、Incr2(disk1)、Incr3(disk2)、Incr4(disk1,disk2)	1。Full1, Incr1, Incr2, Incr4 2。Full2, Incr1, Incr3, Incr4 3。Full1、Full2、Incr1、Incr2、Incr3、Incr4	1。如果您选择从 Incr4 会话还原 disk1 2。如果您选择从 Incr4 会话还原 disk2 3。如果您选择从 Incr4 还原 disk1 和 disk2
Full1(disk1)、Incr1(disk1)、Incr2(disk1, disk2) => 回退到完整 => Full2(disk1, disk2)、Incr3 (disk1, disk2)、Incr4(disk1)	1。Full1、Incr1 2。Full2、Incr3 和 Incr4 3。Full2、Incr3	1。如果您选择从 Incr1 会话还原 disk1 2。如果您选择从 Incr4 会话还原 disk1 3。如果您选择从 Incr3 会话还原 disk2
Full1(disk1,disk2)、Incr1(disk1,disk2)、Diff1(disk1)	1。Full1、Incr1 2。Full1、Diff1	1。如果您选择从 Incr1 会话还原 disk1 2。如果您选择从 Diff1 会话还原 disk1

适用于 Microsoft Hyper-V 的虚拟环境集成

本主题介绍如何配置和使用适用于 Microsoft Hyper-V 的 Data Protector 虚拟环境集成。它描述了备份和还原 Microsoft Hyper-V 虚拟机需要了解的概念和方法。

该集成支持独立的 Microsoft Hyper-V 系统环境 (独立环境) 以及在群集中配置 Microsoft Hyper-V 系统的环境 (群集环境)。

备份

备份期间，可以关闭虚拟机的电源 (脱机备份) 或正常使用 (联机备份)。

可以使用以下备份类型:

- Hyper-V (VSS) 映像备份
- Hyper-V RCT 备份

Hyper-V (VSS) 映像备份

由于涉及 Microsoft Hyper-V 和 VSS，您应为每个备份会话指定以下备份类型:

- **Microsoft Hyper-V (VSS) 映像备份类型**

  Data Protector 提供以下类型的交互式备份和安排的备份：

  - 完整
  - 增量

- **VSS 备份类型**

  支持的 VSS 备份类型包括:

  - 本地备份
  - 可传输备份

Hyper-V RCT 备份:

Data Protector 支持以下类型的 Hyper-V RCT 备份:

- 完整
- 增量

还原

可以使用 Hyper-V 映像或 Hyper-V RCT 备份方法还原 Microsoft Hyper-V 虚拟机:

- **到默认 (原始) 位置**

  使用此选项，可以将虚拟机还原到原始或其他 Microsoft Hyper-V 系统上的原始位置。

- **到不同位置**

  使用此选项，可以将虚拟机还原到原始或其他 Microsoft Hyper-V 系统上的不同位置。

- **到目录**

  使用此选项，可以将虚拟机文件还原到安装了 Data Protector 虚拟环境集成 和 MS 卷影复制集成组件的任何客户机。还原之后，需要将虚拟机导入虚拟机的 Microsoft Hyper-V 系统，从而恢复正常功能。

适用于 Hyper-V 的 Data Protector 虚拟环境集成不支持即时恢复。

本节提供特定于适用于 Microsoft Hyper-V 的 Data Protector 虚拟环境集成的信息。

集成概念

Data Protector 支持独立和群集 Microsoft Hyper-V 环境。

独立环境

在独立 Microsoft Hyper-V 环境中，Cell Manager 向备份主机传递备份请求，然后备份主机将该请求发送至相应的独立 Microsoft Hyper-V 系统。备份主机是 Data Protector 单元中安装了 Data Protector 虚拟环境集成 (VEPA) 和 MS 卷影复制集成组件的系统，它控制 Microsoft Hyper-V 虚拟机的备份过程。

在单个会话中，可以选择驻留在同一 Microsoft Hyper-V 系统上的虚拟机进行备份。实际备份数据的位置取决于 Microsoft Hyper-V 虚拟机复制的配置和在 Data Protector 备份规范中选择的选项。

支持的 Hyper-V (VSS) 映像备份阵列:

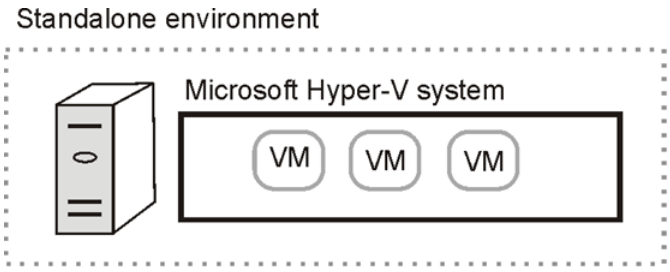
- 3 PAR
- NetApp 9.x
- Dell EMC Unity

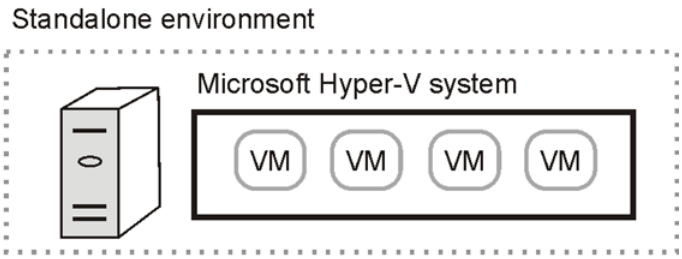
先决条件：

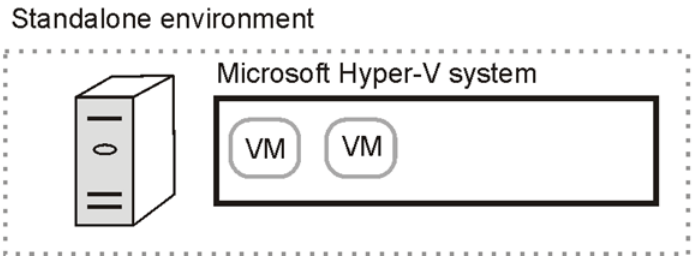
VSS 硬件提供程序:

- NetApp: **安装 NetApp SmartDrive** 应用程序，可在其支持站点中获得
- Dell EMC Unity: **安装 Unity VSS 硬件提供程序**，可从 EMC 支持站点中获得

Hyper-V 独立环境







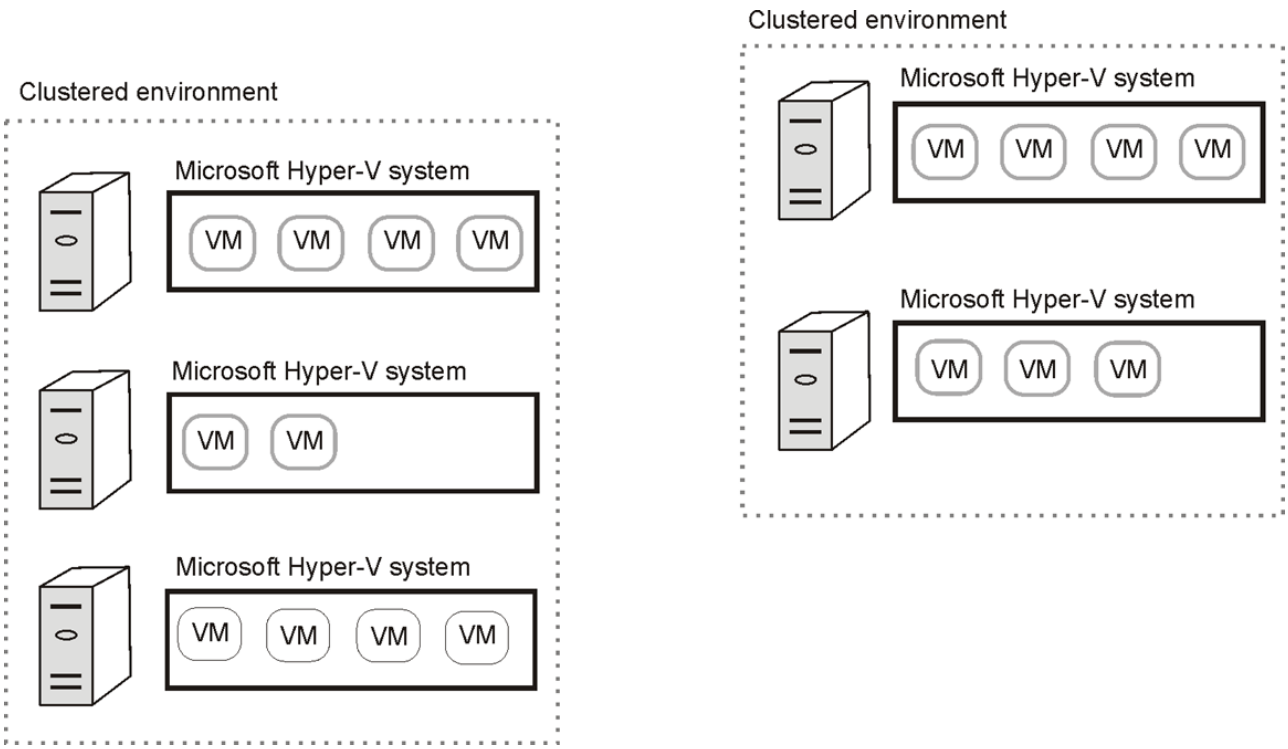
对于独立 Microsoft Hyper-V 系统，只能通过从一个 Microsoft Hyper-V 系统手动导出虚拟机，然后导入另一个 Microsoft Hyper-V 系统来迁移虚拟机。

群集环境

在群集 Microsoft Hyper-V 环境中，Cell Manager 向备份主机传递备份请求，然后备份主机将该请求发送至要备份的虚拟机所在的 Microsoft Hyper-V 系统。

在单个会话中，可以选择驻留在同一 Microsoft Hyper-V 群集中的虚拟机进行备份。实际备份数据的位置取决于 Microsoft Hyper-V 虚拟机复制的配置和在 Data Protector 备份规范中选择的选项。

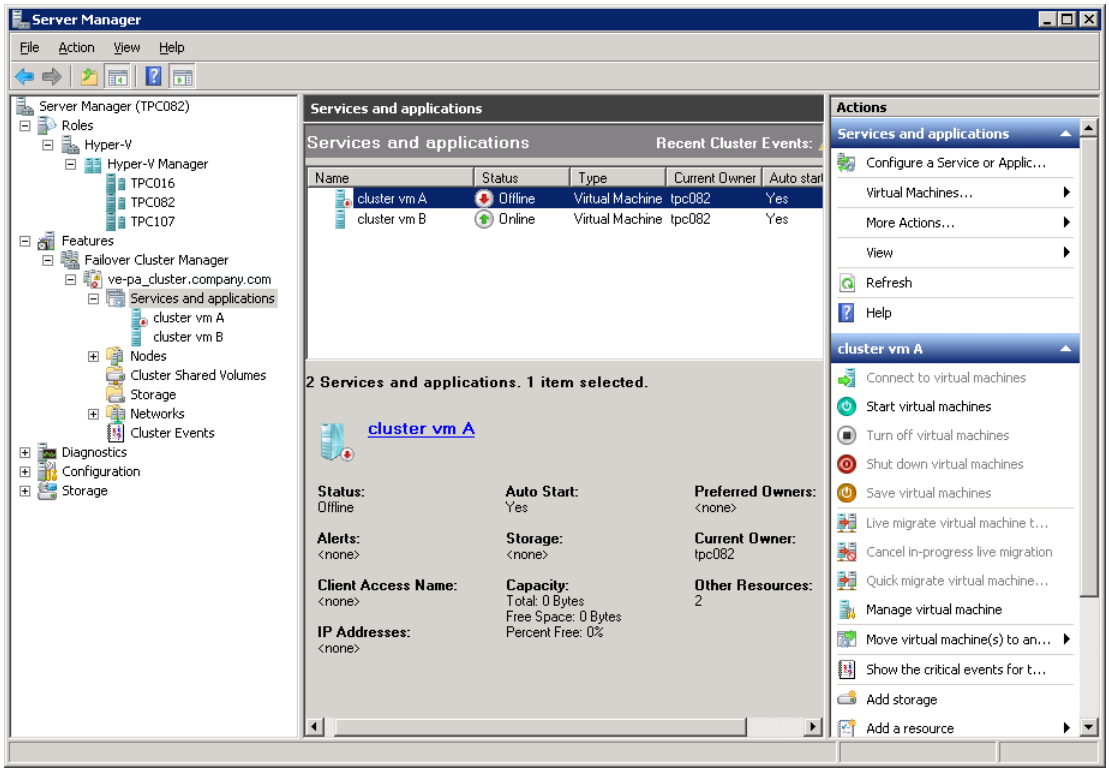
Hyper-V 群集环境



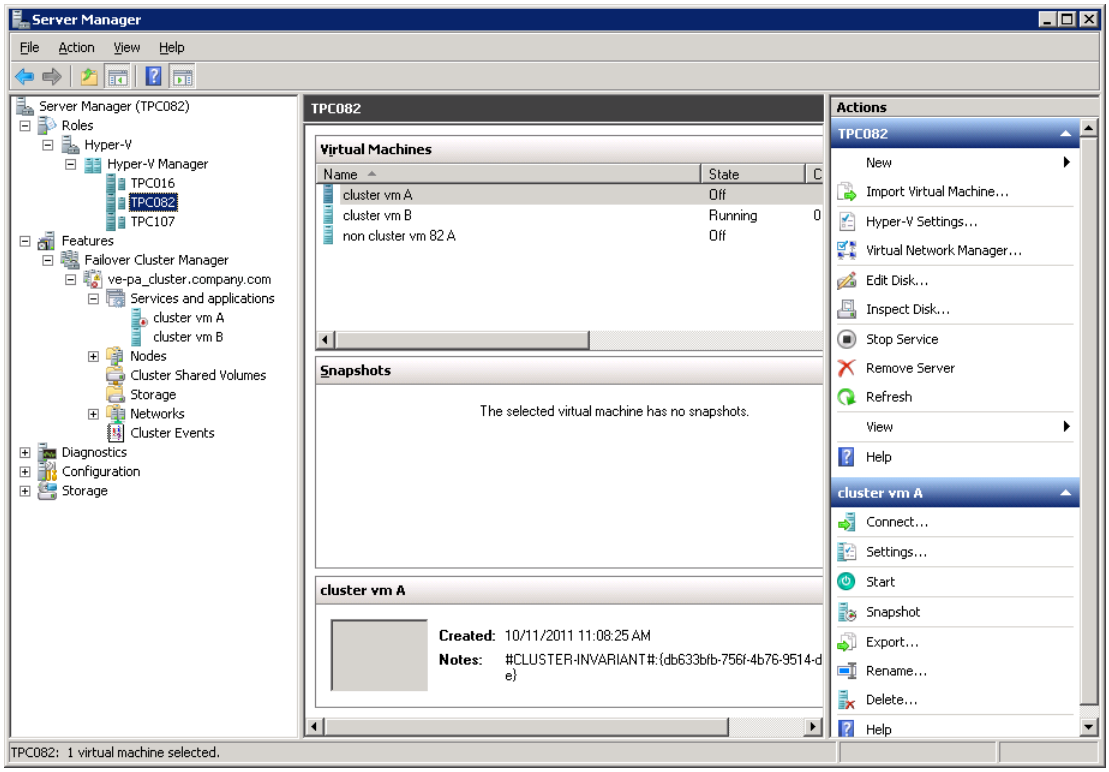
示例

下图说明了由非群集和群集虚拟机组成的环境。这些图显示了如何在 Windows Server Manager 和 Data Protector 备份规范中呈现虚拟机。

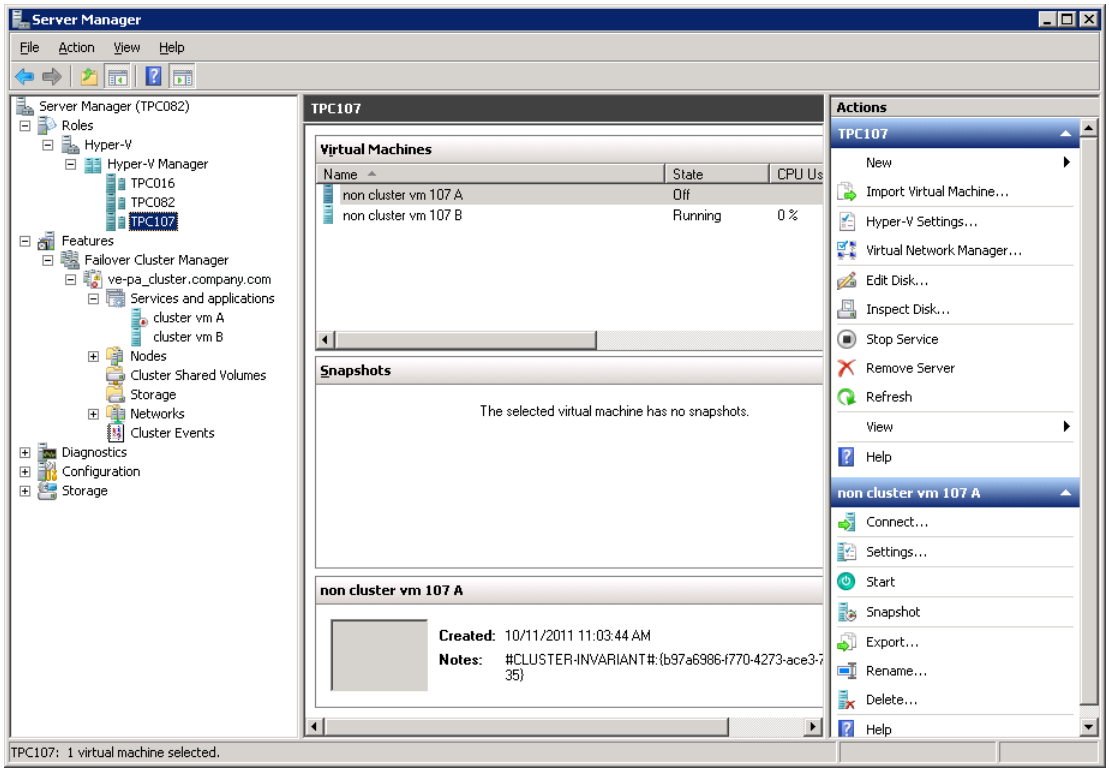
Windows Server Manager - 群集 虚拟机



Windows Server Manager - 在 TPC082 上运行的 虚拟机



Windows Server Manager - 在 TPC107 上运行的 虚拟机



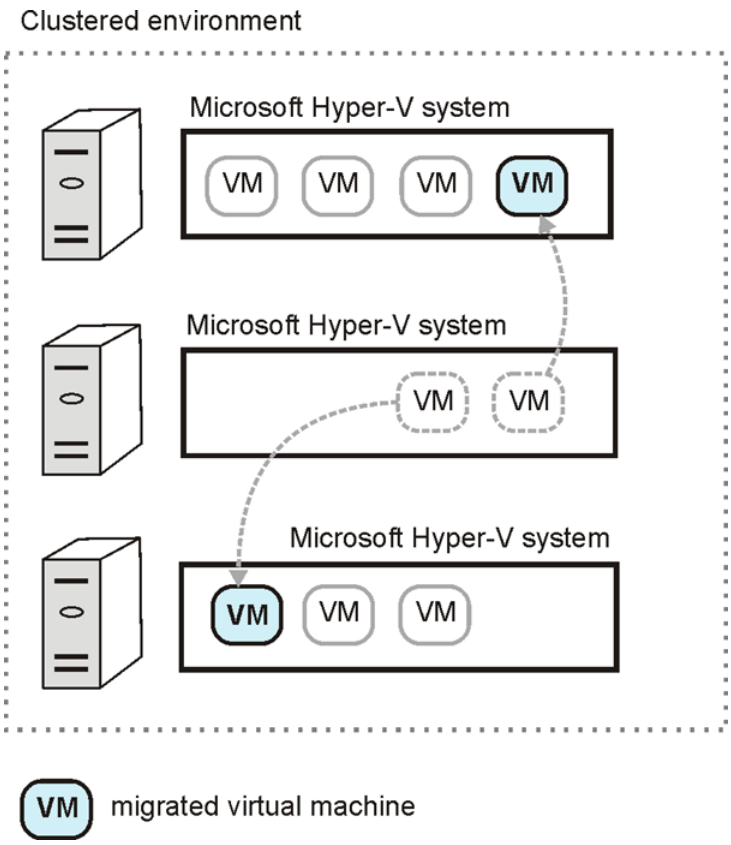
在 Data Protector 备份规范中，将为群集的所有节点显示非群集虚拟机和群集虚拟机；非群集虚拟机列在其物理节点下，群集虚拟机列在其虚拟系统下。

迁移虚拟机

Data Protector 虚拟环境集成支持在群集环境中的 Microsoft Hyper-V 系统之间迁移虚拟机。在此类群集中迁移虚拟机后，您无需更改备份规范；Data Protector 将使用 Microsoft Hyper-V WMI 服务找到待备份虚拟机的迁移位置，并对其进行备份。

注意: 如果在备份或还原会话期间发生了故障转移，则会话将失败，必须重新启动。同样，如果虚拟机在 Data Protector 尝试备份时处于实时迁移过程，则会话将失败。

迁移虚拟机



群集共享卷

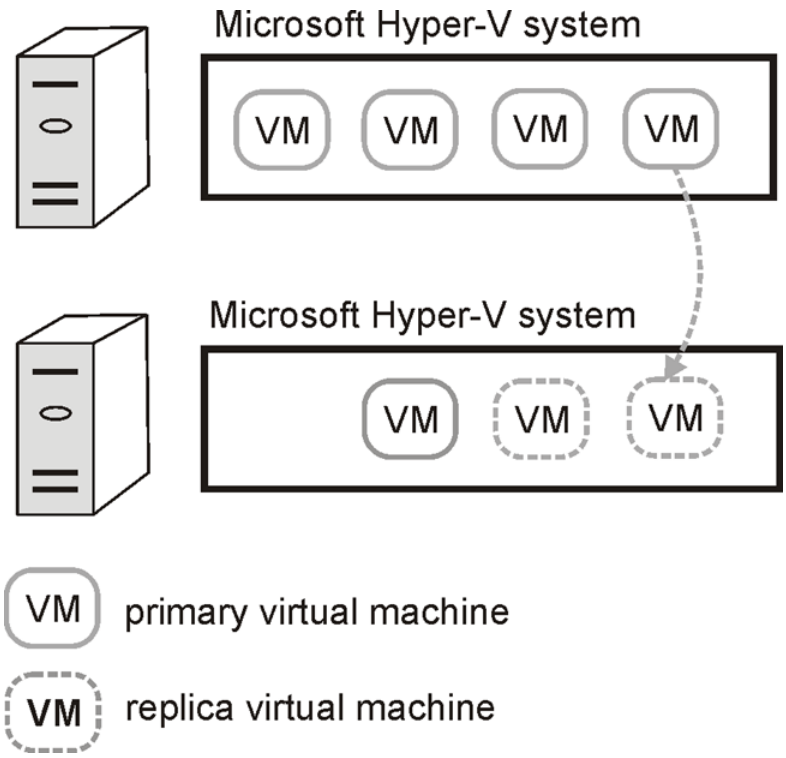
Data Protector 支持使用故障转移群集的群集共享卷 (CSV) 功能的 Microsoft Hyper-V 环境。在使用 CSV 的群集中，可以将多个虚拟机配置为使用相同的 LUN (磁盘)，同时仍可从一个 Microsoft Hyper-V 系统移至另一个 Microsoft Hyper-V 系统且彼此独立。

Hyper-V 复本

在复制配置中，虚拟机 (主 VM) 将复制到另一个 Hyper-V 服务器 (复本服务器)。如果主 VM 损坏，则复制可以进行故障转移，虚拟机复本 (复本 VM) 将成为主 VM。RCT 备份和还原不支持此功能。

复本 VM 是主 VM 在给定时间的快照，可以保留用于备份或进行备份 (而不是主 VM)，从而减少主机系统上的负载。即使主 VM 驻留在群集中，主 VM 和复本 VM 也无法使用常见的共享卷。

虚拟机复制



Windows 文件共享上的虚拟机

Data Protector 支持 Windows Server Hyper-V 系统 (2012 及更高版本) 上的虚拟机，该系统将虚拟机的数据存储在 Windows Server 文件共享 (SMB 3.0) 上。

Data Protector 安装组件

Data Protector 安装由以下组件组成:

Data Protector Cell Manager

Data Protector Cell Manager 可以安装在 Microsoft Hyper-V 虚拟机上或虚拟环境之外的单独系统上。

Data Protector 虚拟环境集成组件

Data Protector 虚拟环境集成 组件应安装在 Data Protector 单元中的至少一个客户机上。此客户机将成为备份主机。对于 Hyper-V RCT，该组件也应该安装在您计划备份或还原虚拟机的所有 Microsoft Hyper-V 主机上。在群集设置中，必须在所有群集节点上安装此组件。

Data Protector 磁盘代理组件

如果要使用“浏览”按钮，则必须在备份主机上安装 Data Protector 磁盘代理组件。此按钮用于选择备份主机上的还原目录。

Data Protector MS 卷影复制集成组件

必须在计划从中备份虚拟机或将虚拟机还原到其中的所有 Microsoft Hyper-V 系统上安装 Data Protector MS 卷影复制集成组件。如果 Microsoft Hyper-V 系统在群集中配置，它们必须安装在所有群集节点上。对于 VSS 可传输备份，也必须在备份系统上安装该组件。此外，还必须在备份主机上安装该组件。

> **注意**备用系统和备份主机这两个术语不是指同一实体。备份主机是安装了 Data Protector 虚拟环境集成组件的系统，因此可控制备份会话，而备份系统仅用于 VSS 可传输备份会话；它从磁盘阵列导入卷影复制，支持对其进行访问，可以将数据传输到备份介质。

Data Protector 介质代理组件

必须在与备份设备相连的 Data Protector 客户机上安装 Data Protector 常规介质代理组件。这可以是任何 Microsoft Hyper-V 系统，也可以是 Microsoft Hyper-V 虚拟环境之外的单独系统。

备份概念

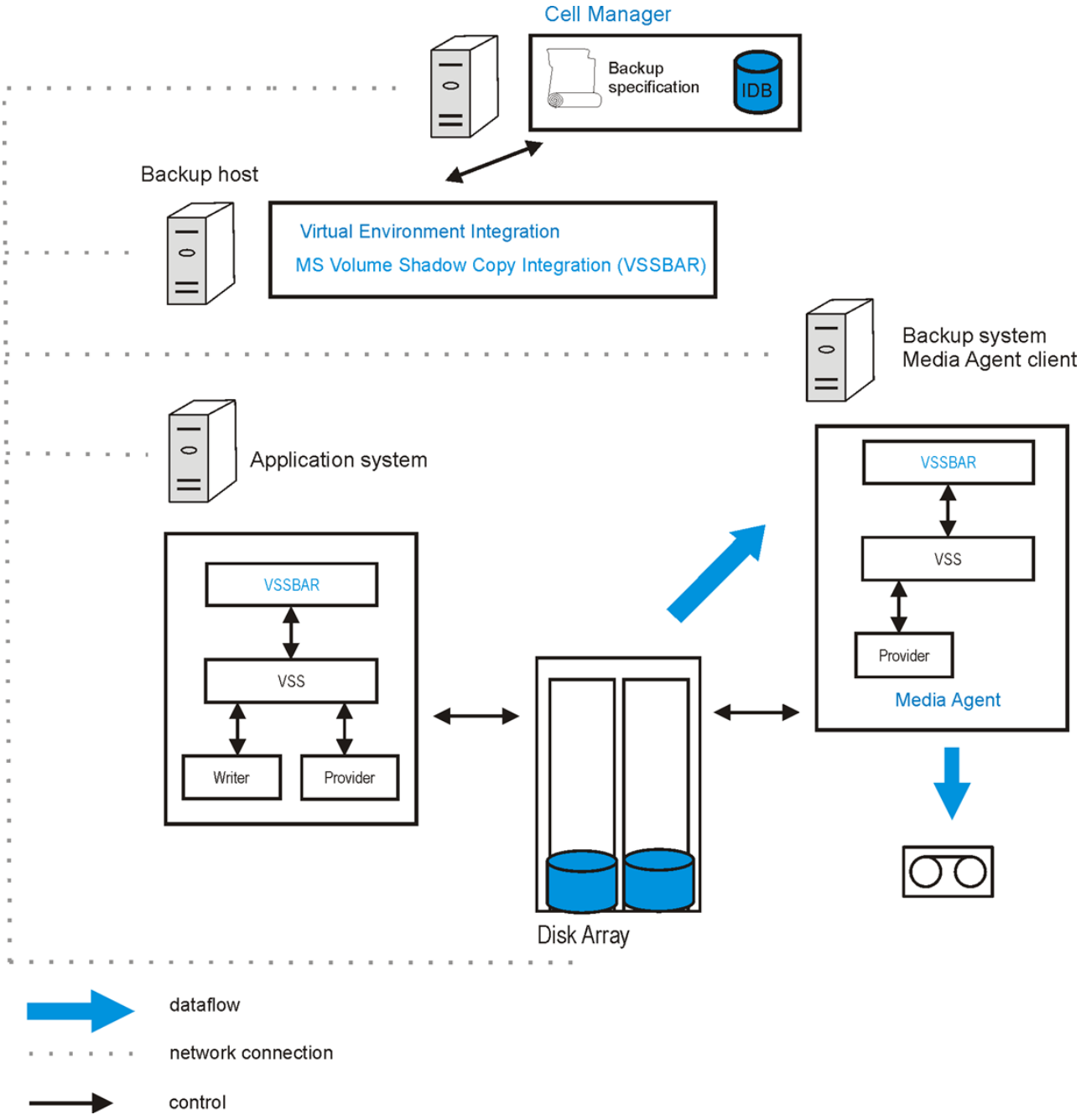
Hyper-V (VSS) 映像备份方法

通过 Hyper-V 映像备份方法，您可以选择 Microsoft Hyper-V 虚拟机作为 Data Protector 备份对象。Hyper-V (VSS) 映像备份会话按如下步骤进行:

1. Cell Manager 与备份主机建立连接以发送备份请求，并在备份主机上启动虚拟环境集成代理 (vepa_bar.exe)。
2. 使用自定义动态链接库 (dpvssapi.dll ，是安装在备份主机上的 MS Volume Shadow Copy 集成组件)， vepa_bar.exe 在应用程序系统上启动 vss_bar.exe 。
3. 反过来，应用程序系统上的 vss_bar.exe 代理向卷影复制服务发送请求以创建卷影复制。对于 VSS 可传输备份， vss_bar.exe 还在备份系统上启动 vss_bar.exe 。
4. 创建卷影复制后， vss_bar.exe 将卷影复制数据传递给介质代理客户机，后者将数据传输到备份介质。
5. vss_bar.exe 通知 vepa_bar.exe 备份已完成。

> **注意**您可以使用 omnirc 选项 OB2VEPA_HYPERV_TIMEOUT 指定 vepa_bar.exe 应等待 vss_bar.exe 多长时间才发送“备份已完成”消息。默认情况下，没有时间限制 (该选项设置为 INFINITE)。

Hyper-V 映像备份方法 (VSS 可传输备份)



在 Hyper-V 映像备份方法 (VSS 可传输备份) 中，备份系统也是介质代理客户机。因此，它安装了常规介质代理组件并与设备相连。

Hyper-V (VSS) 映像备份类型

由于涉及 Microsoft Hyper-V 和 VSS，必须为每个备份会话指定以下备份类型:

- Microsoft Hyper-V 备份类型
- VSS 备份类型

要执行的备份类型在备份规范级别指定。

Microsoft Hyper-V 备份类型

可以从以下 Microsoft Hyper-V 备份类型进行选择:

- 完整 (**Full**)

  完整备份虚拟机，包括其完整的虚拟磁盘。

- 增量 (**Incr**)

  虚拟机快照首先由 Microsoft Hyper-V 创建，然后由 Data Protector 备份。仅自上次备份虚拟机以来所做的更改包含在 Data Protector 备份映像中。

在特定环境中，增量备份会话会回退，而 Data Protector 会执行一次完整备份。无法对复制的虚拟机执行增量备份。

> **注意**由于已知的 Microsoft 问题，无法联机备份驻留在 Hyper-V 2008 R2 上的 Windows 2012 或 Windows 2012 R2 操作系统虚拟机。这些虚拟机仅支持脱机备份。

VSS 备份类型

可以从以下 VSS 备份类型进行选择:

- 本地备份 (本地或网络备份)

  此类型用于单主机 VSS 配置。该备份在创建 VSS 卷影复制的 Microsoft Hyper-V 系统上完成。这可以是 Data Protector 零宕机时间备份 (使用 VSS 硬件提供程序) 或标准 Data Protector 备份 (使用软件提供程序)。

  > **注意**在 Microsoft Hyper-V 群集环境中，不支持使用 VSS 硬件提供程序执行本地备份。这是 Microsoft 产品的限制。

- 可传输备份 (VSS 可传输备份)

  此类型用于双主机 VSS 配置。它在应用程序系统 (Microsoft Hyper-V 系统) 上创建 VSS 卷影复制，并将其呈现给备份系统，从备份系统中可以执行备份到备份介质。此类型的备份需要 VSS 硬件提供程序。

  > **注意**在 Microsoft Hyper-V 群集环境中，备份主机不能是在其中一个 Microsoft Hyper-V 系统上运行的虚拟机。这是 Microsoft 产品的限制。

Hyper-V (VSS) 映像备份注意事项

- 使用 Data Protector 虚拟环境集成，无法备份 Microsoft Hyper-V 系统配置数据。
- 由于 Data Protector 虚拟环境集成的体系结构基础，请考虑 Microsoft 卷影复制服务 中所述的 Microsoft Hyper-V 写入程序详细信息。

虚拟机存储

- 由于 Microsoft Hyper-V 的限制，无法备份以下内容:
  - 驻留在直接连接到虚拟机的物理磁盘上的数据。
  - 驻留在虚拟机使用 iSCSI 启动器直接访问的存储上的数据。

  有关详细信息，请在 Microsoft TechNet 库中搜索词语“Hyper-V, Planning for Backup”。
- ***Windows Server 2012、2016 和 2019 系统:*** 在此操作系统上，无法备份以下内容:
  - 驻留在虚拟光纤通道 HBA 直接访问的存储上的数据

并发会话

- 使用相同设备的备份会话不能并发运行。如果同时启动多个会话，则一个会话将等待另一个会话完成。

群集共享卷 (CSV)

- 尝试从同一 CSV 备份虚拟机的备份会话不能并行运行。如果启动了两个会话，则第二个会话将失败。

  Windows Server 2012、2016 和 2019 系统: 不在 CSV 上的虚拟机必须在单独的会话中备份，否则会话将失败。如果虚拟机的任何部分 (例如，配置或快照文件) 位于 CSV 之外，则会话将失败。

SMB 文件共享上的虚拟机

Data Protector 支持备份位于 Windows 文件系统共享 (SMB 3.0) 上的虚拟机。必须满足以下先决条件:

- 必须在 Windows 文件服务器上安装并启用 Windows 角色“文件服务器 VSS 代理服务”。

  要检查该服务是否已启用，请打开 PowerShell 窗口并执行:

  ```
  Get-WindowsOptionalFeature -Online -FeatureName FileServerVSSAgent
  ```

要启用该服务，请执行:

```
Enable-WindowsOptionalFeature -Online -FeatureName FileServerVSSAgent
```

或者，打开服务器管理器并使用“添加角色和功能”向导检查该角色的状态，在必要时启用“文件服务器 VSS 代理服务”。

- 为使用 SMB 文件共享的所有 Hyper-V 节点添加约束委派:

  在“Active Directory 用户和计算机”中，依次选择域和“计算机”以列出所有系统。右键单击所选的 Hyper-V 节点，然后选择“属性”。在“属性”对话框中，选择“委派”并将 `cifs` 服务添加到受信任的服务列表中。

- 必须准备 SMB 文件共享并将其配置为托管 Hyper-V 虚拟机:
  - 该虚拟机必须已配置并正在 SMB 3.0 文件共享上运行。不支持早期版本的 SMB 文件共享。
  - 确保所有 Hyper-V 主机的计算机帐户、SYSTEM 帐户和管理虚拟机的所有 Hyper-V 管理员都具有对该共享的完全控制权限。此外，确保 Hyper-V 群集虚拟名称的所有计算机帐户都具有对该共享的完全控制权限。

    为了避免为每个其他 Hyper-V 主机或 Hyper-V 管理员手动添加权限，您可以将 Hyper-V 主机和 Hyper-V 管理员添加到域安全组中，并将完全控制权限授予给此组而不是单个用户帐户。在配置该共享之前，您需要创建此类域安全组并将所有计算机帐户和用户帐户添加到该组中。向该共享添加权限时，现在只需为此安全组 (而不是所有单个帐户) 添加完全控制权限。
  - 在群集环境中创建 SMB 文件共享时，需要执行以下其他步骤:
    - 创建文件服务器群集角色。在路径 `C:\ClusterStorage` 下的 CSV 中 (对于用于应用程序数据的横向扩展文件服务器) 或在群集磁盘上 (对于用于一般用途的文件服务器) 创建该共享。
    - 如果动态 DNS 注册在您的环境中不起作用，请使用服务器管理器在 DNS 服务器上为分布式服务器名称注册所有群集节点的 IP 地址。
- 备份联机虚拟机时，不会备份包含 SMB 文件共享上的数据和本地卷上的虚拟磁盘的单个虚拟机。例如，如果备份规范包含两个 VM，并且 VM1 具有 SMB 文件共享上的数据和本地卷上的虚拟磁盘，而 VM2 完全位于 SMB 文件共享上，则仅备份 VM2。

  如果备份驻留在混合位置的多个虚拟机 (其中每个虚拟机仅位于一个位置)，则会中止整个主机的备份。请创建单独的备份规范以备份此类配置。例如，如果备份规范包含三个 VM，其中 VM1 具有本地卷上的数据，VM2 具有 CSV 上的数据，VM3 具有 SMB 文件共享上的数据，并且所有 VM 驻留在同一系统上，则不会备份整个系统。

  如果备份规范同时包含二者，即在多个位置具有数据的 VM 和仅在一个位置具有数据的 VM，则首先跳过在另一个位置具有数据的虚拟机。如果其余 VM 位于同一位置，则会备份主机。否则，将中止备份。

  通过将 omnirc 变量 `OB2_VEAGENT_ENABLE_SMB_MIX_LOCATIONS` 设置为 `1`，可以停用对混合位置的检查。但请注意，虽然备份了所有虚拟机，但如果执行了联机备份，则给定 Hyper-V 主机上的完整备份将失败。
- 不支持 SMB 文件共享上使用分布式文件系统命名空间 (DFSN) 或分布式文件系统替换 (DFSR) 的虚拟机。
- 如果系统是 Hyper-V 服务器兼文件服务器，则虚拟机无法在同一系统的 SMB 文件共享上具有数据。

增量备份

- 只有使用 Microsoft Hyper-V Server 2012 及更高版本，才能在虚拟机运行时对虚拟磁盘执行增量备份。
- 在为每个 Microsoft Hyper-V 虚拟机运行第一个增量备份会话之前，该虚拟机需要事先为增量备份做好准备。您可以通过两种方式准备虚拟机 (启用其增量备份):
  - 为虚拟机运行完整备份会话，在这种情况下选择相关备份规范中的“启用虚拟机的增量备份”选项
  - 在为虚拟机执行 `vepa_util.exe command --enable-incremental` 命令后为其运行完整备份会话。
- 在以下任何条件下，增量备份会话将回退，Data Protector 会改为执行完整备份:
  - 虚拟机未准备好进行增量备份
  - 为选择进行备份的虚拟机配置了到另一个 Microsoft Hyper-V 系统的复制
  - Data Protector 内部数据库中已不存在对先前为虚拟机创建的备份映像的引用
  - 虚拟机的最新备份快照不是由 Data Protector 所创建
  - 您的备份规范是针对虚拟机复本而配置
  - Microsoft Hyper-V 系统或群集上的操作系统不支持虚拟机的增量快照。

> **注意**根据您的 Microsoft Hyper-V 环境，回退范围是整个 Microsoft Hyper-V 系统或群集。如果发生回退，则当前会话中使用的备份类型将针对所有参与的虚拟机进行更改。

虚拟机复本

- **虚拟机备份映像的一致性**

  复本 VM 是虚拟机的定期快照。如果还原复本 VM，则还原的 VM 仅处于持续崩溃状态。

此外，您可以配置虚拟机替换过程来创建并存储恢复点。但是，这些恢复快照也仅处于持续崩溃状态。要创建应用程序一致的快照，请启用增量 VSS 副本的复制。

备份复本 VM 时，Data Protector 会备份当前快照和所有存储的恢复点。要确保每个 Data Protector 备份包含应用程序一致的恢复点，请为增量 VSS 复制选择比 Data Protector 备份更短或相等的间隔。例如，选择每小时执行一次 VSS 增量复制，并且必须保留四个恢复点。计划每四小时执行一次 Data Protector 备份。

- **在初始** 虚拟机**替换期间备份**

  在初始虚拟机替换期间，请勿备份虚拟机。备份主 VM 时，备份会话可能失败。备份复本 VM 时，会话也将失败。但是，如果选择复本 VM 并使用选项“备份选定的 VM”，则会话将完成而不会出现错误，但仅备份在此之前复制的数据。

- **备份持续时间和复制间隔**

  在备份会话期间，虚拟机配置已锁定，因此虚拟机替换失败。Hyper-V 服务尝试在指定时间内同步复本。如果不成功，Hyper-V 服务将停止尝试自动重新同步。您必须在备份会话完成后重新启用复制。

  请确保备份会话在指定时间内完成，或更改允许 Hyper-V 自动重新同步替换的虚拟机的时间间隔。

- 虚拟机 **替换状态和运行状况**

  - 如果复制连接不起作用，则复本 VM 的备份将失败。要避免此问题，请选择在连接不起作用时使用主复本的选项。
  - 虚拟机故障转移后，替换状态和运行状况分别为 Error 和 FailedOverWaitingCompletion ，因此新的复本 VM 不用于备份。

    取消替换后，虚拟机替换状态和运行状况分别为 Replicating 和 Normal ，但是 Hyper-V 提供的信息仅在下次虚拟机替换成功后才更新，而备份会话只能在之后恢复。

虚拟机迁移

- *Windows Server 系统 (2012 及更高版本):* 在迁移期间，虚拟机已锁定且无法备份，反之亦然。

ZDB 环境

- 如果虚拟机文件位于磁盘阵列上，并且您打算执行的 ZDB 会话将在备份会话完成后保留复本存储卷，请以这种方式创建备份规范，使选择的所有虚拟机驻留在相同备份规范中的同一存储卷上。否则，在 ZDB 会话中创建的复本存储卷还包含未选择的虚拟机的备份，但这些备份不具有应用程序一致性，因为在创建复本存储卷之前这些虚拟机未静止；此类虚拟机备份仅处于持续崩溃状态。如果执行 ZDB 到磁带会话，则仅将所选的虚拟机备份到备份介质。
- ***P4000 SAN 解决方案:*** 由于 VSS 硬件提供程序限制，其文件驻留在 P4000 SAN 解决方案磁盘阵列上的虚拟机在联机时无法备份。

  有两种变通方法:

  - 使用软件提供程序在联机时备份虚拟机 (标准备份)。
  - 在脱机时备份虚拟机 (零宕机时间备份)。

对象复制注意事项

- 要对 Microsoft Hyper-V 虚拟机快照正确使用 Data Protector 对象复制功能，您需要复制在同一会话中使用 Hyper-V 映像备份方法创建的所有 Data Protector 备份对象。确保在为交互式、备份后或计划复制会话选择 Data Protector Microsoft Hyper-V 对象时选择整个备份会话。

  为了表明此准则，Data Protector GUI 不会在“对象操作”上下文的“复制”>“对象复制”>“交互式”>“对象范围”中列出 Microsoft Hyper-V 备份对象。

Hyper-V RCT 备份方法

从 Microsoft Windows 2016 版本开始，Hyper-V 虚拟机支持 Hyper-V 弹性更改跟踪 (RCT) 功能。它在数据块级别跟踪备份之间虚拟机上发生的更改。

支持以下备份类型:

- 完整备份
  在完整 RCT 备份期间，获取整个虚拟机的快照。该快照将用作参考点，以后用于增量备份。
- 增量备份

  虚拟机快照首先由 Microsoft Hyper-V 创建，然后由 Data Protector 备份。在增量备份期间，仅自上次备份虚拟机以来所做的更改包含在 Data Protector RCT 备份中。

Hyper-V RCT 备份会话按如下步骤进行:

1. Cell Manager 与备份主机建立连接以发送备份请求，并在备份主机上启动虚拟环境集成代理 (vepa_bar.exe)。该代理为每个 Hyper-V 客户机准备虚拟机列表，并创建备份规范。
2. 它在 Hyper-V 客户机主机上启动虚拟环境集成代理 (vepa_bar.exe)。
3. 在虚拟机监控程序上运行的 vepa_bar.exe 代理连接到备份主机上运行的进程，以接收使用更新的备份规范执行备份的请求。
4. 初始验证后，服务器进程将创建一个虚拟机任务以检查 Hyper-V 客户机主机和虚拟机硬件版本。每个虚拟机任务都并行运行。
5. 然后执行备份。

Hyper-V RCT 注意事项:

- 在为 Hyper-V 客户机创建 Hyper-V RCT 备份规范时，Data Protector GUI 只会列出同时安装了 Data Protector 虚拟环境集成和 MS 卷影复制集成组件的备份主机。

- 仅当 Hyper-V 客户机同时安装了 Data Protector 虚拟环境集成和 MS 卷影复制集成组件时，才会显示 Hyper-V RCT 备份类型。
- 如果在虚拟机上配置了“静止”，并且将静止错误级别设置为“警告”，则会启用回退到非静止快照 (崩溃一致备份) 的功能。
- Hyper-V RCT 解决方案除了支持将磁盘备份到传统目标设备，还支持将磁盘备份到 Smart-cache、Storeonce、DD Boost。
- 磁盘 UUID 应当是唯一的，不应更改。
- 由于 Microsoft Hyper-V 的限制，不支持直通磁盘。无法备份以下内容:
  - 驻留在直接连接到虚拟机的物理磁盘上的数据。
  - 驻留在虚拟机使用 iSCSI 启动器直接访问的存储上的数据。
    有关详细信息，请在 Microsoft TechNet 库中搜索词语“Hyper-V, Planning for Backup”。
  - 驻留在虚拟光纤通道 HBA 直接访问的存储上的数据。
- 使用相同设备的备份会话不能并发运行。如果同时启动多个会话，则一个会话将等待另一个会话完成。
- Data Protector 支持备份位于 Windows 文件系统共享 (SMB 3.0 及更高版本) 上的虚拟机。必须满足以下先决条件:
  - 为使用 SMB 文件共享的所有 Hyper-V 节点添加约束委派:

    在“Active Directory 用户和计算机”中，依次选择域和“计算机”以列出所有系统。右键单击所选的 Hyper-V 节点，然后选择“属性”。在“属性”对话框中，选择“委派”并将 cifs 服务添加到受信任的服务列表中。
  - 必须准备 SMB 文件共享并将其配置为托管 Hyper-V 虚拟机:
    - 该虚拟机必须已配置并正在 SMB 文件共享上运行。不支持早期版本的 SMB 文件共享。
    - 确保所有 Hyper-V 主机的计算机帐户、SYSTEM 帐户和管理虚拟机的所有 Hyper-V 管理员都具有对该共享的完全控制权限。此外，确保 Hyper-V 群集虚拟名称的所有计算机帐户都具有对该共享的完全控制权限。

      为了避免为每个其他 Hyper-V 主机或 Hyper-V 管理员手动添加权限，您可以将 Hyper-V 主机和 Hyper-V 管理员添加到域安全组中，并将完全控制权限授予给此组而不是单个用户帐户。在配置该共享之前，您需要创建此类域安全组并将所有计算机帐户和用户帐户添加到该组中。向该共享添加权限时，现在只需为此安全组 (而不是所有单个帐户) 添加完全控制权限。
    - 在群集环境中创建 SMB 文件共享时，需要执行以下其他步骤:
      - 创建文件服务器群集角色。在路径 C:\ClusterStorage 下的 CSV 中 (对于用于应用程序数据的横向扩展文件服务器) 或在群集磁盘上 (对于用于一般用途的文件服务器) 创建该共享。
      - 如果动态 DNS 注册在您的环境中不起作用，请使用服务器管理器在 DNS 服务器上为分布式服务器名称注册所有群集节点的 IP 地址。
  - 不支持 SMB 文件共享上使用分布式文件系统命名空间 (DFSN) 或分布式文件系统替换 (DFSR) 的虚拟机。
  - 如果系统是 Hyper-V 服务器兼文件服务器，则虚拟机无法在同一系统的 SMB 文件共享上具有数据。
- 对于 Hyper-V RCT，可以考虑将虚拟机上的所有配置和磁盘对象用于对象复制。
- Data Protector 使用标签 "DP_VEPA" 为 Hyper-V RCT 创建恢复快照。此标签不得用于任何其他检查点，也不得为任何其他检查点更改此标签。

并行磁盘备份

通过此功能，您可以并行备份 VM 下的多个磁盘。要进行并行备份，请将 omnirc 变量 OB2_VEAGENT_THREADED_DISK_BACKUP 设置为 1 (默认行为)。要切换到顺序备份，请将变量设置为 0。您可以通过更新 omnirc 变量 OB2_VEAGENT_DISK_CONCURRENCY 来指定要并行备份的磁盘数。默认情况下，可以并行备份 10 个磁盘。您可以根据需要增加或减少要备份的磁盘数量。

Hyper-V RCT 备份限制

- Hyper-V RCT 解决方案仅在 Windows Server 2016 及更高版本上受支持。
- 仅在 VM 级别支持并行磁盘备份。
- 由于 Microsoft 限制，Data Protector 不会在备份开始时锁定虚拟机。在不锁定虚拟机的情况下，如果同时触发迁移过程，则可能导致备份或还原失败。
- 不支持使用共享虚拟磁盘来备份虚拟机。不支持 VHD 集。
- 当虚拟机处于暂停状态时，Data Protector 只能为其创建崩溃一致快照。在这种情况下，不支持创建应用程序一致快照。
- 不支持在同一虚拟机上同时运行并行备份。

注意

- 如果虚拟机具有 VHD 磁盘，磁盘有用户快照并且已在 Data Protector 2020.11 中备份，则在升级到 Data Protector 2021.02 时，第一个增量备份将恢复为“完整”。
- 如果备份会话突然结束，建议:
  - 不删除标签为 ***DP_VEPA*** 的任何 Data Protector 快照 (如果有的话)
  - 不还原突然结束的会话
  - 执行完整或增量 (Incr) 备份，这将自动清除 ***DP_VEPA*** 快照和突然终止的会话。

静止

对于来宾操作系统在备份时已启动且正在运行的 Windows 虚拟机，Data Protector 在备份之前使用 VSS 框架冻结或静止虚拟机中运行的应用程序的状态。这可确保相关程序的数据一致性 (创建应用程序一致的备份)。对于 RCT 备份，Data Protector 使用 WMI API 创建应用程序一致快

照。

> **注意**要使静止正常运行，请确保在所有 Microsoft Windows 虚拟机上安装 Microsoft Hyper-V 集成服务。

如果来宾操作系统不是 Windows 操作系统，或者未安装 Microsoft Hyper-V 集成服务，则无法进行静止。此类虚拟机在备份时处于暂挂状态。

静止备份流 (Hyper-V VSS)

1. Microsoft Hyper-V 写入程序触发虚拟机中的集成服务。
2. 集成服务触发虚拟机中的 VSS 框架以创建卷影复制 (创建内部卷影复制)。
3. Microsoft Hyper-V 系统中的 VSS 框架创建虚拟机文件所在磁盘的卷影复制 (创建外部卷影复制)在 ZDB 用例中，创建复本存储卷。
4. Microsoft Hyper-V 写入程序在继续备份之前执行自动恢复以使内部和外部卷影复制保持一致，因为内部和外部卷影复制的创建之间有一定的时间差距，并且存储在虚拟机上的某些数据可能在此期间发生更改。

还原概念

您可以从使用 Data Protector Hyper-V 映像或 **Hyper-V RCT** 方法执行的备份中还原完整的虚拟机。

还原虚拟机

使用 Hyper-V 映像或 **Hyper-V RCT** 方法备份的虚拟机可以还原:

- 到默认位置
- 到不同位置
- 到目录

还原到默认位置

从 Hyper-V 映像或 **Hyper-V RCT** 备份还原时，默认情况下，虚拟机将还原到其原始 Microsoft Hyper-V 系统。如果原始 Microsoft Hyper-V 系统上仍存在要还原的虚拟机，则会在还原备份文件之前将其删除。

要保留现有虚拟机 (例如，出于安全原因)，您应在执行还原之前从系统中导出该虚拟机。

> **注意**
>
> - 如果导出的虚拟机被重新导入，那么它实际上就是原始虚拟机的克隆。导入计算机时，系统会询问您是否要使用旧虚拟机 GUID。如果创建导出计算机的原始虚拟机仍然存在，则保留原始 GUID 会导致导入失败。另外，在导入之后，除非更改虚拟机的 IP 地址，否则可能会出现网络问题。
> - 从 Hyper-V RCT 备份还原时，将使用新的 VM GUID 创建虚拟机。

对于还原，您还可以指定:

- 是否应将虚拟机还原到其他 Microsoft Hyper-V 系统
- 是否应启动还原的虚拟机

默认情况下，“选项”页中的选项设置为将具有相同名称和 GUID 的虚拟机和磁盘还原到同一 Microsoft Hyper-V 系统 (或群集)。

在群集中还原

还原在群集中配置的虚拟机时，将运行已还原虚拟机的群集节点取决于选择的还原客户机和还原时的环境状态。它不依赖于备份时的环境状态，即备份时运行虚拟机的位置。

> **注意**如果使用共享群集磁盘 (而不是 CSV)，则只能将虚拟机还原到当前注册虚拟机的节点，因为只有此节点可以访问共享群集磁盘。

还原到不同位置

要将虚拟机还原到其他位置 (在同一系统或其他系统上)，请选择“还原到目标存储路径”。使用 Hyper-V 写入程序执行还原，因此还原的虚拟机可

以正常运行。

还原到目录

还原到目录 (在 Microsoft Hyper-V 系统之外还原) 时，可以将所有虚拟机文件还原到您在所选还原系统上选择的目录 (例如， C:\tmp)。

此类还原完成之后，虚拟机及其各自的虚拟磁盘无法正常运行。需要将文件导入 Microsoft Hyper-V 系统才能使虚拟机正常运行。

还原到目录后，执行以下操作:

1. 通过执行以下操作创建父子关系:
    1. 导航到 Hyper-V 管理器并选择“检查磁盘”操作。
    2. 浏览最新的差异文件以创建从基准磁盘 (VHDx/VHD) 到最新差异文件 (aVHDx/aVHD) 的父子关系。

    > **注意**请注意，如果失败，请通过选中 '忽略 ID 不匹配' 复选框来“重新连接”。

2. 使用以下链接中提供的 Hyper-V PowerShell cmdlet Merge-VHD 将差异文件合并到基准磁盘:
   https://technet.microsoft.com/en-us/library/hh848581.aspx
3. 导航到虚拟机并编辑设置，然后按步骤 2 中所述连接合并的磁盘。

还原单个虚拟机磁盘

从 Data Protector 2018.09(10.10) 开始，可以选择和还原单个磁盘，而无需整体还原虚拟机。

Data Protector 按以下方式自动还原各个磁盘:

选项	描述
到默认位置	磁盘文件将还原到 Hyper-V 主机上执行备份的原始位置。还原后，将合并磁盘或快照中的每个差异。 例如， 假设 C:\hyperv\virtual_hard_disk\disk01.vhd 是备份 disk01.vhd 的原始位置。 通过选择此选项，磁盘将还原到 C:\hyperv\virtual_hard_disk\disk01.vhd 位置。
到不同位置	磁盘文件将还原到 Hyper-V 主机上的给定位置。还原后，将合并每个差异磁盘 (或快照文件)。 例如， 假设 C:\Virtual_Hard_Disk 是备份磁盘的原始位置， C:\hyperv\Restored_Virtual_Hard_Disk 是还原这些磁盘的位置。 通过选择此选项，磁盘将从原始备份位置 (C:\Virtual_Hard_Disk) 还原到用户指定的新位置 (C:\hyperv\Restored_Virtual_Hard_Disk)。
到目录	磁盘文件将还原到 Hyper-V 主机上的给定目录。还原后，不合并任何差异文件 (*.avhdx)。 例如， 还原到目录时，所有虚拟机磁盘文件将还原到您在 Hyper-V 主机上所选的目录 (例如， C:\tmp)。

磁盘还原先决条件

- 虚拟机必须在 Hyper-V 系统中可访问和可用。
- 必须删除或合并快照。(或者) 使用“还原”上下文中的“还原前合并快照”选项。
- 备份期间连接的控制器必须可访问。
- 备份期间磁盘所连接的磁盘或控制器位置必须可用，不能用于连接其他磁盘。否则，还原失败。要使用控制器 (驱动器) 位置强制还原，必须在备份 (vepa) 主机上将 omnirc 变量 (OB2_VEAGENT_FORCE_DISK_RESTORE) 设置为 1 。

  例如，如果磁盘连接到驱动器位置 0 处的“SCSI 控制器”，则虚拟机必须存在相同的“SCSI 控制器”和驱动器位置才能确保磁盘还原成功。“控制器”由控制器 GUID 标识。如果不存在具有 GUID 的控制器，则还原将失败。
- 将新磁盘添加到虚拟机后，请确保为更新的虚拟机运行完整备份会话。

成功还原会话流

成功还原会话包括以下阶段:

1. 关闭虚拟机。
2. 从备份还原磁盘。如果要还原的磁盘仍然存在，则会将其覆盖。
3. 合并差异文件。然后，将合并的磁盘文件连接到具有相同控制器和驱动器位置的虚拟机。
4. 启动虚拟机。

> - 如果磁盘路径位置中有磁盘，则会覆盖与虚拟机关联的磁盘文件。
> - 在磁盘还原之后，合并所有用户创建的和 Data Protector 创建的快照。

还原链验证

选择增量备份会话将虚拟机还原到相应状态时，Data Protector 会自动处理还原链，从在所选会话之前创建的完整备份映像开始，然后还原所有后续增量备份映像，一直到所选会话。为了确保还原数据的完整性，Data Protector 在开始实际数据还原之前检查整个链的有效性。还原链无效会导致会话失败，而不会对虚拟机及其快照进行任何更改。

通过将 omnirc 选项 OB2_VEAGENT_DISABLE_RESTORE_CHAIN_PROTECTION 设置为值 1 ，可以禁用还原链验证。请注意，无法验证不受保护的还原链。Data Protector 尝试验证不受保护的还原链会导致还原会话失败。

还原链保护

在 Microsoft Hyper-V 环境中，为防止还原期间数据丢失，Data Protector 虚拟环境集成将在增量备份会话期间保护还原链。例如，只要在 Data Protector 之外创建或删除虚拟机的备份快照，或者从 Data Protector 内部数据库中删除备份会话，该集成就会在后续增量备份会话开始时检测到此类更改。因此，Data Protector 会自动将受影响会话中的备份类型切换为完整备份。根据您的 Microsoft Hyper-V 环境，回退范围是整个 Microsoft Hyper-V 系统或群集，这意味着将为参与会话的所有虚拟机切换备份类型。

通过将 omnirc 选项 OB2_VEAGENT_DISABLE_RESTORE_CHAIN_PROTECTION 设置为值 1 ，可以禁用还原链保护。Hyper-V RCT 还原不支持此 omnirc 选项。

还原注意事项

- 由于 Data Protector 虚拟环境集成的体系结构基础，请考虑 Microsoft 卷影复制服务 中所述的 Microsoft Hyper-V 写入程序详细信息。
- 如果在 Hyper-V 主机上配置的 HTTPS 端口不是 5986 ，则在备份主机上设置 omnirc 变量 OB2_VEAGENT_HTTPFS_PORT 。
- 对于单个磁盘还原，必须满足以下条件:
  - 在开始还原单个磁盘之前手动删除快照。(或者) 使用“还原”上下文中的“还原前合并快照”选项。
  - 仅适用于作为 Hyper-V 主机的 Windows 2012 及更高版本或 R2。
  - 磁盘还原不考虑较旧的备份。因此，在升级到最新 Data Protector 版本之后，如果需要磁盘级别还原，请执行完整备份。

    此外，如果完成了以下任何操作，请执行完整备份:
    - 删除快照
    - 恢复到快照
    - 添加新的虚拟机磁盘或重命名现有虚拟机磁盘
    - 还原虚拟机
    - 还原虚拟机磁盘
  - 要还原的磁盘必须是完整备份的一部分。如果添加了新磁盘，则需要启动完整备份。
  - WinRM 服务必须在 Hyper-V 主机 (群集中的所有节点) 上已启动并正在运行。
  - 在 Hyper-V 主机上配置 WinRM HTTPS。要配置 WinRM HTTPS，您需要创建 SSL 证书。
  - 在 Hyper-V 主机上启用 PowerShell 远程处理。这适用于群集中的所有节点。

- 对于复制:
  - 从 Hyper-V 群集管理器手动禁用主服务器和复制服务器的复制。
  - 执行复本虚拟机备份时，由于磁盘位置不同，还原到主虚拟机会失败。主虚拟机备份也是如此。
  - 还原后手动启用复制。
- 只能从 Hype-V VSS 备份进行 Hyper-V VSS 还原，只能从 Hyper-V RCT 备份进行 Hyper-V RCT 还原。

还原限制

- Hyper-V RCT 方法不支持单个磁盘还原。
- 对于 Hyper-V RCT 还原，在备份后手动删除群集资源或尝试将虚拟机还原到其他 Hyper-V 群集客户机时，不会自动重新创建它们，而必须手动重新创建它们。
- 不支持将 Hyper-V RCT 虚拟机从 2019 Hyper-V 服务器还原到 2016 Hyper-V 服务器。
- 还原后，所有附加到虚拟机的网络适配器将连接到公用虚拟交换机，而不是连接到备份期间所连接的虚拟交换机。
- 对于 Hyper-V RCT 还原，“还原到目录”和“目标存储路径”选项不支持映射的驱动器。
- 对于 Hyper-V RCT 还原，将使用新的 UUID 重新创建在 Data Protector 2020.11 中备份的 VM。

Data Protector 备份解决方案

- 使用 Data Protector Microsoft 卷影复制服务集成创建的 Hyper-V 备份对象无法使用 Data Protector 虚拟环境集成进行还原。

还原并行性

- 使用相同设备或还原到同一 Microsoft Hyper-V 系统 (或群集) 的还原会话不能并发运行。
- Data Protector 最大限度地优化每个还原会话。选择多个虚拟机进行还原时，如果备份映像是在同一 Data Protector 备份会话中创建的，则该映像中的数据将并行还原。
- 在以下磁盘还原方案中按顺序还原磁盘:
  - 在单个虚拟机中还原磁盘。
  - 在多个虚拟机中还原磁盘。

还原到备份主机

- 无法选择不是作为 Hyper-V 客户机导入的 Data Protector 客户机进行还原。将要用作备份主机的系统导入为 Data Protector Hyper-V 客户机。如果仅将该系统用于还原，则不必在导入期间输入用户凭据。导入后，您可以从“还原客户机”下拉列表中选择客户机。

  还原后，您可以删除 Hyper-V 客户机并将其重新导入为常规 Data Protector 客户机。

  请注意，对于备份主机，您可以选择安装了 Data Protector 虚拟环境集成和 MS 卷影复制集成组件的任何客户机。如果还原规范仅包含要还原的磁盘，则只需要 Data Protector 虚拟环境集成组件。

还原到不同位置

- 如果使用“还原到目标存储路径”选项将配置了自定义路径 (“快照文件位置”和“智能分页文件位置”未设置为默认虚拟机位置) 的复本 VM 或主 VM 还原到默认位置，则“智能分页文件位置”和“快照文件位置”路径不会更新。如果还原包含恢复点的复本 VM，则只有“智能分页文件位置”不会更新。

  还原后，检查“智能分页文件位置”和“快照文件位置”路径，并在必要时进行更新。

  > **提示**要确保在还原后自动更新“快照文件位置”，建议您为复本 VM 配置至少一个恢复点。

还原虚拟机复本

- 选择要还原的虚拟机时，无法确定是否已备份主 VM 或复本 VM。但是，还原后的替换状态取决于备份的虚拟机是主 VM 还是复本 VM:
  - 如果是主 VM，则禁用复制。
  - 对于复本 VM，启动故障转移，使复本 VM 成为主 VM。

    注意执行虚拟机或磁盘还原时，请确保还原不会影响在复本节点上运行的虚拟机。
- **为复制的虚拟机配置网络适配器**

  默认情况下，复本 VM 未连接到网络。还原后，即使已将其还原为主 VM，也没有网络连接。在启动还原的虚拟机之前，应手动将虚拟网络交换机映射到 NIC。

  如果复本 VM 连接到虚拟网络交换机，则主端和复本端使用的虚拟交换机名称应相同，否则无法启动还原的虚拟机。为避免启动问题，请将网络适配器连接到现有虚拟网络交换机或删除连接。
- **群集环境**
  - 如果将具有群集共享卷 (CSV) 数据的主 VM 替换到非群集系统，则还原后虚拟机可能不具备高可用性。

    默认情况下，Data Protector 会将虚拟机还原到原始备份位置。对于复本 VM，这是本地卷，因此 VM 将还原到本地卷，并且现有群集资源组无法联机，因为它不在 CSV 上。Data Protector 删除群集资源组并将虚拟机重新连接到群集。如果还原的虚拟机数据驻留在本地卷上，则存储资源不包含在群集资源组中。

- 如果主虚拟机替换到另一个 Hyper-V 群集上的 CSV，并且主端和复制端上的 CSV 路径相同，则还原后 VM 将高度可用。
- 如果虚拟机不在 CSV 上并且还原虚拟机的存储位置已更改，例如，通过还原到新存储位置或将复本 VM 还原到主群集，则 Data Protector 无法重新创建群集资源组，您必须手动删除并重新创建它。

Windows 共享上的虚拟机

- 在还原到 SMB 文件共享期间，Data Protector VSS 代理需要足够的权限来修改还原虚拟机文件的 ACL。因此，您需要在具有适当权限的域用户帐户下的 Hyper-V 主机上运行 Data Protector Inet 服务。

  或者，将 Hyper-V 主机的计算机帐户添加到文件服务器的 Administrators 组 (SMB 文件共享主机)。
- 在磁盘还原到 SMB 文件共享期间，Data Protector DMA 代理需要足够的权限来修改还原虚拟机文件的 ACL。因此，您需要在具有适当权限的域用户帐户下的 Hyper-V 主机上运行 Data Protector Inet 服务。

  或者，将 Hyper-V 主机的计算机帐户添加到文件服务器的 Administrators 组 (SMB 文件共享主机)。
- 仅当 Hyper-V 计算机帐户 (domain\hyperv$) 对 SMB 文件共享和还原文件具有完全控制权限时，才能将从 SMB 文件共享备份的虚拟机还原到其他 Hyper-V 主机文件。为此，您可以在原始 Hyper-V 主机使用的域安全组中添加目标 Hyper-V 主机。
- 您可以将从 SMB 文件共享或本地卷备份的虚拟机还原到其他 SMB 文件共享。在这两种情况下，Data Protector 将 Hyper-V 计算机域帐户 (domain\hyperv$) 添加到具有完全控制权限的 SMB 文件共享上还原虚拟机文件的 ACL 中。
- 在还原也用作 SMB 文件服务器的虚拟机 (在 Hyper-V 服务器上运行) 期间，您可能会遇到问题。有关详细信息，请阅读以下 Microsoft TechNet 库文章中的“Considerations when using Hyper-V with SMB” 章节: http://technet.microsoft.com/en-us/library/jj134187.aspx#BKMK_prereq

使用其他设备进行还原

您可以使用与备份不同的设备进行还原。

满足 Microsoft Hyper-V 的先决条件

- 确保您已正确安装并配置 Microsoft Hyper-V 虚拟环境。
- 确保您已正确安装 Data Protector。
- 确保您的环境中至少有一个客户机同时安装了 Data Protector 虚拟环境集成和 MS 卷影复制集成组件。此类客户机称为备份主机。备份主机必须与所有 Microsoft Hyper-V 系统/群集建立网络连接。安装后无需进行特殊配置。

  如果要将虚拟机文件还原到备份主机上的目录，还要在备份主机上安装磁盘代理组件。否则，您将无法使用“浏览”按钮指定目标目录 (但是，仍可自行键入该目录)。
- Data Protector 使用 Windows Management Instrumentation (WMI) 查找 Hyper-V 资源。WMI 使用目标系统上的端口 135 创建连接。建立连接后，使用短端口进行通信。
- 配置用于 Data Protector 的设备和介质。
- 要测试 Cell Manager 是否与 Microsoft Hyper-V 系统和备份系统正常通信，请配置和运行 Data Protector 文件系统备份，并在环境中的每个 Microsoft Hyper-V 系统和备份主机上进行还原。

Hyper-V VSS 特定先决条件

- 确保要从其备份或还原到的每个 Microsoft Hyper-V VSS 系统都安装了 MS 卷影复制集成组件。如果您的 Microsoft Hyper-V 系统在群集中配置，它们必须像群集感知客户机那样安装。
- ZDB 环境:
  - 如果虚拟机文件位于磁盘阵列上，请确保已配置并安装相应的 VSS 硬件提供程序。
  - 对于 VSS 可传输备份，还必须在备份系统上安装 MS Volume Shadow Copy 集成。
- 需要将 Data Protector 客户机的主机系统重新导入为 Hyper-V 服务器。

> **注意**对于群集，需要将群集虚拟名称重新导入为 Hyper-V 服务器。

- 您必须首先将 Hyper-V 服务器作为已安装 VSS 组件的客户机导入，然后按照导入和配置 Microsoft Hyper-V 系统中的说明将其导入为 Hyper-V 服务器。
- 确保以下 Windows 组件已安装并在备份和 Hyper-V 主机中可用:

> **注意**Windows 远程管理服务必须在 Hyper-V 主机上运行。还必须在 Hyper-V 主机上启用 PowerShell 远程处理。对于群集，必须使用 PowerShell 远程处理启用所有节点。WinRM 服务支持 Windows PowerShell 远程处理功能，该服务是 Web 管理服务 (WS-Management) 协议的 Microsoft 实现。在群集配置中，WinRM 服务必须在群集的所有节点中运行。要配置和启用 Windows PowerShell 远程处理以接收远程命令，请在 Hyper-V 主机中执行以下操作:

1. 使用 Run as administrator 选项启动 Windows PowerShell。
2. 执行 PowerShell 命令 enable-psremoting 以启用 PowerShell 远程处理并禁用 HTTP 侦听程序。
3. 启用 HTTPS 传输模式。要使用 HTTPS 传输侦听程序机制，您必须拥有 SSL 证书。

   WinRM HTTPS 要求本地计算机服务器身份验证证书的 CN 与主机名匹配、未过期或未撤销。

   为此，请执行以下步骤：

   1. 如果 SSL 证书不可用，则验证并生成自签名证书。

      要验证 SSL 证书，请执行以下操作:

      1. 单击开始。
      2. 在“运行”窗口中，输入 MMC 并单击“确定”。

         此时将显示“控制台根”页。
      3. 在“文件”菜单中，单击“添加/删除管理单元”。

         此时将显示“添加或删除管理单元”页。
      4. 从“可用的管理单元”区域中，选择“证书”并单击“添加”。

         此时将显示“证书管理单元”页。
      5. 选择“计算机帐户”并按照向导说明操作。
      6. 导航到以下位置验证是否在“控制台根”中安装了证书:

         Certificates (Local computer) > Personal > Certificates

         请注意，如果证书未安装在个人文件夹中，则必须手动安装。

      如果证书不可用，您可以使用 makcert 命令创建自签名证书。可从以下位置下载 makecert：

      https://www.microsoft.com/en-us/download/details.aspx?id=8279

      以下命令行包含使用 makecert.exe 在 WinRM 主机上创建证书的语法示例:

      makecert.exe -r -pe -n "CN=host_name,O=organization_name" -e mm/dd/yyyy -eku 1.3.6.1.5.5.7.3.1 -ss my -sr local Machine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12

      certificate_name.cer

      例如：

      makecert.exe -r -pe -n "CN=iwf114072.dprnd.net,O=" -e 02/08/2017 -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12

      cert_iwf1114072.cer

      请注意，必须相应地更改主机名、组织名称和证书名称。
   2. 如果使用以下命令可获取 SSL 证书，则使用正确的指纹和主机名配置 HTTPS 侦听程序:

      winrm create winrm/config/Listener?Address=*+Transport=HTTPS

      '@{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}'

      请注意，要查看 CertificateThumbprint ，您必须访问 **MMC**，双击证书并导航到“详细信息”选项卡。单击“指纹”并选择指纹。将指纹复制并粘贴到记事本中，然后删除空格。此指纹可用于配置 HTTPS。

      例如：

      winrm create winrm/config/Listener?Address=*+Transport=HTTPS

      '@{Hostname="iwf1114072.dprnd.net";CertificateThumbprint="0965bfe4b3170e8e9cb0447daafc1fc09dea7803"}'

      请注意，默认端口 5986 用于执行此命令。如果使用任何其他端口，则必须使用该端口的详细信息执行上述命令。此外，必须在备份主机上使用 omnirc 变量 OB2_VEAGENT_HTTPS_PORT 。

      请注意，必须相应地更改“主机名”和“证书指纹”。此处，“主机名”是指 makecert 命令中使用的完全限定域名。
   3. 检查 Hyper-V 主机上的防火墙例外，然后打开 WinRM HTTPS 端口。

      例如：

      netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow protocol=TCP localport=5986

      请注意，默认情况下，WinRM HTTPS 传输使用 5986 作为默认端口号。如果使用任何其他端口号，请使用该特定端口号。
   4. 从 vepa 主机测试连接，如下所示:

      winrm identify -r:https://host_name:port_number -u:user_name -p:password -encoding:utf-8

- Windows PowerShell 2.0 或更高版本。
- Microsoft .NET Framework 3.5。

> **注意**对于单个磁盘还原，即使您安装了更高版本的 Microsoft .NET Framework，也需要 Microsoft .NET Framework 3.5。

- Windows 远程管理 2.0 或更高版本。

Hyper-V RCT 特定先决条件

- Hyper-V RCT 解决方案要求在 Hyper-V 客户机上安装 Data Protector 虚拟环境集成组件和 MS 卷影复制集成组件。
- 对于 Hyper-V RCT，您必须将 VEPA 服务器作为客户机安装，然后将其作为 Hyper-V 服务器导入。
- 确保 Microsoft WMI 服务在 Hyper-V 客户机和备份主机上都在运行。
- 虚拟机硬件版本应高于 8。

安装 Microsoft Hyper-V 客户机

需要在 Microsoft Hyper-V 系统上安装的 Data Protector 组件会因您要使用的备份和还原解决方案而异。可以从下列解决方案中选择：

- 安装 Microsoft Hyper-V 客户机
- Data Protector Microsoft 卷影复制服务集成

Data Protector 虚拟环境集成

假设您打算安装组件的所有系统已启动并正在运行。在应当控制备份和还原会话 (“备份主机”) 的系统上安装以下 Data Protector 组件:

- Virtual Environment Integration
- MS Volume Shadow Copy Integration
- Disk Agent

  Disk Agent 组件使您在备份主机上还原到某目录时能够使用**浏览**按钮。如果没有安装组件，您必须自行键入目标目录。

在 Microsoft Hyper-V 系统上，安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration

> **注意**如果您的 Microsoft Hyper-V 系统在群集中配置，它们必须像群集感知客户机那样安装。

在备份系统（适用于 VSS 可传输备份）上，安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration

> **注意***备份主机*和*备份系统*不是同一个系统。

配置 Hyper-V 集成

This feature is available in the Express Edition

要配置集成，请执行以下操作:

- 启用自动装载新卷。请参阅在 Microsoft Hyper-V 系统上启用自动装载新卷。
- 导入和配置 Microsoft Hyper-V 系统。请参阅导入和配置 Microsoft Hyper-V 系统。
- ***Microsoft Hyper-V 群集:*** 解析群集节点。请参阅配置 Microsoft Hyper-V 群集。

以下限制适用:

- 对于还原到目录 (在这种情况下，备份主机用作还原客户机)，您使用的应用程序客户机和备份主机必须安装相同的操作系统版本。

在 Microsoft Hyper-V 系统上启用自动装载新卷

为了能够执行联机备份，请通过在每个系统上执行 MOUNTVOL /E 命令，在所有 Microsoft Hyper-V 系统上启用自动装载新卷。

配置 Microsoft Hyper-V 群集

在 Microsoft Hyper-V 群集环境中执行备份之前，通过执行以下命令解析每个群集节点:

```
omnidbvss -resolve -apphost HyperVNode
```

解析需要按顺序执行，通常只需执行一次。

导入和配置 Microsoft Hyper-V 系统

需要将 Microsoft Hyper-V 系统作为 **Hyper-V** 客户机导入 Data Protector 单元。

重要说明无法同时将客户机导入并配置为 Hyper-V 客户机和 VMware vCenter 客户机。

注意群集环境: 如果在群集中配置了 Microsoft Hyper-V 系统，则需要将所有群集节点和虚拟服务器导入为 **Hyper-V** 客户机。

必须配置 Microsoft Hyper-V 系统上的用户帐户控制以自动提升用户权限。

要将客户机导入 Data Protector 单元，请执行以下步骤:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开 Data Protector 单元，右键单击“客户机”，然后单击“导入客户机”。
3. 在“导入客户机”页中，在“名称”选项中输入客户机名称，从“类型”下拉列表中选择 Hyper-V 类型，然后单击“下一步”。。
4. 指定登录凭据:

   用户名和**密码**: 指定对 Microsoft Hyper-V WMI 服务具有相应访问权限的操作系统用户帐户。可以使用以下格式指定用户帐户:

   ```
   DOMAIN\Username
   ```

   如果未指定域，则会自动检测到域。对于 Microsoft Hyper-V 群集，必须同时指定域和用户名。
5. 选择“下一步”。仅当使用的许可证类型为 *Data Protector Express* 时，此选项才可用。否则，该选项将灰显。

   对于 *Data Protector Express*，将列出所选客户机中的 Hyper-V 系统，以及主机名、主机套接字和主机 UUID 信息。
6. 选择要获得许可的 Hyper-V 系统，然后选择“完成”。

   所选系统将获得许可。

   添加或重新申请许可证

   要添加或重新申请许可证，请重新导入 Hyper-V 客户机或转至客户机属性页。未经许可的 Hyper-V 系统与已获许可的 Hyper-V 系统一起列出。

- 要重新申请许可证，请取消选择 Hyper-V 系统，然后选择“完成”以取消许可 Hyper-V 系统。
- 要添加许可证，请选择新服务器，然后选择“完成”以许可 Hyper-V 系统。

更改 Microsoft Hyper-V 系统配置

仅当您具有 Data Protector“客户机配置” 用户权限时，才能更改用于连接到 Microsoft Hyper-V 系统的凭据。

要更改登录凭据，请使用 Data Protector GUI 或 CLI。

使用 **Data Protector GUI**

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“客户机”，然后选择要更改登录凭据的客户机。
3. 在“结果区域”中，单击“登录”选项卡。
4. 根据需要更新凭据，然后单击“应用”。

使用 **Data Protector CLI**

1. 登录到备份主机。
2. 打开“命令提示符”窗口并将当前目录更改为 vepa_util.exe 命令的目录。
3. 执行：

   ```
   vepa_util.exe command --config --virtual-environment hyperv --host HyperVClient --username Username {--password Password | --encoded-password Password}
   ```

   消息 *RETVAL*0 表示配置成功。

使用 omnirc 选项自定义 Data Protector 行为

omnirc 选项可用于对影响 Data Protector 客户机行为的其他设置进行故障诊断或覆盖。适用于虚拟环境集成的选项带有前缀 OB2_VEAGENT 。

备份 Hyper-V 集成

要备份虚拟机，请创建备份规范，然后启动备份会话。

创建备份规范

使用 Data Protector GUI (**Data Protector Manager**) 创建备份规范。

可以使用两种备份方法来创建备份规范:

- Hyper-V 映像备份 (VSS) 方法
- Hyper-V RCT 备份方法

Hyper-V 映像备份 (VSS) 方法

完成以下步骤，以使用 Hyper-V 映像备份方法创建备份规范:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，指定 VSS 备份类型。
4. 单击**确定**。
5. 从“客户机”下拉列表中，选择要从中备份数据的 Microsoft Hyper-V 系统。该列表包含作为 **Hyper-V** 客户机导入 Data Protector 的所有客户机。

   在群集环境中，选择任何群集节点或虚拟服务器。无论选择群集的哪个部分，您都可以备份驻留在群集中的所有 VM。

   从“备份主机”下拉列表中，选择要用于控制备份的系统。该列表包含安装有 Data Protector“虚拟环境集成” 和Data Protector“MS Volume Shadow Copy 集成” 组件的所有客户机。
6. 从“备份方法” 下拉列表中，选择“Hyper-V 映像 (VSS)”
7. 单击“下一步”。
8. 此步骤取决于环境类型:
   - 在非 ZDB 环境中，选择“使用软件提供程序”并单击“下一步”。
   - 在 ZBD 环境中，选择“使用硬件提供程序”并单击“下一步”。
     - 请注意，“跟踪复本以用于即时恢复”选项不可用，因为不支持即时恢复。
9. 对于 IR 备份，“复本类型”下拉列表具有两个选项: “差异 (快照)”和“Plex (克隆/镜像)”
10. 选择要备份的虚拟机。

    在群集中，将为群集的所有节点显示非群集 VM 和群集 VM；非群集 VM 列在其节点下，群集 VM 列在其虚拟服务器下。

    > **注意**如果清除某个对象对应的复选框，则该对象将从备份规范中排除。此后，如果将新虚拟机添加到现有逻辑对象，它将自动包含在备份中。您无需创建新的备份规范。已排除对象的复选框在所选视图中标有红色叉号。
    >
    > 如果排除群集主机，但未明确排除属于该主机的 VM，则即使选中该复选框，VM 也不会包含在备份中。会话管理器中将显示以下警告消息:
    >
    > ```
    > [警告] 来自：VEPALIB_VMWARE@hostname "<DataCenter>" 时间: 日期时间
    > ```
    >
    > ```
    > 正在跳过虚拟机 'VM': 父主机 'hostname1' 已排除 ...
    > ```
11. 单击“下一步”。
12. 选择用于备份的设备。

    要指定设备选项，请右键单击该设备，然后单击“属性”。设置设备并发、介质池和预分配策略。有关详细信息，请按 **F1** 或单击“帮助”。

    还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。有关详细信息，请按 **F1**。
13. 单击“下一步”。
14. 设置备份选项。有关备份规范选项和常用应用程序选项的信息，请按 **F1**。
15. 单击“下一步”。
16. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 可以使用“保存并计划”选项保存并计划备份规范。

Hyper-V RCT 备份方法

完成以下步骤，以使用 Hyper-V RCT 备份方法创建备份规范:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后单击“添加备份”。
3. 在“创建新备份”对话框中，选择空模板。从“备份类型” 下拉列表中选择“本地或网络备份” 。选中“负载已均衡” 复选框。
4. 单击**确定**。
5. 从“客户机”下拉列表中，选择要从中备份数据的 Microsoft Hyper-V 系统。该列表包含作为 **Hyper-V** 客户机导入 Data Protector 单元的所有客户机，这些客户机已安装了 Data Protector 虚拟环境集成 和 Data Protector MS 卷影复制集成组件。

   在群集环境中，选择任何群集节点或虚拟服务器。无论选择群集的哪个部分，您都可以备份驻留在群集中的所有 VM。

   从“备份主机”下拉列表中，选择要用于控制备份的系统。该列表包含安装有 Data Protector“虚拟环境集成” 和Data Protector“MS Volume Shadow Copy 集成” 组件的所有客户机。
6. 从“备份方法” 下拉列表中，选择“Hyper-V RCT”
7. 单击“下一步”。
8. 选择要备份的虚拟机。您可以选择 VM 下的多个磁盘进行并行备份。最多可以选择 10 个磁盘。

   在群集中，将为群集的所有节点显示非群集 VM 和群集 VM；非群集 VM 列在其节点下，群集 VM 列在其虚拟服务器下。
9. 单击“下一步”。
10. 选择用于备份的设备。

    要指定设备选项，请右键单击该设备，然后单击“属性”。设置设备并发、介质池和预分配策略。有关详细信息，请按 **F1** 或单击“帮助”。

    还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。有关详细信息，请按 **F1**。
11. 单击“下一步”。
12. 设置备份选项。有关备份规范选项和常用应用程序选项的信息，请按 **F1**。
13. 单击“下一步”。
14. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 可以使用“保存并计划”选项保存并计划备份规范。

特定于应用程序的备份选项

选项	描述
Pre-exec、**Post-exec**	在备份之前 (**Pre-exec**) 或之后 (**Post-exec**)，在备份主机上调用指定的命令、脚本或应用程序。 在指定的命令行中，不要使用双引号。仅键入可执行文件的名称并确保该文件位于备份主机上的默认 Data Protector 管理命令目录中。
启用 **VM** 的增量备份 (Hyper-V VSS 备份方法支持此 UI 选项)	选择此选项并运行完整备份会话以基于将配置的 Data Protector 备份规范启用 Microsoft Hyper-V 增量备份会话。然后可以稍后在计划或启动后续 Data Protector 备份会话时在 Microsoft Hyper-V 虚拟机的完整备份或增量备份之间进行选择。如果已为其正确准备了要备份的虚拟机，则只能执行增量备份。它会存储自上次任意类型的备份之后对虚拟机进行的任何更改，并在每个备份会话之后进行更新。 此选项可准备备份规范中包含的所有虚拟机。如果清除此选项并运行备份会话，则关于增量备份准备的虚拟机配置将保持不变。 如果选择此选项，则将自动选择**备份选定的 VM** 选项，并且**备份复本 VM** 和**复制链接断开时使用主 VM** 选项将变得不可用。 默认：未选择。
备份选定的 VM(E) (对支持虚拟机替换的系统可用。仅 Hyper-V VSS 备份支持此选项)	选择此选项以备份所选的虚拟机 (VM)，而不考虑它是主 VM 或复本 VM。 默认：选择。

备份复本 VM (对支持虚拟机替换的系统并且未选择“启用 VM 的增量备份”时可用。仅 Hyper-V VSS 备份支持此选项)	即使选择主 VM，也选择此选项以命令 Data Protector 始终备份复本 VM。 如果复制连接断开，则即使选择主 VM，备份也将失败。 默认：未选择。
复制链接断开时使用主 VM (选择“备份复本 VM”时可用。仅 Hyper-V VSS 备份支持此选项)	选择此选项可命令 Data Protector 在复制连接无法正常工作时备份主 VM 而不是复本 VM。 默认：未选择。此选项在选择了“备份复本 VM”时处于选中状态。

修改备份规范

要修改备份规范，请在“上下文列表”中选择“备份”，然后单击“范围窗格”中的备份规范名称。在“结果区域”中，单击相应的选项卡并进行所需的更改。完成后，单击“应用”进行应用。

要显示虚拟环境设置，请在“结果区域”中单击“VE 设置”。并非所有设置都可以修改。

> **注意**要查看源页中的所有虚拟机，而不仅仅是您选择的虚拟机，请从“显示”列表中选择“所有”。

计划备份会话

您可以将备份会话计划为在特定时间自动启动或定期启动。

启动备份会话

交互式备份按需运行。它们对于紧急备份或重新启动失败的备份很有用。

要开始备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。
3. 右键单击所选的备份规范，然后单击“启动备份”。
4. 在“启动备份”对话框的“备份类型”下拉列表中，选择“完整”进行完整备份，或选择“增量”进行增量备份。
5. 从“网络负载”下拉列表中，选择会话所需的网络负载。
6. 单击**确定**。

在成功备份会话结束时，将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录到 Data Protector 客户机，其中安装有 Data Protector 用户界面组件。
2. 打开“命令提示符”窗口并将当前目录更改为 omnib 命令的目录。
3. 执行：

   omnib -veagent_list BackupSpecificationName [-barmode VirtualEnvironmentMode][LIST_OPTIONS]

   其中， VirtualEnvironmentMode 可以是 full（对于完整备份）或 incr（对于增量备份）。

   如果未指定选项 -barmode ，则 Data Protector 会尝试启动完整备份。

   示例

   要使用备份规范 MyVirtualMachines 启动完整备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode full

还原 Hyper-V 集成

可以使用 Data Protector GUI 或 CLI 还原 Microsoft Hyper-V 虚拟机。

查找要还原的信息

您可以从 Data Protector 内部数据库 (IDB) 检索有关备份会话的信息 (例如，有关所用备份介质的信息以及备份期间报告的消息)。

要进行检索，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开“对象”或“会话”。

   如果展开“对象”，则会根据与创建时对应的 Microsoft Hyper-V 系统对备份对象进行排序。

   > **注意**备份对象名称包含虚拟机 GUID。
   >
   > 例如，对于 Hyper-V 映像备份，具有 GUID 4844CA0C-E952-48D9-AE04-C68DDE08F1BR 的数据库的备份对象为:
   >
   > /%2FHyperV/6/4844CA0C-E952-48D9-AE04-C68DDE08F1BR [VEAgent]
   >
   > 对于 Hyper-V RCT 备份方法，具有 GUID 4844CA0C-E952-48D9-AE04-C68DDE08F1BR 和 Hyper-V 系统 hyperv.company.com 的数据库的备份对象为:
   >
   > /12/hyperv.company.com/%2F4844CA0C-E952-48D9-AE04-C68DDE08F1BR [VEAgent]

   如果展开“会话”，则会根据创建备份对象的会话对备份对象进行排序。例如，在会话 2011/02/7-7 中创建的备份对象列在 2011/02/7-7 下方。

   要查看备份对象的详细信息，请右键单击该对象，并单击“属性”。

   > **提示**要查看会话期间报告的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 登录到 Data Protector 客户机，其中安装有 Data Protector 用户界面组件。
2. 打开“命令提示符”窗口并将当前目录更改为 omnidb 命令的目录。
3. 要获取在备份会话 SessionID 中创建的备份对象的列表，请执行:

   ```
   omnidb -session SessionID
   ```
4. 要获取有关备份对象 BackupObjectName 的详细信息，请执行:

   ```
   omnidb -veagent BackupObjectName -session SessionID -catalog
   ```

   以下是备份对象名称的一个示例:

   ```
   quark.company.com:/%2FHyperV/6/4844CA0C-E952-48D9-AE04-C68DDE08F1BR [VEAgent]
   ```

使用 Data Protector GUI 还原

1. 在“上下文列表”中，单击“还原”。
2. 在“范围窗格”中，依次展开“虚拟环境”和要从中进行还原的客户机，然后单击“虚拟环境 [HyperV]”。
3. 在“源”页上，选择使用的备份方法 (Hyper-V 映像 (VSS) 或 Hyper-V RCT)。选择要还原的虚拟机。
4. 在“目标”页中，指定还原目标。
5. 在“选项”页中，指定还原选项。
6. 在“设备”页中，指定用于还原的设备。
7. 单击**还原**。
8. 在“启动还原会话”对话框中，单击“下一步”。
9. 指定“报告级别”和“网络负载”。

注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。

10. 单击**完成**启动还原。

会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

> **注意**如果将虚拟机还原到目录，同时还在会话期间还原其增量备份映像中的数据，要访问还原的虚拟机中的文件夹和文件，则必须先合并虚拟机快照。

还原目标

GUI 选项 omnir 命令选项	描述
备份主机 -barhost	选择应控制还原过程的 Data Protector 客户机。下拉列表包含安装了 Data Protector 虚拟环境集成和 MS Volume Shadow Copy 集成组件的所有客户机。
还原客户机 -apphost，-destination	选择应将所选虚拟机还原到的 Microsoft Hyper-V 客户机。默认情况下，会选择从中备份虚拟机的客户机。
还原到默认位置	选择此选项可将虚拟机还原到所选还原客户机上的原始位置。
还原到目标存储路径 -targetstoragepath	选择此选项可将虚拟机还原到所选还原客户机上的不同位置。 即使 VM 最初在不同的卷上，也会将所有 VM 还原到单个卷。对于每个 VM，原始路径将追加到目标存储路径。
还原到目录 -directory	选择此选项可将虚拟机文件还原到所选还原客户机上的目录。可以使用“浏览”按钮查找目标目录。

还原选项

GUI 选项 omnir 命令选项	描述
在还原之后启动虚拟机 -poweron	选择此选项可在还原之后启动虚拟机。还原到目录时，此选项不可用。
恢复前合并快照 -removeSnapshots	选择此选项可在执行磁盘还原之前合并快照。此选项将合并所有用户创建的和 Data Protector 创建的快照。

现有虚拟机处理	指定在还原现有虚拟机时 Data Protector 的行为。
还原前删除 -deletebefore	选择此选项可在还原之前删除现有虚拟机，然后从新虚拟机将其还原。 仅 Hyper-V VSS 还原支持此选项。 默认 (GUI): 已选定。

跳过还原 -skip	选择此选项可跳过对现有虚拟机的还原。还原多个虚拟机时，选择此选项可以只还原在还原时不存在的虚拟机。

使用 Data Protector CLI 还原

1. 登录到 Data Protector 客户机，其中安装有 Data Protector 用户界面组件。
2. 打开“命令提示符”窗口并将当前目录更改为 omnir 命令的目录。
3. 执行：

```
omnir -veagent -virtual–environment hyperv   -method Hyper-V RCT -barhost BackupHost -apphost OriginalHypervClient [-session BackupID] -vm GUID [-disk diskpath] [-vm GUID...] [–destination DifferentHyperVClient] [-targetstoragepath TargetStoragPathOfAllHyper-V-VMs| -directory RestoreDirectory] [–poweron] [–removeSnapshots]
```

默认情况下，还原类型设置为 Hyper-V VSS 方法。添加 -Hyperv-RCT 方法以执行 Hyper-V RCT 还原。

重要说明备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是*对象复制*会话的会话 ID。

如果存在同一对象的多个副本，则 omnir 语法不允许您指定要从哪个对象副本还原。只有通过设置介质分配优先级列表，才能使用 Data Protector GUI。

注意如果将虚拟机还原到目录，同时还在会话期间还原其增量备份映像中的数据，要访问还原的虚拟机中的文件夹和文件，则必须先合并虚拟机快照。

示例：将虚拟机还原到 Microsoft Hyper-V 系统

假定您要还原的虚拟机是 GUID 为 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C 的 VM1 和 GUID 为 54C22930-E3B9-43AA-AFCD-1E90BB99F130 的 VM2 。在备份时，这些虚拟机在 Microsoft Hyper-V 系统 hyperv1.company.com 上运行。这些虚拟机采用“Hyper-V 映像”备份方法进行备份。

要使用备份会话 2011/01/11–1，将这些虚拟机还原到 Microsoft Hyper-V 系统 hyperv2.company.com 上的默认位置，并启动新还原的虚拟机，请执行:

```
omnir -veagent -virtual–environment hyperv -barhost backuphost.company.com -apphost hyperv1.company.com –session 2011/1/11-1 –vm 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C –vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination hyperv2.company.com –poweron
```

示例：将虚拟机还原到不同位置

假定您要还原的虚拟机是 GUID 为 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C 的 VM1 和 GUID 为 54C22930-E3B9-43AA-AFCD-1E90BB99F130 的 VM2 。在备份时，这些虚拟机在 Microsoft Hyper-V 系统 hyperv1.company.com 上运行。这些虚拟机采用 Hyper-V Image 备份方法进行备份。

要使用备份会话 2011/01/11–1，将这些虚拟机还原到 Microsoft Hyper-V 系统 hyperv2.company.com 上的位置 c:\machines ，并启动新还原的虚拟机，请执行:

```
omnir -veagent -virtual–environment hyperv -barhost backuphost.company.com -apphost hyperv1.company.com –session 2011/1/11-1 –vm 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C –vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination hyperv2.company.com -targetstoragepath c:\machines -poweron
```

示例：将各个虚拟机磁盘还原到 Microsoft Hyper-V 系统中的目录

假设在会话 2016/02/02-5 期间使用 Hyper-V Image 备份方法在 Microsoft Hyper-V 系统 hyperv.company.com 中备份了 GUID 为 54C22930-E3B9-43AA-AFCD-1E90BB99F130 的虚拟机 VM1。要将磁盘 (DiskPath1 C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx 和 DiskPath2 c:\Disk2.vhdx)

还原到还原客户机 client.company.com 上的目录 C:\tmp ，请执行:

```
omnir -veagent -virtual-environment hyperv -barhost client.company.com -apphost hyperv.company.com -instance hyperv -destination hyperv.company.com -session 2016/02/02-5 -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -disk C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx -disk c:\Disk2.vhdx -directory C:\tmp
```

示例：将单个虚拟机磁盘还原到 Microsoft Hyper-V 系统中的原始位置

假设在会话 2016/02/02-5 期间使用 Hyper-V Image 备份方法在 Microsoft Hyper-V 系统 hyperv.company.com 中备份了 GUID 为 54C22930-E3B9-43AA-AFCD-1E90BB99F130 的虚拟机 VM1。要将磁盘 (DiskPath1 C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx 和 DiskPath2 c:\Disk2.vhdx) 还原到还原客户机 client.company.com 上的相应原始位置，请执行:

```
omnir -veagent -virtual-environment hyperv -barhost client.company.com -apphost hyperv.company.com -instance hyperv -destination hyperv.company.com -session 2016/02/02-5 -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -disk C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx -disk c:\Disk2.vhdx
```

> **注意**如果磁盘路径 (示例中为 DiskPath1 和 DiskPath2) 包含特殊字符，则路径必须用单引号括起来。

示例：在 Microsoft Hyper-V 系统之外还原虚拟机

假设在会话 2011/02/12-5 期间使用 Hyper-V Image 备份方法从 Microsoft Hyper-V 系统 hyperv.company.com 备份了 GUID 为 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C 的虚拟机 VM1 和 GUID 为 54C22930-E3B9-43AA-AFCD-1E90BB99F130 的 VM2 。要将 Microsoft Hyper-V 系统之外的虚拟机还原到备份主机 backuphost.company.com 上的目录 C:\tmp ，请执行:

```
omnir -veagent -virtual–environment hyperv -barhost backuphost.company.com -apphost hyperv.company.com -session 2011/2/12-5 -vm 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -directory c:\tmp
```

还原到目录后恢复虚拟机

完成以下步骤以恢复还原到目录的虚拟机 (使用 ***Hyper-V VSS*** *映像备份*方法时):

1.打开 Hyper-V 主机上的 Hyper-V 管理器并选择“导入虚拟机”。

2.指定包含虚拟机配置文件的文件夹。例如: helios

3.选择要导入的虚拟机，然后单击“完成”。

完成以下步骤以恢复还原到目录的虚拟机 (使用 ***Hyper-V RCT*** *备份*方法时):

1.打开 Hyper-V 主机上的 Hyper-V 管理器并选择“导入虚拟机”。

2.指定包含要导入的虚拟机文件的文件夹。例如: C:\tmp\helios

3. 将列出默认的虚拟机名称 **DP_VEPA**。选择要导入的虚拟机，然后单击“完成”。您可以稍后手动更改虚拟机名称。

> **注意**
>
> - 确保在使用现有 UUID 注册或还原之前删除旧虚拟机。
> - 如果虚拟机已还原到网络共享目录上，则将该目录复制到 Hyper-V 主机以进行导入。

手动合并虚拟机快照

当 Microsoft Hyper-V 虚拟机或单个磁盘还原到目录并涉及还原链时，Data Protector 不会自动将增量备份映像合并到其基本备份映像中。相反，Data Protector 将每个备份映像还原到所选目标目录的子目录。要使虚拟机磁盘的卷与上次增量备份会话运行时的状态相同并访问包含的文件夹和文件，则必须手动合并备份映像。

请遵循以下步骤：

1. 在备份主机上目标还原目录的子目录中，枚举文件名不包含字符串 ChildVhd 的所有虚拟硬盘文件 (类型为 *.vhd 、 *.vhdx 、 *.avhd 或 *.avhdx 的文件)。将所有此类文件复制到单个目录。
2. 启动 Hyper-V 管理器。在“操作”窗格中，单击“编辑磁盘”。
3. 在“编辑虚拟硬盘向导”中，单击“浏览”。
4. 在“打开”对话框中，浏览到包含复制的虚拟硬盘文件的目录。
5. 选择最旧的差异虚拟硬盘文件 (类型为 *.avhd 或 *.avhdx 的文件) 并确认所做的选择。
6. 在“编辑虚拟硬盘向导”中，选择“合并”，然后单击“下一步 >”。

7. 选择“到父虚拟硬盘”，单击“下一步 >”，然后单击“确定”确认操作。
8. 重复步骤选择最旧的差异虚拟硬盘文件 (类型为 *.avhd 或 *.avhdx 的文件) 并确认所做的选择。到选择“到父虚拟硬盘”，单击“下一步 >”，然后单击“确定”确认操作。，直到所有虚拟硬盘快照均已合并。
9. 右键单击虚拟硬盘，然后选择“装载”将其卷装载到驱动器号或目录。
10. 复制所需的文件夹和文件。
11. 使用管理工具“计算机管理”，通过右键单击虚拟硬盘卷并选择“分离 VHD”来将其卸除。

还原群集虚拟机

在还原已删除的群集虚拟机之后，因此该虚拟机的任何群集资源都不再可用，还原的虚拟机将成为在节点上运行的本地虚拟机。原因是缺少 Data Protector 无法还原的群集资源配置。虚拟机需要手动配置才能再次成为群集虚拟机，执行方式如下:

1. 确保虚拟机已关闭。
2. 在“服务器管理器”中，展开“功能”、“故障转移群集管理器”和虚拟服务器，右键单击“服务和应用程序”，然后单击“配置服务或应用程序”。
3. 在“高可用性向导”的“选择服务或应用程序”页中，选择“虚拟机”并单击“下一步”。
4. 在“选择虚拟机”页中，选择要配置的虚拟机，然后单击“下一步”。
5. 在“摘要”页中，查看计划的更改，然后单击“完成”。

还原复制的虚拟机

还原 VM (主 VM 或复本 VM) 后，必须手动重新启用复制:

1. 在主服务器上禁用 VM 复制。复制状态将是“失败”。
2. 在主服务器上启用 VM 替换，在“启用替换”向导中转到“选择初始替换方法”页，然后选择“使用复本服务器上现有的虚拟机作为初始副本”。

还原复本 VM 之后，VM 的复制状态为“已故障转移，等待完成”。要将 VM 还原为所选恢复快照，请执行以下操作:

1. 使用 Hyper-V 管理器或故障转移群集管理器取消故障转移。如果最新的 VM 状态是所需的还原状态，则可以直接删除 VM 复制。
2. 启动新的故障转移。在“故障转移”窗口中，选择相应的恢复点，然后单击“故障转移”。VM 将恢复到所选恢复点并自动启动。

监视会话

您可以从 Data Protector GUI 中安装有用户界面组件的任何 Data Protector 客户机监视当前运行的会话。运行备份或还原会话时，监视窗口会显示会话进度。关闭 GUI 不会影响会话。您还可以使用 GUI 的“监视器”上下文监视会话。

适用于 VMware 的虚拟环境集成

本主题介绍如何配置和使用适用于 VMware vSphere 的 Data Protector 虚拟环境集成。Data Protector 与 VMware vSphere (包括 ESX Server、ESXi Server 系统和 vCenter Server 系统) 集成，可以备份和还原下列 VMware 对象:

- 虚拟机
- 虚拟机磁盘
- 虚拟机模板

备份

可以使用以下备份方法：

- vStorage 映像

这些是基于快照的方法，可用于在关闭电源 (脱机备份) 或正常使用 (联机备份) 时备份虚拟机。

Data Protector 提供以下类型的交互式备份和安排的备份：

- 完整
- 增量
- 差异备份

还原

虚拟机可以还原:

- **到数据中心** (与 VMware vSphere 集成)

  此数据中心可以是独立 ESX(i) Server 系统，也可以是由 vCenter Server 系统创建和管理的任何数据中心。

- 到目录

  这可以是安装了 Data Protector 虚拟环境组件的任何客户机上的目录。此类还原完成之后，需要使用 VMware Converter 将已还原的虚拟机映像手动移至 ESX Server 或 ESXi Server 系统。

下一节提供特定于适用于 VMware 的 Data Protector 虚拟环境集成的信息。

建议不要在 VMware vCenter Server 系统或 VMware ESX(i) Server 系统上安装任何 Data Protector 组件。

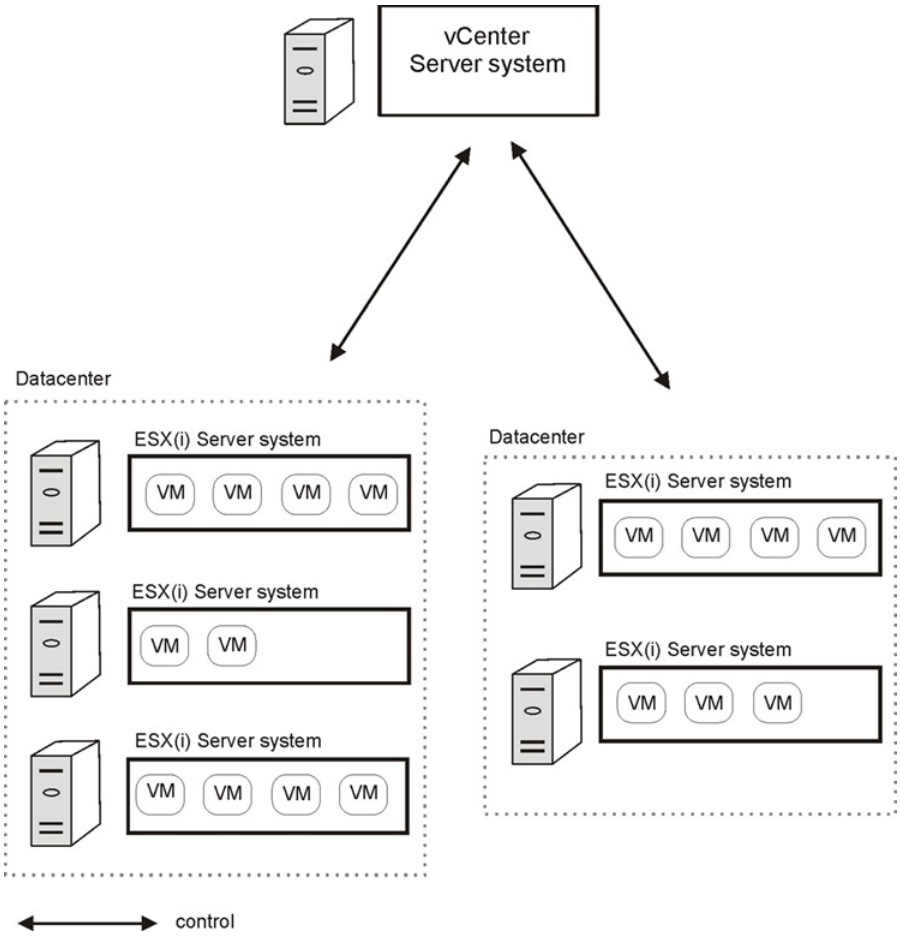
集成概念

Data Protector 支持通过 vCenter Server 管理 ESX 和/或 ESXi Server 系统 (ESX(i) Server 系统) 的环境 (vCenter 环境) 以及具有独立 ESX(i) Server 系统的环境 (独立 ESX(i) Server 环境)。此外，它还支持具有独立 ESX(i) Server 系统的环境，以及混合环境（其中一些 ESX(i) Server 系统通过 vCenter Server 系统进行管理，而另一些系统则为独立系统）。环境中甚至可以有多个 vCenter Server 系统，每个系统都管理自己的一组 ESX(i) Server 系统。

vCenter 环境

在 vCenter 环境中，Data Protector 通过 vCenter Server 系统与 VMware vSphere 进行通信。所有备份和还原请求均在此处发送。

在一个会话中，您可以从一个或多个数据中心备份虚拟机。



vCenter 环境

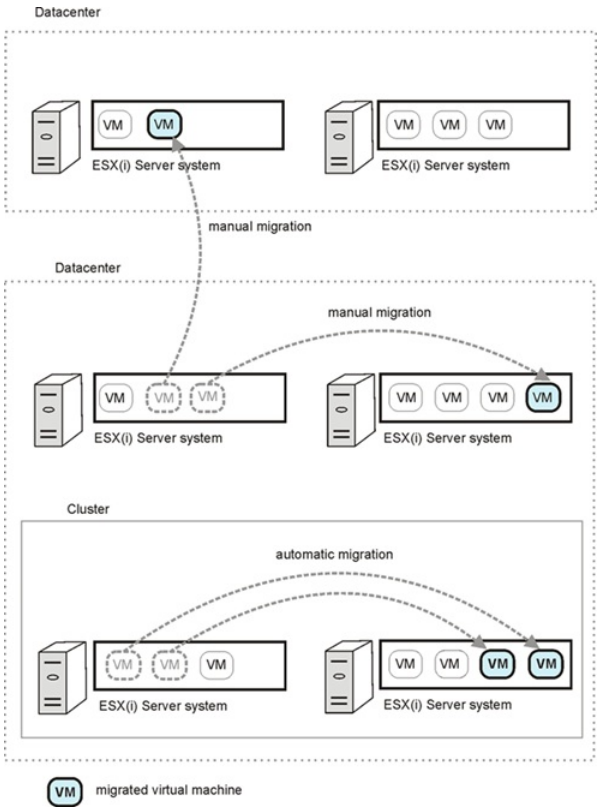
vCenter 环境	描述
ESX Server 或 ESXi Server 系统	VMware 平台能够托管多个虚拟机。
VM	虚拟机。虚拟化 x86 或 x64 PC 环境，在其中可以运行来宾操作系统和相关的应用程序软件。
数据中心	由一个或多个 ESX Server 和/或 ESXi Server 系统以及虚拟机 (数据存储) 的相关存储组成的组织单元。数据存储可以驻留在本地磁盘/RAID、iSCSI 或 SAN 存储上。

迁移虚拟机

在 vCenter 环境中，Data Protector 支持在同一数据中心和 (对于支持的 VMware vSphere 版本) 不同数据中心的 ESX(i) Server 系统之间迁移虚拟机 (使用 VMotion 和 Storage VMotion)。

由于各种原因，虚拟机从一个 ESX(i) Server 系统迁移到另一个 ESX(i) Server 系统:

- 如果在 VMware 高可用性群集中配置了 ESX(i) Server 系统，则虚拟机会在原始 ESX(i) Server 系统发生故障时自动迁移。
- 如果在 VMware 负载均衡群集中配置了 ESX(i) Server 系统，则虚拟机会自动迁移到工作负载更少的 ESX(i) Server 系统。
- 您可以使用 VMware vSphere 客户机手动启动虚拟机迁移。



无论迁移的原因是什么，之后都不需要创建新的备份规范。Data Protector 将自动查找迁移的虚拟机并进行备份。

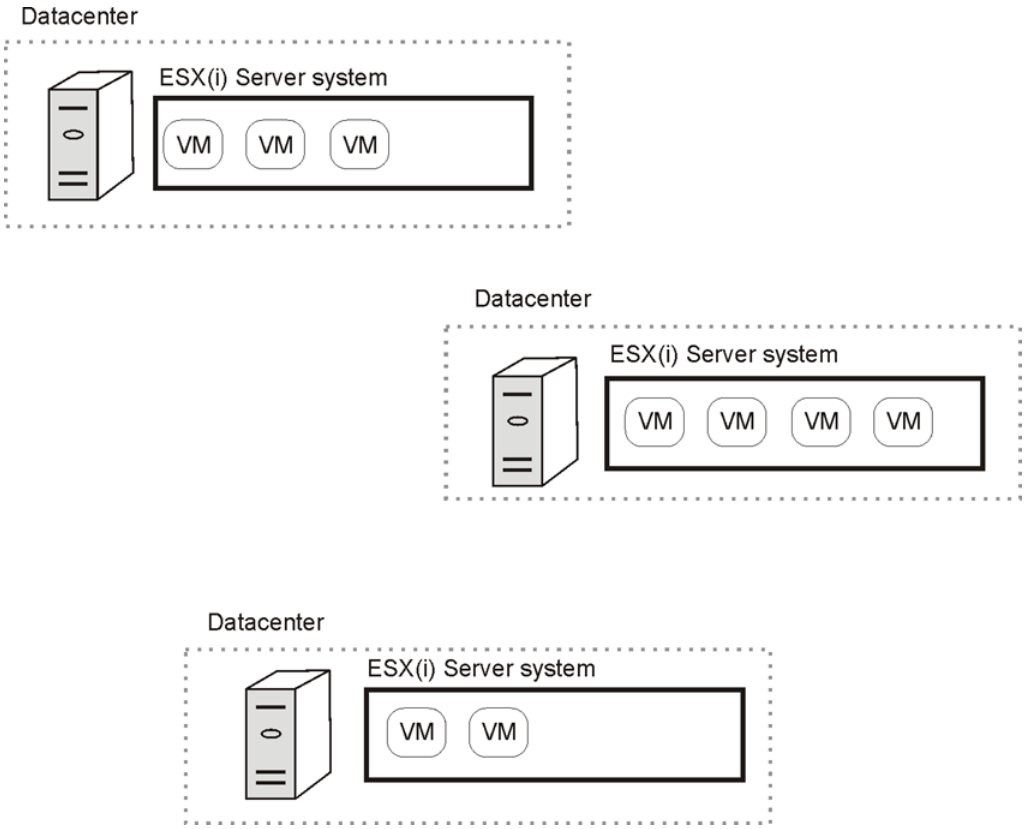
群集中的 vCenter Server 系统

Data Protector 还支持在 Microsoft Cluster Service 群集中运行 vCenter Server 系统的环境。在此类群集中进行故障转移后，您无需更改备份规范。但是，如果在备份或还原会话期间发生了故障转移，则会话将失败，必须重新启动。

独立 ESX/ESXi Server 环境

在独立 ESX(i) Server 环境中，Data Protector 通过 ESX(i) Server 系统与 VMware vSphere 进行通信。所有备份和还原请求均在此处发送。

在单个会话中，您只能从一个 ESX(i) Server 系统备份虚拟机。



Data Protector 组件

Data Protector Cell Manager

Data Protector Cell Manager 可以安装在虚拟机、vCenter Server 系统上或虚拟环境之外的单独系统上。

Data Protector 虚拟环境集成组件

Data Protector 虚拟环境集成组件 (**VEAgent**) 必须安装在单元中的至少一个 Data Protector 客户机上。此客户机称为备份系统，可以是:

- 虚拟机
- vCenter Server 系统
- Data Protector Cell Manager
- 专用的物理备份系统

该组件包括以下主要部分:

- vepa_bar.exe ，在虚拟环境上执行备份和还原操作期间激活。
- vepa_util.exe ，在虚拟环境上执行浏览和查询操作期间激活。
- vepalib_vmware.dll ，用于 VMware vSphere 特定备份、还原、查询和浏览任务的动态链接库。
- vepalib_hyperv.dll ，用于 Microsoft Hyper-V 特定备份、还原、查询和浏览任务的动态链接库。
- vepalib_h3ccas.dll ，用于 H3C CAS 特定备份、还原、查询和浏览任务的动态链接库。

> **注意**VEPA 代表虚拟环境保护代理。

Data Protector 磁盘代理组件

必须在备份系统上安装 Data Protector Disk Agent组件才能使用浏览目录按钮 (还原到备份主机上的目录时，将使用此按钮)。

Data Protector 介质代理

必须在将数据传输到备份设备的客户机上安装 Data Protector 介质代理组件。

> **注意** Virtual Environment Integration 组件不允许备份主机写入备份设备。您仍然需要安装了 Media Agent 组件的客户机。但请注意， Cell Manager 、 Virtual Environment Integration 和 Media Agent 组件可以安装在同一系统上 (物理或虚拟)。

注意事项

- 常规注意事项
  - 从链接克隆创建的卷影 VM 不在考虑范围内。
- 仅当后续备份会话也连接到 vCenter 客户机时，才能清理连接到 vCenter 客户机的备份会话留下的陈旧磁盘，并且仅当后续备份会话连接到 ESX 客户机时才能清理连接到 ESX 客户机的备份会话留下的陈旧磁盘。
  - 如果具有通过连接到 ESX 客户机创建的备份规范的备份会话突然结束，则后续的备份会话也应具有通过连接到 ESX 客户机创建的备份规范。这将成功清理以前连接的磁盘。
  - 如果具有通过连接到 vCenter 客户机创建的备份规范的备份会话突然结束，则后续的备份会话也应具有通过连接到 vCenter 客户机创建的备份规范。这将成功清理以前连接的磁盘。
- 还原注意事项
  - 如果要还原的 Nova 实例的备份卷影 VM 部分已附加到任何其他 Nova 实例，则无法进行还原。
  - 如果要还原的 Nova 实例已附加较新的卷影 VM (备份时无法使用)，则在还原-分离过程中，Nova 实例中的卷影 VM 将会分离。
  - 还原期间分离的卷影 VM 在还原之后不会附加。
  - 如果备份的卷影卷与原始实例在还原时分离，则卷影卷也会还原。
  - 在还原过程中，不会并发显示所有所需的介质。这是因为对于任何 VMWare 备份，至少有两个对象 - 一个用于备份 VM 配置数据 (VEAgent)，另一个用于备份 VM 磁盘 (VEAgentDisk)。在还原期间，首先还原 VM 配置数据，仅显示用于备份配置数据的介质，不显示磁盘备份介质。还原 VM 配置数据后还原 VM 磁盘，显示用于备份 VM 磁盘的其余介质。

静止

如果选择了静止，则快照进程将静止所有系统写入程序和已注册的应用程序写入程序。在 Windows 来宾操作系统中，VSS 框架在创建快照之前冻结或静止在虚拟机中运行的应用程序。每次为备份选择“使用静止”选项时，Data Protector 都会执行应用程序一致的静止。

选中“使用静止快照”复选框。您可以选择要报告的错误级别。可选择以下错误级别:

- **致命**: 如果静止快照失败，则会话将失败。
- **警告**: 如果静止快照失败，则会显示一条警告消息并继续备份过程。

> 启用“静止”选项后，针对 MS SQL、MS SharePoint、MS Exchange 和 Oracle 的虚拟机备份具有应用程序一致性。当按照供应商的建议配置应用程序时，一致性效果最佳。Data Protector 建议在虚拟机中安装相应的集成代理以保护这些应用程序。

以下先决条件适用:

- 对于共享点服务器的基于 VEPA 的静止备份，必须在开始备份虚拟机之前注册 VSS 写入程序。有关详细信息，请参阅《适用于 Microsoft 卷影复制服务的集成指南》中的“Microsoft SharePoint Services Writer 详细信息”一节。
- 对于 Oracle 11g 版本 2 数据库的基于 VEPA 的静止备份，在开始备份虚拟机之前，Oracle VSS 写入程序服务应处于活动/运行状态。可以通过执行命令 `oravssw /q /start` 完成此操作。对于 SQL 和 SharePoint 等其他应用程序，默认情况下，VSS 写入程序已注册并处于活动状态。

以下限制适用：

- “静止”功能可能会大幅降低备份会话的速度。
- VEPA 静止功能不支持 Windows OS 群集中的“可用性组”群集应用程序上的 Microsoft SQL 数据库。
- VEPA 备份不支持在共享模式下对磁盘使用 SCSI 控制器的群集应用程序。
- vRDM 磁盘只能用于完整备份。
- 处于“关闭”状态的虚拟机的静止备份无效。

静止操作注意事项

- VMware 注意事项
  - 不要禁用虚拟机的 UUID 属性。
  - 虚拟机只能使用 SCSI 磁盘。具有 IDE 磁盘的虚拟机不支持应用程序一致的静止。虚拟机中的空闲 SCSI 插槽数量必须与磁盘数量相同。
  - 物理 RDM 不能用于静止，因而不支持快照。
  - Microsoft 群集上的虚拟机备份不支持静止。有关详细信息，请参阅在使用总线共享配置的虚拟机上备份。
- 虚拟机注意事项
  - 虚拟机不得使用动态磁盘。
  - 确保在虚拟机中安装了最新版本的 VMware 工具。有关详细信息，请参阅验证 Vmware 工具内部版本。
  - 必须在 VMware 工具升级过程中明确指定 VSS 组件。VSS 不会以非交互式模式安装。有关详细信息，请参阅使用 Vmware 工具安装卷影复制服务。
  - 必须在 VMware 工具安装期间运行分布式事务处理协调器服务。否则，VSS 无法使 Windows 系统处于静默状态。
  - 确保所有相应的 VSS 应用程序服务正在运行并正确列出了启动类型。

有关 VSS 静止相关问题的详细信息，请参阅卷影复制 (VSS) 静止相关问题故障诊断。

磁盘空间要求

虚拟机备份要求虚拟机磁盘所在的数据存储中具有足够的磁盘空间，可以容纳存储系统上的快照和复本。

所需可用空间选项

您可以使用 Data Protector 的“所需可用空间 (%)”选项确保仅当具有足够的可用空间时才备份虚拟机。

所需的可用空间根据创建快照之前的虚拟机磁盘大小进行计算。Data Protector 会检查虚拟机磁盘所在的所有数据存储。如果其中一个数据存储不满足指定的可用空间百分比，则不会创建任何快照，并且虚拟机的备份将失败并显示错误。

备份多个虚拟机时，该检查将分别应用于每个虚拟机。将备份通过检查的虚拟机，而不备份未通过检查的虚拟机。

如果指定 0％，则省略该检查。

示例

以下示例说明了“所需可用空间 (%)”选项的工作原理:

1. 使用驻留在数据存储 "datastore1" 上的磁盘 "disk1" 备份单个虚拟机 "test1":

   如果在“所需可用空间 (%)”选项中指定 30% 且数据存储的大小为 100 GB，当数据存储上至少有 30 GB 的可用空间时，备份将成功。

2. 使用驻留在 "datastore1" 和 "datastore2" 这两个数据存储上的 "disk1" 和 "disk2" 这两个磁盘备份单个虚拟机 "test1":

   如果指定需要 30% 的可用空间，当每个数据存储上至少有 30 GB 的可用空间时，备份将成功。

3. 备份两个虚拟机，即使用数据存储 "datastore1" 上的磁盘 "disk1" 备份虚拟机 "test1"，使用数据存储 "datastore2" 上的磁盘 "disk2" 备份虚拟机 "test2":

   如果需要 30% 的可用空间，当每个数据存储上至少有 30 GB 的可用空间时，这两个虚拟机的备份将成功。例如，如果数据存储 "datastore1" 的可用空间少于 30% 且数据存储 "datastore2" 至少具有 30% 的可用空间，则虚拟机 "test1" 的备份将失败，虚拟机 "test2" 的备份将成功。如果这两个数据存储的可用空间均少于 30%，则两个虚拟机的备份都将失败。

磁盘空间要求

备份方法	数据存储上需要的磁盘空间	说明
vStorage 映像	所有虚拟机磁盘大小的总和，加上: • 任何静止 zip 文件的大小 (如果指定了静止)。	创建虚拟机快照时，对虚拟机磁盘所做的更改将记录到单独的文件中 (为每个虚拟机磁盘创建一个差量文件)。差量文件可以增长到原始虚拟磁盘的大小。

备份磁盘缓冲区

您可以使用 omnirc 选项 OB2_VEAGENT_BACKUP_DISK_BUFFER_SIZE 指定备份磁盘缓冲区。

SAN 和 HotAdd 备份支持 1 MB 到 256 MB 的磁盘缓冲区大小。默认情况下，其磁盘缓冲区大小为 8 MB。但是，NBD 和 NBD (SSL) 等网络备份始终使用默认磁盘缓冲区大小 1 MB 执行。

注意

- 如果没有足够的内存用于指定的磁盘缓冲区大小，则将回退至 1 MB 磁盘缓冲区大小以保持备份运行，并显示一条警告消息。
- 使用更大的磁盘缓冲区大小可以提高备份性能，但也会增加内存消耗。在一定程度上，由于备份主机的限制，备份性能不再提高。

备份并行性

默认情况下，虚拟机并行备份。在极少数情况下，这可能会导致问题。例如，备份会话可能意外结束。在这种情况下，您可以将备份主机上的 Data Protector OB2_VEAGENT_THREADED_BACKUP omnirc 选项设置为 0 以禁用并行备份。在这两种情况下，都会按顺序备份虚拟机磁盘。

注意默认情况下，使用 VEAgent 集成备份虚拟机时，最多会执行 10 个并发线程。此处，每个线程引用一个用于处理备份集并将其从虚拟机主机流式传输到备份目标的 Data Protector 服务。虽然默认设置为受保护的虚拟机提供增强的备份性能，但由于 10 个 I/O 连接并非由虚拟化层管理，且因此不受虚拟化主机上的负载均衡服务的限制，它将为虚拟基础架构施加中度负载。但是，您可以使用 OB2_VEAGENT_VCENTER_CONNECTION_LIMIT 变量修改此设置，以满足系统设置的要求。

备份考虑事项

- **更改块跟踪 (CBT) 和混合快照处理模式**
  支持 CBT 备份方法和混合快照处理模式。
- 并发备份会话
  使用相同设备的备份会话无法并行运行。
  无法与 ESX(i) Server 系统或虚拟机所在的数据中心并行备份虚拟机。
  备份同一数据存储中的虚拟机的备份会话无法在同一个 Cell Manager 或不同的 Cell Manager 中并行运行。
- **传输模式**

可以使用各种传输模式进行备份。

建议使用 CBT 进行增量/差异备份，因为其速度更快且在备份设备上占用的空间更少。

传输模式可以是 SAN 或 NBD，可以通过 Data Protector GUI 选择 (这决定了阵列访问方式)。也可以在虚拟机选项中配置传输模式。在虚拟机选项中配置的传输模式优先执行，并遵循以下顺序 SAN:HOTADD:NBDSSL:NBD:FILESYSTEM

例如，

- ◦ 如果已从 Data Protector GUI 的虚拟机选项中选择 NBD
  ◦ 如果 SAN 不可用
  ◦ 如果 HOTADD 解决方案无法进行零宕机时间备份
- **厚磁盘和精简磁盘**

Data Protector 无法检测虚拟机磁盘是厚磁盘还是精简磁盘。在这两种情况下，都会备份完整的磁盘 (即，即使空间仍为空，也会备份在磁盘创建时分配的完整空间)。请注意，并非所有数据存储都支持更改后的块跟踪。

- **LUN 的呈现**

要从 3PAR 复本对虚拟机进行零宕机时间备份，请确保用于创建源数据存储 (要备份的虚拟机的驻留位置) 的 LUN 未呈现给配置为装载代理主机的系统。

- **备份到 StoreOnce Catalyst 设备**

从 9.07 开始，到 StoreOnce Catalyst 设备的所有 VEPA 备份都使用“每个存储介质单个对象”模式执行。即使未在 StoreOnce Catalyst 设备上选择此选项，也将强制执行此模式。
将忽略您在“存储介质大小阈值 (GB)”字段中输入的任何值，以从完成到 StoreOnce Catalyst 设备的备份启用缓存 GRE 或启动和实时迁移。

- **Data Protector 许可证**

从 3PAR 复本执行虚拟机的零宕机时间备份无需以下许可证:

- 适用于 UNIX 的 Data Protector 即时恢复扩展 - 1 TB
- 适用于 Linux 的 Data Protector 即时恢复扩展 - 1 TB
- 适用于 Windows 的 Data Protector 即时恢复扩展 - 1 TB

还原概念

您能够以不同的方式还原使用任一 vStorage 映像备份方法所备份的 VMware 对象。

还原使用“vStorage 映像”方法备份的 VMware 对象

那些使用 **vStorage 映像**方法备份的虚拟机、虚拟机磁盘和虚拟机模板可以恢复：

- 到数据中心
- 到备份主机上的目录

还原到数据中心

默认情况下，虚拟机恢复到原始数据中心和原始数据存储，但您可以根据需要选择其他数据中心。

默认情况下，Data Protector 将在恢复之前删除虚拟机（如果存在），即使虚拟机所在的数据中心与恢复到的数据中心不同时也是如此。

> **注意**如果在还原向导的“还原客户机”选项中选择 ESX(i) Server 客户机 (目标客户机)，将不会删除迁移的虚拟机，因为 ESX(i) Server 客户机无法检测位于不同 ESX(i) Server 客户机上的虚拟机 (只有 vCenter 客户机才能做到这一点)。因此，最后会得到两个拥有相同 UUID 的虚拟机。

或者，您可以选择仅当虚拟机不存在时还原虚拟机，使现有虚拟机保持不变。

对于该还原，您还可以指定以下内容:

- 是否应在数据中心注册还原的虚拟机
- 还原完成时是否应合并还原的虚拟机快照
- 是否应启动还原的虚拟机

默认情况下，提供的还原选项设置为将虚拟机还原到原始数据中心。

您可以将虚拟机和虚拟机磁盘从复本还原到数据中心。请注意，不支持从复本到目录的还原会话。在“磁盘 + 磁带”备份中，如果管理员循环或删除了复本，则从磁带进行还原。

还原单个虚拟机磁盘

为了能够将单个虚拟机磁盘还原到数据中心，原始虚拟机必须仍然存在。否则，还原失败。

还原会话的进度如下:

1. 关机虚拟机的电源。
2. 如果要还原的磁盘仍然存在，则会将其删除。
3. 从备份还原磁盘。

> **注意**还原之后，属于动态磁盘集或来自不同时间点的虚拟磁盘可能需要用户在来宾操作系统和/或其中运行的应用程序上执行其他操作 (例如，装载、重签名或恢复)。

还原到目录

恢复到目录（在数据中心外部恢复）时，虚拟机的所有文件将恢复到您在备份主机上所选的目录（例如， C:\tmp ）。

在指定的目录中，使用与备份时虚拟机（及其虚拟磁盘）所在的数据存储对应的名称创建子目录。与虚拟磁盘相关的文件恢复到各自的子目录。

此类恢复完成之后，虚拟机无法正常运行。需要使用 VMware Converter 将已还原的虚拟机映像手动移至 ESX(i) Server 系统，如还原到目录后恢复虚拟机中所述。

还原使用“vStorage 映像 + OpenStack”方法备份的 Nova 实例和卷影 VM

还原会话的进度:

1. 查询 IDB 以获取附加到 Nova 实例的卷影 VM 列表。
2. 查询 vCenter 以创建 Nova 实例和卷影 VM 的映射。
3. 相关的卷影 VM 将添加到还原对象列表中。
4. 查询 vCenter 以创建映射 (步骤 3) 并验证卷影 VM 是否附加到原始实例。
5. 从 IDB 查询还原版本以获取还原链。
6. 从 vCenter 中删除卷影 VM 文件。
7. 从 vCenter 中删除 Nova 实例文件。
8. 在相同的文件夹结构中还原 Nova 实例和磁盘文件。
9. 还原卷影 VM 配置文件。
10. 注册虚拟机并还原网络。

> **注意**如果还原期间 vCenter 中提供了所选 Nova 实例，则会在删除该 Nova 实例之前分离卷影 VM。

Data Protector 还原之后，要将 OpenStack Horizon 仪表板中的 OpenStack 实例恢复到正确的状态，请执行以下步骤:

1. 通过执行以下命令在“Nova 代理”节点中重新启动“Nova 计算”服务:

   Service nova-compute restart

2. 刷新 Horizon 仪表板以检查 Nova 实例是否可用。如果 Nova 实例不可用，请连接到“OpenStack 管理”节点并执行以下命令:

   - Nova list : 列出 Nova 实例。
   - Nova reset-state –active “instance-uuid” : 将 Nova 实例的状态重置为活动。
   - Nova reboot “instance-uuid” : 重新启动 Nova 实例。

   重新启动之后，刷新 Horizon 仪表板并检查 Nova 实例的可用性。

还原链

从在增量或差异会话中创建的备份还原虚拟机时，Data Protector 会自动还原整个备份链，从上次完整备份开始，然后是差异备份和所有后续增量备份 (如果存在)，一直到所选会话。

并行磁盘还原

此功能允许您通过将 omnirc 变量 OB2_VEAGENT_THREADED_DISK_BACKUP 设置为 1 (默认行为) 来并行还原 VM 下的多个磁盘。要切换到顺序还原，请将该变量设置为 0。要切换到顺序还原，请将该变量设置为 0。您可以通过更新 omnirc 变量 OB2_VEAGENT_DISK_CONCURRENCY 来指定要并行还原的磁盘数量。 默认情况下，可以并行还原 10 个磁盘。您可以根据需要增加或减少要还原的磁盘数量。

启动和实时迁移

启动

可以在几秒钟内从驻留在 3PAR 复本 (本地或远程复制)、智能缓存、StoreOnce Catalyst 和数据域设备上的 Data Protector 备份映像即时启动虚拟机。之前，仅在完整的数据迁移到生产数据中心之后才必须开启虚拟机。如果想要验证备份的健全性，请使用此功能。请注意，启动虚拟机后对其所做的更改将一直可用，直到您执行执行清理操作为止。

启动虚拟机时，备份映像将呈现给目标 ESX Server。将创建一个新的虚拟机，其数据磁盘指向 Data Protector 备份映像。其他文件驻留在目标

数据中心。

> **注意**数据域系统 (OS 版本 6.1) 的阈值限制为每个进程 64 个连接。此限制影响“启动”和“实时迁移”操作支持的增量会话数。如果达到此阈值限制，将显示一条消息。要继续执行“启动”和“实时迁移”操作，请通过关闭当前处于活动状态的“启动”请求释放连接。

实时迁移

此选项将从备份映像启动虚拟机，并同时启动到目标数据存储的数据迁移。在此过程中，虚拟机一直可访问。由于数据移动是后端操作，因此对已启动的虚拟机的使用和可访问性产生的影响最小。对虚拟机数据所做的任何修改都将合并，在迁移的虚拟机上，所有修改的内容都将覆盖从备份还原的映像。

数据迁移完成后，虚拟机将从目标数据存储运行，不依赖于备份映像。此外，将删除备份映像呈现。

> **注意**
>
> - 在 Windows 备份主机上使用“启动”和“实时迁移”时，确保 Data Protector INET 服务和 Data Protector 过滤器侦听程序服务正在使用相同的用户凭据运行。
> - 仅当原始备份驻留在其中一个受支持的设备上时，才可以执行“启动”和“实时迁移”操作。如果备份驻留在不受支持的设备上并且对受支持的设备执行了对象复制，则无法执行这些操作。
> - 仅当原始备份已过期且副本提升为原始备份时，才能从复制的会话执行“启动”和“实时迁移”操作 (如果在受支持的设备上)。
> - 数据域系统 (OS 版本 6.1) 的阈值限制为每个进程 64 个连接。此限制影响“启动”和“实时迁移”操作支持的增量会话数。如果达到此阈值限制，将显示一条消息。要继续执行“启动”和“实时迁移”操作，请通过关闭当前处于活动状态的“启动”请求释放连接。

仅 StoreOnce Catalyst 和数据域设备

- 支持从完整备份，增量备份和差异备份执行“启动”和“实时迁移”操作。
- 9.05 和 9.06 备份支持从对象副本执行“启动”和“实时迁移”操作。应该基于会话执行对象复制以确保数据一致性。

  > **注意**如果要将 Data Protector 9.05 或 9.06 版本的备份迁移到 StoreOnce Catalyst 和数据域设备以使用“启动”和“实时迁移”功能，则建议您通过单独的会话执行对象操作。如果同时选择多个会话，则无法确保数据一致性。

- 如果从 StoreOnce Catalyst 设备启动虚拟机，则必须在执行“实时迁移”操作之前清理虚拟机。

清理/关闭

Data Protector 存储所有已启动虚拟机的列表。它将有关所有已启动虚拟机的详细信息以 XML 文件的形式存储在 Cell Server 中。清理和关闭操作如下所列:

- 如果虚拟机已开机超过 24 小时，则会关闭并清理相关存储。
- 如果从复本启动虚拟机，则将卸除数据存储并从阵列中删除在启动过程中创建的复本。
- 如果从智能缓存、StoreOnce Catalyst 或数据域设备启动虚拟机，则在清理过程中将删除数据存储，并删除 NFS 共享。

请注意，上述操作适用于通过“启动”功能启动的虚拟机。

开机超过 24 小时的虚拟机将在下次日常维护作业期间进行清理操作。在日常维护作业中清理的所有虚拟机均记录在 poweronvms_cleanup.log 文件中。

有关启动和实时迁移过程的详细信息，请参阅使用 Data Protector GUI 还原。

请注意，智能缓存设备上的增量和差异备份不支持启动和实时迁移。

还原注意事项

- **并发会话**

  使用相同设备的还原会话不能并发运行。

- **失败还原会话**

  有时，当虚拟机还原失败时，Data Protector 会在数据存储上创建额外的文件，您需要在会话完成时手动清理这些文件。否则，可能会在后续会话中创建损坏的虚拟机备份，而且从此类备份还原也会失败。有关详细信息，请参阅在还原失败后清理数据存储。

  当虚拟机还原到块大小与虚拟机磁盘大小不兼容 (即 .vmdk 文件大小不是多个数据存储的块大小) 的非原始数据存储时，还原将失败。

- **vApp 中的虚拟机**

  还原备份时驻留在 vApp 容器中的虚拟机时，该虚拟机不会还原到 vApp 容器，而是还原到 ESX(i) Server 根级别。如果 vApp 容器中的虚拟机仍然存在，则会将其删除或跳过还原，具体取决于您在“现有的虚拟机处理”选项中所做的选择。

- **从 vStorage 映像备份执行部分还原**

  当从 vStorage 映像备份执行部分还原 (例如，还原许多已备份的 VM 磁盘中的仅其中一些时)，忽略默认选项“还原后删除”并改用“还原前删除”选项。

- **传输模式**

  以下建议适用于特定的虚拟机传输模式:

  - *SAN 传输模式:* 要使用 SAN 传输模式进行还原，请执行以下操作:
    - 为还原会话选择物理备份主机。
    - 确保呈现给备份主机和 ESX(i) Server 系统的存储卷并非只读。有关如何检查存储卷属性的详细信息，请参阅“使用 SAN 传输模式的还原会话失败”。
    - 确保存储卷大小是基础 VMFS 块大小的倍数。否则，对余数的写操作将失败。例如，如果存储卷大小为 16.3 MB 且块大小为 1 MB，则写入余数 0.3 MB 将失败。有关详细信息，请参阅以下位置的 VMware 知识库文章:

      http://kb.vmware.com/selfservice/microsites/searchEntry.do。

      搜索“使用 SAN 传输进行备份和还原的最佳实践”。
  - 建议使用 CBT 进行增量/差异备份，因为其速度更快且在备份设备上占用的空间更少。

- *Hotadd 传输模式:* Hotadd 传输模式可用于还原，但 VMware 不支持多个磁盘。因此，在 HotAdd 环境中，使用 omnirc 选项 OB2_VEAGENT_RESTORE_TRANSPORT_METHOD 将还原传输模式设置为 NBD。

  启动注意事项

  - 在备份主机上安装以下 NFS 包:
    - 对于智能缓存备份: NFS 3 或更高版本
    - 对于 StoreOnce Catalyst 和数据域设备备份: NFS 4 或更高版本
  - Data Protector 使用 Windows PowerShell 脚本 nfsServiceCheck.ps1 启动 NFS 服务，在启动过程中需要该服务。执行此脚本需要将执行策略设置为 *RemoteSigned*。如果您需要“限制”策略，则将 omnirc 变量 OB2_NO_NFSSERVICE_CHECK 设置为 1。如果该脚本失败，则需要手动执行此操作。导致 NFS 服务安装失败的一些可能原因可能是:
    - NFS 端口被另一个应用程序使用。
    - Powershell 可能需要重新启动。
    - Powershell 存储库中不存在 NFS 模块。

    使用以下命令手动执行 NFS 服务:
    - Windows 命令行: powershell.exe NFSServiceCheck.ps1
    - PowerShell 命令行: NFSServiceCheck.ps1
  - 将跳过作为“启动”功能的一部分创建的非永久性虚拟机的备份。尝试执行备份操作时，将显示以下消息: “发现已开机的非永久性虚拟机，正在跳过备份”。
  - 将在从智能缓存或 StoreOnce Catalyst 和数据域设备启动的虚拟机中禁用网络。
  - 要手动清除备份设备中已启动的所有 VM，请执行以下操作:

    1. 在用于开机的备份主机 (已开机的 VM 或导出到 ESXi 主机的 NFS) 上，将 omnirc 变量 FORCE_PURGE_POWERON_VMS 设置为 1。
    2. 在 Cell Manager 中运行以下命令:

       /opt/omni/sbin/omnidbutil -purge_expired_poweron_vms
    3. 等待该过程完成，然后将 FORCE_PURGE_POWERON_VMS 更改为 0。

> **注意**所有已启动的 VM 将被关闭并删除。

仅 3PAR 存储系统

- 必须在 Linux 装载代理主机中安装 vmfs-tools-0.2.5 。.
- 必须确保多路径服务在 Linux 装载代理主机中运行。
- 必须在 Linux 装载代理主机中安装 sg3_utils rpm package 。
- 要从 3PAR 复本执行 GRE 操作，GRE 装载代理主机和源 ESX Server 必须存在于同一个 3PAR 区域中。

StoreOnce Recovery Manager Central 集成

StoreOnce Recovery Manager Central (RMC) 软件将 3PAR StoreServ 主存储与 StoreOnce 备份系统相集成。RMC 将 3PAR StoreServ 主存储与 StoreOnce 备份系统相集成，可提供融合数据保护，从而通过灵活的恢复选项确保应用程序一致的恢复点实现恢复。

Express Protect 功能支持从 3PAR StoreServ 直接备份到 StoreOnce 设备，而不依赖于备份软件，提供了另一层数据保护。到 StoreOnce 的备份是自包含卷，经过重复数据删除以节省空间，可用于恢复到原始或不同的 3PAR StoreServ 阵列，即便原始基本卷丢失也如此。Express Protect 功能支持从主存储直接备份到备份存储，从数据路径中完全删除应用程序服务器。

借助适用于 VMware 的 StoreOnce RMC，可以使用应用程序一致的快照保护 VMware 虚拟机磁盘 (VMDK) 和数据存储，从而实现快速的联机恢复。

使用 Data Protector，您可以将 RMC 创建的虚拟机快照备份到 Data Protector 支持的辅助存储设备。您随后可以执行到所需目标的还原操作。请注意，Granular Recovery Extension (GRE) 操作只能对快照+磁带备份执行。

Data Protector 支持以下备份类型:

- **快照备份**: 使用快照备份，您可以创建原始卷的快照。
- **快照 + 磁带**: 使用快照 + 磁带备份，您可以创建快照并将数据备份到 Data Protector 支持的辅助存储设备。
- **Express Protect 备份**: 使用 Express Protect 备份，您可以将快照从 3PAR StoreServ 备份到 StoreOnce。

下表列出了支持的备份类型，即支持 Granular Recovery Extension、“启动”和“实时迁移”操作的备份。

支持的备份	备份类型	GRE	启动和实时迁移
快照	• 完整	不受支持	不受支持
快照 + 磁带	• 完整	如果磁带设备是智能缓存、StoreOnce Catalyst 或数据域，则支持缓存 GRE。对于任何其他类型的磁带设备，支持非缓存 GRE。	如果磁带设备是智能缓存、StoreOnce Catalyst 或数据域，则支持。
快照 + 磁带	• 增量 • 差异备份	如果磁带设备是 StoreOnce Catalyst 或数据域，则支持缓存 GRE。对于任何其他类型的磁带设备，支持非缓存 GRE。	如果磁带设备是 StoreOnce Catalyst 或数据域，则支持。
Express Protect	• 完整 • 增量	不受支持	不受支持

RMC 集成注意事项

- RMC 备份不支持由多个 LUN 组成的单个数据存储。
- 创建备份规范时提供的 RMC 服务器详细信息在保存规范后无法修改。
- 对于 RMC 集成备份，如果使用自动化脚本创建 barlist，请确保为创建 barlist 而指定的恢复集名称唯一。
- 对于 RMC Express Protect 备份，Data Protector 在内部保留 2 个快照。这对于执行增量备份必不可少。当快照计数超过 2 时，Data Protector 会循环旧快照。
- 仅从 Inform OS 版本 3.2.1 MU1 开始支持 RMC Express Protect 备份。
- 仅 Windows 和 Linux Cell Manager 平台中支持 RMC 计划和备份报告。
- 对于从快照执行的 RMC 还原会话，必须使用 omnidbzdb 命令添加阵列凭据。
- 对于 RMC 还原会话，只有 Data Protector 磁带还原可以还原到目录。
- 对于 RMC 快照和 Express Protect 备份，GRE GUI 中不显示会话信息。
- 从 3PAR Management Console 或通过运行 3PAR CLI 命令 showhost 可以看到，备份和应用程序主机名应与 3PAR 上的主机名匹配。主机名区分大小写。

您应当已熟悉 StoreOnce RMC 概念和过程。有关 RMC 的详细信息，请参阅《StoreOnce Recovery Manager Central 用户指南》和《适用于 VMware 的 StoreOnce Recovery Manager Central 用户指南》。

Express Protect 还原

如果在 Express Protect 将数据从 StoreOnce 还原到新快照时中止还原会话，则 Data Protector 会话将中止。但是，在后台继续从 StoreOnce 还原到快照。您需要等到 RMC 还原操作完成，然后才能触发来自同一会话的其他 Data Protector 还原操作。

RMC 集成过程

1. **添加 RMC 服务器详细信息**: 使用命令行界面添加 RMC 服务器。

   执行命令 omnidb -addhost -servername <rmcservername> -user <username> -passwd <password>。

2. **备份**: 通过在 Data Protector GUI 中选择 StoreOnce RMC 作为“备份类型”执行备份操作。

3. **还原**: 使用 GUI 执行还原操作或 GRE 操作。

使用 omnirc 选项自定义 Data Protector 行为

omnirc 选项可用于对影响 Data Protector 客户机行为的其他设置进行故障诊断或覆盖。适用于 VMware 的虚拟环境 ZDB 集成的选项带有前缀 OB2_VEAGENT。

使用命令行界面在 Data Protector 中添加 RMC 服务器详细信息

您可以使用 omnidb 命令添加 RMC 服务器详细信息。执行：

```
omnidb -addhost -servername <clientname> -user <username> -psswd <password>
```

还可以使用以下命令列出并删除所需的服务器。执行：

```
omnidb -listhost -servername <clientname>
```

```
omnidb -removehost -servername <clientname> -user <username>
```

为灾难恢复做准备

要执行灾难恢复，您需要备份以下 VMware 对象:

必须备份哪些内容:

VMware 对象	如何备份
ESX/ESXi Server 控制台	ESX Server 系统: 1. 确保在所有 ESX Server 系统上安装 Data Protector 磁盘代理组件。 2. 在 Data Protector GUI 的“备份”上下文中，右键单击“文件系统”，然后选择“添加备份”以创建文件系统类型的备份规范。在备份规范的“源”页中，选择所有 ESX Server 系统的 ESX Server 控制台。 有关备份内容的详细信息，请参阅 http://kb.vmware.com/selfservice/microsites/microsite.do 中的“ESX Server 配置备份和还原过程”主题。 3. 使用新创建的备份规范启动备份。 ESXi Server 系统: 对于 ESXi Server 系统，无法安装 Data Protector 磁盘代理，因此您需要使用 VMware 实用程序备份配置。 VMware 提供了 esxcfg-cfgbackup 工具。有关信息，请参阅 VMware 网站。
vCenter 配置数据库（仅适用于 VirtualCenter 环境）	vCenter 配置数据库可以是 Oracle 数据库或 Microsoft SQL Server 数据库。要备份该数据库，请使用相应的 Data Protector 集成。例如，如果它是 Oracle 数据库，请执行以下步骤: 1. 确保在 vCenter Server 系统上安装 Data Protector Oracle 集成组件。 2. 在 Data Protector GUI 的“备份”上下文中，右键单击“Oracle Server”，然后选择“添加备份”以创建 Oracle 类型的备份规范。在“应用程序数据库”中，键入 vCenter 配置数据库的名称。 继续创建备份规范。 3. 使用新创建的备份规范启动备份。
VMware 虚拟机	按照本节中所述备份虚拟机。

限制

以下限制适用：

常规限制

- 从 Data Protector 9.07 起，vStorage 映像 + OpenStack 方法不支持启动和实时迁移功能。
- 虚拟机具有 IDE 磁盘时，不支持 HotADD。有关其他详细信息，请参阅 VMware 文档。
- 由于某些快照限制，无法备份某些 VMware 磁盘。有关这些限制的详细信息，请参阅 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-53F65726-A23B-4CF0-A7D5-48E584B88613.html。

备份限制

- 在执行备份之前，请确保在任何 VMware vCenter、VMware ESX(i) 对象 (例如虚拟机、数据存储、数据中心等) 的名称中仅使用受支持的字符，因为不支持特殊字符。以下列表包括受支持的字符:

  - 字母 a-z，不带任何特殊字符
  - 数字 0-9
  - 单引号 (')
  - 空格
  - 下划线 (_)
  - 连字符 (-)
  - 冒号 (:)
  - 问号 (?)
  - 星号 (*)

- 不支持的特殊字符的部分列表如下:

  - 百分比 (%)
  - 加号 (+)
  - 相等 (=)
  - @ 符号 (@)
  - 小于 (<)
  - 大于 (>)
  - 双引号 (")
  - 正斜杠 (/)
  - 反斜杠 (\ )
  - 竖线或管道 (|)
- 仅 vCenter 服务器支持带有标记和类别 的备份和还原功能，而 ESX(i) 服务器不支持。
- “标记和类别” 视图不支持集成安全模式。
- Data Protector 仅支持与虚拟机的标记关联。

  如果标记与虚拟机模板相关联，则这些标记不会在“标记和类别” 视图中列出，因此不考虑进行备份。使用“VM 和模板” 视图选择虚拟机模板。

还原限制

- 不支持将具有虚拟 RDM 磁盘的虚拟机还原到不同的 vCenter。
- 将 VM 还原到具有在几个库存对象（主机或群集）或几个群集节点之间共享的数据存储的数据中心，并且选择了用于其后续注册的还原选项时，还原的 VM 可能无法在原始清单位置注册：
  - 如果多个库存对象共享数据存储，则将向第一个可用主机或群集注册 VM。
  - 如果多个群集节点共享数据存储，则将向第一个可用群集节点注册 VM。

如果必须在原始库存位置上注册 VM，请在还原会话完成后适当地迁移它。

- 在执行还原之前，请确保在任何 VMware vCenter、VMware ESX(i)、对象（例如虚拟机、数据存储、数据中心、vApp 等）的名称中仅使用受支持的字符，因为不支持特殊字符。
- 在开始还原使用 vCD vStorage Image 备份方法备份的虚拟机之前，出于一致性原因，所选 VM 所在的 vApp 进入维护模式。结果，该 vApp 中的所有 VM 都将关闭。
- 使用 vCD vStorage 映像备份方法不支持将虚拟机还原到特定数据存储。
- 禁用的 vDatacenter 不允许添加或删除 vApp。因此，不支持还原到禁用的 vDatacenter。
- 在 vSphere 环境中，请勿在 vSphere 分布式端口组的名称中使用左括号（(字符）。Data Protector 无法将还原的虚拟机连接到使用分布式交换机且已分配了此类分布式端口组的非原始 vSphere 网络。在这种情况下，还原后，您需要使用 vSphere 客户机将还原的虚拟机手动连接到所需的网络。
- 增量或差异备份不支持在还原到目录后恢复虚拟机。用于将还原的 VM 映像移至 ESX Server 或 ESXi Server 系统的 VMware Converter 仅识别完整备份类型。
- 只有还原到数据中心才支持从备份链还原虚拟机（例如完整、增量、增量、增量...）。
- 与会话相关的所有介质都应一起导出或导入。如果完整备份对象中缺少介质，则增量/差异备份将不会检测到缺少的介质，并继续以选定的模式运行。从此类会话还原将不会成功。
- 根据备份规范的创建方式，可将虚拟机视为内部数据库 (IDB) 和还原上下文中的不同对象。
- 无法还原已挂起的虚拟机。
- 在早期版本的 Data Protector 中，即使您仅选择一个磁盘进行还原，也会读取所有磁盘。从 Data Protector 8.11 起，仅读取和还原选定的磁盘。这适用于使用 Data Protector 8.11（而不是其早期版本）创建的备份。
- 无法从磁带上的一个磁盘移动到另一个磁盘。如果选择连续的磁盘（scsi0:1 和 scsi0:2）进行还原，则将读取和还原两个磁盘。如果选择 scsi0:1 和 scsi0:4 进行还原，则会发生以下组合：
  - 读取 scsi0:0。
  - 读取并还原 scsi0:1。
  - 读取 scsi0:2。
  - 读取 scsi0:3。
  - 读取并还原 scsi0:4。

因此，与单个或连续磁盘选择相比，随机选择磁盘可能会导致更高的还原窗口。

- 在 VEPA（虚拟化环境代理）还原过程中，虚拟环境集成代理会建立与 vCenter/ESX 的连接，以将虚拟机配置文件上载到 VC/ESX。即使还原会话完成后，vCenter 中仍可能存在这种连接。达到默认超时值 30 分钟后，VMware 将清除此空闲会话。或者，可以从 vCenter 中手动清除此会话。

vStorage 映像 + OpenStack 还原限制

- 不支持从复本还原。
- 从 Data Protector 还原上下文中删除了诸如“还原为”、“之后删除”和“取证”之类的功能。
- Nova 实例和卷影 VM 不支持 Granular Recovery Extension。
- 如果从 OpenStack 仪表板中删除了实例，则无法将实例从 Data Protector 恢复到仪表板。
- 如果卷影 VM 已附加到备份时所附加到的原始实例之外的其他任何实例，则还原将失败。
- 不支持还原到其他群集。
- **vStorage 映像 + OpenStack** 方法不支持启动和实时迁移功能。

启动和实时迁移限制

- 在 CIFS 和 NFS 共享上创建的智能缓存设备不支持启动和实时迁移选项。
- Windows 和 Linux 备份主机仅支持来自 StoreOnce Catalyst 的启动和实时迁移操作。

- 对于在智能缓存和 StoreOnce Catalyst 设备上创建的虚拟机，一次只能启动八个虚拟机。
- 如果使用“仅磁盘”选项备份了虚拟机，则不支持还原到 ESX 服务器。
- 如果使用“磁盘 + 磁带”选项备份了虚拟机，则支持从磁带还原到 ESX 服务器。
- 如果从智能缓存和 StoreOnce Catalyst 设备启动虚拟机，则将在没有虚拟 RDM 磁盘的情况下启动虚拟机。
- 如果您从智能缓存和 StoreOnce Catalyst 设备执行实时迁移过程，则虚拟 RDM 磁盘将作为密集磁盘迁移，即迁移后，它们将作为置零密集配置 vmdk 磁盘驻留在目标数据存储上。如果要还原具有虚拟 RDM 磁盘的虚拟机，请使用正常的还原过程。
- 不支持将虚拟机启动并实时迁移到 vCenter 之外的 ESX 服务器。
- 仅支持通过 CLI 实时迁移使用 ESX 服务器作为备份客户机执行的备份。
- 在 StoreOnce Catalyst 设备上具有备份的虚拟机上，您一次只能执行一项操作（还原/GRE/启动/实时迁移）。
- 如果虚拟机正在进行来自 StoreOnce Catalyst 设备的还原操作（启动、实时迁移或 GRE），请清除虚拟机，然后再从同一备份会话执行任何还原操作。这也适用于还原链中的备份会话。
- StoreOnce Catalyst 设备不支持非 CBT 备份会话的启动和实时迁移选项。
- 如果使用软件压缩或 AES 加密来执行到 StoreOnce Catalyst 设备的备份，则不支持启动和实时迁移操作。
- 如果通过选择 vApp 作为目标来执行虚拟机的启动和实时迁移，则虚拟机将启动并实时迁移到 vApp 外部。您可以根据需要将其手动移动到 vApp 内部。
- 如果使用任何活动的启动或实时迁移请求重新引导装载代理主机，则在重新引导后的 4 小时内将无法访问该请求。
- 如果将通过 Data Protector 9.04 或更早版本备份的数据通过 9.07 或更高版本中的对象复制转移到 StoreOnce Catalyst，则不支持实时迁移和启动操作。
- 如果在备份过程中 VM 上存在用户快照，则 Power On 和 Live Migrate 将不起作用。
- 启动和实时迁移操作不支持在不同设备上执行完整备份、差异备份和增量备份。

例如：

分别对 StoreOnce Catalyst 和智能缓存设备进行同一虚拟机的完整备份。

对 StoreOnce Catalyst 设备执行增量备份。此增量备份不适合启动和实时迁移操作，因为此增量链的完整备份首选项位于智能缓存中。

标记和类别限制

- “标记和类别” 功能仅适用于 VMware vCenter 客户机。
- 不支持将标记附加到启用了 powerOn 选项的 VM。

> 注意**:** 如果标记与 VM 模板相关联，建议使用“VM 和模板” 视图进行备份和还原。

相关主题

有关 omnirc 命令的详细信息，请参阅最常用的 omnirc 选项。

配置 VMware 集成

按如下所示配置集成:

- 将 VMware 客户机导入 Data Protector 单元。
- 配置要备份的虚拟机。

建议

- 建议不要在将使用 Data Protector 备份、还原和恢复的虚拟机的名称中使用百分号。如果虚拟机名称包含 % ，则该名称会在 Data Protector GUI 和 Data Protector 会话消息中错误地显示。

以下先决条件适用:

- 确保已正确安装和配置 VMware vSphere 环境。

  有关受支持版本、平台、设备和其他信息，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。

- 确保已为用于连接到 vCenter Server 的用户帐户授予“禁用方法”和“启用方法”全局特权。
- 确保已为用于连接到 vCenter Server 的用户帐户授予必要的 VMware vSphere 特权。
- 确保已正确安装 Data Protector。

  必须正确安装和配置适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成。确保环境中至少有一个客户机安装了 ZDB 代理 (适用于存储阵列的存储提供程序组件或 3PAR 存储提供程序 组件) 和虚拟环境集成 组件 (“备份系统”)。安装后，备份主机无需特殊配置。

  > **重要说明**您打算作为备份系统使用的客户机不必安装 VMware Consolidated Backup (VCB) 软件。

  如果要将虚拟机文件还原到备份主机上的某个目录，还要在备份系统上安装“磁盘代理” 组件。否则，您将无法使用“浏览”按钮指定目标目录 (但是，仍然能够自行键入目录)。

- 备份主机应该能够在网络文件复制 (NFC) 端口 (默认为 TCP 端口 902) 上连接到 ESX(i) 主机，因为 VDDK API 使用它们来查询分配的块。

开始之前:

- 配置要与 Data Protector 配合使用的设备和介质。

导入和配置 VMware 客户机

使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成，不必在 VMware 客户机上安装任何 Data Protector 组件 (vCenter Server 系统、ESX(i) Server 系统、vCloud Director)。要使它们成为 Data Protector 客户机，必须将 VMware 客户机正确导入 Data Protector 单元并进行配置。

> **重要说明**无法同时将一个客户机导入并配置为 VMware vCenter 客户机和 Hyper-V 客户机。

> **注意**在 *Data Protector Express* 中，按每个单元计算套接字许可证。可以将客户机 (vCenter/ESX 服务器) 同时导入多个单元，并为每个单元中的每个客户机导入计算套接字许可证。

将客户机导入 Data Protector 单元:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“Data Protector 单元”，右键单击“客户机”，然后选择“导入客户机”。
3. 在“导入客户机”页面的“名称”选项中输入客户机名称，从“类型”下拉列表中选择适当的客户机类型 (**VMware ESX(i)**、**VMware vCenter**)，然后单击“下一步”。
4. 如果选择“标准安全”，则需要手动指定 Data Protector 应用于连接到 VMware 客户机的登录凭据:

   端口: 指定 VMware vSphere 将使用的端口。默认情况下，VMware 使用端口 443。对于将用作装载主机的 VMware ESX(i) Server，请指定端口 443。

用户名和**密码**: 指定一个在根 vCenter 级别上有以下 VMware vSphere 特权的操作系统用户帐户:

下表列出了 VMware vSphere 中的特权:

数据存储 -> 分配空间
数据存储 -> 浏览数据存储
数据存储 -> 低级别文件操作
数据存储 -> 删除文件
数据存储 -> 重命名数据存储
扩展 -> 注册扩展
扩展 -> 取消注册扩展
扩展 -> 更新扩展
文件夹 -> 删除文件夹
文件夹 -> 重命名文件夹
全局 -> 禁用方法
全局 -> 启用方法
全局 -> 许可证
主机 -> 配置 -> 维护
主机 -> 配置 -> 存储分区配置
主机 -> 库存 -> 添加独立主机
网络 -> 分配网络
资源 -> 向资源池分配虚拟机
资源 -> 删除资源池
资源 -> 重命名资源池
会话 -> 验证会话
vApp -> 删除
vApp -> 重命名
vApp -> 添加虚拟机
虚拟机 -> 快照管理 -> 恢复到快照
虚拟机 -> 配置 *
虚拟机 -> 交互 -> 回答问题
虚拟机 -> 交互 -> 关闭电源
虚拟机 -> 交互 -> 打开电源
虚拟机 -> 库存 -> 新建
虚拟机 -> 库存 -> 注册
虚拟机 -> 库存 -> 删除
虚拟机 -> 库存 -> 取消注册
虚拟机 -> 设置 *
虚拟机 -> 快照管理 -> 创建快照
虚拟机 -> 快照管理 -> 删除快照
vSphere 标记 -> 分配或取消分配 vSphere 标记

- **Web 服务**: 可选，更改 Web 服务入口点 URI。默认值： /sdk

如果选择“集成安全”(仅可用于应用程序客户机和备份主机均为 Windows 系统的 VMware vCenter Server 系统)，则 Data Protector 会使用用以运行备份系统上的 Data Protector Inet 服务的用户帐户连接到 VMware vCenter Server 系统。确保此用户帐户拥有适当的 VMware vSphere 权限可以连接到 VMware vCenter Server 系统且备份主机上的 Data Protector Inet 服务已针对用户模拟进行了配置。

对于“端口”和“Web 服务根”选项，Data Protector 使用当前为标准安全指定的值。集成安全基于安全支持提供程序接口 (SSPI)。

5. 选择“下一步”。仅当使用的许可证类型为 *Data Protector Express* 时，此选项才可用。否则，该选项将灰显。

   如果是 **Data Protector express**，则会列出选定 vCenter 中的 ESX(i) 服务器，以及主机名、主机套接字和主机 UUID 信息。

6. 选择要许可的 ESX(i) 服务器，然后选择“完成”。

   选定服务器将获得许可。

   要添加或回收许可证，请重新导入 vCenter 客户机。在这种情况下，未获得许可的 ESX(i) 服务器与已获得许可的 ESX(i) 服务器一起列出。

   - 要回收，请取消选择 ESX(i) 服务器并选择“完成”以取消许可 ESX(i) 服务器。
   - 要添加，请选择新服务器，然后选择“完成”以许可 ESX(i) 服务器。

更改 VMware 客户机的配置

当您更新用于连接到 VMware 客户机 (vCenter Server、ESX(i) Server 或 vCloud Director 客户机) 的凭据时，您实际上会更新驻留在 Data Protector Cell Manager 上的 cell_info 文件。因此，仅当您拥有 Data Protector“客户机配置” 用户权限时，才能更改登录凭据。有关 Data Protector 用户权限的详细信息，请参阅《Data Protector 帮助》索引: “用户组”。

要更新凭据，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

您可以在两个不同的位置更新凭据: 在客户机中或备份上下文中。

客户机上下文

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“客户机”，然后选择要更改其登录凭据的客户机。
3. 在“结果区域”中，单击“登录”选项卡。
4. 更新凭据，然后单击“应用”。

备份上下文

假定要更改其登录凭据的 VMware 客户机的备份规范已存在。

1. 在上下文列表中，单击**备份**。
2. 打开要更改其登录凭据的 VMware 客户机的备份规范。
3. 在“源”页面中，右键单击顶部的客户机，然后选择“配置”。
4. 在“配置虚拟环境”对话框中，更新值并单击“确定”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   对于“集成安全”:

   ```
   vepa_util.exe command --config --virtual-environment vmware --host VMwareClient --security-model 1
   ```

   对于“标准安全”:

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   vepa_util.exe command --config --virtual-environment vmware --host VMwareClient --security-model 0 --username Username {--password Password | --encoded-password Password} [--webroot WebServiceRoot] [--port WebServicePort]
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

检查 VMware 客户机的配置

在配置检查期间，Data Protector 尝试使用 Data Protector Cell Manager 上的 cell_info 文件中的登录凭据连接到 VMware 客户机。

要验证连接，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在为 VMware 客户机创建至少一个备份规范后，您可以验证与此客户机的连接。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。单击要检查的 VMware 客户机的备份规范。
3. 在“源”页面中，右键单击 VMware 客户机，然后选择“检查配置”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   vepa_util.exe command --check-config --virtual-environment vmware --host VMwareClient
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

配置虚拟机

配置虚拟机意味着指定应如何备份虚拟机。

您可以指定以下内容:

- (仅限 Windows 虚拟机) 是否应捕获静止快照，以使虚拟机内运行的应用程序的备份一致。
- 备份期间应使用的传输模式。

对于每个数据中心，您可以指定:

- 应用于数据中心中的所有虚拟机的*常用设置*。
- 覆盖常用设置的*特定于虚拟机的设置*。如果没有特定于虚拟机的设置，则为该特定虚拟机使用常用设置。

所有这些设置都保存在 Cell Manager 上的特定于数据中心的文件 VMwareClient%DatacenterPath 中。该文件用于使用此数据中心的任何备份规范的所有备份会话。

同样，使用“所有数据中心”的任何备份规范的备份会话使用来自文件 VMwareClient%AllDatacenters 的设置。

当您分别为特定数据中心或所有数据中心创建或更新备份规范时，将创建或更新文件 VMwareClient%DatacenterPath 和 VMwareClient%AllDatacenters 。

要配置虚拟机，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在创建或修改备份规范时，您可以配置虚拟机。在备份规范的“源”页面中，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。

在“设置”页面的“配置虚拟机”对话框中，指定以下设置:

虚拟机设置

可用选项	描述/操作
选择是否要指定常用虚拟机设置 (“常用 VM 设置”) 或特定虚拟机的设置。特定于虚拟机的设置会覆盖常用虚拟机设置。	
配置虚拟机	
使用所选 VM 的常用设置	仅当选择虚拟机时可用。 如果希望常用设置应用于所选虚拟机，请选择此选项。 默认：选择
使用默认设置	仅当选择“常用 VM 设置”时可用。 选择此选项可设置常用虚拟机设置的默认值。 默认：选择
启用更改后的块跟踪	为所选虚拟机启用 VMware 更改后的块跟踪功能。 默认: 选定并灰显
允许回退到非 CBT 备份	仅当选择“使用更改后的块跟踪”时启用。 选择此选项可以继续在非 CBT 模式下进行备份，以实现 Data Protector 的成功备份。 有关非 CBT 的详细信息，请参阅主题。 默认：未选择。
快照处理	

使用静止快照	适用于 Windows 虚拟机。 如果选择“使用默认设置”或“对所选 VM 使用常用设置”，则不可用。 选择此选项可使用 Microsoft 卷影复制服务 (VSS) 功能在执行 VEPA 备份之前，通过 VSS 写入程序使所有应用程序静止。这会生成应用程序一致的备份。 默认：未选择。有关详细信息，请参见。
错误级别	仅当选择“使用静止快照”时可用。 指定在静止快照失败时要报告的错误级别。 默认值：警告。
传输模式(R)	
	选择备份虚拟机时要使用的传输模式。 • **NBD**: 当 ESX(i) Server 系统无权访问 SAN、但使用本地存储设备或 NAS 存储虚拟机磁盘时，请使用此模式。这是一种通过本地局域网进行的、使用网络块设备 (NBD) 驱动器协议的未加密传输模式。此传输模式通常比光纤通道慢。 • **NBD (SSL)**: 除通过网络进行的通信使用安全套接字层 (SSL) 加密协议进行加密外，与 NBD 相同。 • **Hotadd**: 如果备份主机 (安装了 Data Protector“虚拟环境集成”组件的客户机) 是虚拟机，则使用此模式。通过此类配置，您可以备份驻留在对托管备份主机的 ESX(i) Server 可见的数据存储上的其他虚拟机。 • **SAN**: 当 ESX(i) Server 系统将其虚拟机磁盘存储在光纤通道 SAN 或 iSCSI SAN 中时，请使用此模式。这是一种通过光纤通道或 iSCSI 进行的未加密传输模式。 此传输模式要求将虚拟机所在的存储卷提供给安装了“虚拟环境集成” 组件的客户机 (“备份主机”)。 ◦ **警告：**请勿重新格式化这些存储卷。否则，您将删除所有虚拟机。 如果您不关心所使用的模式，请选择“最快可用”。 默认值：**最快可用**

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

```
vepa_util.exe command --configvm --virtual-environment { vmware | vCD } --host AppHostName --instance DatacenterPath --vm VMpathVM_OPTIONSVM_OPTIONS --transportation-mode {san | nbd | nbdssl | hotadd | fastest} --quiescence { 0 | 1 } --quiescenceErrLvl { 0 | 1 } --uuid UUID_of_VM
```

要将特定于虚拟机的设置更改回常用虚拟机设置，请执行:

```
vepa_util.exe command --configvm --virtual-environment { vmware | vCD } --host AppHostName --instance DatacenterPath --vm VMpath --uuid UUID_of_VM --default
```

消息 *RETVAL*0 表示配置成功。

示例

要在最快可用传输模式下，使用驻留在数据中心 /MyDatacenter 中并在 vCenter Server 系统 vc.company.com 中注册的虚拟机路径 /MyDatacenter/MyVM 和 UUID 42375365-ebe1-e9da-7068-7beb727cab19 配置虚拟机，

执行:

```
vepa_util.exe command --configvm --virtual-environment vmware --host vc.company.com --instance /MyDatacenter --vm /MyDatacenter/MyVM --quiescence 1 --quiescenceErrLvl 0 --transportation-mode fastest --uuid 42375365-ebe1-e9da-7068-7beb727cab19
```

备份 VMware 集成

本节包含备份虚拟机所需的过程。

创建备份规范

使用 Data Protector GUI 创建备份规范。

单击“下一步”。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择“快照或拆分镜像备份”作为备份类型，并选择“存储提供程序插件”作为子类型。有关选项的说明，请按 **F1**。单击**确定**。
4. 指定要备份的应用程序:
   - 在客户机下拉列表中，选择 VMware 客户机。

     > **注意**下拉列表包含已作为 VMware vCenter 或 VMware ESX(i) 客户机导入 Data Protector 单元的所有客户机。这些客户机名称的末尾附加了相应的标签，例如 *(VMware vCenter)* 或 *(VMware ESX(i))*。

     如果未正确配置所选 VMware 客户机，则会显示一条警告。单击“确定”打开“配置虚拟环境”对话框，并按导入和配置 VMware 客户机中所述提供连接参数。
   - 在“备份主机”下拉列表中，选择要用于控制备份的 VMware vCenter 系统。该列表包含安装了 Data Protector Virtual Environment Integration 组件的所有客户机。
   - 在“数据中心/组织”中，选择要从中进行备份的数据中心。

     > **注意**如果在“客户机”选项中选择了独立 ESX(i) Server 系统，则只有一个数据中心可用 - **/ha-datacenter**。
     >
     > 如果在**客户机**选项中选择了 vCenter Server 系统，则您可以选择**所有数据中心**以备份不同数据中心中的虚拟机。
     >
     > 如果在**客户机**选项中选择了 vCloud Director，则您可以选择**所有组织**以备份不同组织中的虚拟机。
   - 在“装载主机”中，选择要用于装载复本的 ESX(i) Server 系统。

     > **注意**如果 ESXi 版本为 5.5 U2 的装载代理主机属于源数据中心，则远程复制故障转移备份将失败。从属于同一 vCenter 的其他数据中心选择 ESXi 装载代理主机。
   - 在“备份方法”中，将显示备份方法:
     - 适用于 VMware vCenter 和 VMware ESX(i) 客户机的 vStorage 映像
     - 适用于 VMware vCenter 的 vStorage 映像
   - 在“所需可用空间[%]”中，指定在备份虚拟机之前，数据存储应具有的可用磁盘空间的百分比。可用空间基于虚拟机磁盘所处的数据存储大小进行计算。

     需对每个虚拟机单独执行检查。

   单击“下一步”。

   > **注意**保存备份规范后，无法更改向导的此页面中指定的设置。要更改设置，您必须创建新的备份规范。

5. 选择要备份的对象。在“显示”下拉列表中，通过选择“主机和群集”、“VM 和模板”、“标记和类别”或“数据存储和存储”视图来简化您的选择。按 F1 获得这些选项的说明。默认情况下，会显示主机和群集。

注意
- 如果在已选择一个或多个对象进行备份之后切换视图，则会显示警告对话框。对其进行确认会清除已选择的对象，单击“否”不对视图进行任何更改。对于模板备份，将视图从“标记和类别” 更改为“VM 和模板” 时，将保存选定的标记。
- 您必须具有 vSphere 读取和附加权限才能使用“标记和类别” 视图。
- “标记和类别” 视图仅适用于 vCenter Server。
- 您不能在“标记和类别” 视图下查看模板。

您可以在不同级别进行选择:

- 对于 VMware vCenter 和 VMware ESX(i) 客户机:
  - ESX/ESXi Server 系统
  - 池
  - vApp
  - VM 文件夹
  - 单个 VM
  - VM 磁盘
  - VM 模板
  - 标记
  - 类别

如果选择高于单个 VM 的任何级别 (例如 vApp)，则所选项目中包含的所有 VM 和 VM 磁盘都将包含在备份规范中。如果在保存备份规范后在项目中添加了 VM，则也会备份这些 VM。

注意如果清除某个对象对应的复选框，则该对象将从备份规范中排除。此后，如果将新虚拟机、池或 vApp 添加到现有逻辑对象，它将自动包含在备份中。您无需创建新的备份规范。已排除对象的复选框在所选视图中标有红色叉号。

注意在“vStorage 映像 + Openstack”备份规范创建期间，卷影 VM 在备份和还原操作期间无法选择。

重要说明在特定 VMware 客户机的对象树中，虚拟机可能会显示为以两种不同的方式选择：
- “蓝色”复选标记表示已选择虚拟机以进行完整备份，包括其配置及其所有虚拟磁盘。

  如果备份了此类虚拟机，即使原始虚拟机不再存在，也可以还原它。
- “灰色”或“黑色”复选标记表示选择了属于虚拟机的部分或全部虚拟磁盘。备份中省略了虚拟机本身及其配置。

  如果备份了此类虚拟机，则仅当在还原时仍然配置了原始虚拟机时，才能还原其磁盘。

如果您的虚拟机尚未配置，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。有关详细信息，请参见配置虚拟机。

单击“下一步”。

6. 选择用于备份的设备。

   要指定设备选项，请右键单击设备，然后选择“属性”。在“并发”选项卡中指定并行备份流的数量以及要使用的介质池。

   单击“下一步”。
7. 设置备份选项。
8. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后计划备份规范。
9. 单击“启动备份”以启动备份会话。如果您使用的是 3PAR 存储系统，则可以选择“备份类型”、“网络负载”和“快照备份”选项。

提示在将备份规范用于实际备份之前预览备份规范。

VMware 备份选项

选项	描述
Pre-exec、**Post-exec**	指定在 (pre-exec) 备份前或 (post-exec) 备份后在备份主机上运行的命令行。 不要使用双引号。仅键入命令的名称并确保该命令位于备份主机上的默认 Data Protector 管理命令目录中。 *Windows 系统：* Data_Protector_home\bin *Linux 系统*: /opt/omni/bin

为 RMC 备份创建备份规范

请考虑“StoreOnce Recovery Manager Central 集成”部分中列出的所有先决条件和限制。

使用 Data Protector GUI 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择“StoreOnce RMC”作为备份类型:根据需求，选择“快照”、“快照 + 磁带”或“Express Protect”作为子类型。单击**确定**。
   - **快照**: 如果选择此选项，则会创建源卷的复本。
   - **快照 + 磁带**: 如果选择此选项，则会创建源卷的复本，并将数据备份到所选磁带设备。保在后续步骤中指定“装载主机”和所需“设备”。
   - **Express Protect**: 如果选择此选项，您可以将快照从 3PAR StoreServ 备份到 StoreOnce。备份按照在 RMC 中创建的备份策略进行。
4. 指定要备份的应用程序:
   - 在客户机下拉列表中，选择 VMware 客户机。如果未正确配置所选 VMware 客户机，则会显示一条警告。单击“确定”打开“配置虚拟环境”对话框，并按导入和配置 VMware 客户机中所述提供连接参数。
   - 在“备份主机”下拉列表中，选择要用于控制备份的 VMware vCenter 系统。
   - 在“数据中心/组织”中，选择要从中进行备份的数据中心。
   - 在“装载主机”中，选择要用于装载复本的 ESX(i) Server 系统。对于“快照 + 磁带”备份，此字段是强制性的。
   - 在“备份方法”中，选择要用于备份的方法。

     > **注意**RMC 不支持 **vStorage 映像 + OpenStack** 备份方法。
5. 指定 RMC 配置详细信息:
   - **RMC 服务器**: 选择用于备份的 RMC 服务器。
   - **备份策略** (*仅适用于 Express Protect 备份*): 选择在 RMC 中创建的策略名称。备份策略通常包含备份系统和备份存储。
   - **快照计数**: 指定应在存储阵列中保留的最大快照计数。最多可以创建 1000 个，最少 1 个。默认值是 10。
   - **Express Protect 计数** (*仅适用于 Express Protect 备份*): 指定应在 StoreOnce 中为备份规范保留的最大备份数。可以设置的最小值是 2。默认值是 10。
6. 选择要备份的对象。在“显示”下拉列表中，通过选择“主机和群集”、“VM 和模板”、“标记和类别”或“数据存储和存储”视图来简化您的选择。 按 F1 以获取这些选项的说明。默认情况下，会显示主机和群集。
7. 选择要用于备份的设备。如果已指定装载主机，则默认选择该设备。

   单击“下一步”。

   > 此步骤不适用于“快照”和“Express Protect”备份。
8. 设置备份选项。单击“下一步”。
9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。
10. 单击“启动备份”以启动备份会话。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

在“源”页面中，您可以使用“显示”下拉列表修改备份对象。在下拉列表中，“主机和群集”视图、“VM 和模板”视图、“标记和类别”视图和“数据存储和存储”视图可用。 备份规范创建过程中使用的视图附加了字符串 (Original)。如果切换视图，则会显示警告对话框，对其进行确认会清除已选择的对象。

注意在修改使用以前的 Data Protector 版本之一创建的备份规范时，可以在“已选定”、“全部”、“主机和群集”、“VM 和模板”、“标记和类别”以及“数据存储和存储” 视图之间进行切换。**全部**视图仅对旧版备份规范可用，提供旧版浏览机制。选择“主机和群集”、“VM 和模板”、“标记和类别” 或“数据存储和存储” 并在警告对话框中单击“是”可清除以前选择的备份对象并升级浏览机制。在保存备份规范之后，只有“主机和群集”、“VM 和模板”、“标记和类别” 和“数据存储和存储” 视图可用。

要显示虚拟环境设置，请在“结果区域”中单击“VE 设置”。并非所有设置都可以修改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

注意一段时间不活动后，防火墙会关闭 BSM 和 Inet 之间的连接。因此，建议在客户机上的 omnirc 文件中进行以下设置，以启用 keepalive 包，保持连接处于活动状态:

- OB2IPCKEEPALIVE = 1
- OB2IPCKEEPALIVETIME = 600
- OB2IPCKEEPALIVEINTERVAL = 600

虽然在所有系统上都遵守 OB2IPCKEEPALIVE ，但某些系统可能不支持由 OB2IPCKEEPALIVETIME 和 OB2IPCKEEPALIVEINTERVAL 定义的按套接字的保持活动设置。

Windows、Linux 系统: 支持 OB2IPCKEEPALIVE 和 OB2IPCKEEPALIVEINTERVAL

HP-UX 系统: 仅支持 OB2IPCKEEPALIVETIME

其他系统: 只能进行系统范围内的保持活动设置。要更改 TCP 保持活动设置，请参考相应的操作系统文档。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要预览的备份规范，然后选择“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   ```
   omnib -veagent_list BackupSpecificationName -test_bar
   ```

预览期间会发生什么?

测试以下内容:

- 备份主机与 Data Protector 之间的通信
- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于执行紧急备份或重新启动失败的备份非常有用。

要以交互方式启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要使用的备份规范，然后选择“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录安装了 Data Protector User Interface 组件的任何客户机。
2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   omnib -veagent_list BackupSpecificationName [-barmode VirtualEnvironmentMode][ListOptions]

   其中， VirtualEnvironmentMode 是以下备份类型之一:

   full|diff|incr

   默认为 full 。

   有关 ListOptions ，请参阅 omnib 手册页或《Data Protector 命令行界面参考》。

   示例

   要使用备份规范 MyVirtualMachines 启动完整备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode full

   要使用同一备份规范启动差异备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode diff

备份概念

使用适用于 VMware 的 Data Protector 虚拟环境集成，可备份以下 VMware 对象:

VMware vSphere:

- 虚拟机
- 虚拟机磁盘
- 虚拟机模板

Data Protector 根据 VMware vSphere 库存路径标识数据中心和虚拟机。独立 ESX Server 系统只有一个数据中心 /ha-datacenter 和两个文件夹： /host 和 /vm 。虚拟机存储在文件夹 /host 中。

示例：

数据中心： /ha-datacenter

虚拟机： /vm/myvm1

在 vCenter 环境中，可以在自行创建的文件夹中组织虚拟机和数据中心。如果随后移动虚拟机，则无需创建新的备份规范，因为 Data Protector 将使用其 UUID 查找虚拟机。

示例：

虚拟机： /vm/myfolder1/myfolder2/.../myvm2

数据中心： /myfolder/mydatacenter

在 vCloud Director 环境中，可以在自行创建的 vApp、vDatacenter 和组织中组织虚拟机。

示例：

虚拟机： /ORG22/vDCOrg22/vAppORG22/vm1Org22

组织: /vCD1/Mngmt/ORG22

虚拟机

备份虚拟机时，实际上备份以下类型的虚拟机文件:

- .vmx
- .vmdk

虚拟机磁盘

使用 vStorage 映像备份方法时，Data Protector 支持备份单个虚拟机磁盘。在这种情况下，将备份所有虚拟机文件，但未指定的虚拟机磁盘除外。您可以运行完整备份、增量备份和差异备份。

从 Data Protector 9.05 开始，虚拟机磁盘将并行备份，而不是按先后顺序备份。

为实现虚拟机磁盘并行性，将虚拟机磁盘将视为对象。指定对象操作 (如对象复制和对象验证) 时，不显示磁盘对象。为对象操作选择虚拟机对象时，将考虑磁盘。

> **注意**将新磁盘添加到虚拟机后，请确保为更新的虚拟机运行完整备份会话。

虚拟机模板

使用 vStorage 映像备份方法时，也可以备份虚拟机模板。创建备份规范时，展开 **vm** 文件夹并选择所需的虚拟机模板。

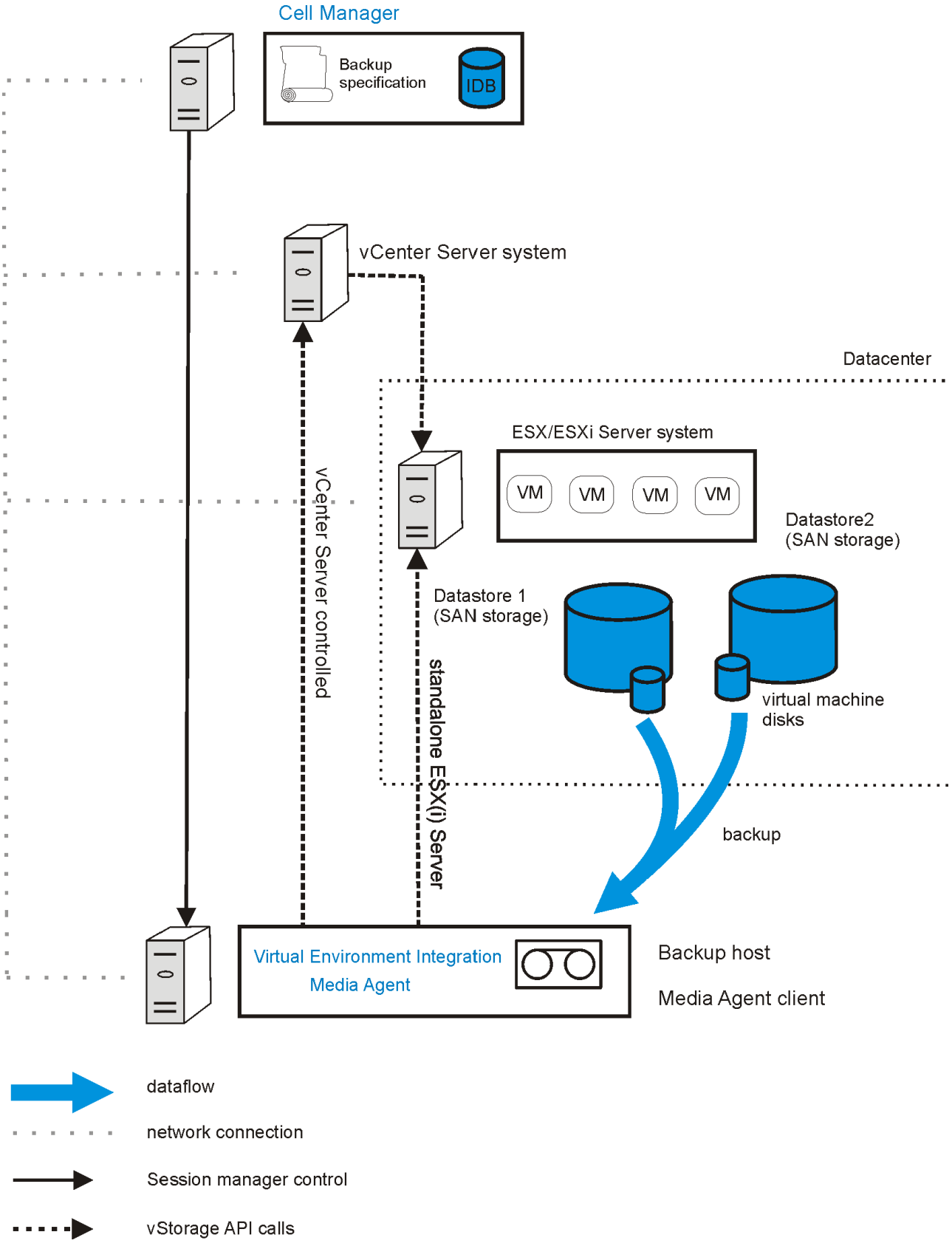
vStorage 映像备份方法

适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成提供的 vStorage 映像备份方法基于 VMware vStorage 技术。对于此方法，使用单个中央“备份主机”备份 Data Protector 单元中的 ESX(i) Server 系统托管的所有虚拟机。此备份主机可以是专用物理主机、虚拟机或 Cell Manager。重要的是它安装了 Data Protector“虚拟环境集成” 组件 (**VEAgent**)。

在 vStorage 映像备份期间，VEAgent 首先在备份主机和虚拟化主机 (ESX(i) Server 系统) 之间建立连接。此连接可以通过 vCenter Server 系统 (在 vCenter 环境中) 或直接 (在独立 ESX(i) Server 环境中) 进行。然后，它通过 VMware vSphere Storage API - 数据保护 (以前称为 Data Protection 或 VADP 的 VMware vStorage API) 请求要备份的虚拟机的快照。在备份期间使用此快照，以使虚拟机保持一致状态。

然后，VEAgent 将通过 LAN 或 SAN 打开虚拟机磁盘，初始化介质代理客户机并控制对虚拟机及其所有关联数据的传输。

> **注意**您可以使用 OB2_VEAGENT_OPEN_DISK_TIMEOUT omnirc 选项指定打开两个不同磁盘之间的时间间隔。默认情况下，每 2 秒打开一个新磁盘。



在“vStorage 映像”方法中，备份主机也是介质代理客户机 (它安装有“介质代理” 组件并连接一台设备)。

vStorage 映像 + OpenStack 备份方法

Data Protector 虚拟环境集成提供的 vStorage 映像 + OpenStack 备份方法是 vStorage 映像备份方法的变式。创建备份规范时，强烈建议在选择 vStorage 映像 + OpenStack 备份方法时仅选择 Nova 实例 VM。否则，所选 vSphere 托管 VM 仅限于 vStorage 映像备份方法。

备份考虑事项

- 如果备份卷影 VM 之前出现任何中止，则附加到 Nova 实例的卷影 VM 不会备份。
- 如果使用 vStorage 映像备份方法执行备份，则可以还原 Nova VM，但不会上载卷影 VM 配置文件，从而使卷影 VM 取消注册到 vCenter。
- 无法仅备份卷影 VM。但是，可以备份与 Nova 实例关联的卷影 VM。

快照管理

vStorage 映像备份方法依赖能够创建虚拟机快照。虚拟机快照是一种将虚拟机置于一致状态的操作。对虚拟机磁盘进行的所有后续更改都将记录到创建的快照中。

> **注意**所有虚拟机磁盘都不支持快照操作。例如，不支持独立磁盘的快照；因此，无法使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成来备份此类虚拟磁盘。有关详细信息，请参阅 VMware 文档。

在 vStorage 映像备份期间，Data Protector 会创建快照，复制虚拟机磁盘并将数据从一致状态复制到 Data Protector 介质。然后，Data Protector 将删除复本和快照。请注意，Data Protector 创建的快照 (“DP 快照”) 通过包含产品名、描述和时间戳的标签 _DP_VEPA_SNAP_ 区别于其他快照。

> **注意**如果虚拟机在启用 CBT 的备份期间具有用户创建的快照，则用户创建的快照将与其他 VM 磁盘块一起备份。如果 Data Protector 在还原时在虚拟机中检测到用户创建的快照，则不会还原该 VM。要还原此类 VM，您需要手动删除所有现有用户创建的快照。

现有虚拟机快照会降低虚拟机的整体性能。因此，Data Protector 会在不再需要 DP 快照时自动删除它们。

> **重要说明**不要将标签 _DP_VEPA_SNAP_ 用于为其他目的创建的快照，否则 Data Protector 将删除这些快照。

备份类型

要执行的备份类型在备份规范级别，在“调度程序”页面中或在“启动备份”对话框中 (对于交互式备份) 指定。

使用 vStorage 映像或 vCD vStorage 映像备份方法，可以执行以下备份类型:

备份类型

备份类型	描述
完整	备份完整虚拟机 (磁盘)。
增量	备份自上一次完整备份、增量备份或差异备份以来对虚拟机所做的更改。
差异备份	备份自上一次完整备份以来对虚拟机所做的更改。

对于增量备份或差异备份会话，还必须指定 Data Protector 应如何识别磁盘块级别的更改。

为了识别磁盘块级别的更改，Data Protector 使用 VMware 更改后的块跟踪功能。有关详细信息，请参见备份。

> **注意**备份后剩余的快照数始终为 0。仅支持混合快照处理模式。

混合快照处理模式支持所有可能的备份链形式的完整备份、差异备份和增量备份。

在对备份的虚拟机执行快照操作时，必须注意不要破坏备份链。

重要说明未使用 Data Protector 创建的 VMware 对象的快照不能用于为该对象设置 Data Protector 备份链 (还原链)。

如果执行以下任何操作，备份链将被破坏:

- 删除快照
- 恢复到快照
- 创建快照而不涉及 Data Protector
- 更改快照处理模式
- 添加新的虚拟机磁盘或重命名现有虚拟机磁盘
- 还原虚拟机
- 启用更改后的块跟踪

完成上述任何操作后，必须先运行完整备份才能启动新的备份链。如果您改为运行增量备份或差异备份的会话，则 Data Protector 会切换 VEAgentdisk 对象以使有效备份类型为完整备份，而对于 VEAgent 对象，备份类型仍为增量备份或差异备份。这可能会在还原期间创建具有多个会话的备份链；这会影响性能。因此，建议执行完整备份。

注意使用更改后的块跟踪时，请记下以下几点:

- 使用 CBT 备份时，请确保符合 VMware 的先决条件。
- 并非所有类型的虚拟磁盘都支持更改后的块跟踪。如果磁盘不受支持，则虚拟机备份将失败。
- 首次启用更改后的块跟踪时，虚拟机的下一个备份将始终为完整备份，以便为跟踪提供参考点。即，启动一个新的备份链。
- 执行还原会话时，CBT 备份链 (完整, 差异, 增量,...) 会被破坏。还原会话完成后，再次运行完整备份以启动新的备份链，否则后续增量备份和差异备份会话将失败。

更改后的块跟踪

更改后的块跟踪 (CBT) 是 VMware 更高版本的一个功能，可用于提高备份效率和速度。

对于 CBT，使用更改 ID。更改 ID 是虚拟磁盘在特定时间点所处状态的标识符。每当创建磁盘快照时，更改 ID 都由虚拟磁盘逻辑保存。

使用更改后的块跟踪的主要优点在增量或差异备份上最为明显，因为:

- 不必将虚拟机快照一直留到下次备份之时，因而大幅减少系统开销。
- 通过从内核获取更改信息而不是从快照进行计算，可以更轻松地计算要备份的更改。

在完整备份期间，仅备份磁盘上的活动块，未分配的块将被忽略。这可以提高备份的空间利用率和速度。

启用更改后的块跟踪时，虚拟机的性能会受到轻微影响，但这与您获得的好处相比微不足道。如果在 VMware vSphere 中启用更改后的块跟踪，则 Data Protector 将使用它。可以根据需要使用 Data Protector GUI 启用它。

注意“vStorage 映像 + OpenStack”备份方法支持 CBT 功能。

使用更改后的块跟踪时，仍要使用 Data Protector 快照，确保虚拟机处于一致状态。但在备份完成后，将删除这些快照。仅保留更改后的块跟踪日志文件更改 ID。

注意使用更改后的块跟踪时，请记下以下几点:

- 使用 CBT 备份时，请确保符合 VMware 的先决条件。有关详细信息，请转到

https://kb.vmware.com/kb/1020128

- 并非所有类型的虚拟磁盘都支持更改后的块跟踪。如果磁盘不受支持，则虚拟机备份将失败。

- 首次启用更改后的块跟踪时，虚拟机的下一个备份将始终为完整备份，以便为跟踪提供参考点。即，启动一个新的备份链。
- 执行还原会话时，CBT 备份链 (完整, 差异, 增量,...) 会被破坏。还原会话完成后，再次运行完整备份以启动新的备份链，否则后续增量备份和差异备份会话将失败。

备份流程

1. Data Protector 触发快照。
2. 创建源卷的复本。
3. 记录当前备份的更改 ID。

   如果这是启用更改后的块跟踪后捕获的第一个快照，则会识别所有活动块并记录更改 ID 0。

   在完整备份的情况下，此更改 ID 会成为新备份链的起始参考点。
4. 此步骤取决于所选备份类型:
   - *完整备份*: 由于识别到更改 ID 0，块已更改。
   - *增量备份*: 由于识别到上一次备份 (完整备份、增量备份或差异备份) 的更改 ID，块已更改。
   - *差异备份* : 由于识别到上一次完整备份的更改 ID，块已更改。
5. 备份识别到的块。
6. 删除复本和快照。

具有更改后的块跟踪的备份链示例

快照	更改 ID	识别到的块	备份的块
启用 CBT 后的第一个	ID 0	所有活动块	—
完整备份	ID *n*	自 ID 0 后已更改	来自 ID 0 的所有活动块 + 自 ID 0 后已更改的块
增量备份	ID *n+m*	自 ID *n* 后已更改	自 ID *n* 后已更改的块
增量备份	ID *n+p*	自 ID *n+m* 后已更改	自 ID *n+m* 后已更改的块
差异备份	ID *n+q*	自 ID *n* 后已更改	自 ID *n* 后已更改的块
完整备份	ID *r*	自 ID 0 后已更改	来自 ID 0 的所有活动块 + 自 ID 0 后已更改的块

非更改块跟踪 (非 CBT) 备份

非更改块跟踪（非 CBT）备份是一种不依赖于要备份的块级更改的功能。

- 使用此功能，将备份虚拟机磁盘的所有块。
- 此功能不使用 VMware CBT 功能来识别要备份的修改后的块。
- 备份的映像大小会增加，因为将备份磁盘的所有块。

更改块跟踪备份失败时，将启用**允许回退至非 CBT 备份**选项。

在以下情况下，可使用非 CBT 备份：

- 当虚拟机的硬件版本低于 7 时。
- 当备份未安装较低版本操作系统（例如 Windows 2003）的虚拟机时。
- 当快照在虚拟机上可用而且 CBT 未启用时。

备份并行性

默认情况下，虚拟机并行备份。在极少数情况下，这可能会导致问题。例如，备份会话可能意外结束。在这种情况下，您可以将备份主机上的 Data Protector `OB2_VEAGENT_THREADED_BACKUP` omnirc 选项设置为 `0` 以禁用并行备份。

注意在这两种情况下，都会按顺序备份虚拟机磁盘。

注意默认情况下，使用 VEAgent 集成备份虚拟机时，最多会执行 10 个并发线程。此处，每个线程引用一个用于处理备份集并将其从虚拟机主机流式传输到备份目标的 Data Protector 服务。虽然默认设置为受保护的虚拟机提供增强的备份性能，但由于 10 个 I/O 连接并非由虚拟化层管理，且因此不受虚拟化主机上的负载均衡服务的限制，它将为虚拟基础架构施加中度负载。但是，您可以使用 `OB2_VEAGENT_VCENTER_CONNECTION_LIMIT` 变量修改此设置，以满足系统设置的要求。

备份考虑事项

- 更改块跟踪 (CBT) 和混合快照处理模式

  支持 CBT 备份方法和混合快照处理模式。

- **并发备份会话**

  使用相同设备的备份会话无法并行运行。

  无法与 ESX(i) Server 系统或虚拟机所在的数据中心并行备份虚拟机。

  备份同一数据存储中的虚拟机的备份会话无法在同一个 Cell Manager 或不同的 Cell Manager 中并行运行。

- **传输模式**

  可以使用各种传输模式进行备份。有关详细信息，请参阅配置集成。

  建议使用 CBT 进行增量/差异备份，因为其速度更快且在备份设备上占用的空间更少。

  传输模式可以是 SAN 或 NBD，可以通过 Data Protector GUI 选择 (这决定了阵列访问方式)。也可以在虚拟机选项中配置传输模式。在虚拟机选项中配置的传输模式优先执行，并遵循 SAN:HOTADD:NBDSSL:NBD:FILESYSTEM 的顺序。

  例如，

  - 如果已从 Data Protector GUI 的虚拟机选项中选择 NBD
  - 如果 SAN 不可用
  - 如果 HOTADD 解决方案无法进行零宕机时间备份

  然后备份将通过 NBDSSL。但是，如果您希望备份通过 NBD 传输模式，则必须在虚拟机选项中配置 NBD 传输模式。

  SAN 传输模式下的模板备份不受支持，并将回退到 NBD 传输模式。此外，如果在选择了 SAN 传输模式后无法将复本呈现给备份主机，则 VM 备份将回退到 NBD 传输模式。

- **复本配置类型**

  要管理存储资源，您可以选择精简配置或完全分配的复本配置类型，以确保存储系统上有足够的可用磁盘空间。

- **厚磁盘和精简磁盘**

  Data Protector 无法检测虚拟机磁盘是厚磁盘还是精简磁盘。在这两种情况下，实际备份数据大小依赖 VMware VDDK API。Data Protector 无法控制实际备份数据大小。请注意，并非所有数据存储都支持更改后的块跟踪。

- **LUN 的呈现**

  要从 3PAR 复本对虚拟机进行零宕机时间备份，请确保用于创建源数据存储 (要备份的虚拟机的驻留位置) 的 LUN 未呈现到配置为装载代理主机的系统。

- **备份到 StoreOnce Catalyst 设备**

  从 9.07 开始，到 StoreOnce Catalyst 设备的所有 VEPA 备份都使用“每个存储介质单个对象”模式执行。即使未在 StoreOnce Catalyst 设备上选择此选项，也将强制执行此模式。

  将忽略您在“存储介质大小阈值 (GB)”字段中输入的任何值，以从完成到 StoreOnce Catalyst 设备的备份启用缓存 GRE 或启动和实时迁移。

- **Data Protector 许可证**

  从 3PAR 复本执行虚拟机的零宕机时间备份无需以下许可证:

  - 适用于 UNIX 的 Data Protector 即时恢复扩展 - 1 TB
  - 适用于 Linux 的 Data Protector 即时恢复扩展 - 1 TB
  - 适用于 Windows 的 Data Protector 即时恢复扩展 - 1 TB

还原 VMware 集成

本节包含还原虚拟机所需的过程。

查找要还原的信息

您可以在 Data Protector IDB 中找到有关备份对象的信息，如所使用的备份类型和介质，以及备份期间显示的消息。要检索此信息，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在“内部数据库”上下文中，展开“对象”或“会话”。

如果展开“对象”，则会根据为其创建备份对象的虚拟机对这些对象进行排序。例如：

- 在 vCenter 环境中，虚拟机 /vm/mach1 的备份对象在 /4/vCenterName%2FvmInstanceUUID 下列出。

  其中，

  vCenterName 是虚拟中心的名称。

  vmInstanceUUID 是 vCenter 上的虚拟机 /vm/mach1 的唯一标识符。

  要在 vCenter 环境中查看会话，请双击 /object1/vCenter%2FvmInstanceUUID 。

如果展开“会话”，则会根据在其中创建备份对象的会话对这些对象进行排序。例如，在会话 2012/07/10–82 中创建的备份对象列在 2012/07/10–82 下方。

要查看有关备份对象的详细信息，请右键单击备份对象，然后选择“属性”。

> **提示**要查看会话期间显示的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnidb 命令所在的目录。
3. 获取在备份会话中创建的会话 ID 为 *SessionID* 的 VMware 备份对象列表:

   omnidb -session SessionID
4. 获取有关备份对象名称为 *BackupObjectName* 的备份对象的详细信息:

   omnidb -veagent BackupObjectName -session SessionID -catalog

   以下是备份对象名称的一个示例:

   gabriel.company.com::/%2FElDatacentro/0/%2Fvm%2Fharbour

使用 Data Protector GUI 进行还原

使用此过程还原、启动和实时迁移虚拟机。

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“虚拟环境”，展开相关客户机，然后单击从中备份的数据中心。
3. 在“源”页面中，指定以下项:
   1. 从“备份方法”下拉列表中，选择以下任一备份方法:
      - 适用于 VMware vCenter 和 VMware ESX(i) 客户机的 vStorage 映像
      - 适用于 VMware vCenter 的 vStorage 映像
   2. 通过“从”和“到”下拉列表，您可以将显示的虚拟机范围缩小到在指定时间间隔内备份的虚拟机。
   3. 在“VM 过滤器”文本框中，输入 VM 的过滤器文本，然后按 Enter 键，或单击“应用过滤器”。过滤器会隐藏与过滤器模式不匹配的 VM、vApp 和资源池，使您能够轻松找到所需对象。

   选择要还原的 VMware 对象。

> **注意**您可以通过将 omnirc 变量 OB2_VEAGENT_THREADED_DISK_BACKUP 更新为 1 来并行还原 VMware 对象。有关详细信息，请参阅最常用的 omnirc 选项。

您可以选择“还原”、“启动”或“实时迁移”它们。从“VM 选项”下拉列表中选择所需选项。

请注意，仅当选择一个对象时，“启动”和“实时迁移”选项才可用。

注意过滤器区分大小写，并应用于 VMware 虚拟机对象、VMware 虚拟应用程序 (vApp) 对象和资源池。如果找到匹配的子节点 (如，另一个 VM、vApp 或资源池)，则会显示它们。如果将“VM 过滤器”文本框保留为空，则会显示所有 VM、vApp 和资源池。但是，如果输入过滤器文本，则仅显示匹配的子节点 (如果有)。如果使用“从”或“至”下拉列表修改过滤器值，则会重新应用过滤。过滤器不适用于已选择的 VM、vApp 或资源池。这意味着您可以使用一个过滤器过滤机器，选择对象，然后再次更改过滤器。在新的过滤器中，先前标记的对象仍然可见。

4. 下面是过滤器使用的类型:
   - **使用简单子字符串** - 如果输入 VM、vApp 或资源池名称的一部分，则对象树中名称中包含输入字符串的所有 VM、vApp 或资源池仍然可见。所有其他对象都将过滤掉。
   - **使用通配符和问号** - 下面是过滤选项:
     - <filter string>* - 过滤以 <filter string> 开头并以任何字符集结尾的 VM、vApp 或资源池名称。
     - *<filter string>* - 过滤以任何字符集开头和结尾且中间包含 <filter string> 的 VM、vApp 或资源池名称。
     - *<filter string> - 过滤以任何字符集开头，并以 <filter string> 结尾的 VM、vApp 或资源池名称。
     - <filter string>*01 - 过滤以 <filter string> 开头，以 "01" 结尾，且具有任何字符集代替通配符 (*) 的 VM、vApp 或资源池名称。例如， Production_VM01 。
     - <filter string>*0? - 过滤以 <filter string> 开头，以 "0" 结尾，且具有字符、数字或字母代替问号 (?) 的 VM、vApp 或资源池名称。例如， Production_VM01 和 Production_VM0A ，而不是 Production_VM11 。

   选择要还原的对象。

> **注意**Data Protector 会还原每个选定 VMware 对象的完整还原链，以上一个完整备份会话开头 (即使该完整备份超出指定时间间隔)，并以在指定时间间隔内执行的上一个备份会话结尾。

启动 (PowerOnOption ON): 从备份的映像、智能缓存、StoreOnce Catalyst 或数据域设备启动虚拟机。

实时迁移 (PowerOnOption MIGRATE): 从备份的映像、智能缓存、StoreOnce Catalyst 或数据域设备实时迁移虚拟机。

还原为新虚拟机

右键单击所选虚拟机，然后单击“还原为/还原至”，以将其还原为 vStorage 映像备份方法的新虚拟机。将打开一个新对话框以指定虚拟机的名称。

> **注意**“还原为/还原至”选项特定于 vStorage 映像备份方法。

当您选择“vStorage 映像 + OpenStack”备份方法时，您可以查看已备份的 Nova 实例及其版本。还原期间不会显示卷影 VM 对象。

还原所选备份版本

右键单击所选虚拟机，然后单击“还原版本”以选择要还原的备份版本。

将打开一个新的对话框以选择备份版本。将显示所选 Nova 实例的对象版本。

注意(特定于“vStorage 映像”备份方法) 当从其他数据中心选择备份版本时，对话框中会显示警告消息“VM 正还原至不同的数据中心” 。

5. 在“目标”页中，指定还原目标。请参阅下面的“还原目标” 表中说明的选项。
6. 如果已选择“启动”或“实时迁移”，请单击相应按钮以完成操作。
7. 在“选项”页面中，指定 VMware 还原选项。请参阅下面的“还原选项” 表中说明的选项。

   这里，在还原前将删除 VM，并在还原后在 vCenter 中注册 Nova 实例和卷影 VM。
8. 在“设备”页中，选择要用于还原的设备。
9. 单击**还原**。
10. 在“启动还原会话”对话框中，单击“下一步”。
11. 指定“报告级别”和“网络负载”。

注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。

12. 单击**完成**启动还原。

    会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

> **注意**如果还原失败，请参阅还原失败后清理数据存储。

RMC 集成还原

- 对于 RMC 备份，如果备份类型为“快照 + 磁带”，则会优先从快照执行还原操作。如果快照缺失，则从磁带设备执行还原。
- 如果备份类型为 **Express Protect**，则首先还原到 3PAR LUN，然后还原到指定位置。

还原目标 (VMware vCenter Server 和 VMware ESX(i) Server 客户机)

GUI/CLI 选项	描述
备份主机/ -barhost	指定安装了适用于 VMware 的虚拟环境 ZDB 集成的客户机以控制还原会话。默认情况下，选择与用于备份的客户机相同的客户机。
还原客户机/ -apphost	指定所选虚拟机对象应注册并还原到的客户机。默认情况下，会选择从中备份虚拟机的客户机。 要更改客户机配置，请单击“连接”按钮。
还原到数据中心/ –instance –new instance	选择此选项可将虚拟机还原到数据中心。默认情况下，将虚拟机还原到原始数据中心。 可以从 3PAR 阵列还原到数据中心。
主机/群集/ -host/cluster	选择应将虚拟机还原到的 ESX(i) Server 系统或群集。默认情况下，将虚拟机还原到原始 ESX(i) Server 系统或群集。
特定主机/ -specificHost	选择应将虚拟机还原到的群集中的特定 ESX(i) Server 系统。默认情况下，将虚拟机还原到原始 ESX(i) Server 系统。
资源池 / -resourcePool	选择应将虚拟机还原到的 ESX(i) Server 系统或群集上的资源池。默认情况下，将虚拟机还原到原始资源池。
数据存储/ –store	指定应将虚拟机还原到的数据存储。您可以从可从所选还原目标主机访问的所有数据存储中进行选择。如果将此选项保留为空，则会将虚拟机还原到原始数据存储。
还原到目录/ –directory	选择此选项可将虚拟机文件还原到备份主机上的目标中 (数据中心外部)。可以使用“浏览”按钮查找目标目录。 此类恢复完成之后，虚拟机无法正常运行。您需要使用 VMware Converter 将已还原的虚拟机映像手动移动到 ESX Server 或 ESXi Server 系统，如还原到目录后恢复虚拟机中所述。

还原选项 (VMware vCenter Server 和 VMware ESX(i) Server 客户机)

GUI/CLI 选项	描述

在需要时注册虚拟机 / -register		选择“还原到数据中心”时可用。 选择此选项可注册已还原的虚拟机。 如果未选择此选项，则需要手动恢复已还原的虚拟机，如 [#s_Recovering_virtual_machines_manually_201101281053 手动恢复虚拟机] 中所述。 默认：选择。 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择“在需要时注册虚拟机”选项。
将快照合并为单个文件/ -consolidate		选择此选项可在还原虚拟机之后，将所有快照 (包括非 Data Protector 映像) 提交到虚拟机群。 选择“还原到数据中心”时可用。
在还原后打开虚拟机/ -poweron		选择此选项可在还原之后启动虚拟机。 选择“还原到数据中心”时可用。
现有虚拟机处理 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择此选项。将使用“还原前删除”选项。	指定 Data Protector 在还原现有虚拟机时的行为。	
	还原前删除/ -deletebefore	选择此选项可在还原之前删除现有虚拟机，然后从新虚拟机将其还原。即使现有虚拟机驻留在目标数据中心之外的数据中心，也依然会被删除。 这是提高空间利用率的选项，但是并不安全，因为如果还原失败，旧虚拟机便无法使用，因此请谨慎选择。
	跳过还原/ -skip	选择此选项可跳过对现有虚拟机的还原。这样可以还原缺少的虚拟机而不会影响现有的虚拟机。
	原后删除/ eleteafter	选择此选项可在还原现有虚拟机后将其删除。即使现有虚拟机驻留在目标数据中心之外的数据中心，也依然会被删除。如果恢复失败，现有虚拟机不会被删除。 默认：选择。 如果虚拟机处于挂起状态，则无法使用此选项。如果虚拟机处于挂起状态，请执行以下任一操作: • 还原到不同位置。 • 选择“还原前删除”选项。 • 打开或关闭虚拟机。
	保留以用于取证/ _ keep_for_forensics	选择此选项可使用时间戳来标记现有虚拟机。保留争议源的虚拟机应该在恢复后关机并保留在原始位置。这不会影响原始虚拟机的后续备份。 此选项对于 Microsoft Hyper-V 客户机不可用。

文件冲突处理 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择此选项。将使用“覆盖”选项。	指定 Data Protector 在还原现有文件时的行为。	
	覆盖/ verwrite	选择此选项可使用备份中的文件覆盖现有文件。 默认：选择。
	持最新/ atest	如果文件比备份中的文件更新，则选择此选项可原封不动保留现有文件。否则，用备份中的相应文件覆盖现有文件。
	跳过/ -skip	选择此选项可保留现有文件 (文件不从备份中还原)。
类别和标记	仅在目标页面中选择 VCenter 客户机作为还原客户机时，此部分才可供选择。	
	类别/标记处理	指定在客户机还原期间 Data Protector 与标记有关的行为。 从下拉菜单中选择以下任一选项以选择如何使用标记: • 跳过附加标记 • 从备份时开始附加标记 • 附加自定义标记
	类别 *-categoryName*	仅当在“类别/标记处理” 下拉菜单中选择“附加客户标记” 时，才启用此选项。选择将所需标记分组的类别。
	标记 *- tagName/- tagId*	仅当选择类别时才启用此选项。选择要附加到还原的客户机的标记。

使用 Data Protector CLI 进行还原

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnir 命令所在的目录。
3. 执行：

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   omnir -veagent -virtual–environment vmware -barhost BackupHost -apphost OriginalVMwareClient
   ```

   ```
   –instance OriginalDatacenter –method vStorageImage| vStorageImageOpenStack [-session BackupID] VirtualMachine [VirtualMachine...] [VMwareClient | Directory] VirtualMachine -vm VMPath -instanceUUID vmInstanceUUID [-new_name NewVirtualMachineName][-disk DiskName [-disk Disk...]] VMwareClient [–newinstance TargetDatacenter] [-store TargetDatastore] [-network_name TargetNetwork] [–destination TargetVMwareClient] [-consolidate] [–register][–poweron] [–deletebefore | -deleteafter | -skip | -keep_for_forensics] Directory -directory RestoreDirectory [–overwrite | -skip | -latest]
   ```

   ```
   还原选项
   ```

   ```
   [-deletebefore | -skip | -keep_for_forensics]
   ```

   ```
   常见选项
   ```

   ```
   [-consolidate] [-register] [-poweron] [-PowerOnOption { ON | MIGRATE }] [-skipTagAttach | { [-categoryName CategoryName] [-tagName TagName] | [-tagId TagId ]}]
   ```

   有关所有选项的说明，请参阅 omnir 手册页或《Data Protector 命令行界面参考》。

   注意在还原从 Data Protector 8.1 及更低版本备份的虚拟机时，不应指定用于还原的 instanceUUID 参数。

   重要说明备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

   镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是*对象复制*会话的会话 ID。

如果存在同一对象的多个副本，则 omnir 语法不允许您指定要从哪个对象副本还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

注意如果还原失败，请参阅还原失败后清理数据存储。

示例 (将虚拟机还原到数据中心)

假设您要还原虚拟机 /vm/machineA 和虚拟机 /vm/machineB 的单个磁盘 (scsi0:0 和 scsi0:1)。在备份时，虚拟机在属于由 vCenter Server 系统 vcenter.company.com 管理的数据中心 /MyDatacenter 的 ESX Server 系统上运行。这些虚拟机采用 vStorage Image 备份方法进行备份。

要使用备份会话 2011/01/11–1 将它们还原到原始位置，并确保在会话完成时将新还原的虚拟机置于联机状态，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com –instance /MyDatacenter -method vStorageImage –session 2011/1/11-1 –vm /vm/machineA –vm /vm/machineB -disk scsi0:0 –disk scsi0:1 –poweron
```

要使用 instanceUUID 503eeaac-6fae-7898-73e1-93b722a0517c 还原虚拟机 /vm/machineA ，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com –instance /MyDatacenter -method vStorageImage –session 2011/1/11-1 –vm /vm/machineA -instanceUUID 503eeaac-6fae-7898-73e1-93b722a0517c -disk scsi0:0 –disk scsi0:1 –poweron
```

示例 (将虚拟机还原到目录)

假设使用 vStorage Image 备份方法，在会话 2011/02/12-5 中从由 vCenter Server 系统 vcenter.company.com 管理的数据中心 /MyDatacenter 备份了虚拟机 /MyVirtualMachines/machineA 和 /MyVirtualMachines/machineB 。要将数据中心以外的虚拟机还原到备份主机 backuphost.company.com 上的目录 C:\tmp ，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method vStorageImage -session 2011/2/12-5 -vm /MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB -directory c:\tmp
```

示例 (使用名称中的 instanceUUID 还原对象名称)

要支持使用名称中的 instanceUUID 还原对象名称，请执行:

```
omnir.exe -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance instanceName -method vStorageImage -session sessionID -vm vmPath –instanceUUID vminstanceUUID -register -poweron -deletebefore
```

示例 (将 Nova 实例还原到其原始位置)

要使用名称中的 instanceUUID 还原对象名称，请执行:

```
omnir -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance /Datacenter -method vStorageImageOpenStack -session sessionID -vm vmPath -instanceUUID novainstanceUUID -register -deletebefore
```

示例 (将虚拟机还原到原始位置，并将备份标记附加到还原的虚拟机**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -register -poweron
```

示例 (还原到原始位置，并跳过将标记附加到还原的虚拟机的操作**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -skipTagAttach register -poweron
```

示例 **(**还原到其他位置并将自定义标记附加到虚拟机**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -categoryName DP -tagName Gold -register –poweron
```

示例 (还原到其他位置并使用 **tagId** 附加自定义标记**):**

omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST -register –poweron

示例 （ 通过指定多个 tagId 将多个标记附加到虚拟机):

omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST2,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST3,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST4 -register –poweron

手动恢复虚拟机

有两种不同的情况需要在已使用 Data Protector 还原虚拟机后手动恢复它们:

- 如果已将虚拟机还原到备份主机上的目录 (“还原到目录”)。
- 如果已将虚拟机还原到数据中心 (“还原到数据中心”)，而未选择还原选项“在需要时注册虚拟机”。

还原到目录后恢复虚拟机

还原到目录后恢复虚拟机的步骤取决于备份虚拟机配置文件的格式。

使用 VMX 格式的 VM 配置文件进行恢复

假设使用以下备份会话将虚拟机 helios 还原到备份主机上的目录 C:\tmp\helios :

- 备份方法: **vStorage 映像**
- 备份类型: 增量
- CBT: 启用并使用

要使用 VMware Converter 将虚拟机文件手动移动到由 vCenter Server 系统 bmwvc2.company.com 管理的 ESX(i) Server 系统 dioxide.company.com :

1. 显示目录 C:\tmp\helios 的内容:

   ```
   helios.vmdk helios.vmx helios.vmdk scsi0–0.cbt scsi0–0.meta helios-flat.vmdk helios.vmx-1 helios.vmdk-1 scsi0–0.cbt-1 scsi0–0.meta-1
   helios.vmx-2 helios.vmdk-2 scsi0–0.cbt-2 scsi0–0.meta-2
   ```

   请注意，将还原在上一个完整备份、差异备份和所选增量备份会话中备份的所有文件。
2. 共享文件夹 C:\tmp\helios ，以便可以从安装了 VMware Converter 的系统访问它。
3. 登录安装了 VMware Converter 的系统，然后打开 VMware Converter 用户界面。
4. 单击“转换机器”以打开转换向导。
5. 在“源系统”页面中，为源类型选择“VMware Workstation 或其他 VMware 虚拟机”，浏览至 C:\tmp\helios 目录，然后选择 helios.vmx 文件。

   单击“下一步”。

   > **注意**在我们的示例中，备份主机上安装了 VMware Converter。
6. 在“目标系统”页面中，为目标类型选择“VMware Infrastructure 虚拟机”，并提供 vCenter Server 系统的登录凭据。

   单击“下一步”。
7. 在“目标虚拟机”页面中，指定应用于恢复虚拟机的名称。

   单击“下一步”。
8. 在“目标位置”页面中，选择目标 ESX(i) Server 系统和数据存储。
9. 在“选项”页面中，编辑选项并单击“下一步”。
10. 在“摘要”页面中，查看您的选择并单击“完成”。
11. 打开数据存储浏览器并将增量备份和差异备份会话中创建的文件上载到虚拟机目录:

```
helios.vmx-1 helios.vmdk-1 scsi0–0.cbt-1 scsi0–0.meta-1 helios.vmx-2 helios.vmdk-2 scsi0–0.cbt-2 scsi0–0.meta-2
```

12. 打开虚拟机。

使用 XML 格式的 VM 配置文件进行恢复

请遵循以下步骤:

1. 打开 vSphere 客户机并登录 ESX(i) Server 或 vCenter Server 系统。

   如果虚拟机仍处于已配置状态，则请删除其所有硬盘:

   a. 在库存对象树中，右键单击虚拟机并选择“编辑设置”。

   b. 在“虚拟机属性”窗口的“硬件”选项卡中，选择每个硬盘，并单击“删除”。

   c. 单击“确定”，确定删除。

   如果虚拟机已不存在，则请配置不包含硬盘的新虚拟机，并使用原始虚拟机的名称。

   在任何情况下，请牢记关联数据存储名称。

2. 上载在备份会话过程中创建的虚拟机文件:

   a. 在库存对象树中选择托管虚拟机的 ESX(i) Server 系统。

   b. 单击“配置”选项卡，并选择“硬件”下的“存储”。

   c. 右键单击数据存储名称，并选择“浏览数据存储”。

   d. 在“数据存储浏览器”窗口的文件夹树中，选择虚拟机文件夹，单击窗口工具栏上对应的图标。根据需要选择“上载文件”或“上载文件夹”。

   e. 选择所有适用文件并完成上载。

3. 重用备份副本时将硬盘添加到虚拟机:

   a. 在库存对象树中，右键单击虚拟机并选择“编辑设置”。

   b. 在“虚拟机属性”窗口中单击“添加”。

   c. 在“添加硬件”窗口中选择“硬盘”并单击“下一步”。

   d. 选择“使用现有虚拟磁盘”并单击“下一步”。

   e. 单击**浏览**。

   f. 在“浏览数据存储”窗口中，浏览到合适的数据存储，并打开虚拟机文件夹。选择虚拟磁盘文件并单击“确定”。

   g. 遵循“添加硬件”向导以完成步骤。

   h. 为每个存在备份副本的其他硬盘重复从 b 到 g 的子步骤。

4. 打开虚拟机。

还原到数据中心后恢复虚拟机

如果已将虚拟机还原到数据中心，而未选择选项“在需要时注册虚拟机”:

1. 打开数据存储浏览器并浏览到已还原的虚拟机目录。
2. 右键单击虚拟机 *.vmx 文件，然后选择“添加到库存”。
3. 按照向导操作，然后单击“完成”。

使用其他设备进行还原

您可以使用与用于备份的设备不同的设备进行还原。有关详细信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

还原失败后清理数据存储

有时，当虚拟机还原失败时，Data Protector 会在虚拟机数据存储上创建额外的文件。如果未删除这些文件，则可能会在后续会话中创建损坏的虚拟机备份，因此从此类备份还原也会失败。

假设虚拟机 MyVirtualMachine 无法还原。要在还原后清理数据存储，请执行以下操作:

1. 打开 VMware vSphere 客户机。
2. 右键单击虚拟机，然后选择“从磁盘删除”。

3. 打开“数据存储浏览器”。

   目录 MyVirtualMachine 应该不再存在。

   检查是否存在任何额外目录:

   MyVirtualMachine_1

   MyVirtualMachine_2

   等等。

   右键单击每个此类目录，然后选择“从磁盘删除”。

灾难恢复

灾难恢复极其复杂，涉及到来自不同供应商的不同产品。请查看来宾操作系统和 VMware 中关于如何为其做好准备的说明。

下面是发生灾难后恢复虚拟机所需的主要步骤:

1. 重新安装 VMware 环境。配置应与备份期间的配置相同。
2. 在新配置的环境中安装 Data Protector。
3. 将运行虚拟机的 ESX Server 系统的服务控制台从 Data Protector 文件系统备份还原到新配置的 ESX Server 系统。

   有关要还原内容的详细信息，请参阅 http://kb.vmware.com/selfservice/microsites/microsite.do 上的“ESX Server 配置备份和还原过程”主题。

   有关如何从文件系统备份还原的详细信息，请参阅《Data Protector 帮助》。
4. 还原原始 vCenter 数据库 (如果需要)。有关详细信息，请参阅用于备份数据库的 Data Protector 集成。
5. 如本节所述，从 Data Protector 虚拟环境备份还原虚拟机。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了“用户界面” 组件的任何 Data Protector 客户机中监视会话。

要监视会话，请参阅《Data Protector 帮助》索引: “查看当前正在运行的会话”。

适用于 VMware 的虚拟环境 ZDB 集成

本节说明如何配置和使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成。它介绍备份和还原使用 Dell EMC Unity、NetApp 或 3PAR 存储的 VMware vSphere 虚拟环境需要了解的概念和方法。

Data Protector 零宕机时间备份 (ZDB) 功能提供联机备份功能，并最大程度地避免应用程序系统性能下降。应用程序系统上的负载显著降低，因为备份是非中断的，不需要虚拟机宕机时间。使用单独的备份系统对复制的数据执行磁带备份。

适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成功能支持使用 Dell EMC Unity、NetApp 和 3PAR 存储系统进行设置、且通过 vCenter Server (vCenter 环境) 加以管理的 ESX(i) Server 系统环境。

Data Protector 支持：

- **NetApp 存储**: ZDB 到磁带、ZDB 到磁盘和 ZDB 到磁盘 + 磁带
- **3PAR 存储**: ZDB 到磁盘、ZDB 到磁带和 ZDB 到磁盘 + 磁带
- **Dell EMC Unity**: ZDB 到磁带、ZDB 到磁盘和 ZDB 到磁盘 + 磁带

在创建复本期间，应用程序系统全面运行，并主动使用 VMware 虚拟环境。随后，备份系统上将执行数据向磁带介质的流式传送。可以使用标准的 Data Protector“从磁带恢复”恢复备份数据。

Data Protector 提供交互式和计划 ZDB 到磁带和标准还原方法。

支持的磁盘阵列和磁盘阵列配置

支持的阵列	支持的配置
NetApp 存储系统	运行 Data ONTAP 8.2 7-Mode 的系统 运行 Data ONTAP 8.2 C-Mode 的系统 对于高级 VMware 和 GRE 操作，仅支持 ONTAP 9.55 P5 C-Mode。
3PAR 存储系统	运行 InForm OS 版本 3.1.2、3.1.3 和 3.2.1 的系统
Dell EMC Unity	4.5.0

本节提供特定于适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成的信息。

建议不要在 VMware vCenter Server 系统或 VMware ESX(i) Server 系统上安装任何 Data Protector 组件。

以下限制适用：

- 升级到 Data Protector 9.05 或更高版本后，您无法从更早的 Data Protector 版本重新启动已失败的 VMware 备份会话。
- 从 7.03 或较早版本升级之后，如果不运行完整备份，就无法运行增量备份或差异备份。
- Linux 备份主机仅支持来自 StoreOnce Catalyst 的启动和实时迁移操作。
- 在升级到 VDDK 6.0 Update 1 之后，SAN 传输模式将在 vSphere 5.5 环境中回退到 NBDSSL。
- 对于更改后的块跟踪要求，请参见以下 URL：

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128

- 不支持在 vSphere VVol（虚拟卷）数据存储上进行虚拟机 3PAR 零宕机时间备份 (ZDB) 和即时恢复。

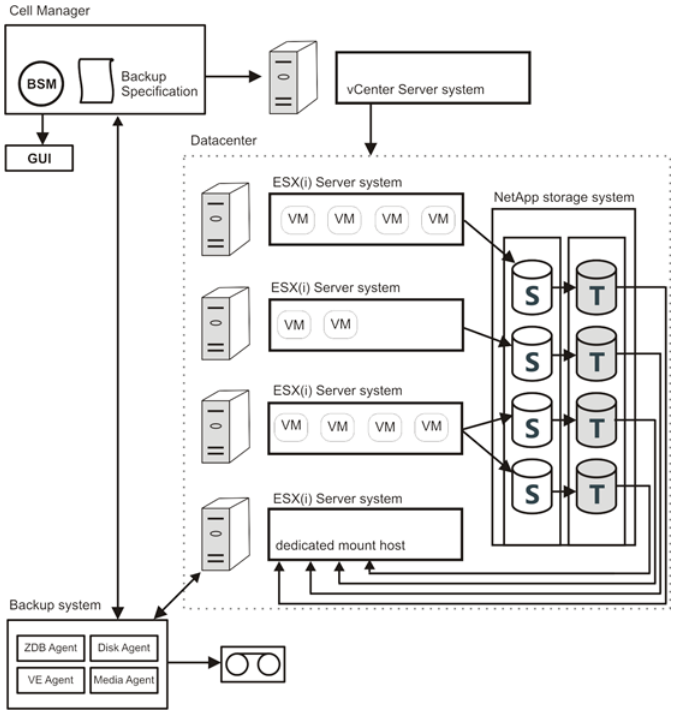
集成概念

Data Protector 支持通过 vCenter Server 管理 ESX 和/或 ESXi Server 系统 (ESX(i) Server 系统) 的环境 (vCenter 环境) 以及具有独立 ESX(i) Server 系统的环境 (独立 ESX(i) Server 环境)。此外，它还支持具有独立 ESX(i) Server 系统的环境，以及混合环境（其中一些 ESX(i) Server 系统通过 vCenter Server 系统进行管理，而另一些系统则为独立系统）。环境中甚至可以有多个 vCenter Server 系统，每个系统都管理自己的一组 ESX(i) Server 系统。

但您设置了虚拟环境，对于适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成，需要使用光纤通道将 ESX(i) Server 系统连接到同一存储系统。只有在 Dell EMC Unity、NetApp 和 3PAR 存储系统上运行的虚拟环境支持适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成。

以下 VMware ZDB 集成体系结构显示了适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成。

VMware ZDB 集成体系结构



虚拟环境:

在此图中，虚拟环境是管理四个 ESX(i) Server 系统的 vCenter 系统。ESX(i) 服务器通过光纤通道 SAN 连接到存储系统。前三个 ESX(i) 服务器是活动应用程序系统，第四个是装载主机，一个专用于装载复本的系统，仅用于 ZDB 备份。

> **注意**建议使用专用 ESX(i) Server 进行 ZDB 备份 (装载主机)。

Dell EMC Unity、NetApp 和 3PAR 存储系统支持对虚拟机使用的磁盘卷进行快照复制。包含源或原始数据对象 (S) 的卷将复制到等量目标卷 (T) 中。当复制过程完成后，目标卷中的数据将构成快照复本。有关磁盘复制的详细信息，请参阅关键概念。

vCenter 系统作为 **VMware vCenter** 客户机导入 Data Protector 单元。

备份系统:

备份系统用于启动备份过程并将已解析的复本备份到磁带。建议使用专用的物理备份系统。

Data Protector 组件:

要启用适用于 VMware 环境的 Data Protector 虚拟环境 ZDB 集成，应安装以下 Data Protector 组件:

- ZDB 集成代理 (NetApp 存储提供程序或 P6000/3PAR SMI-S 代理)

  > **注意**存储提供程序插件可在 Data Protector ZDB SMI-S 代理中启用 ZDB 集成。

- Data Protector 虚拟环境集成 (VEAgent)
- Data Protector Disk Agent
- Data Protector General Media Agent

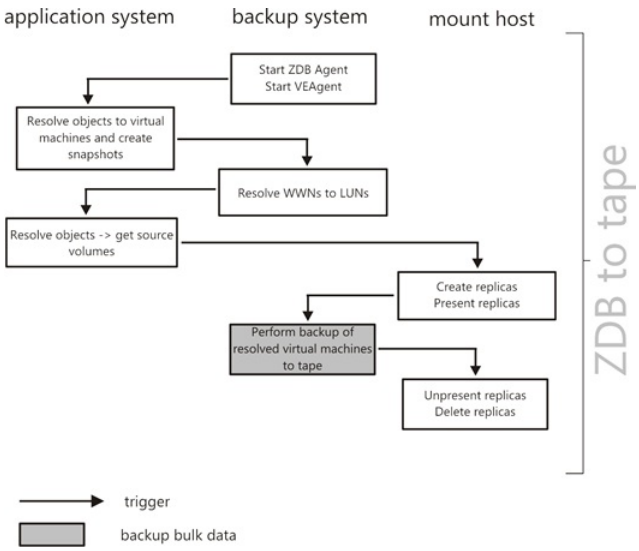
ZDB 集成代理、Data Protector 虚拟环境集成组件和 Data Protector 磁盘代理必须同时安装在单元中的至少一个 Data Protector 客户机上。此客户机称为备份系统。

必须在将数据传输到备份设备的客户机上安装 Data Protector 常规介质代理。它可以安装在备份系统上。

使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成恢复虚拟机，与从“本地或网络备份”备份类型恢复虚拟机相同。

备份过程

VMware ZDB 备份流



本节仅提供有关适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成的信息。

以下复本操作依赖于 ZDB 选项，或由 ZDB 选项触发。

1. 开始对虚拟环境进行零宕机时间备份时，Data Protector 将在备份系统上启动 VEAgent 和 ZDB 代理。应用程序系统上的 VEAgent 解析要备份到虚拟机的所选对象，并创建虚拟机快照。
2. VEAgent 解析要备份到数据存储 WWN 的所选对象，ZDB 代理将 WWN 解析为 LUN。
3. ZDB 代理创建已解析 LUN 的复本。
4. 复本呈现给 ESX(i) 装载主机，备份系统将所有已解析的虚拟机备份到磁带。
5. 备份完成之后，将隐藏并删除复本。

静止

如果选择了静止，则快照进程将静止所有系统写入程序和已注册的应用程序写入程序。在 Windows 来宾操作系统中，VSS 框架在创建快照之前冻结或静止在虚拟机中运行的应用程序。每次为备份选择“使用静止”选项时，Data Protector 都会执行应用程序一致的静止。

选中“使用静止快照”复选框。您可以选择要报告的错误级别。可选择以下错误级别:

- **致命**: 如果静止快照失败，则会话将失败。
- **警告**: 如果静止快照失败，则会显示一条警告消息并继续备份过程。

有关 CLI 选项，请参阅《CLI 参考指南》。导航到“第 1M 部分”:*“管理命令”>“vepa_util.exe(1M)”*。

> 启用“静止”选项后，针对 MS SQL、MS SharePoint、MS Exchange 和 Oracle 的虚拟机备份具有应用程序一致性。当按照供应商的建议配置应用程序时，一致性效果最佳。Data Protector 建议在虚拟机中安装相应的集成代理以保护这些应用程序。

以下先决条件适用:

- 对于共享点服务器的基于 VEPA 的静止备份，必须在开始备份虚拟机之前注册 VSS 写入程序。有关详细信息，请参阅《适用于 Microsoft 卷影复制服务的集成指南》中的“Microsoft SharePoint Services Writer 详细信息”一节。
- 对于 Oracle 11g 版本 2 数据库的基于 VEPA 的静止备份，在开始备份虚拟机之前，Oracle VSS 写入程序服务应处于活动/运行状态。可以通过执行命令 `oravssw /q /start` 完成此操作。对于 SQL 和 SharePoint 等其他应用程序，默认情况下，VSS 写入程序已注册并处于活动状态。

以下限制适用：

- “静止”功能可能会大幅降低备份会话的速度。
- VEPA 静止功能不支持 Windows OS 群集中的“可用性组”群集应用程序上的 Microsoft SQL 数据库。
- VEPA 备份不支持在共享模式下对磁盘使用 SCSI 控制器的群集应用程序。

- vRDM 磁盘只能用于完整备份。
- 处于“关闭”状态的虚拟机的静止备份无效。

静止操作注意事项

VMware 注意事项

- 不要禁用虚拟机的 UUID 属性。
- 虚拟机只能使用 SCSI 磁盘。具有 IDE 磁盘的虚拟机不支持应用程序一致的静止。虚拟机中的空闲 SCSI 插槽数量必须与磁盘数量相同。
- 物理 RDM 不能用于静止，因而不支持快照。
- Microsoft 群集上的虚拟机备份不支持静止。有关详细信息，请参阅在使用总线共享配置的虚拟机上备份。

虚拟机注意事项

- 虚拟机不得使用动态磁盘。
- 确保在虚拟机中安装了最新版本的 VMware 工具。有关详细信息，请参阅验证 Vmware 工具内部版本。
- 必须在 VMware 工具升级过程中明确指定 VSS 组件。VSS 不会以非交互式模式安装。有关详细信息，请参阅使用 Vmware 工具安装卷影复制服务。
- 必须在 VMware 工具安装期间运行分布式事务处理协调器服务。否则，VSS 无法使 Windows 系统处于静默状态。
- 确保所有相应的 VSS 应用程序服务正在运行并正确列出了启动类型。

有关 VSS 静止相关问题的详细信息，请参阅卷影复制 (VSS) 静止相关问题故障诊断。

磁盘空间要求

虚拟机备份要求虚拟机磁盘所在的数据存储中具有足够的磁盘空间，可以容纳存储系统上的快照和复本。

有两种复本配置类型可用于管理存储资源:

- 精简配置

  通过精简配置，可以节省存储资源。磁盘空间分配动态地适应存储需求。它允许您在 LUN 之间共享可用空间，并支持 LUN 仅消耗其实际使用的空间。

  所需的可用空间基于 Data Protector 快照创建的差量文件。仅将自上次备份会话以来所做的更改写入复本

- 完全分配

  通过此配置类型，保留空间的 LUN 和快照副本具有能够持续覆盖的预分配空间。这一保证空间不可用于卷内的任何其他 LUN 或快照副本。

  所需的可用空间根据创建快照之前的虚拟机磁盘大小进行计算。所需的总磁盘空间是快照所需空间的两倍。复本需要的空间量与源 LUN 相同。如果目标不保留空间，请确保卷具有足够的可用空间来容纳复本。

所需可用空间选项

您可以使用 Data Protector 的“所需可用空间 (%)”选项确保仅当具有足够的可用空间时才备份虚拟机。

所需的可用空间根据创建快照之前的虚拟机磁盘大小进行计算。Data Protector 会检查虚拟机磁盘所在的所有数据存储。如果其中一个数据存储不满足指定的可用空间百分比，则不会创建任何快照，并且虚拟机的备份将失败并显示错误。

备份多个虚拟机时，该检查将分别应用于每个虚拟机。将备份通过检查的虚拟机，而不备份未通过检查的虚拟机。

如果指定 0％，则省略该检查。

示例

以下示例说明了“所需可用空间 (%)”选项的工作原理:

1. 使用驻留在数据存储 "datastore1" 上的磁盘 "disk1" 备份单个虚拟机 "test1":

   如果在“所需可用空间 (%)”选项中指定 30% 且数据存储的大小为 100 GB，当数据存储上至少有 30 GB 的可用空间时，备份将成功。

2. 使用驻留在 "datastore1" 和 "datastore2" 这两个数据存储上的 "disk1" 和 "disk2" 这两个磁盘备份单个虚拟机 "test1":

   如果指定需要 30% 的可用空间，当每个数据存储上至少有 30 GB 的可用空间时，备份将成功。

3. 备份两个虚拟机，即使用数据存储 "datastore1" 上的磁盘 "disk1" 备份虚拟机 "test1"，使用数据存储 "datastore2" 上的磁盘 "disk2" 备份虚拟机 "test2":

   如果需要 30% 的可用空间，当每个数据存储上至少有 30 GB 的可用空间时，这两个虚拟机的备份将成功。例如，如果数据存储 "datastore1" 的可用空间少于 30% 且数据存储 "datastore2" 至少具有 30% 的可用空间，则虚拟机 "test1" 的备份将失败，虚拟机 "test2" 的备份将成功。如果这两个数据存储的可用空间均少于 30%，则两个虚拟机的备份都将失败。

磁盘空间要求

备份方法	数据存储上需要的磁盘空间	说明
vStorage 映像	所有虚拟机磁盘大小的总和，加上: • 任何静止 zip 文件的大小 (如果指定了静止)。	创建虚拟机快照时，对虚拟机磁盘所做的更改将记录到单独的文件中 (为每个虚拟机磁盘创建一个差量文件)。差量文件可以增长到原始虚拟磁盘的大小。

备份磁盘缓冲区

您可以使用 omnirc 选项 OB2_VEAGENT_BACKUP_DISK_BUFFER_SIZE 指定备份磁盘缓冲区。

SAN 和 HotAdd 备份支持 1 MB 到 256 MB 的磁盘缓冲区大小。默认情况下，其磁盘缓冲区大小为 8 MB。但是，NBD 和 NBD (SSL) 等网络备份始终使用默认磁盘缓冲区大小 1 MB 执行。

> **注意**
>
> - 如果没有足够的内存用于指定的磁盘缓冲区大小，则将回退至 1 MB 磁盘缓冲区大小以保持备份运行，并显示一条警告消息。
> - 使用更大的磁盘缓冲区大小可以提高备份性能，但也会增加内存消耗。在一定程度上，由于备份主机的限制，备份性能不再提高。

还原概念

您能够以不同的方式还原使用任一 vStorage 映像备份方法所备份的 VMware 对象。

还原使用“vStorage 映像”方法备份的 VMware 对象

那些使用 **vStorage 映像**方法备份的虚拟机、虚拟机磁盘和虚拟机模板可以恢复：

- 到数据中心
- 到备份主机上的目录

还原到数据中心

默认情况下，虚拟机恢复到原始数据中心和原始数据存储，但您可以根据需要选择其他数据中心。

默认情况下，Data Protector 将在恢复之前删除虚拟机（如果存在），即使虚拟机所在的数据中心与恢复到的数据中心不同时也是如此。

> **注意**如果在还原向导的“还原客户机”选项中选择 ESX(i) Server 客户机 (目标客户机)，将不会删除迁移的虚拟机，因为 ESX(i) Server 客户机无法检测位于不同 ESX(i) Server 客户机上的虚拟机 (只有 vCenter 客户机才能做到这一点)。因此，最后会得到两个拥有相同 UUID 的虚拟机。

或者，您可以选择仅当虚拟机不存在时还原虚拟机，使现有虚拟机保持不变。

对于该还原，您还可以指定以下内容:

- 是否应在数据中心注册还原的虚拟机
- 还原完成时是否应合并还原的虚拟机快照
- 是否应启动还原的虚拟机

默认情况下，提供的还原选项设置为将虚拟机还原到原始数据中心。

您可以将虚拟机和虚拟机磁盘从复本还原到数据中心。请注意，不支持从复本到目录的还原会话。在“磁盘 + 磁带”备份中，如果管理员循环或删除了复本，则从磁带进行还原。

还原单个虚拟机磁盘

为了能够将单个虚拟机磁盘还原到数据中心，原始虚拟机必须仍然存在。否则，还原失败。

还原会话的进度如下:

1. 关机虚拟机的电源。
2. 如果要还原的磁盘仍然存在，则会将其删除。
3. 从备份还原磁盘。

> **注意**还原之后，属于动态磁盘集或来自不同时间点的虚拟磁盘可能需要用户在来宾操作系统和/或其中运行的应用程序上执行其他操作 (例如，装载、重签名或恢复)。

还原到目录

恢复到目录（在数据中心外部恢复）时，虚拟机的所有文件将恢复到您在备份主机上所选的目录（例如， C:\tmp ）。

在指定的目录中，使用与备份时虚拟机（及其虚拟磁盘）所在的数据存储对应的名称创建子目录。与虚拟磁盘相关的文件恢复到各自的子目录。

此类恢复完成之后，虚拟机无法正常运行。需要使用 VMware Converter 将已恢复的虚拟机映像手动移至 ESX(i) Server 系统。

还原使用“vStorage 映像 + OpenStack”方法备份的 Nova 实例和卷影 VM

还原会话的进度:

1. 查询 IDB 以获取附加到 Nova 实例的卷影 VM 列表。
2. 查询 vCenter 以创建 Nova 实例和卷影 VM 的映射。
3. 相关的卷影 VM 将添加到还原对象列表中。
4. 查询 vCenter 以创建映射并验证卷影 VM 是否附加到原始实例。
5. 从 IDB 查询还原版本以获取还原链。
6. 从 vCenter 中删除卷影 VM 文件。
7. 从 vCenter 中删除 Nova 实例文件。
8. 在相同的文件夹结构中还原 Nova 实例和磁盘文件。
9. 还原卷影 VM 配置文件。
10. 注册虚拟机并还原网络。

> **注意**如果还原期间 vCenter 中提供了所选 Nova 实例，则会在删除该 Nova 实例之前分离卷影 VM。

Data Protector 还原之后，要将 OpenStack Horizon 仪表板中的 OpenStack 实例恢复到正确的状态，请执行以下步骤:

1. 通过执行以下命令在“Nova 代理”节点中重新启动“Nova 计算”服务:

   ```
   Service nova-compute restart
   ```

2. 刷新 Horizon 仪表板以检查 Nova 实例是否可用。如果 Nova 实例不可用，请连接到“OpenStack 管理”节点并执行以下命令:
   - Nova list : 列出 Nova 实例。
   - Nova reset-state –active “instance-uuid” : 将 Nova 实例的状态重置为活动。
   - Nova reboot “instance-uuid” : 重新启动 Nova 实例。

   重新启动之后，刷新 Horizon 仪表板并检查 Nova 实例的可用性。

还原链

从在增量或差异会话中创建的备份还原虚拟机时，Data Protector 会自动还原整个备份链，从上次完整备份开始，然后是差异备份和所有后续增量备份 (如果存在)，一直到所选会话。

启动和实时迁移

启动

可以在几秒钟内从驻留在 3PAR 复本 (本地或远程复制)、智能缓存、StoreOnce Catalyst 和数据域设备上的 Data Protector 备份映像即时启动虚拟机。之前，仅在完整的数据迁移到生产数据中心之后才必须开启虚拟机。如果想要验证备份的健全性，请使用此功能。请注意，启动虚拟机后对其所做的更改将一直可用，直到您执行执行清理操作为止。

启动虚拟机时，备份映像将呈现给目标 ESX Server。将创建一个新的虚拟机，其数据磁盘指向 Data Protector 备份映像。其他文件驻留在目标数据中心。

> **注意**数据域系统 (OS 版本 6.1) 的阈值限制为每个进程 64 个连接。此限制影响“启动”和“实时迁移”操作支持的增量会话数。如果达到此阈值限制，将显示一条消息。要继续执行“启动”和“实时迁移”操作，请通过关闭当前处于活动状态的“启动”请求释放连接。

实时迁移

此选项将从备份映像启动虚拟机，并同时启动到目标数据存储的数据迁移。在此过程中，虚拟机一直可访问。由于数据移动是后端操作，因此对已启动的虚拟机的使用和可访问性产生的影响最小。对虚拟机数据所做的任何修改都将合并，在迁移的虚拟机上，所有修改的内容都将覆盖从备份还原的映像。

数据迁移完成后，虚拟机将从目标数据存储运行，不依赖于备份映像。此外，将删除备份映像呈现。

> **注意**
>
> - 在 Windows 备份主机上使用“启动”和“实时迁移”时，确保 Data Protector INET 服务和 Data Protector 过滤器侦听程序服务正在使用相同的用户凭据运行。
> - 仅当原始备份驻留在其中一个受支持的设备上时，才可以执行“启动”和“实时迁移”操作。如果备份驻留在不受支持的设备上并且对受支持的设备执行了对象复制，则无法执行这些操作。
> - 仅当原始备份已过期且副本提升为原始备份时，才能从复制的会话执行“启动”和“实时迁移”操作 (如果在受支持的设备上)。
> - 数据域系统 (OS 版本 6.1) 的阈值限制为每个进程 64 个连接。此限制影响“启动”和“实时迁移”操作支持的增量会话数。如果达到此阈值限制，将显示一条消息。要继续执行“启动”和“实时迁移”操作，请通过关闭当前处于活动状态的“启动”请求释放连接。

仅 StoreOnce Catalyst 和数据域设备

- 支持从完整备份，增量备份和差异备份执行“启动”和“实时迁移”操作。
- 9.05 和 9.06 备份支持从对象副本执行“启动”和“实时迁移”操作。应该基于会话执行对象复制以确保数据一致性。

  > **注意**如果要将 Data Protector 9.05 或 9.06 版本的备份迁移到 StoreOnce Catalyst 和数据域设备以使用“启动”和“实时迁移”功能，则建议您通过单独的会话执行对象操作。如果同时选择多个会话，则无法确保数据一致性。

- 如果从 StoreOnce Catalyst 设备启动虚拟机，则必须在执行“实时迁移”操作之前清理虚拟机。

清理/关闭

Data Protector 存储所有已启动虚拟机的列表。它将有关所有已启动虚拟机的详细信息以 XML 文件的形式存储在 Cell Server 中。清理和关闭操作如下所列:

- 如果虚拟机已开机超过 24 小时，则会关闭并清理相关存储。
- 如果从复本启动虚拟机，则将卸除数据存储并从阵列中删除在启动过程中创建的复本。
- 如果从智能缓存、StoreOnce Catalyst 或数据域设备启动虚拟机，则在清理过程中将删除数据存储，并删除 NFS 共享。

请注意，上述操作适用于通过“启动”功能启动的虚拟机。

开机超过 24 小时的虚拟机将在下次日常维护作业期间进行清理操作。在日常维护作业中清理的所有虚拟机均记录在 poweronvms_cleanup.log 文件中。

请注意，智能缓存设备上的增量和差异备份不支持启动和实时迁移。

还原注意事项

- **并发会话**

  使用相同设备的还原会话不能并发运行。

- **失败还原会话**

  有时，当虚拟机还原失败时，Data Protector 会在数据存储上创建额外的文件，您需要在会话完成时手动清理这些文件。否则，可能会在后续会话中创建损坏的虚拟机备份，而且从此类备份还原也会失败。

  当虚拟机还原到块大小与虚拟机磁盘大小不兼容 (即 .vmdk 文件大小不是多个数据存储的块大小) 的非原始数据存储时，还原将失败。

- **vApp 中的虚拟机**

还原备份时驻留在 vApp 容器中的虚拟机时，该虚拟机不会还原到 vApp 容器，而是还原到 ESX(i) Server 根级别。如果 vApp 容器中的虚拟机仍然存在，则会将其删除或跳过还原，具体取决于您在“现有的虚拟机处理”选项中所做的选择。

- **从 vStorage 映像备份执行部分还原**

  当从 vStorage 映像备份执行部分还原 (例如，还原许多已备份的 VM 磁盘中的仅其中一些时)，忽略默认选项“还原后删除”并改用“还原前删除”选项。

- **传输模式**

  以下建议适用于特定的虚拟机传输模式:

  - *SAN 传输模式:* 要使用 SAN 传输模式进行还原，请执行以下操作:
    - 为还原会话选择物理备份主机。
    - 确保呈现给备份主机和 ESX(i) Server 系统的存储卷并非只读。有关如何检查存储卷属性的详细信息，请参阅“使用 SAN 传输模式的还原会话失败”。
    - 确保存储卷大小是基础 VMFS 块大小的倍数。否则，对余数的写操作将失败。例如，如果存储卷大小为 16.3 MB 且块大小为 1 MB，则写入余数 0.3 MB 将失败。有关详细信息，请参阅以下位置的 VMware 知识库文章:

      http://kb.vmware.com/selfservice/microsites/searchEntry.do。

      搜索“使用 SAN 传输进行备份和还原的最佳实践”。
  - 建议使用 CBT 进行增量/差异备份，因为其速度更快且在备份设备上占用的空间更少。

- *Hotadd 传输模式:* Hotadd 传输模式可用于还原，但 VMware 不支持多个磁盘。因此，在 HotAdd 环境中，使用 omnirc 选项 OB2_VEAGENT_RESTORE_TRANSPORT_METHOD 将还原传输模式设置为 NBD。

  启动注意事项

  - 在备份主机上安装以下 NFS 包:
    - 对于智能缓存备份: NFS 3 或更高版本
    - 对于 StoreOnce Catalyst 和数据域设备备份: NFS 4 或更高版本
  - Data Protector 使用 Windows PowerShell 脚本 nfsServiceCheck.ps1 启动 NFS 服务，在启动过程中需要该服务。执行此脚本需要将执行策略设置为 *RemoteSigned*。如果您需要“限制”策略，则将 omnirc 变量 OB2_NO_NFSSERVICE_CHECK 设置为 1。如果该脚本失败，则需要手动执行此操作。导致 NFS 服务安装失败的一些可能原因可能是:
    - NFS 端口被另一个应用程序使用。
    - Powershell 可能需要重新启动。
    - Powershell 存储库中不存在 NFS 模块。

    使用以下命令手动执行 NFS 服务:
    - Windows 命令行: powershell.exe NFSServiceCheck.ps1
    - PowerShell 命令行: NFSServiceCheck.ps1
  - 将跳过作为“启动”功能的一部分创建的非永久性虚拟机的备份。尝试执行备份操作时，将显示以下消息: “发现已开机的非永久性虚拟机，正在跳过备份”。
  - 将在从智能缓存或 StoreOnce Catalyst 和数据域设备启动的虚拟机中禁用网络。
  - 要手动清除 Cell Manager 中已启动的所有 VM，请执行以下操作:

    1. 在所有备份主机上将 omnirc 变量 FORCE_PURGE_POWERON_VMS 设置为 1。
    2. 在 Cell Manager 中运行以下命令:

       ```
       /opt/omni/sbin/omnidbutil -purge_expired_poweron_vms
       ```

> **注意**所有已启动的 VM 将被关闭并删除。

仅 3PAR 存储系统

- 必须在 Linux 装载代理主机中安装 vmfs-tools-0.2.5 。.
- 必须确保多路径服务在 Linux 装载代理主机中运行。
- 必须在 Linux 装载代理主机中安装 sg3_utils rpm package 。
- 要从 3PAR 复本执行 GRE 操作，GRE 装载代理主机和源 ESX Server 必须存在于同一个 3PAR 区域中。

StoreOnce Recovery Manager Central 集成

StoreOnce Recovery Manager Central (RMC) 软件将 3PAR StoreServ 主存储与 StoreOnce 备份系统相集成。RMC 将 3PAR StoreServ 主存储与 StoreOnce 备份系统相集成，可提供融合数据保护，从而通过灵活的恢复选项确保应用程序一致的恢复点实现恢复。

Express Protect 功能支持从 3PAR StoreServ 直接备份到 StoreOnce 设备，而不依赖于备份软件，提供了另一层数据保护。到 StoreOnce 的备份是自包含卷，经过重复数据删除以节省空间，可用于恢复到原始或不同的 3PAR StoreServ 阵列，即便原始基本卷丢失也如此。Express Protect 功能支持从主存储直接备份到备份存储，从数据路径中完全删除应用程序服务器。

借助适用于 VMware 的 StoreOnce RMC，可以使用应用程序一致的快照保护 VMware 虚拟机磁盘 (VMDK) 和数据存储，从而实现快速的联机恢复。

使用 Data Protector，您可以将 RMC 创建的虚拟机快照备份到 Data Protector 支持的辅助存储设备。您随后可以执行到所需目标的还原操作。请注意，Granular Recovery Extension (GRE) 操作只能对快照+磁带备份执行。

Data Protector 支持以下备份类型:

- **快照备份**: 使用快照备份，您可以创建原始卷的快照。
- **快照 + 磁带**: 使用快照 + 磁带备份，您可以创建快照并将数据备份到 Data Protector 支持的辅助存储设备。
- **Express Protect 备份**: 使用 Express Protect 备份，您可以将快照从 3PAR StoreServ 备份到 StoreOnce。

下表列出了支持的备份类型，即支持 Granular Recovery Extension、“启动”和“实时迁移”操作的备份。

支持的备份	备份类型	GRE	启动和实时迁移
快照	• 完整	不受支持	不受支持
快照 + 磁带	• 完整	如果磁带设备是智能缓存、StoreOnce Catalyst 或数据域，则支持缓存 GRE。对于任何其他类型的磁带设备，支持非缓存 GRE。	如果磁带设备是智能缓存、StoreOnce Catalyst 或数据域，则支持。
快照 + 磁带	• 增量备份 • 差异备份	如果磁带设备是 StoreOnce Catalyst 或数据域，则支持缓存 GRE。对于任何其他类型的磁带设备，支持非缓存 GRE。	如果磁带设备是 StoreOnce Catalyst 或数据域，则支持。
Express Protect	• 完整 • 增量	不受支持	不受支持

RMC 集成注意事项

- RMC 备份不支持由多个 LUN 组成的单个数据存储。
- 创建备份规范时提供的 RMC 服务器详细信息在保存规范后无法修改。
- 对于 RMC 集成备份，如果使用自动化脚本创建 barlist，请确保为创建 barlist 而指定的恢复集名称唯一。
- 对于 RMC Express Protect 备份，Data Protector 在内部保留 2 个快照。这对于执行增量备份必不可少。当快照计数超过 2 时，Data Protector 会循环旧快照。
- 仅从 Inform OS 版本 3.2.1 MU1 开始支持 RMC Express Protect 备份。
- 仅 Windows 和 Linux Cell Manager 平台中支持 RMC 计划和备份报告。
- 对于从快照执行的 RMC 还原会话，必须使用 omnidbzdb 命令添加阵列凭据。
- 对于 RMC 还原会话，只有 Data Protector 磁带还原可以还原到目录。
- 对于 RMC 快照和 Express Protect 备份，GRE GUI 中不显示会话信息。
- 从 3PAR Management Console 或通过运行 3PAR CLI 命令 showhost 可以看到，备份和应用程序主机名应与 3PAR 上的主机名匹配。主机名区分大小写。

您应当已熟悉 StoreOnce RMC 概念和过程。有关 RMC 的详细信息，请参阅《StoreOnce Recovery Manager Central 用户指南》和《适用于 VMware 的 StoreOnce Recovery Manager Central 用户指南》。

Express Protect 还原: 如果在 Express Protect 将数据从 StoreOnce 还原到新快照时中止还原会话，则 Data Protector 会话将中止。但是，在后台继续从 StoreOnce 还原到快照。您需要等到 RMC 还原操作完成，然后才能触发来自同一会话的其他 Data Protector 还原操作。

RMC 集成过程

1. **添加 RMC 服务器详细信息**: 使用命令行界面添加 RMC 服务器。

   执行命令 omnidb -addhost -servername <rmcservername> -user <username> -passwd <password>。

2. **备份**: 通过在 Data Protector GUI 中选择 StoreOnce RMC 作为“备份类型”执行备份操作。

3. **还原**: 使用 GUI 执行还原操作或 GRE 操作。

使用 omnirc 选项自定义 Data Protector 行为

omnirc 选项可用于对影响 Data Protector 客户机行为的其他设置进行故障诊断或覆盖。适用于 VMware 的虚拟环境 ZDB 集成的选项带有前缀 OB2_VEAGENT。

有关如何使用 Data Protector omnirc 选项的详细信息，请参阅《Data Protector 帮助》索引:“omnirc 选项”。

使用命令行界面在 Data Protector 中添加 RMC 服务器详细信息

您可以使用 omnidb 命令添加 RMC 服务器详细信息。执行：

```
omnidb -addhost -servername <clientname> -user <username> -psswd <password>
```

还可以使用以下命令列出并删除所需的服务器。执行：

```
omnidb -listhost -servername <clientname>
```

```
omnidb -removehost -servername <clientname> -user <username>
```

为灾难恢复做准备

要执行灾难恢复，您需要备份以下 VMware 对象:

必须备份哪些内容

VMware 对象	如何备份
ESX/ESXi Server 控制台	ESX Server 系统: 1. 确保在所有 ESX Server 系统上安装 Data Protector 磁盘代理组件。 2. 在 Data Protector GUI 的“备份”上下文中，右键单击“文件系统”，然后选择“添加备份”以创建文件系统类型的备份规范。在备份规范的“源”页中，选择所有 ESX Server 系统的 ESX Server 控制台。 有关备份内容的详细信息，请参阅 http://kb.vmware.com/selfservice/microsites/microsite.do 中的“ESX Server 配置备份和还原过程”主题。 3. 使用新创建的备份规范启动备份。 ESXi Server 系统: 对于 ESXi Server 系统，无法安装 Data Protector 磁盘代理，因此您需要使用 VMware 实用程序备份配置。 VMware 提供了 esxcfg-cfgbackup 工具。有关信息，请参阅 VMware 网站。
vCenter 配置数据库 (仅适用于 VirtualCenter 环境)	vCenter 配置数据库可以是 Oracle 数据库或 Microsoft SQL Server 数据库。要备份该数据库，请使用相应的 Data Protector 集成。例如，如果它是 Oracle 数据库，请执行以下步骤: 1. 确保在 vCenter Server 系统上安装 Data Protector Oracle 集成组件。 2. 在 Data Protector GUI 的“备份”上下文中，右键单击“Oracle Server”，然后选择“添加备份”以创建 Oracle 类型的备份规范。在“应用程序数据库”中，键入 vCenter 配置数据库的名称。 继续创建备份规范。 3. 使用新创建的备份规范启动备份。
VMware 虚拟机	按照本节中所述备份虚拟机。

安装 VMware ZDB 客户机

确保您打算安装组件的所有系统均已启动并正在运行。在应当控制备份和还原会话（备份系统）的系统上安装以下 Data Protector 组件：

- Virtual Environment Integration
- 存储阵列的存储提供程序（NetApp Storage Provider）
- General Media Agent
- Disk Agent
  - Disk Agent 组件使您在备份主机上还原到某目录时能够使用**浏览**按钮。如果没有安装组件，您必须自行键入目标目录。
  - 您打算作为备份主机使用的客户机*不必*安装 VMware Consolidated Backup (VCB) 软件。

以下限制适用：

- 仅支持 VMware vCenter 环境。
- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

配置 VMware ZDB 集成

按如下所示配置集成:

- 将 VMware 客户机导入 Data Protector 单元。
- 配置要备份的虚拟机。

建议

- 建议不要在将使用 Data Protector 备份、还原和恢复的虚拟机的名称中使用百分号。如果虚拟机名称包含 % ，则该名称会在 Data Protector GUI 和 Data Protector 会话消息中错误地显示。

以下先决条件适用:

- 确保已正确安装和配置 VMware vSphere 环境。

  有关受支持版本、平台、设备和其他信息，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。

- 确保已为用于连接到 vCenter Server 的用户帐户授予“禁用方法”和“启用方法”全局特权。
- 确保已为用于连接到 vCenter Server 的用户帐户授予必要的 VMware vSphere 特权。
- 确保已正确安装 Data Protector。

  必须正确安装和配置适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成。确保环境中至少有一个客户机安装了 ZDB 代理 (适用于非存储阵列的存储提供程序组件或“3PAR 存储提供程序”组件) 和“虚拟环境集成”组件 (“备份系统”)。安装后，备份主机无需特殊配置。

  > **重要说明**您打算作为备份系统使用的客户机不必安装 VMware Consolidated Backup (VCB) 软件。

  如果要将虚拟机文件还原到备份主机上的某个目录，还要在备份系统上安装“磁盘代理” 组件。否则，您将无法使用“浏览”按钮指定目标目录 (但是，仍然能够自行键入目录)。

开始之前:

- 配置要与 Data Protector 配合使用的设备和介质。

导入和配置 VMware 客户机

使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成，不必在 VMware 客户机 (vCenter Server 系统、ESX(i) Server 系统) 上安装任何 Data Protector 组件。要使它们成为 Data Protector 客户机，必须将 VMware 客户机正确导入 Data Protector 单元并进行配置。

> **注意**在 *Data Protector Express* 中，按每个单元计算套接字许可证。可以将客户机 (vCenter/ESX 服务器) 同时导入多个单元，并为每个单元中的每个客户机导入计算套接字许可证。

将客户机导入 Data Protector 单元:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“Data Protector 单元”，右键单击“客户机”，然后选择“导入客户机”。
3. 在“导入客户机”页面的“名称”选项中输入客户机名称，从“类型”下拉列表中选择适当的客户机类型 (**VMware ESX(i)**、**VMware vCenter**)，然后单击“下一步”。
4. 如果选择“标准安全”，则需要手动指定 Data Protector 应用于连接到 VMware 客户机的登录凭据:

   端口: 指定 VMware vSphere 将使用的端口。默认情况下，VMware 使用端口 443。对于将用作装载主机的 VMware ESX(i) Server，请指定端口 443。

   用户名和**密码**: 指定一个在根 vCenter 级别上有以下 VMware vSphere 特权的操作系统用户帐户:

   下表列出了 VMware vSphere 中的特权:

数据存储 -> 分配空间
数据存储 -> 浏览数据存储
数据存储 -> 低级别文件操作
数据存储 -> 删除文件
数据存储 -> 重命名数据存储

扩展 -> 注册扩展
扩展 -> 取消注册扩展
扩展 -> 更新扩展
文件夹 -> 删除文件夹
文件夹 -> 重命名文件夹
全局 -> 禁用方法
全局 -> 启用方法
全局 -> 许可证
主机 -> 配置 -> 维护
主机 -> 配置 -> 存储分区配置
主机 -> 库存 -> 添加独立主机
网络 -> 分配网络
资源 -> 向资源池分配虚拟机
资源 -> 删除资源池
资源 -> 重命名资源池
会话 -> 验证会话
vApp -> 删除
vApp -> 重命名
vApp -> 添加虚拟机
虚拟机 -> 快照管理 -> 恢复到快照
虚拟机 -> 配置 *
虚拟机 -> 交互 -> 回答问题
虚拟机 -> 交互 -> 关闭电源
虚拟机 -> 交互 -> 打开电源
虚拟机 -> 库存 -> 新建
虚拟机 -> 库存 -> 注册
虚拟机 -> 库存 -> 删除
虚拟机 -> 库存 -> 取消注册
虚拟机 -> 设置 *
虚拟机 -> 快照管理 -> 创建快照
虚拟机 -> 快照管理 -> 删除快照
vSphere 标记 -> 分配或取消分配 vSphere 标记

- **Web 服务**: 可选，更改 Web 服务入口点 URI。默认值： /sdk

如果选择“集成安全”(仅可用于应用程序客户机和备份主机均为 Windows 系统的 VMware vCenter Server 系统)，则 Data Protector 会使用用以运行备份系统上的 Data Protector Inet 服务的用户帐户连接到 VMware vCenter Server 系统。确保此用户帐户拥有适当的 VMware vSphere 权限可以连接到 VMware vCenter Server 系统且备份主机上的 Data Protector Inet 服务已针对用户模拟进行了配置。

对于“端口”和“Web 服务根”选项，Data Protector 使用当前为标准安全指定的值。集成安全基于安全支持提供程序接口 (SSPI)。

5. 选择“下一步”。仅当使用的许可证类型为 *Data Protector Express* 时，此选项才可用。否则，该选项将灰显。

   如果是 **Data Protector express**，则会列出选定 vCenter 中的 ESX(i) 服务器，以及主机名、主机套接字和主机 UUID 信息。

6. 选择要许可的 ESX(i) 服务器，然后选择“完成”。

   选定服务器将获得许可。

   要添加或回收许可证，请重新导入 vCenter 客户机。在这种情况下，未获得许可的 ESX(i) 服务器与已获得许可的 ESX(i) 服务器一起列出。

   - 要回收，请取消选择 ESX(i) 服务器并选择“完成”以取消许可 ESX(i) 服务器。
   - 要添加，请选择新服务器，然后选择“完成”以许可 ESX(i) 服务器。

更改 VMware 客户机的配置

当您更新用于连接到 VMware 客户机 (vCenter Server、ESX(i) Server) 的凭据时，实际上会更新驻留在 Data Protector Cell Manager 上的 cell_info 文件。因此，仅当您拥有 Data Protector“客户机配置” 用户权限时，才能更改登录凭据。有关 Data Protector 用户权限的详细信息，请参阅《Data Protector 帮助》索引: “用户组”。

要更新凭据，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

您可以在两个不同的位置更新凭据: 在客户机中或备份上下文中。

客户机上下文

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“客户机”，然后选择要更改其登录凭据的客户机。

3. 在“结果区域”中，单击“登录”选项卡。
4. 更新凭据，然后单击“应用”。

备份上下文

假定要更改其登录凭据的 VMware 客户机的备份规范已存在。

1. 在上下文列表中，单击**备份**。
2. 打开要更改其登录凭据的 VMware 客户机的备份规范。
3. 在“源”页面中，右键单击顶部的客户机，然后选择“配置”。
4. 在“配置虚拟环境”对话框中，更新值并单击“确定”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   对于“集成安全”:

   ```
   vepa_util.exe command --config --virtual-environment vmware --host VMwareClient --security-model 1
   ```

   对于“标准安全”:

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   vepa_util.exe command --config --virtual-environment vmware --host VMwareClient --security-model 0 --username Username {--password Password | --encoded-password Password} [--webroot WebServiceRoot] [--port WebServicePort]
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

检查 VMware 客户机的配置

在配置检查期间，Data Protector 尝试使用 Data Protector Cell Manager 上的 cell_info 文件中的登录凭据连接到 VMware 客户机。

要验证连接，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在为 VMware 客户机创建至少一个备份规范后，您可以验证与此客户机的连接。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。单击要检查的 VMware 客户机的备份规范。
3. 在“源”页面中，右键单击 VMware 客户机，然后选择“检查配置”。

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   vepa_util.exe command --check-config --virtual-environment vmware --host VMwareClient
   ```

   消息 *RETVAL*0 表示配置成功。

   有关各选项的说明，请参阅 vepa_util.exe 手册页或《Data Protector 命令行界面参考》。

配置虚拟机

配置虚拟机意味着指定应如何备份虚拟机。

您可以指定以下内容:

- (仅限 Windows 虚拟机) 是否应捕获静止快照，以使虚拟机内运行的应用程序的备份一致。
- 备份期间应使用的传输模式。

对于每个数据中心，您可以指定:

- 应用于数据中心中的所有虚拟机的*常用设置*。
- 覆盖常用设置的*特定于虚拟机的设置*。如果没有特定于虚拟机的设置，则为该特定虚拟机使用常用设置。

所有这些设置都保存在 Cell Manager 上的特定于数据中心的文件 VMwareClient%DatacenterPath 中。该文件用于使用此数据中心的任何备份规范的所有备份会话。

同样，使用“所有数据中心”的任何备份规范的备份会话使用来自文件 VMwareClient%AllDatacenters 的设置。

当您分别为特定数据中心或所有数据中心创建或更新备份规范时，将创建或更新文件 VMwareClient%DatacenterPath 和 VMwareClient%AllDatacenters 。

要配置虚拟机，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在创建或修改备份规范时，您可以配置虚拟机。在备份规范的“源”页面中，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。

在“设置”页面的“配置虚拟机”对话框中，指定以下设置:

虚拟机设置

可用选项	描述/操作
选择是否要指定常用虚拟机设置 (“常用 VM 设置”) 或特定虚拟机的设置。特定于虚拟机的设置会覆盖常用虚拟机设置。	
配置虚拟机	
使用所选 VM 的常用设置	仅当选择虚拟机时可用。 如果希望常用设置应用于所选虚拟机，请选择此选项。 默认：选择
使用默认设置	仅当选择“常用 VM 设置”时可用。 选择此选项可设置常用虚拟机设置的默认值。 默认：选择
启用更改后的块跟踪	为所选虚拟机启用 VMware 更改后的块跟踪功能。 默认: 选定并灰显
允许回退到非 CBT 备份	仅当选择“使用更改后的块跟踪”时启用。 选择此选项可以继续在非 CBT 模式下进行备份，以实现 Data Protector 的成功备份。 有关非 CBT 的详细信息，请参阅主题。 默认：未选择。
快照处理	

使用静止快照	适用于 Windows 虚拟机。 如果选择“使用默认设置”或“对所选 VM 使用常用设置”，则不可用。 选择此选项可使用 Microsoft 卷影复制服务 (VSS) 功能在执行 VEPA 备份之前，通过 VSS 写入程序使所有应用程序静止。这会生成应用程序一致的备份。 默认：未选择。有关详细信息，请参见。
错误级别	仅当选择“使用静止快照”时可用。 指定在静止快照失败时要报告的错误级别。 默认值：警告。
传输模式(R)	
	选择备份虚拟机时要使用的传输模式。 • **NBD**: 当 ESX(i) Server 系统无权访问 SAN、但使用本地存储设备或 NAS 存储虚拟机磁盘时，请使用此模式。这是一种通过本地局域网进行的、使用网络块设备 (NBD) 驱动器协议的未加密传输模式。此传输模式通常比光纤通道慢。 • **NBD (SSL)**: 除通过网络进行的通信使用安全套接字层 (SSL) 加密协议进行加密外，与 NBD 相同。 • **Hotadd**: 如果备份主机 (安装了 Data Protector“虚拟环境集成”组件的客户机) 是虚拟机，则使用此模式。通过此类配置，您可以备份驻留在对托管备份主机的 ESX(i) Server 可见的数据存储上的其他虚拟机。 • **SAN**: 当 ESX(i) Server 系统将其虚拟机磁盘存储在光纤通道 SAN 或 iSCSI SAN 中时，请使用此模式。这是一种通过光纤通道或 iSCSI 进行的未加密传输模式。 此传输模式要求将虚拟机所在的存储卷提供给安装了“虚拟环境集成”组件的客户机 (“备份主机”)。 ◦ **警告：**请勿重新格式化这些存储卷。否则，您将删除所有虚拟机。 如果您不关心所使用的模式，请选择“最快可用”。 默认值：**最快可用**

使用 Data Protector CLI

1. 登录备份主机，打开命令提示符并更改为 vepa_util.exe 命令所在的目录。
2. 执行：

   ```
   vepa_util.exe command --configvm --virtual-environment { vmware | vCD } --host AppHostName --instance DatacenterPath --vm VMpathVM_OPTIONSVM_OPTIONS --transportation-mode {san | nbd | nbdssl | hotadd | fastest} --quiescence { 0 | 1 } --quiescenceErrLvl { 0 | 1 } --uuid UUID_of_VM
   ```

   要将特定于虚拟机的设置更改回常用虚拟机设置，请执行:

   ```
   vepa_util.exe command --configvm --virtual-environment { vmware | vCD } --host AppHostName --instance DatacenterPath --vm VMpath --uuid UUID_of_VM --default
   ```

   消息 *RETVAL*0 表示配置成功。

示例

要在最快可用传输模式下，使用驻留在数据中心 /MyDatacenter 中并在 vCenter Server 系统 vc.company.com 中注册的虚拟机路径 /MyDatacenter/MyVM 和 UUID 42375365-ebe1-e9da-7068-7beb727cab19 配置虚拟机，

执行:

```
vepa_util.exe command --configvm --virtual-environment vmware --host vc.company.com --instance /MyDatacenter --vm /MyDatacenter/MyVM --quiescence 1 --quiescenceErrLvl 0 --transportation-mode fastest --uuid 42375365-ebe1-e9da-7068-7beb727cab19
```

备份 VMware ZDB 集成

本节包含执行虚拟机零宕机时间备份所需的过程。

使用适用于 VMware 的虚拟环境 ZDB 集成，可执行以下零宕机时间备份:

- **NetApp 存储**: ZDB 到磁带
- **3PAR 存储**: ZDB 到磁盘、ZDB 到磁带和 ZDB 到磁盘 + 磁带

您应熟悉 NetApp 和 3PAR 存储概念和过程以及基本 Data Protector ZDB 功能。

以下限制适用：

- 仅 vCenter 服务器支持带有标记和类别 的备份和还原功能，而 ESX(i) 服务器不支持。
- Data Protector 仅支持与虚拟机的标记关联。

  如果标记与虚拟机模板相关联，则这些标记不会在“标记和类别” 视图中列出，因此不考虑进行备份。使用“VM 和模板” 视图选择虚拟机模板。

创建备份规范

使用 Data Protector GUI 创建备份规范。NetApp 存储和 3PAR 存储系统的 ZDB 备份步骤类似。

单击“下一步”。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择“快照或拆分镜像备份”作为备份类型，并选择“存储提供程序插件”作为子类型。有关选项的说明，请按 **F1**。单击**确定**。
4. 指定要备份的应用程序:
   - 在客户机下拉列表中，选择 VMware 客户机。

     > **注意**下拉列表包含已作为 VMware vCenter 或 VMware ESX(i) 导入 Data Protector 单元的所有客户机。这些客户机名称的末尾附加了相应的标签，例如 *(VMware vCenter)* 或 *(VMware ESX(i))*。

     如果未正确配置所选 VMware 客户机，则会显示一条警告。单击“确定”打开“配置虚拟环境”对话框，并提供连接参数。
   - 在“备份主机”下拉列表中，选择要用于控制备份的 VMware vCenter 系统。该列表包含安装了与 Data Protector 相关的 ZDB 集成组件 (“NetApp 存储提供程序”或“3PAR 存储提供程序”) 和“虚拟环境集成”组件的所有客户机。
   - 在“数据中心/组织”中，选择要从中进行备份的数据中心。

     > **注意**如果在“客户机”选项中选择了独立 ESX(i) Server 系统，则只有一个数据中心可用 - **/ha-datacenter**。
     >
     > 如果在**客户机**选项中选择了 vCenter Server 系统，则您可以选择**所有数据中心**以备份不同数据中心中的虚拟机。

   - 在“装载主机”中，选择要用于装载复本的 ESX(i) Server 系统。

     > **注意**如果 ESXi 版本为 5.5 U2 的装载代理主机属于源数据中心，则远程复制故障转移备份将失败。从属于同一 vCenter 的其他数据中心选择 ESXi 装载代理主机。

   - 在“备份方法”中，将显示备份方法:
     - 适用于 VMware vCenter 和 VMware ESX(i) 客户机的 vStorage 映像
     - 适用于 VMware vCenter 的 vStorage 映像
   - 在“所需可用空间[%]”中，指定在备份虚拟机之前，数据存储应具有的可用磁盘空间的百分比。可用空间基于虚拟机磁盘所处的数据存储大小进行计算。

     需对每个虚拟机单独执行检查。

   单击“下一步”。

单击**确定**。

5. 在“添加存储提供程序”下，从“存储提供程序”下拉列表中选择所需存储提供程序，然后单击“添加”。此时将打开特定于存储提供程序的选项对话框。选择复本配置类型，为驻留在群集中的 NetApp 存储系统输入复本描述，输入目标阵列和 Vserver 名称。如果可用，请指定特定于其他存储提供程序的选项:

   - 复本配置类型: “精简配置”或“完全分配”复本配置类型可用于 NetApp 和 3PAR 存储提供程序。
   - 传输模式: **SAN** 和 **NBD** 传输模式可用于 NetApp 存储提供程序。

   单击**确定**。即会将存储提供程序添加到列表中。您可以通过单击“编辑”来更改其选项，或者单击“删除”从列表中将其删除。有关详细信息，请按 **F1**。单击“下一步”。

6. 在复制模式下，默认选择“3PAR 本地复制”。您也可以选择“3PAR 远程复制”。

7. 对于 3PAR 存储系统，请选中“在备份完成之后保留复本”复选框。为“循环的复本数”选择所需值。(可选) 选中“跟踪复本以用于即时恢复”复选框。

8. 选择要备份的对象。在“显示”下拉列表中，通过选择“主机和群集”、“VM 和模板”或“标记和类别”视图来简化您的选择。 默认情况下，会显示主机和群集。

   注意
   - 如果在已选择一个或多个对象进行备份之后切换视图，则会显示警告对话框。对其进行确认会清除已选择的对象，单击“否”不对视图进行任何更改。 对于模板备份，将视图从“标记和类别” 更改为“VM 和模板” 时，将保存选定的标记。
   - 您必须具有 vSphere 读取和附加权限才能使用“标记和类别” 视图。
   - “标记和类别” 视图仅适用于 vCenter Server。
   - 您不能在“标记和类别” 视图下查看模板。

   您可以在不同级别进行选择:

   - 对于 VMware vCenter 和 VMware ESX(i) 客户机:
     - ESX/ESXi Server 系统
     - 池
     - vApp
     - VM 文件夹
     - 单个 VM
     - VM 磁盘
     - VM 模板
     - 标记
     - 类别

   如果选择高于单个 VM 的任何级别 (例如 vApp)，则所选项目中包含的所有 VM 和 VM 磁盘都将包含在备份规范中。如果在保存备份规范后在项目中添加了 VM，则也会备份这些 VM。

   注意如果清除某个对象对应的复选框，则该对象将从备份规范中排除。此后，如果将新虚拟机、池或 vApp 添加到现有逻辑对象，它将自动包含在备份中。您无需创建新的备份规范。已排除对象的复选框在所选视图中标有红色叉号。

   注意在“vStorage 映像”备份规范创建期间，卷影 VM 在备份和还原操作期间无法选择。

   重要说明在特定 VMware 客户机的对象树中，虚拟机可能会显示为以两种不同的方式选择：
   - “蓝色”复选标记表示已选择虚拟机以进行完整备份，包括其配置及其所有虚拟磁盘。

     如果备份了此类虚拟机，即使原始虚拟机不再存在，也可以还原它。
   - “灰色”或“黑色”复选标记表示选择了属于虚拟机的部分或全部虚拟磁盘。备份中省略了虚拟机本身及其配置。

     如果备份了此类虚拟机，则仅当在还原时仍然配置了原始虚拟机时，才能还原其磁盘。

如果您的虚拟机尚未配置，右键单击顶部的客户机系统或下面列出的任何虚拟机，然后选择“配置虚拟机”。

单击“下一步”。

9. 选择用于备份的设备。

   要指定设备选项，请右键单击设备，然后选择“属性”。在“并发”选项卡中指定并行备份流的数量以及要使用的介质池。

   单击“下一步”。

10. 设置备份选项。
11. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后计划备份规范。
12. 单击“启动备份”以启动备份会话。如果您使用的是 3PAR 存储系统，则可以选择“备份类型”、“网络负载”和“快照备份”选项。

> **提示**在将备份规范用于实际备份之前预览备份规范。

VMware 备份选项

选项	描述
Pre-exec、**Post-exec**	指定在 (pre-exec) 备份前或 (post-exec) 备份后在备份主机上运行的命令行。 不要使用双引号。仅键入命令的名称并确保该命令位于备份主机上的默认 Data Protector 管理命令目录中。 *Windows 系统：* Data_Protector_home\bin *Linux 系统*: /opt/omni/bin

为 RMC 备份创建备份规范

请考虑“StoreOnce Recovery Manager Central 集成”部分中列出的所有先决条件和限制。

使用 Data Protector GUI 创建备份规范。

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，右键单击“虚拟环境”，然后选择“添加备份”。
3. 在“创建新备份”对话框中，选择“StoreOnce RMC”作为备份类型:根据需求，选择“快照”、“快照 + 磁带”或“Express Protect”作为子类型。单击**确定**。
   - **快照**: 如果选择此选项，则会创建源卷的复本。
   - **快照 + 磁带**: 如果选择此选项，则会创建源卷的复本，并将数据备份到所选磁带设备。保在后续步骤中指定“装载主机”和所需“设备”。
   - **Express Protect**: 如果选择此选项，您可以将快照从 3PAR StoreServ 备份到 StoreOnce。备份按照在 RMC 中创建的备份策略进行。
4. 指定要备份的应用程序:
   - 在客户机下拉列表中，选择 VMware 客户机。如果未正确配置所选 VMware 客户机，则会显示一条警告。单击“确定”打开“配置虚拟环境”对话框，并提供连接参数。
   - 在“备份主机”下拉列表中，选择要用于控制备份的 VMware vCenter 系统。
   - 在“数据中心/组织”中，选择要从中进行备份的数据中心。
   - 在“装载主机”中，选择要用于装载复本的 ESX(i) Server 系统。对于“快照 + 磁带”备份，此字段是强制性的。
   - 在“备份方法”中，选择要用于备份的方法。

     > **注意**RMC 不支持“vStorage 映像”备份方法。

5. 指定 RMC 配置详细信息:
   - **RMC 服务器**: 选择用于备份的 RMC 服务器。
   - **备份策略** (*仅适用于 Express Protect 备份*): 选择在 RMC 中创建的策略名称。备份策略通常包含备份系统和备份存储。有关详细信息，请参阅《StoreOnce RMC 用户指南》。

- **快照计数**: 指定应在存储阵列中保留的最大快照计数。最多可以创建 1000 个，最少 1 个。默认值是 10。
- **Express Protect 计数** (*仅适用于 Express Protect 备份*): 指定应在 StoreOnce 中为备份规范保留的最大备份数。可以设置的最小值是 2。默认值是 10。

6. 选择要备份的对象。在“显示”下拉列表中，通过选择“主机和群集”、“VM 和模板”或“标记和类别”视图来简化您的选择。 默认情况下，会显示主机和群集。
7. 选择要用于备份的设备。如果已指定装载主机，则默认选择该设备。

   单击“下一步”。

   > 此步骤不适用于“快照”和“Express Protect”备份。

8. 设置备份选项。单击“下一步”。
9. 单击“另存为”以保存备份规范，指定名称和备份规范组。(可选) 您可以单击“保存并计划”进行保存，然后对备份规范进行调度。
10. 单击“启动备份”以启动备份会话。

修改备份规范

要修改备份规范，请在备份上下文的“范围窗格”中单击其名称，然后单击相应的选项卡并应用所做的更改。

在“源”页面中，您可以使用“显示”下拉列表修改备份对象。在下拉列表中，“主机和群集”视图、“VM 和模板”视图和“标记和类别”视图可用。 备份规范创建过程中使用的视图附加了字符串 (Original)。如果切换视图，则会显示警告对话框，对其进行确认会清除已选择的对象。

> **注意**在修改使用以前的 Data Protector 版本之一创建的备份规范时，可以在“已选定”、“全部”、“主机和群集”、“VM 和模板”以及“标记和类别” 视图之间进行切换。**全部**视图仅对旧版备份规范可用，提供旧版浏览机制。选择“主机和群集”、“VM 和模板”或“标记和类别” 并在警告对话框中单击“是”可清除以前选择的备份对象并升级浏览机制。在保存备份规范之后，只有“主机和群集”、“VM 和模板”和“标记和类别” 视图可用。

要显示虚拟环境设置，请在“结果区域”中单击“VE 设置”。并非所有设置都可以修改。

计划备份会话

您可以在特定时间或定期运行无人看管的备份。

预览备份会话

预览备份会话以对其进行测试。可以使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要预览的备份规范，然后选择“预览备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

预览成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   ```
   omnib -veagent_list BackupSpecificationName -test_bar
   ```

预览期间会发生什么?

测试以下内容:

- 备份主机与 Data Protector 之间的通信

- 备份规范的语法
- 如果正确指定设备
- 如果必要的介质位于设备中

启动备份会话

交互式备份按需运行。它们对于执行紧急备份或重新启动失败的备份非常有用。

要以交互方式启动备份，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“备份规范”，然后展开“虚拟环境”。右键单击要使用的备份规范，然后选择“启动备份”。
3. 指定“备份类型”和“网络负载”。单击**确定**。

备份会话成功后将显示消息“会话已成功完成”。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnib 命令所在的目录。
3. 执行：

   omnib -veagent_list BackupSpecificationName [-barmode VirtualEnvironmentMode][ListOptions]

   其中， VirtualEnvironmentMode 是以下备份类型之一:

   full|diff|incr

   默认为 full 。

   有关 ListOptions ，请参阅 omnib 手册页或《Data Protector 命令行界面参考》。

   示例

   要使用备份规范 MyVirtualMachines 启动完整备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode full

   要使用同一备份规范启动差异备份，请执行:

   omnib -veagent_list MyVirtualMachines -barmode diff

备份概念

使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成，可备份以下 VMware 对象:

VMware vSphere:

- 虚拟机
- 虚拟机磁盘
- 虚拟机模板

Data Protector 根据 VMware vSphere 库存路径标识数据中心和虚拟机。独立 ESX Server 系统只有一个数据中心 /ha-datacenter 和两个文件夹： /host 和 /vm 。虚拟机存储在文件夹 /host 中。

示例：

数据中心： /ha-datacenter

虚拟机： /vm/myvm1

在 vCenter 环境中，可以在自行创建的文件夹中组织虚拟机和数据中心。如果随后移动虚拟机，则无需创建新的备份规范，因为 Data Protector 将使用其 UUID 查找虚拟机。

示例：

虚拟机： /vm/myfolder1/myfolder2/.../myvm2

数据中心： /myfolder/mydatacenter

示例：

虚拟机： /ORG22/vDCOrg22/vAppORG22/vm1Org22

组织: /vCD1/Mngmt/ORG22

虚拟机

备份虚拟机时，实际上备份以下类型的虚拟机文件:

- .vmx
- .vmdk

虚拟机磁盘

使用 vStorage 映像备份方法时，Data Protector 支持备份单个虚拟机磁盘。在这种情况下，将备份所有虚拟机文件，但未指定的虚拟机磁盘除外。您可以运行完整备份、增量备份和差异备份。

从 Data Protector 9.05 开始，虚拟机磁盘将并行备份，而不是按先后顺序备份。

为实现虚拟机磁盘并行性，将虚拟机磁盘将视为对象。指定对象操作 (如对象复制和对象验证) 时，不显示磁盘对象。为对象操作选择虚拟机对象时，将考虑磁盘。

> **注意**将新磁盘添加到虚拟机后，请确保为更新的虚拟机运行完整备份会话。

虚拟机模板

使用 vStorage 映像备份方法时，也可以备份虚拟机模板。创建备份规范时，展开 **vm** 文件夹并选择所需的虚拟机模板。

vStorage 映像备份方法

适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成提供的 vStorage 映像备份方法基于 VMware vStorage 技术。对于此方法，使用单个中央“备份主机”备份 Data Protector 单元中的 ESX(i) Server 系统托管的所有虚拟机。此备份主机可以是专用物理主机、虚拟机或 Cell Manager。重要的是它安装了 Data Protector“虚拟环境集成”组件 (**VEAgent**)。

在 ZDB 备份期间，VEAgent 会执行 vStorage 映像备份。VEAgent 首先在备份系统和虚拟化主机 (ESX(i) Server 系统) 之间建立连接。此连接可以通过 vCenter Server 系统 (在 vCenter 环境中) 或直接 (在独立 ESX(i) Server 环境中) 进行。然后，它通过 VMware vSphere Storage API - 数据保护 (以前称为 Data Protection 或 VADP 的 VMware vStorage API) 请求要备份的虚拟机的快照。这样可确保虚拟机处于一致状态。然后，ZDB 代理会创建虚拟机磁盘的复本。该复本将呈现给 ESX(i) 装载主机，介质代理客户机会初始化，且备份的数据将流式传输到磁带。

快照管理

vStorage 映像备份方法依赖能够创建虚拟机快照。虚拟机快照是一种将虚拟机置于一致状态的操作。对虚拟机磁盘进行的所有后续更改都将记录到创建的快照中。

> **注意**所有虚拟机磁盘都不支持快照操作。例如，不支持独立磁盘的快照；因此，无法使用适用于 VMware 的 Data Protector 虚拟环境 ZDB 集成来备份此类虚拟磁盘。有关详细信息，请参阅 VMware 文档。

在 vStorage 映像备份期间，Data Protector 会创建快照，复制虚拟机磁盘并将数据从一致状态复制到 Data Protector 介质。然后，Data Protector 将删除复本和快照。请注意，Data Protector 创建的快照 (“DP 快照”) 通过包含产品名、描述和时间戳的标签 _DP_VEPA_SNAP_ 区别于其他快照。

注意如果虚拟机在启用 CBT 的备份期间具有用户创建的快照，则用户创建的快照将与其他 VM 磁盘块一起备份。如果 Data Protector 在还原时在虚拟机中检测到用户创建的快照，则不会还原该 VM。要还原此类 VM，您需要手动删除所有现有用户创建的快照。

现有虚拟机快照会降低虚拟机的整体性能。因此，Data Protector 会在不再需要 DP 快照时自动删除它们。

重要说明不要将标签 _DP_VEPA_SNAP_ 用于为其他目的创建的快照，否则 Data Protector 将删除这些快照。

完成 ZDB 备份后，将始终删除 ZDB 代理创建的复本。

备份类型

要执行的备份类型在备份规范级别，在“调度程序”页面中或在“启动备份”对话框中 (对于交互式备份) 指定。

使用 vStorage 映像或 vCD vStorage 映像备份方法，可以执行以下备份类型:

备份类型

备份类型	描述
完整	备份完整虚拟机 (磁盘)。
增量	备份自上一次完整备份、增量备份或差异备份以来对虚拟机所做的更改。
差异	备份自上一次完整备份以来对虚拟机所做的更改。

对于增量备份或差异备份会话，还必须指定 Data Protector 应如何识别磁盘块级别的更改。

为了识别磁盘块级别的更改，Data Protector 使用 VMware 更改后的块跟踪功能。

注意备份后剩余的快照数始终为 0。仅支持混合快照处理模式。

混合快照处理模式支持所有可能的备份链形式的完整备份、差异备份和增量备份。

在对备份的虚拟机执行快照操作时，必须注意不要破坏备份链。

重要说明未使用 Data Protector 创建的 VMware 对象的快照不能用于为该对象设置 Data Protector 备份链 (还原链)。

如果执行以下任何操作，备份链将被破坏:

- 删除快照
- 恢复到快照
- 创建快照而不涉及 Data Protector
- 更改快照处理模式
- 添加新的虚拟机磁盘或重命名现有虚拟机磁盘
- 还原虚拟机
- 启用更改后的块跟踪

完成上述任何操作后，必须先运行完整备份才能启动新的备份链。如果您改为运行增量备份或差异备份的会话，则 Data Protector 会切换 VEAgentdisk 对象以使有效备份类型为完整备份，而对于 VEAgent 对象，备份类型仍为增量备份或差异备份。这可能会在还原期间创建具有多个会话的备份链；这会影响性能。因此，建议执行完整备份。

更改后的块跟踪

更改后的块跟踪 (CBT) 是 VMware 更高版本的一个功能，可用于提高备份效率和速度。

对于 CBT，使用更改 ID。更改 ID 是虚拟磁盘在特定时间点所处状态的标识符。每当创建磁盘快照时，更改 ID 都由虚拟磁盘逻辑保存。

使用更改后的块跟踪的主要优点在增量或差异备份上最为明显，因为:

- 不必将虚拟机快照一直留到下次备份之时，因而大幅减少系统开销。
- 通过从内核获取更改信息而不是从快照进行计算，可以更轻松地计算要备份的更改。

在完整备份期间，仅备份磁盘上的活动块，未分配的块将被忽略。这可以提高备份的空间利用率和速度。

启用更改后的块跟踪时，虚拟机的性能会受到轻微影响，但这与您获得的好处相比微不足道。如果在 VMware vSphere 中启用更改后的块跟踪，则 Data Protector 将使用它。可以根据需要使用 Data Protector GUI 启用它。

注意“vStorage 映像”备份方法支持 CBT 功能。

使用更改后的块跟踪时，仍要使用 Data Protector 快照，确保虚拟机处于一致状态。但在备份完成后，将删除这些快照。仅保留更改后的块跟踪日志文件更改 ID。

注意使用更改后的块跟踪时，请记下以下几点:

- 使用 CBT 备份时，请确保符合 VMware 的先决条件。
- 并非所有类型的虚拟磁盘都支持更改后的块跟踪。如果磁盘不受支持，则虚拟机备份将失败。
- 首次启用更改后的块跟踪时，虚拟机的下一个备份将始终为完整备份，以便为跟踪提供参考点。即，启动一个新的备份链。
- 执行还原会话时，CBT 备份链 (完整, 差异, 增量,...) 会被破坏。还原会话完成后，再次运行完整备份以启动新的备份链，否则后续增量备份和差异备份会话将失败。

备份流程

1. Data Protector 触发快照。
2. 创建源卷的复本。
3. 记录当前备份的更改 ID。

   如果这是启用更改后的块跟踪后捕获的第一个快照，则会识别所有活动块并记录更改 ID 0。

   在完整备份的情况下，此更改 ID 会成为新备份链的起始参考点。
4. 此步骤取决于所选备份类型:
   - *完整备份*: 由于识别到更改 ID 0，块已更改。
   - *增量备份*: 由于识别到上一次备份 (完整备份、增量备份或差异备份) 的更改 ID，块已更改。
   - *差异备份* : 由于识别到上一次完整备份的更改 ID，块已更改。
5. 备份识别到的块。
6. 删除复本和快照。

具有更改后的块跟踪的备份链示例

快照	更改 ID	识别到的块	备份的块
启用 CBT 后的第一个	ID 0	所有活动块	—
完整备份	ID *n*	自 ID 0 后已更改	来自 ID 0 的所有活动块 + 自 ID 0 后已更改的块
增量备份	ID *n+m*	自 ID *n* 后已更改	自 ID *n* 后已更改的块
增量备份	ID *n+p*	自 ID *n+m* 后已更改	自 ID *n+m* 后已更改的块
差异备份	ID *n+q*	自 ID *n* 后已更改	自 ID *n* 后已更改的块
完整备份	ID *r*	自 ID 0 后已更改	来自 ID 0 的所有活动块 + 自 ID 0 后已更改的块

非更改块跟踪 (非 CBT) 备份

非更改块跟踪（非 CBT）备份是一种不依赖于要备份的块级更改的功能。

- 使用此功能，将备份虚拟机磁盘的所有块。
- 此功能不使用 VMware CBT 功能来识别要备份的修改后的块。
- 备份的映像大小会增加，因为将备份磁盘的所有块。

更改块跟踪备份失败时，将启用**允许回退至非 CBT 备份**选项。

在以下情况下，可使用非 CBT 备份：

- 当虚拟机的硬件版本低于 7 时。
- 当备份未安装较低版本操作系统（例如 Windows 2003）的虚拟机时。
- 当快照在虚拟机上可用而且 CBT 未启用时。

备份并行性

默认情况下，虚拟机并行备份。在极少数情况下，这可能会导致问题。例如，备份会话可能意外结束。在这种情况下，您可以将备份主机上的 Data Protector OB2_VEAGENT_THREADED_BACKUP omnirc 选项设置为 0 以禁用并行备份。

> **注意**在这两种情况下，都会按顺序备份虚拟机磁盘。

> **注意**默认情况下，使用 VEAgent 集成备份虚拟机时，最多会执行 10 个并发线程。此处，每个线程引用一个用于处理备份集并将其从虚拟机主机流式传输到备份目标的 Data Protector 服务。虽然默认设置为受保护的虚拟机提供增强的备份性能，但由于 10 个 I/O 连接并非由虚拟化层管理，且因此不受虚拟化主机上的负载均衡服务的限制，它将为虚拟基础架构施加中度负载。但是，您可以使用 OB2_VEAGENT_VCENTER_CONNECTION_LIMIT 变量修改此设置，以满足系统设置的要求。

备份考虑事项

- 更改块跟踪 (CBT) 和混合快照处理模式

  支持 CBT 备份方法和混合快照处理模式。

- **并发备份会话**

  使用相同设备的备份会话无法并行运行。

  无法与 ESX(i) Server 系统或虚拟机所在的数据中心并行备份虚拟机。

  备份同一数据存储中的虚拟机的备份会话无法在同一个 Cell Manager 或不同的 Cell Manager 中并行运行。

- **传输模式**

  可以使用各种传输模式进行备份。

  建议使用 CBT 进行增量/差异备份，因为其速度更快且在备份设备上占用的空间更少。

  传输模式可以是 SAN 或 NBD，可以通过 Data Protector GUI 选择 (这决定了阵列访问方式)。也可以在虚拟机选项中配置传输模式。在虚拟机选项中配置的传输模式优先执行，并遵循 SAN:HOTADD:NBDSSL:NBD:FILESYSTEM 的顺序。

  例如，

  - 如果已从 Data Protector GUI 的虚拟机选项中选择 NBD
  - 如果 SAN 不可用
  - 如果 HOTADD 解决方案无法进行零宕机时间备份

  然后备份将通过 NBDSSL。但是，如果您希望备份通过 NBD 传输模式，则必须在虚拟机选项中配置 NBD 传输模式。

  SAN 传输模式下的模板备份不受支持，并将回退到 NBD 传输模式。此外，如果在选择了 SAN 传输模式后无法将复本呈现给备份主机，则 VM 备份将回退到 NBD 传输模式。

- **复本配置类型**

  要管理存储资源，您可以选择精简配置或完全分配的复本配置类型，以确保存储系统上有足够的可用磁盘空间。

- **厚磁盘和精简磁盘**

  Data Protector 无法检测虚拟机磁盘是厚磁盘还是精简磁盘。在这两种情况下，实际备份数据大小依赖 VMware VDDK API。Data Protector 无法控制实际备份数据大小。请注意，并非所有数据存储都支持更改后的块跟踪。

- **LUN 的呈现**

  要从 3PAR 复本对虚拟机进行零宕机时间备份，请确保用于创建源数据存储 (要备份的虚拟机的驻留位置) 的 LUN 未呈现到配置为装载代理主机的系统。

- **备份到 StoreOnce Catalyst 设备**

  从 9.07 开始，到 StoreOnce Catalyst 设备的所有 VEPA 备份都使用“每个存储介质单个对象”模式执行。即使未在 StoreOnce Catalyst 设备上选择此选项，也将强制执行此模式。

  将忽略您在“存储介质大小阈值 (GB)”字段中输入的任何值，以从完成到 StoreOnce Catalyst 设备的备份启用缓存 GRE 或启动和实时迁移。

- **Data Protector 许可证**

  从 3PAR 复本执行虚拟机的零宕机时间备份无需以下许可证:

  - 适用于 UNIX 的 Data Protector 即时恢复扩展 - 1 TB
  - 适用于 Linux 的 Data Protector 即时恢复扩展 - 1 TB
  - 适用于 Windows 的 Data Protector 即时恢复扩展 - 1 TB

还原 VMware ZDB 集成

本节包含还原虚拟机所需的过程。

以下限制适用:

- 不支持将具有虚拟 RDM 磁盘的虚拟机还原到不同的 vCenter。

标记和类别限制

- “标记和类别” 功能仅适用于 VMware VCenter 客户机。
- 不支持将标记附加到启用了 powerOn 选项的 VM。

> 如果标记与 VM 模板相关联，建议使用“VM 和模板” 视图进行备份和还原。

查找要还原的信息

您可以在 Data Protector IDB 中找到有关备份对象的信息，如所使用的备份类型和介质，以及备份期间显示的消息。要检索此信息，请使用 Data Protector GUI 或 CLI。

使用 Data Protector GUI

在“内部数据库”上下文中，展开“对象”或“会话”。

如果展开“对象”，则会根据为其创建备份对象的虚拟机对这些对象进行排序。例如：

- 在 vCenter 环境中，虚拟机 /vm/mach1 的备份对象在 /4/vCenterName%2FvmInstanceUUID 下列出。

  其中，

  vCenterName 是虚拟中心的名称。

  vmInstanceUUID 是 vCenter 上的虚拟机 /vm/mach1 的唯一标识符。

  要在 vCenter 环境中查看会话，请双击 /object1/vCenter%2FvmInstanceUUID 。

如果展开“会话”，则会根据在其中创建备份对象的会话对这些对象进行排序。例如，在会话 2012/07/10–82 中创建的备份对象列在 2012/07/10–82 下方。

要查看有关备份对象的详细信息，请右键单击备份对象，然后选择“属性”。

> **提示**要查看会话期间显示的消息，请单击“消息”选项卡。

使用 Data Protector CLI

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnidb 命令所在的目录。
3. 获取在备份会话中创建的会话 ID 为 *SessionID* 的 VMware 备份对象列表:

   omnidb -session SessionID
4. 获取有关备份对象名称为 *BackupObjectName* 的备份对象的详细信息:

   omnidb -veagent BackupObjectName -session SessionID -catalog

   以下是备份对象名称的一个示例:

   gabriel.company.com::/%2FElDatacentro/0/%2Fvm%2Fharbour

使用 Data Protector GUI 进行还原

使用此过程还原、启动和实时迁移虚拟机。

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“虚拟环境”，展开相关客户机，然后单击从中备份的数据中心。

3. 在“源”页面中，指定以下项:

   1. 从“备份方法”下拉列表中，选择以下任一备份方法:

      - 适用于 VMware vCenter 和 VMware ESX(i) 客户机的 vStorage 映像
      - OpenStack 环境中适用于 VMware vCenter 的 vStorage 映像 + OpenStack

   2. 通过“从”和“到”下拉列表，您可以将显示的虚拟机范围缩小到在指定时间间隔内备份的虚拟机。

   3. 在“VM 过滤器”文本框中，输入 VM 的过滤器文本，然后按 Enter 键，或单击“应用过滤器”。过滤器会隐藏与过滤器模式不匹配的 VM、vApp 和资源池，使您能够轻松找到所需对象。

   选择 VMware 对象后，您可以选择“还原”、“启动”或“实时迁移”它们。从“VM 选项”下拉列表中选择所需选项。请注意，仅当选择一个对象时，“启动”和“实时迁移”选项才可用。

   注意过滤器区分大小写，并应用于 VMware 虚拟机对象、VMware 虚拟应用程序 (vApp) 对象和资源池。如果找到匹配的子节点 (如，另一个 VM、vApp 或资源池)，则会显示它们。如果将“VM 过滤器”文本框保留为空，则会显示所有 VM、vApp 和资源池。但是，如果输入过滤器文本，则仅显示匹配的子节点 (如果有)。如果使用“从”或“至”下拉列表修改过滤器值，则会重新应用过滤。过滤器不适用于已选择的 VM、vApp 或资源池。这意味着您可以使用一个过滤器过滤机器，选择对象，然后再次更改过滤器。在新的过滤器中，先前标记的对象仍然可见。

   下面是过滤器使用的类型:

   - **使用简单子字符串** - 如果输入 VM、vApp 或资源池名称的一部分，则对象树中名称中包含输入字符串的所有 VM、vApp 或资源池仍然可见。所有其他对象都将过滤掉。
   - **使用通配符和问号** - 下面是过滤选项:
     - <filter string>* - 过滤以 <filter string> 开头并以任何字符集结尾的 VM、vApp 或资源池名称。
     - *<filter string>* - 过滤以任何字符集开头和结尾且中间包含 <filter string> 的 VM、vApp 或资源池名称。
     - *<filter string> - 过滤以任何字符集开头，并以 <filter string> 结尾的 VM、vApp 或资源池名称。
     - <filter string>*01 - 过滤以 <filter string> 开头，以 "01" 结尾，且具有任何字符集代替通配符 (*) 的 VM、vApp 或资源池名称。例如， Production_VM01 。
     - <filter string>*0? - 过滤以 <filter string> 开头，以 "0" 结尾，且具有字符、数字或字母代替问号 (?) 的 VM、vApp 或资源池名称。例如， Production_VM01 和 Production_VM0A ，而不是 Production_VM11 。

   选择要还原的对象。

   > **注意**Data Protector 会还原每个选定 VMware 对象的完整还原链，以上一个完整备份会话开头 (即使该完整备份超出指定时间间隔)，并以在指定时间间隔内执行的上一个备份会话结尾。

   启动 (PowerOnOption ON): 从备份的映像、智能缓存、StoreOnce Catalyst 或数据域设备启动虚拟机。

   实时迁移 (PowerOnOption MIGRATE): 从备份的映像、智能缓存、StoreOnce Catalyst 或数据域设备实时迁移虚拟机。

   还原为新虚拟机

   右键单击所选虚拟机，然后单击“还原为/还原至”，以将其还原为 vStorage 映像备份方法的新虚拟机。将打开一个新对话框以指定虚拟机的名称。

   > **注意**“还原为/还原至”选项特定于 vStorage 映像备份方法。

   当您选择“vStorage 映像 + OpenStack”备份方法时，您可以查看已备份的 Nova 实例及其版本。还原期间不会显示卷影 VM 对象。

   还原所选备份版本

   右键单击所选虚拟机，然后单击“还原版本”以选择要还原的备份版本。

   将打开一个新的对话框以选择备份版本。将显示所选 Nova 实例的对象版本。

   注意(特定于“vStorage 映像”备份方法) 当从其他数据中心选择备份版本时，对话框中会显示警告消息“VM 将还原到不同的数据中心”。

4. 在“目标”页中，指定还原目标。请参阅下面的“还原目标” 表中说明的选项。
5. 如果已选择“启动”或“实时迁移”，请单击相应按钮以完成操作。
6. 在“选项”页面中，指定 VMware 还原选项。请参阅下面的“还原选项” 表中说明的选项。

   这里，在还原前将删除 VM，并在还原后在 vCenter 中注册 Nova 实例和卷影 VM。

7. 在“设备”页中，选择要用于还原的设备。
8. 单击**还原**。

9. 在“启动还原会话”对话框中，单击“下一步”。
10. 指定“报告级别”和“网络负载”。

    注意选择“显示统计信息”可查看会话输出中的还原配置文件消息。
11. 单击**完成**启动还原。

    会话输出的末尾会显示还原会话的统计信息以及“会话已成功完成”消息。

RMC 集成还原

- 对于 RMC 备份，如果备份类型为“快照 + 磁带”，则会优先从快照执行还原操作。如果快照缺失，则从磁带设备执行还原。
- 如果备份类型为 **Express Protect**，则首先还原到 3PAR LUN，然后还原到指定位置。

还原目标 (VMware vCenter Server 和 VMware ESX(i) Server 客户机)

GUI/CLI 选项	描述
备份主机/ -barhost	指定安装了适用于 VMware 的虚拟环境 ZDB 集成的客户机以控制还原会话。默认情况下，选择与用于备份的客户机相同的客户机。
还原客户机/ -apphost	指定所选虚拟机对象应注册并还原到的客户机。默认情况下，会选择从中备份虚拟机的客户机。 要更改客户机配置，请单击“连接”按钮。
还原到数据中心/ –instance –newinstance	选择此选项可将虚拟机还原到数据中心。默认情况下，将虚拟机还原到原始数据中心。 可以从 3PAR 阵列还原到数据中心。
主机/群集/ -host/cluster	选择应将虚拟机还原到的 ESX(i) Server 系统或群集。默认情况下，将虚拟机还原到原始 ESX(i) Server 系统或群集。
特定主机/ -specificHost	选择应将虚拟机还原到的群集中的特定 ESX(i) Server 系统。默认情况下，将虚拟机还原到原始 ESX(i) Server 系统。
资源池 / -resourcePool	选择应将虚拟机还原到的 ESX(i) Server 系统或群集上的资源池。默认情况下，将虚拟机还原到原始资源池。
数据存储/ –store	指定应将虚拟机还原到的数据存储。您可以从可从所选还原目标主机访问的所有数据存储中进行选择。如果将此选项保留为空，则会将虚拟机还原到原始数据存储。
还原到目录/ –directory	选择此选项可将虚拟机文件还原到备份主机上的目标中 (数据中心外部)。可以使用“浏览”按钮查找目标目录。 此类恢复完成之后，虚拟机无法正常运行。需要使用 VMware Converter 将已还原的虚拟机映像手动移至 ESX Server 或 ESXi Server 系统。

还原选项 (VMware vCenter Server 和 VMware ESX(i) Server 客户机)

GUI/CLI 选项	描述

在需要时注册虚拟机 / -register		选择“还原到数据中心”时可用。 选择此选项可注册已还原的虚拟机。 如果未选择此选项，则需要手动恢复已还原的虚拟机，如 [#s_Recovering_virtual_machines_manually_201101281053 手动恢复虚拟机] 中所述。 默认：选择。 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择“在需要时注册虚拟机”选项。
将快照合并为单个文件/ -consolidate		选择此选项可在还原虚拟机之后，将所有快照 (包括非 Data Protector 映像) 提交到虚拟机群。 选择“还原到数据中心”时可用。
在还原后打开虚拟机/ -poweron		选择此选项可在还原之后启动虚拟机。 选择“还原到数据中心”时可用。
现有虚拟机处理 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择此选项。将使用“还原前删除”选项。	指定 Data Protector 在还原现有虚拟机时的行为。	
	还原前删除/ -deletebefore	选择此选项可在还原之前删除现有虚拟机，然后从新虚拟机将其还原。即使现有虚拟机驻留在目标数据中心之外的数据中心，也依然会被删除。 这是提高空间利用率的选项，但是并不安全，因为如果还原失败，旧虚拟机便无法使用，因此请谨慎选择。
	跳过还原/ -skip	选择此选项可跳过对现有虚拟机的还原。这样可以还原缺少的虚拟机而不会影响现有的虚拟机。
	原后删除/ eleteafter	选择此选项可在还原现有虚拟机后将其删除。即使现有虚拟机驻留在目标数据中心之外的数据中心，也依然会被删除。如果恢复失败，现有虚拟机不会被删除。 默认：选择。 如果虚拟机处于挂起状态，则无法使用此选项。如果虚拟机处于挂起状态，请执行以下任一操作: • 还原到不同位置。 • 选择“还原前删除”选项。 • 打开或关闭虚拟机。
	保留以用于取证/ _ keep_for_forensics	选择此选项可使用时间戳来标记现有虚拟机。保留争议源的虚拟机应该在恢复后关机并保留在原始位置。这不会影响原始虚拟机的后续备份。 此选项对于 Microsoft Hyper-V 客户机不可用。

文件冲突处理 **注意** 使用“vStorage 映像 + OpenStack”备份方法时，无法选择此选项。将使用“覆盖”选项。	指定 Data Protector 在还原现有文件时的行为。	
	覆盖/ verwrite	选择此选项可使用备份中的文件覆盖现有文件。 默认：选择。
	持最新/ atest	如果文件比备份中的文件更新，则选择此选项可原封不动保留现有文件。否则，用备份中的相应文件覆盖现有文件。
	跳过/ -skip	选择此选项可保留现有文件 (文件不从备份中还原)。
类别和标记	仅在目标页面中选择 VCenter 客户机作为还原客户机时，此部分才可供选择。	
	类别/标记处理	指定在客户机还原期间 Data Protector 与标记有关的行为。 从下拉菜单中选择以下任一选项以选择如何使用标记: • 跳过附加标记 • 从备份时开始附加标记 • 附加自定义标记
	类别 *-categoryName*	仅当在“类别/标记处理” 下拉菜单中选择“附加客户标记” 时，才启用此选项。选择将所需标记分组的类别。
	标记 *- tagName/- tagId*	仅当选择类别时才启用此选项。选择要附加到还原的客户机的标记。

使用 Data Protector CLI 进行还原

1. 登录安装了 Data Protector“用户界面” 组件的任何客户机。
2. 打开命令提示符并更改为 omnir 命令所在的目录。
3. 执行：

   VMware vCenter Server 或 VMware ESX(i) Server 客户机

   ```
   omnir -veagent -virtual–environment vmware -barhost BackupHost -apphost OriginalVMwareClient
   ```

   ```
   –instance OriginalDatacenter –method vStorageImage| vStorageImageOpenStack [-session BackupID] VirtualMachine [VirtualMachine...] [VMwareClient | Directory] VirtualMachine -vm VMPath -instanceUUID vmInstanceUUID [-new_name NewVirtualMachineName][-disk DiskName [-disk Disk...]] VMwareClient [–newinstance TargetDatacenter] [-store TargetDatastore] [-network_name TargetNetwork] [–destination TargetVMwareClient] [-consolidate] [–register][–poweron] [–deletebefore | -deleteafter | -skip | -keep_for_forensics] Directory -directory RestoreDirectory [–overwrite | -skip | -latest]
   ```

   ```
   还原选项
   ```

   ```
   [-PowerOnOption { ON | MIGRATE }] [-deletebefore | -skip | -keep_for_forensics] Common options [ -consolidate ] [ -register ] [ -poweron ] [-skip TagAttach { [-categoryName CategoryName] [-tagName TagName] | [-tagId TagId ]}]
   ```

   有关所有选项的说明，请参阅 omnir 手册页或《Data Protector 命令行界面参考》。

   注意在还原从 Data Protector 8.1 及更低版本备份的虚拟机时，不应指定用于还原的 instanceUUID 参数。

   重要说明备份 ID 是一个时间点。在备份会话中创建的所有对象 (备份数据) 都具有相同的备份 ID，该备份 ID 与备份会话的会话 ID 相同。

   镜像对象和在对象复制会话中创建的对象与在原始备份会话中创建的对象具有相同的备份 ID。假设在原始备份会话中创建的介质集不再存在，但在对象复制会话中创建的介质集仍然存在。要还原对象，您必须指定原始*备份*会话的会话 ID (即备份 ID)，而不是*对象复制*会话的会话 ID。

   如果存在同一对象的多个副本，则 omnir 语法不允许您指定要从哪个对象副本还原。只有使用 Data Protector GUI 设置介质分配优先级列表才能实现此操作。

示例 (将虚拟机还原到数据中心)

假设您要还原虚拟机 /vm/machineA 和虚拟机 /vm/machineB 的单个磁盘（scsi0:0 和 scsi0:1）。在备份时，虚拟机在属于由 vCenter Server 系统 vcenter.company.com 管理的数据中心 /MyDatacenter 的 ESX Server 系统上运行。这些虚拟机采用 vStorage Image 备份方法进行备份。

要使用备份会话 2011/01/11–1 将它们还原到原始位置，并确保在会话完成时将新还原的虚拟机置于联机状态，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com –instance /MyDatacenter -method vStorageImage –session 2011/1/11-1 –vm /vm/machineA –vm /vm/machineB -disk scsi0:0 –disk scsi0:1 –poweron
```

要使用 instanceUUID 503eeaac-6fae-7898-73e1-93b722a0517c 还原虚拟机 /vm/machineA ，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com –instance /MyDatacenter -method vStorageImage –session 2011/1/11-1 –vm /vm/machineA -instanceUUID 503eeaac-6fae-7898-73e1-93b722a0517c -disk scsi0:0 –disk scsi0:1 –poweron
```

示例 (将虚拟机还原到目录)

假设使用 vStorage Image 备份方法，在会话 2011/02/12-5 中从由 vCenter Server 系统 vcenter.company.com 管理的数据中心 /MyDatacenter 备份了虚拟机 /MyVirtualMachines/machineA 和 /MyVirtualMachines/machineB 。要将数据中心以外的虚拟机还原到备份主机 backuphost.company.com 上的目录 C:\tmp ，请执行:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method vStorageImage -session 2011/2/12-5 -vm /MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB -directory c:\tmp
```

示例 (使用名称中的 instanceUUID 还原对象名称)

要支持使用名称中的 instanceUUID 还原对象名称，请执行:

```
omnir.exe -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance instanceName -method vStorageImage -session sessionID -vm vmPath –instanceUUID vminstanceUUID -register -poweron -deletebefore
```

示例 (将 Nova 实例还原到其原始位置)

要使用名称中的 instanceUUID 还原对象名称，请执行:

```
omnir -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance /Datacenter -method vStorageImageOpenStack -session sessionID -vm vmPath -instanceUUID novainstanceUUID -register -deletebefore
```

示例 （ 将虚拟机还原到原始位置，并将备份标记附加到还原的虚拟机**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -register -poweron
```

示例 （还原到原始位置，并跳过将标记附加到还原的虚拟机的操作**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -skipTagAttach register -poweron
```

示例 **(**还原到其他位置并将自定义标记附加到虚拟机**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -categoryName DP -tagName Gold -register –poweron
```

示例 （还原到其他位置并使用 **tagId** 附加自定义标记**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST -register –poweron
```

示例 （ 通过指定多个 **tagId** 将多个标记附加到虚拟机**):**

```
omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST2,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST3,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST4 -register –poweron
```

手动恢复虚拟机

有两种不同的情况需要在已使用 Data Protector 还原虚拟机后手动恢复它们:

- 如果已将虚拟机还原到备份主机上的目录 (“还原到目录”)。
- 如果已将虚拟机还原到数据中心 (“还原到数据中心”)，而未选择还原选项“在需要时注册虚拟机”。

还原到目录后恢复虚拟机

还原到目录后恢复虚拟机的步骤取决于备份虚拟机配置文件的格式。

使用 VMX 格式的 VM 配置文件进行恢复

假设使用以下备份会话将虚拟机 helios 还原到备份主机上的目录 C:\tmp\helios :

- 备份方法: **vStorage 映像**
- 备份类型: 增量
- CBT: 启用并使用

要使用 VMware Converter 将虚拟机文件手动移动到由 vCenter Server 系统 bmwvc2.company.com 管理的 ESX(i) Server 系统 dioxide.company.com :

1. 显示目录 C:\tmp\helios 的内容:

   ```
   helios.vmdk helios.vmx helios.vmdk scsi0–0.cbt scsi0–0.meta helios-flat.vmdk helios.vmx-1 helios.vmdk-1 scsi0–0.cbt-1 scsi0–0.meta-1 helios.vmx-2 helios.vmdk-2 scsi0–0.cbt-2 scsi0–0.meta-2
   ```

   请注意，将还原在上一个完整备份、差异备份和所选增量备份会话中备份的所有文件。

2. 共享文件夹 C:\tmp\helios ，以便可以从安装了 VMware Converter 的系统访问它。
3. 登录安装了 VMware Converter 的系统，然后打开 VMware Converter 用户界面。
4. 单击“转换机器”以打开转换向导。
5. 在“源系统”页面中，为源类型选择“VMware Workstation 或其他 VMware 虚拟机”，浏览至 C:\tmp\helios 目录，然后选择 helios.vmx 文件。

   单击“下一步”。

   > **注意**在我们的示例中，备份主机上安装了 VMware Converter。

6. 在“目标系统”页面中，为目标类型选择“VMware Infrastructure 虚拟机”，并提供 vCenter Server 系统的登录凭据。

   单击“下一步”。

7. 在“目标虚拟机”页面中，指定应用于恢复虚拟机的名称。

   单击“下一步”。

8. 在“目标位置”页面中，选择目标 ESX(i) Server 系统和数据存储。
9. 在“选项”页面中，编辑选项并单击“下一步”。
10. 在“摘要”页面中，查看您的选择并单击“完成”。
11. 打开数据存储浏览器并将增量备份和差异备份会话中创建的文件上载到虚拟机目录:

    ```
    helios.vmx-1 helios.vmdk-1 scsi0–0.cbt-1 scsi0–0.meta-1 helios.vmx-2 helios.vmdk-2 scsi0–0.cbt-2 scsi0–0.meta-2
    ```

12. 打开虚拟机。

使用 XML 格式的 VM 配置文件进行恢复

请遵循以下步骤:

1. 打开 vSphere 客户机并登录 ESX(i) Server 或 vCenter Server 系统。

   如果虚拟机仍处于已配置状态，则请删除其所有硬盘:

   a. 在库存对象树中，右键单击虚拟机并选择“编辑设置”。

b. 在“虚拟机属性”窗口的“硬件”选项卡中，选择每个硬盘，并单击“删除”。

c. 单击“确定”，确定删除。

如果虚拟机已不存在，则请配置不包含硬盘的新虚拟机，并使用原始虚拟机的名称。

在任何情况下，请牢记关联数据存储名称。

2. 上载在备份会话过程中创建的虚拟机文件:

a. 在库存对象树中选择托管虚拟机的 ESX(i) Server 系统。

b. 单击“配置”选项卡，并选择“硬件”下的“存储”。

c. 右键单击数据存储名称，并选择“浏览数据存储”。

d. 在“数据存储浏览器”窗口的文件夹树中，选择虚拟机文件夹，单击窗口工具栏上对应的图标。根据需要选择“上载文件”或“上载文件夹”。

e. 选择所有适用文件并完成上载。

3. 重用备份副本时将硬盘添加到虚拟机:

a. 在库存对象树中，右键单击虚拟机并选择“编辑设置”。

b. 在“虚拟机属性”窗口中单击“添加”。

c. 在“添加硬件”窗口中选择“硬盘”并单击“下一步”。

d. 选择“使用现有虚拟磁盘”并单击“下一步”。

e. 单击**浏览**。

f. 在“浏览数据存储”窗口中，浏览到合适的数据存储，并打开虚拟机文件夹。选择虚拟磁盘文件并单击“确定”。

g. 遵循“添加硬件”向导以完成步骤。

h. 为每个存在备份副本的其他硬盘重复从 b 到 g 的子步骤。

4. 打开虚拟机。

还原到数据中心后恢复虚拟机

如果已将虚拟机还原到数据中心，而未选择选项“在需要时注册虚拟机”:

1. 打开数据存储浏览器并浏览到已还原的虚拟机目录。
2. 右键单击虚拟机 *.vmx 文件，然后选择“添加到库存”。
3. 按照向导操作，然后单击“完成”。

使用其他设备进行还原

您可以使用与用于备份的设备不同的设备进行还原。有关详细信息，请参阅《Data Protector 帮助》索引: “还原, 选择设备”。

还原失败后清理数据存储

有时，当虚拟机还原失败时，Data Protector 会在虚拟机数据存储上创建额外的文件。如果未删除这些文件，则可能会在后续会话中创建损坏的虚拟机备份，因此从此类备份还原也会失败。

假设虚拟机 MyVirtualMachine 无法还原。要在还原后清理数据存储，请执行以下操作:

1. 打开 VMware vSphere 客户机。
2. 右键单击虚拟机，然后选择“从磁盘删除”。
3. 打开“数据存储浏览器”。

   目录 MyVirtualMachine 应该不再存在。

   检查是否存在任何额外目录:

   MyVirtualMachine_1

   MyVirtualMachine_2

   等等。

   右键单击每个此类目录，然后选择“从磁盘删除”。

灾难恢复

灾难恢复极其复杂，涉及到来自不同供应商的不同产品。请查看来宾操作系统和 VMware 中关于如何为其做好准备的说明。

下面是发生灾难后恢复虚拟机所需的主要步骤:

1. 重新安装 VMware 环境。配置应与备份期间的配置相同。
2. 在新配置的环境中安装 Data Protector。
3. 将运行虚拟机的 ESX Server 系统的服务控制台从 Data Protector 文件系统备份还原到新配置的 ESX Server 系统。

   有关要还原内容的详细信息，请参阅 http://kb.vmware.com/selfservice/microsites/microsite.do 上的“ESX Server 配置备份和还原过程”主题。

   有关如何从文件系统备份还原的详细信息，请参阅《Data Protector 帮助》。
4. 还原原始 vCenter 数据库 (如果需要)。有关详细信息，请参阅用于备份数据库的 Data Protector 集成。
5. 如本节所述，从 Data Protector 虚拟环境备份还原虚拟机。

即时恢复

先决条件

- ESX Server
- 3PAR 阵列
- vCenter
- 虚拟机上的应用程序主机
- 物理计算机上的备份主机
-

> **注意**包括 ESX Server 在内的两台主机都应该有权访问 3PAR 阵列。

3PAR ZDB 即时恢复

Data Protector 提供了适用于 VMware 虚拟机 (VM) 内的代理的 3PAR ZDB 即时恢复。仅物理原始设备映射 (RDM) 支持此功能。

要在 Linux 和 Windows 上执行即时恢复，请执行以下操作:

1. 使用 sqlplus 关闭 Oracle 数据库实例。如果是 RAC，请关闭所有实例。

   例如：

   ```
   /sqlplus /nolog
   connect sys/oracle@APPN as sysdba
   sql> shutdown immediate
   sql> exit
   ```
2. 在应用程序主机上启用 omnirc 选项:

   ```
   ZDB_IR_MANUAL_AS_PREPARATION=1
   ```
3. **对于 Linux**：卸除卷:

   ```
   # umount /dev/3PAR_ESX2/lvol0
   ```

   对于 Windows：使磁盘脱机。
4. 准备应用程序主机以删除卷 (导出、停用和备份卷组)。
5. 从 vCenter Server 上的应用程序主机中删除硬盘。
6. 重新扫描 VM 上的卷，并确认应用程序主机上不再呈现该磁盘。
7. 执行即时恢复。

> **注意**如果您使用的是 Oracle 集成，请确保取消选中“恢复”复选框。

8. 从 vCenter Server 将硬盘添加回应用程序主机。
9. 重新扫描应用程序主机是否存在新卷。
10. 添加导出的卷组。
11. **对于 Linux**：装载卷。

    对于 Windows：使磁盘联机。
12. 遵循即时恢复后的 Oracle 数据库恢复一节中所述的步骤。

监视会话

可以在 Data Protector GUI 中监视当前正在运行的会话。运行备份或还原会话时，监视器窗口会显示会话的进度。关闭 GUI 不会影响会话。

还可以使用“监视”上下文从安装了用户界面组件的任何 Data Protector 客户机中监视会话。

要监视会话，请参阅《Data Protector 帮助》索引: “查看当前正在运行的会话”。

管理

包括以下主题:

设置适用于云工作负载的 Data Protector

Micro Focus 引入了适用于云工作负载的 Data Protector 以提供对以下范围的备份和还原支持:

- 云数据存储库，例如 Microsoft 365 (Exchange、SharePoint、Teams、OneDrive)
- 虚拟化环境，例如 Citrix XenServer、KVM、Nutanix
- 其他数据平台，例如 OpenShift、OpenStack

有关受支持平台的列表，请参阅适用于云工作负载的 Data Protector 文档中的“支持矩阵”。

查看以下主题，了解有关部署和使用适用于云工作负载的 Data Protector 的信息:

安装适用于云工作负载的 Data Protector

有关安装和配置适用于云工作负载的 Data Protector(DP4CW) 的信息，请参阅适用于云工作负载的 Data Protector 文档中的“部署”。

有关 DP4CW 许可的信息，请联系您的 Micro Focus 支持代表。

将适用于云工作负载的 Data Protector 导入 Data Protector

要将适用于云工作负载的 Data Protector 导入 Data Protector，您必须在 DP4CW 服务器上使用管理员用户凭据运行以下命令:

```
omnicc -import_dp4cw HostName -port Port -user UserName -passwd Password
```

有关 omnicc CLI 的详细信息，请参阅 omnicc。

创建 Micro Focus 企业备份提供程序目标

如果要使用逻辑设备 (例如重复数据删除、StoreOnce、数据域提升或 Data Protector 中配置的文件库) 备份或还原数据，则必须为此类设备创建 Micro Focus 企业备份提供程序目标:

先决条件:

1. 确保要用作备份目标的逻辑设备的可用性。有关 Data Protector 设备的详细信息，请参阅设备。
2. 在选定适用于云工作负载的 Data Protector 节点上安装 Data Protector 磁盘代理和单元控制台组件。
3. 在 Data Protector Cell Manager 上，运行以下命令将适用于云工作负载的 Data Protector 节点作为客户机导入:
   omnicc -import_host HostName [-virtual] [-accept_host]
4. 在 Data Protector Cell Manager 上，运行以下命令以添加以下客户机用户:
   - omniusers -add -type U -usergroup admin -name "root" -group "root" -client "*<ClientShortHostname>*" -pass *<password>*
   - omniusers -add -type U -usergroup admin -name "vprotect" -group "vprotect" -client "*<ClientShortHostname>*" -pass *<password>*

要创建 Micro Focus 企业备份提供程序目标，请执行以下操作:

1. 登录适用于云工作负载的 Data Protector Web 界面。
2. 转至“备份目标”>“企业”。
3. 单击“创建备份目标” 并选择“Micro Focus Data Protector”。
4. 指定备份目标的名称和要用作备份目标的设备名称。
   要列出可用设备，请使用 omnidownload -list_devices [-detail] 命令。请参阅 omnidownload。
5. 单击 保存。成功创建后，“备份目标”页面会列出新创建的备份目标。

有关详细信息，请参阅 适用于云工作负载的 Data Protector 文档中的“企业备份提供程序”。

保护工作负载

保护虚拟环境	有关保护虚拟环境的信息，请参阅适用于云工作负载的 Data Protector 文档中的“保护虚拟环境”。
保护 Microsoft 365	有关保护 Microsoft 365 工作负载的信息，请参阅适用于云工作负载的 Data Protector 文档中的“保护 Microsoft 365”。
保护应用程序	有关保护应用程序的信息，请参阅适用于云工作负载的 Data Protector 文档中的“保护应用程序”。
保护存储提供程序	有关保护存储提供程序的信息，请参阅适用于云工作负载的 Data Protector 文档中的“保护存储提供程序”。

相关主题

- 有关 omnicc CLI 的信息，请参阅 omnicc。

内部数据库

内部数据库 (IDB) 是位于 Cell Manager 上的嵌入式数据库，存储的信息包括备份数据，数据所处备份介质，备份、还原、对象复制、对象合并、对象验证和介质管理会话的结果，以及配置的备份设备和库。

IDB 中存储的信息有以下用途：

- 快速、方便的还原：可以使用 IDB 中存储的信息迅速找到还原所需的备份介质，从而大大加快了还原速度。它还可方便查找要还原的文件和目录。
- 备份管理：可以使用 IDB 中存储的信息验证备份方式。也可以使用 Data Protector 报告功能配置各种报告。
- 介质管理：可以使用 IDB 中存储的信息在备份、对象复制和对象合并会话期间分配介质、跟踪介质属性、将介质分组到不同的介质池，以及跟踪磁带库中的介质位置。
- 加密/解密管理：Data Protector 可以使用 IDB 中存储的信息为加密备份或对象复制会话分配加密密钥，并提供还原加密备份对象所需的解密密钥。

配置 IDB

内部数据库配置有助于管理以下各项：

- IDB 和可用磁盘空间的大小
- IDB 目录的位置
- IDB 自身的备份，在 IDB 损坏或发生灾难时需要此备份
- IDB 报告和通知的配置

需要提前准备，以便能够及时在任何时间点恢复 IDB。IDB 还原将还原 IDB 中存储的信息，并且必须进行此还原才能在 Cell Manager 受到灾难打击时还原备份的数据。

IDB 恢复的准备由以下各项组成：

- 检查稳定性注意事项
- 重新定位 IDB 目录
- 配置 IDB 备份
- 定期备份 IDB

配置 IDB 后，维护的工作量即降到最低，主要是对通知和报告采取的行动。

为 IDB 分配磁盘空间

内部数据库最终会在 Cell Manager 占用相当大量的磁盘空间。需要提前规划，并考虑分配 IDB 在未来需要的磁盘空间。

先决条件

- 了解影响 IDB 增大的关键因素，如文件数、文件动态、环境增大等等。
- 根据环境要求和可用磁盘空间设置日志记录级别和编目保护策略。
- 估计未来的 IDB 大小 (未来 IDB 所需的磁盘空间)。

需要多少磁盘空间?
根据定义和操作备份中使用的许多配置方面和策略，容纳 IDB 的磁盘空间将显著不同。

以下环境简化场景中，3 个月后 IDB 大约需要 900 MB 磁盘空间，并且以后很少会增大：

- 要备份 100 个系统（每个系统 10,000 个文件；没有邮件服务器）
- 数据卷合计 350 GB
- 文件系统备份的典型动态为每月有 3% 的新文件
- 每周进行一次完整备份和四次增量备份
- 日志记录级别设置为全部记录（可方便地浏览文件名，然后再恢复）。这是最繁重的日志记录选项。
- 完整备份的编目保护设置为三个月，增量备份为两周。

> **注意**IDB 中如果采用大型配置或较长的编目保护期，则 IDB 需要 20 GB 以上的容量。

提前规划哪些内容？

通常 IDB 在开始阶段增大速度很快（直到到达目录保留期为止）。在这之后，IDB 的增大主要由每月新文件占很大比例的系统的动态以及环境（要备份的新系统）的增大决定。

了解不同的 IDB 增大函数很重要：

- IDB 部分（包含文件名和文件元数据）的大小与备份数、单元中的已备份文件数以及编目保护的持续时间成正比。
- 预测归档日志文件占用的存储空间并非易事。影响大小的重要因素是 IDB 备份之间所备份的新文件名数和整体备份活动（如果预定备份是主要操作，则为周）。

IDB 目录的位置

内部数据库位于 Cell Manager 上。您可能希望重新定位某些 IDB 目录，并遵照建议以优化稳定性。

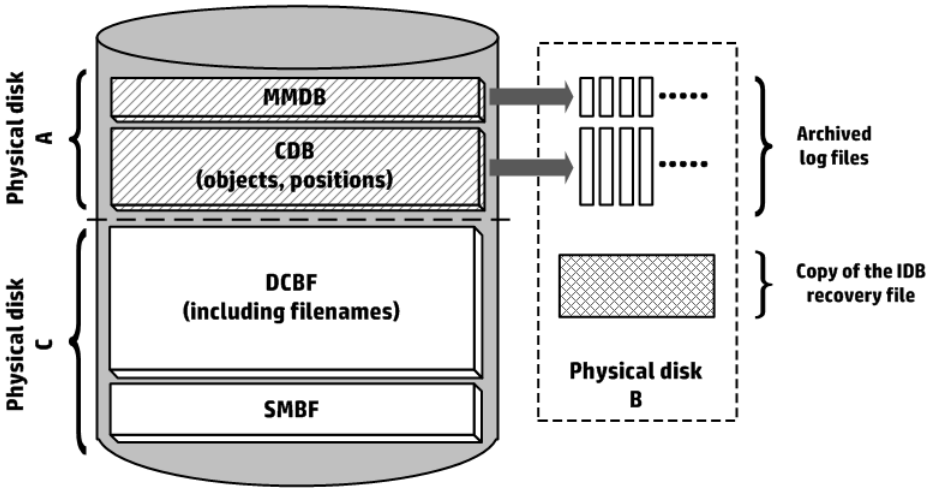
限制

- IDB 文件只能位于本地连接磁盘（未使用 NFS 装载或映射为网络共享文件夹）上的卷中。
- 如果在群集中安装 IDB，则必须将其安装在群集组 (Microsoft 服务器群集) 或群集包 (Serviceguard) 中的卷上。
- 如果 IDB 安装在群集中，则必须将其安装在群集组 (Microsoft 服务器群集)、群集包 (Serviceguard) 或群集服务组 (Symantec Veritas Cluster Server) 中的卷上。

建议 IDB 目录所在的位置

IDB 部分	Windows 系统中的位置	UNIX 系统中的位置	能否重新定位

表空间 （CDB、MMDB）	Data_Protector_program_data\server\db80\idb Data_Protector_program_data\server\db80\jce Data_Protector_program_data\server\db80\kcdb Data_Protector_program_data\server\db80\pg	/var/opt/omni/server/db80/idb /var/opt/omni/server/db80/jce /var/opt/omni/server/db80/kcdb /var/opt/omni/server/db80/pg	目录路径固定，但可以装载不同的卷。
二进制文件 （DCBF、SMBF）	Data_Protector_program_data\server\db80\dcbf Data_Protector_program_data\server\db80\msg Data_Protector_program_data\server\db80\meta	/var/opt/omni/server/db80/dcbf /var/opt/omni/server/db80/msg /var/opt/omni/server/db80/meta	可以修改目录路径。此外，可以装载单独的卷。
归档日志文件	Data_Protector_program_data\server\db80\pg\pg_xlog_archive	/var/opt/omni/server/db80/pg/pg_xlog_archive	目录路径固定，但可以装载不同的卷。
IDB 恢复文件	Data_Protector_program_data\server\db80\logfiles\rlog	/var/opt/omni/server/db80/logfiles/rlog	可以在所需位置放置文件的副本。



稳定性注意事项

- IDB 的核心部分、CDB (对象、位置) 和 MMDB 对于 Data Protector 的运行至关重要。
- 无需 IDB 的 DCBF 和 SMBF 部分即可执行 Data Protector 的基本操作（如备份和还原）。但是，如果没有这些部分，则还原就不太方便（不能浏览文件），并且会丢失会话消息。
- 如果 IDB 恢复文件和归档日志文件丢失，则不会影响正常操作，但 IDB 还原会困难得多，并且无法重放自上次 IDB 备份以来生成的 IDB 数据。而是需要重新导入使用过的介质。

创建新 DC 目录

可以创建新的 DC 目录来为内部数据库的 DCBF 部分提供更多空间，并根据需要对其进行放置。建议各个 DC 目录都位于不同的卷上，最好位于不同的物理磁盘上。

要创建目录，请执行以下操作:

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开“使用情况”。
3. 右键单击**详细编目二进制文件**，然后单击**添加详细编目目录**。
4. 在结果区域中，指定“分配序列”、“路径”、“最大大小”、“最大文件数”和“空间不足”选项。请注意，如果指定的目录路径不是物理路径，则会将其解析并添加为完整的物理目录路径。
5. 单击**完成**退出向导。

存档日志文件的使用情况

在以下位置中创建由内部数据库的 MMDB 和 CDB 部分使用的存档日志文件:

在 Windows 系统上

- Data_Protector_program_data\server\db80\pg\pg_wal Data_Protector_program_data\server\db80\pg\pg_wal_archive

在 UNIX 系统上

- /var/opt/omni/server/db80/pg/pg_wal
- /var/opt/omni/server/db80/pg/pg_wal_archive

从最新的 IDB 备份开始保留归档日志文件，直到下一次备份为止。如果未在相应的 IDB 备份规范中进行其他配置，IDB 备份将删除当前活动的归档日志文件之外的所有现有归档日志文件。在此会话后，IDB 的数据库引擎将开始创建新的归档日志文件。

归档日志文件的重要性

要执行最方便的 IDB 恢复方法，指导下的自动恢复（包括重放日志文件），上一次 IDB 备份会话之后创建的归档日志文件必须可用。

存储空间注意事项

用于归档日志文件的存储空间取决于以下两个因素：

- Data Protector 单元中备份会话和其他类型的会话的总频率
- 两次 IDB 备份之间调用的备份会话数（如果启用在 IDB 备份期间自动执行归档日志文件删除）

IDB 备份配置

管理 Data Protector 单元的关键部分是配置 IDB 备份本身。在进行灾难准备时，可以执行的最重要任务是定期执行 IDB 备份。在 Cell Manager 发生灾难时，脱机恢复 IDB 对于恢复其他备份数据至关重要。

要创建 IDB 备份规范，请在备份上下文的“范围窗格”中选择**内部数据库**，然后按照标准的备份过程操作。

准备和运行 IDB 备份规范的提示

配置 IDB 备份时，请考虑以下各项：

- 排定每天至少执行一次 IDB 备份。这样可确保始终有 IDB 的当前备份。安排它在 Cell Manager 上活动较少的时候运行。

  > ⚠ **警告**始终应在对 IDB 配置进行任何修改后备份内部数据库，例如，在更改“内部数据库服务”和“应用程序服务器”用户帐户的密码后。未执行此操作可能会导致无法成功执行联机 IDB 恢复或脱机 IDB 恢复。

- IDB 备份的设备和介质选择，将对灾难之后执行 IDB 恢复的难易程度或可能性产生巨大的影响。
  - 使用可以通过自动配置进行配置的设备能够大大简化设备配置。
  - 如果使用文件介质库设备，请确保介质库位于包含 IDB 的驱动器以外的其他磁盘驱动器上。
  - 如果可能，请使用本地连接到 Cell Manager 的设备。
  - 不要使用文件库，因为无法将文件库介质导入到文件库。
  - StoreOnce 软件 (SOS) 介质的导入可能十分复杂，因此如果已经记录并测试 SOS 介质导入，请仅使用 SOS 设备进行 IDB 备份。在专用备份设备中的单独备份介质上，使用单独的介质池执行 IDB 备份。
  - 确保了解哪些介质用于 IDB 备份。可以配置**会话介质报告**以收到有关用于备份的介质的通知。这样可大大简化最终的还原。
- 设置数据和编码保护，以便拥有足够的 IDB 备份副本，满足业务需求。
- 除非绝对必要，请勿禁用自动 IDB 一致性检查。控制一致性检查的检查内部数据库备份选项默认情况下处于选中状态。
- 要提高数据的机密性，可以将加密与 IDB 备份配合使用。IDB 备份包括密钥库。

  > **注意:**必须有活动的加密密钥，然后才能启动加密的 IDB 备份，因为备份 IDB 期间无法创建新密钥。
  > 在加密 IDB 备份期间，加密密钥将自动导出到默认 Data Protector 导出加密密钥目录下的 IDB<CellManagerName>-keys.csv 文件中。如果是 Linux 群集感知 Cell Manager，则会为每个活动的节点创建一个密钥 (在 IDB 备份期间格式为 IDB<ActiveNodeName>-keys.csv))。
  > 必须格外注意备份之后的密钥。发生灾难时，需要密钥进行恢复。运行加密 IDB 备份之后，将使用的相应密钥复制到一个非常安全的位置。

- IDB 备份的设备和介质选择，将对灾难之后执行 IDB 恢复的难易程度或可能性产生巨大的影响。StoreOnce 软件 (SOS) 介质的导入可能十分复杂，因此如果已经记录并测试 SOS 介质导入，请仅使用 SOS 设备进行 IDB 备份。在专用备份设备中的单独备份介质上，使用单独的介质池执行 IDB 备份。

  > **注意**: 不支持 IDB 备份到在灾难恢复之后导入的 StoreOnce 软件 (SOS) 介质。

- 强烈建议记录并测试 DP IDB 恢复过程。

相关主题

- IDB 备份期间进行什么操作?
- 定期备份 IDB

相关任务

- 标准备份过程
- 启用或禁用自动 IDB 一致性检查

维护 IDB

如果您已配置内部数据库通知和报告，则系统根据当前 IDB 的情况，在需要执行任何维护任务时会通知您。

情况	可能会通知您，方法是 [1]	执行以下操作
IDB 空间用尽	“IDB 空间不足”通知	扩展 IDB 大小 减小 IDB 增大 减小 IDB 当前大小
要检查 IDB 大小	“IDB 大小”报告	检查 IDB 大小
IDB 运行不正常 - 可能已损坏	“IDB 损坏”通知	检查 IDB 一致性

[1] 只有在配置了通知和报告的情况下，您才能收到它们。

注意建议定期检查 Data Protector 事件日志，并检查是否有最终的 IDB 事件。管理员可能会考虑设置由电子邮件发送的通知，以便对传入的通知做出快速反应。

IDB 的增长和性能

要配置和维护内部数据库，必须了解影响 IDB 增大和性能的关键因素和参数。

此处给出的数据适用于文件系统备份，并阐明最坏的情况（最大或增大最快的 IDB）。如果执行磁盘映像，应用程序集成或 NDMP 备份，则 IDB 中只会存储少量数据。

IDB 增大关键因素

IDB 增大取决于环境和 Data Protector 设置，这些设置定义希望 Data Protector 保留多少历史记录和详细信息以便可以浏览和搜索文件。

关键因素	对 IDB 增大的影响
有关环境的文件和大小的详细信息	Data Protector 可以跟踪文件的每个版本。这意味着在每次备份期间，都将向每个备份文件的 DCBF 部分中存储一个文件名记录（大约 100 字节）。
（完整）备份的频率	备份越频繁，在 IDB 中存储的信息就越多。如果文件系统不常发生变化，则只有 DCBF 部分会增长。
对象副本数	创建的对象副本和对象镜像越多，IDB 中存储的信息就越多。IDB 中存储的对象副本和对象镜像的信息均与备份对象相同。

IDB 性能关键因素

关键因素	备份期间对 IDB 负载和性能的影响
并行驱动器数	同时运行的（磁带）驱动器数影响 IDB 上的负载。例如，如果在 10 个备份会话中同时运行 10 个驱动器，或在 5 个会话中同时运行 10 个驱动器，则数据库上的负载几乎相同。每个新驱动器意味着必须在数据库中存储另一个目录源。
文件平均大小	如果备份小文件，则可以更快地生成目录，并且 IDB 的负载因此也更高。
IDB 磁盘性能	备份期间 Data Protector 的主要活动是读写磁盘。因此，用于 IDB 的 Cell Manager 上磁盘（子系统）的速度会影响性能。

IDB 增大和性能关键参数

关键参数	对 IDB 增大的影响	对 IDB 性能的影响
日志记录级别	定义向 IDB 中写入有关文件和目录的数据量以及所需的存储空间。	浏览数据进行还原的便利程度的影响。
编目保护	定义有关所备份数据的信息（如文件名和文件版本）在 IDB 中保留多久。 如果编目保护到期，不会立即从 IDB 中删除数据。而是将在整个介质上数据的所有编目保护都到期的那一天删除这些数据。	无。

根据为编目保护所设置的时间段（相对较短的一段时间，时间段与数据保护相同）以及有效的日志记录级别，实际 IDB 增长会有所不同。在编目保护到期之前，IDB 的主要增大将持续。在那之后，增大就降低到最小程度，并由备份环境的增大决定。

日志记录级别对 IDB 的影响

不同的日志记录级别设置影响内部数据库增长、浏览文件系统进行恢复的便利程度，在极少的情况下还会影响备份性能。

下方提供的数据适用于文件系统备份。如果执行磁盘映像，联机数据库或 NDMP 备份，则 IDB 中只会存储少量数据。

不记录任何内容	仅存储对象信息，通常每个文件系统对象 2 kB。
日志目录	与**不记录任何内容**相同，额外存储每个备份的目录占用 30 字节。
记录文件	与**记录目录**相同，额外存储每个备份的文件占用 12 字节。
全部记录	与**记录文件**相同，额外存储每个备份的文件占用 18 字节。

编目保护对 IDB 的影响

内部数据库的最大部分与编目保护期和所选的日志记录级别成正比。编目保护期内执行的备份越多，IDB 中积累的数据就越多。换句话说，它是存储每个文件所需的数据乘以编目保护期内备份的文件数得到的。

目录保护到期后，并不会立即从 IDB 中删除信息。Data Protector 每天自动删除一次这些信息。由于 IDB 中的信息是按介质排列的，因此只有在介质上所有对象的编目保护都到期时，才会删除这些信息。如果这样，特定 DC 二进制文件占用的整个空间将变为空闲。

应设置编目保护，以使其至少包括上一次完整备份。例如，可以将完整备份的编目保护设为 8 周，将增量备份的编目保护设为 1 周。

IDB 大小估计

如果主要执行文件系统备份，则内部数据库在某些条件下可能会增长到相当可观的大小（几 TB）。如果执行磁盘映像或联机数据库备份，则 IDB 很可能不会超过几 GB。

维护 DCBF 目录

IDB 允许在存储 IDB 详细编目二进制文件 (DCBF) 部分的位置注册多个目录。这样可以将 DC 二进制文件分发到更多磁盘或卷上。默认情况下，有五个目录，其名称分别为从 dcbf0 到 dcbf4 。

每个 DCBF 目录都有多个配置参数：

- 分配顺序
- 路径
- 最大大小
- 最大文件数
- 空间不足

需要创建新的二进制文件时，Data Protector 就会执行“DCBF 分配过程”：

1. 从所有可能的 DC 目录的列表中，Data Protector 清除所有停用或消失的目录。请注意，在缺少 DC 目录的情况下，将生成 IDBCorrupted 事件。

   不考虑所有已满的 DC 目录。如果至少以下一个条件属实，则 DC 目录即为已满：

   Maximum size - Current size < Low space

   Free disk space < Low space

   Maximum files <= Current files

2. 一组用户可选择的算法 (DCDirAllocation 全局选项) 选择实际 DC 目录:

   - Fill in sequence

     Data Protector 按照配置的顺序在第一个不完整 DC 目录中创建新的 DC 二进制文件。

   - Balance size

     Data Protector 选择包含（与总大小的有效限制成正比）最少的 DCBF 数据的 DC 目录。选择以下值的最小者：

     (Maximum size - Current size - Low space) / (Maximum size - Low space)

   - Balance number

     Data Protector 选择包含（与文件数的有效限制成正比）最少的 DC 二进制文件的 DC 目录。选择以下值的最小者：

     Current files / Maximum files

请参阅影响 DCBF 行为的 DCDirAllocation 和 MaxDCDirs 全局选项。

检查 IDB 大小

可以使用 Data Protector GUI 检查内部数据库各个部分的当前大小。

此外，如果已配置，则“IDB 大小报告”以及“IDB 空间不足”通知会告知您 IDB 大小。

完成以下步骤：

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**使用情况**项。此时将显示以下 IDB 项：编目数据库、介质管理数据库、详细编目二进制文件、会话消息二进制文件及无服务器集成二进制文件。

   “无服务器集成二进制文件”项与安装的 Data Protector 版本中不再支持的功能相关。
3. 通过查看 IDB 各个部分及其记录的属性，检查 IDB 的大小：
   - 右键单击 IDB 项目，例如**编目数据库**，然后单击**属性**以查看 IDB 部分的磁盘使用情况。磁盘使用情况显示 IDB 的特定部分当前占用了多少磁盘空间。单击**记录统计信息**选项卡，以查看 IDB 特定部分中所有记录的统计信息。
   - 要检查 DC 目录的磁盘使用情况，请展开**详细编目二进制文件**，双击 DC 目录，然后单击**磁盘使用情况**选项卡。

定期备份 IDB

必须定期执行内部数据库备份；最好每天执行一次。定期执行 IDB 备份后，即做好在发生灾难时进行恢复的最重要准备。当 Cell Manager 受到灾难的打击时，必须恢复 IDB 才能恢复其他备份的数据。

建议将数据保护和编目保护设置为仅少数几天。设置此选项，以便至少保护最后两个 IDB 备份对象版本。

始终应在对 IDB 配置进行任何修改后备份内部数据库，例如，在更改“内部数据库服务”和“应用程序服务器”用户帐户的密码后。未执行此操作可能会导致无法成功执行联机 IDB 恢复或脱机 IDB 恢复。

减小 IDB 增大

通过降低备份、对象复制和对象合并规范的日志记录级别和编目保护设置，可以减小内部数据库的增大。这些操作不影响 IDB 的当前大小，但影响其未来的增大。

降低日志记录级别会使还原时浏览起来不太方便。

减少编目保护的效果是某些还原（即已超过编目保护的那些备份的还原）中无法浏览。

以下过程介绍如何在备份规范中更改这些设置。

降低日志记录级别

通过降低备份规范的日志记录级别，减少存储在 IDB 上的数据（文件/目录）的数量（**全部记录** -> **日志文件** -> **日志目录** -> **无日志**）。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要更改其日志记录级别的备份规范，然后单击**选项**选项卡。
4. 在“选项”属性页中，单击相应的**高级**按钮（在**文件系统选项**下）。
5. 单击**其他**选项卡，并在**日志记录**下，更改日志记录级别。
6. 单击**确定 (OK)** 应用更改。

降低编目保护

通过降低编目保护，只能降低对 IDB 中还原浏览信息的保护。仍将在介质上存储信息。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要更改其编目保护的备份规范，然后单击**选项**选项卡。
4. 在“选项”属性页中，单击相应的**高级**按钮（在**文件系统选项**下）。
5. 单击**选项**选项卡，并在**编目保护**下，更改编目保护。
6. 单击**确定 (OK)** 应用更改。

减小 IDB 当前大小

通过将编目保护设置更改为完整的备份、对象复制或对象合并会话 (会话中所有对象)，或更改为仅特定对象，降低内部数据库当前大小。

减少编目保护的效果是某些还原（即已超过编目保护的那些备份的还原）中无法浏览。

此操作不影响将来的 IDB 增大。

更改将在以下情况下生效：

- 如果从介质上的所有对象中删除了编目保护。
- 每天在 Data Protector 从 IDB 中自动删除过时数据时（默认情况下为中午）进行。可以使用 DailyMaintenanceTime 全局选项指定时间。请使用二十四小时制表示法。

  可以通过运行 omnidbutil -purge -dcbf 命令立即启动清除。

通过更改编目保护，只能更改对 IDB 中还原浏览信息的保护。仍将在介质上存储信息。因此，如果导出介质，再将其导回，则 Data Protector 将从介质重新读取有关编目保护的信息。

更改对于会话的编目保护

更改对备份会话的保护可更改对会话中所备份所有对象的保护。

完成以下步骤：

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**会话**项。
3. 右键单击要更改其保护的会话，然后单击**更改编目保护**。
4. 指定会话的新编目保护，然后单击**完成**应用更改。

更改对于对象的编目保护

更改对特定对象的保护可更改对此对象的保护，无论是在哪个会话中备份该对象。

完成以下步骤：

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**对象**项。
3. 右键单击要更其改保护的对象，然后单击**更改编目保护**。
4. 指定对象的新编目保护，然后单击**完成**应用更改。

扩展 IDB 大小

由于 IDB 的详细信息部分（备份对象的名称、版本和元数据）需要更多可用磁盘空间存储，因此您可能需要通过创建新的 DC 目录或重新配置现有目录以获得更大容量来扩展内部数据库。

重新配置 DC 目录以获得更大容量

可以通过修改分配序列、最大大小、最大文件数或空间不足选项重新配置现有 DC 目录。请注意，选定 DC 目录中的文件数和当前总大小可能会限制调整范围。

完成以下步骤：

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**使用情况**，然后展开**详细编目二进制文件**。
3. 右键单击选定 DC 目录的路径，然后单击**属性**。
4. 在结果区域中，根据需要修改可用选项。
5. 单击**完成**以应用更改。

IDB 一致性检查

内部数据库的内容必须在逻辑上正确，换句话说各个 IDB 部分必须一致且有序。可以手动对 IDB 的特定部分和整个 IDB 执行一致性检查。

Data Protector 默认情况下在备份 IDB 之前检查 IDB 的一致性（快速检查）。这样做对在 Cell Manager 遇到灾难时恢复 IDB 和备份的数据极其重要。

IDB 检查类型	检查的内容	命令
IDB 的快速检查	核心（MMDB 和 CDB）、文件名以及简单检查 DCBF 部分。	omnidbcheck -quick
DCBF 部分的简单检查	DC 二进制文件是否存在及其大小。	omnidbcheck -bf
DCBF 部分的完整检查	介质位置的一致性和 DC 二进制文件。	omnidbcheck -dc
检查 SMBF 部分	是否存在会话消息二进制文件。	omnidbcheck -smbf
介质一致性检查	介质的一致性。还会在介质一致性失败时列出不一致的介质名称。	omnidbcheck -media_consistency
架构一致性检查	IDB 架构的一致性。还会在 Data Protector 安装期间检测架构中自最初创建以来的所有更改。	omnidbcheck -schema_consistency
数据库一致性检查	数据库的一致性。还会在数据库一致性失败时列出错误。	omnidbcheck -database_consistency
IDB 的扩展检查	执行除 SMBF 检查之外的所有检查。	omnidbcheck -extended

启用或禁用自动 IDB 一致性检查

默认情况下，Data Protector 在备份内部数据库之前，将自动检查内部数据库的一致性。在此过程中，将快速检查 IDB 一致性。此检查类型将检测 IDB 内部的主要不一致。这可确保当 IDB 一致并因此可用于 Cell Manager 灾难恢复时，将仅创建 IDB 备份映像。

尽管可以禁用一致性检查，但强烈建议将其保持启用状态。

若密集使用 Cell Manager 且需要执行 IDB 一致性检查的时间出现严重问题，在这种情况下，可能需要通过选择**检查内部数据库**选项禁用该检查。在此类情况中，请考虑以下建议：

- 在启用了一致性检查的情况下，安排在可接受自动检查活动时执行 IDB 备份。
- 在禁用一致性检查的情况下，安排每日 IDB 备份。
- 至少保留最近检查过一致性的 IDB 备份映像。
- 仅在绝对必要时，才在 IDB 备份规范中禁用一致性检查。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**内部数据库**。
3. 选择 IDB 备份规范。如果没有备份规范，则配置一个新备份规范。
4. 单击**选项**选项卡。
5. 在“应用程序特有选项”下，单击**高级**。
6. 在“应用程序特定选项”对话框中，选择或清除**检查内部数据库**选项以启用或禁用自动 IDB 一致性检查。
7. 单击**确定**。
8. 单击“应用”。

将 IDB 移至不同的 Cell Manager

可以将内部数据库移至运行于相同操作系统上的不同 Cell Manager。

> **注意:** 您不能使用 omnioffir 命令将脱机 IDB 还原到其他磁盘或目录。

相关主题

- 要使用联机或脱机还原过程将 IDB 移至其他 Cell Manager，请参阅还原 IDB。
- 要使用脱机恢复过程将 IDB 移至其他 Cell Manager，请参阅恢复 IDB。

将 IDB 还原到不同磁盘布局

可以将联机内部数据库 (IDB) 还原为:

- 与灾难前的磁盘相比大小不同的磁盘
- 与备份目录不同的目录

> **注意:** 您不能使用 omnioffir 命令将脱机 IDB 还原到其他磁盘或目录。

有关还原 IDB 的详细信息，请参阅还原 IDB。

IDB 备份期间进行什么操作

IDB 备份期间，Data Protector：

- 检查 IDB 的一致性，以防止备份和随后还原的 IDB 损坏。为进行此操作，需要使**检查内部数据库**选项保持选中状态。
- 将 Data Protector 服务置于维护模式后，备份 IDB。
- 备份所有 Data Protector 配置数据，包括有关备份设备、备份规范和计划的数据以及审计信息。这样可在发生灾难时简化恢复。
- 如果启用了加密，则自动将加密密钥导出到默认 Data Protector 加密密钥目录下的 IDB-<CellManagerName>-keys.csv 文件中。如果是 Linux 群集感知 Cell Manager，则会为每个活动的节点创建一个密钥 (在 IDB 备份期间格式为 IDB<ActiveNodeName>-keys.csv))。
- 在 media.log 文件中创建 omnidb 条目，以便可以标识上次 IDB 备份所用的备份介质。在 IDB 丢失并需要从备份介质中恢复时，这一点很有用。

每次只能运行一个 IDB 备份会话。

还原 IDB

可以从标准 IDB 备份过程中创建的备份映像还原内部数据库 (IDB)。您不能使用以下还原方法来还原损坏的 IDB。 要还原损坏的 IDB，请执行 IDB 恢复方法之一。

> **注意:** 通用标准已认证的配置不支持将 IDB 还原到其他 Cell Manager。有关通用标准的详细信息，请参阅通用标准指南部分。

在联机内部数据库还原期间，基本 IDB 部分 (CDB、MMDB、SMBF) 只能还原到与原始位置不同的位置。但是，Cell Manager 的配置数据和 IDB 的详细编目二进制文件 (DCBF) 部分可以还原到它们的原始位置或不同的位置。根据内部数据库备份映像的大小，确保 Cell Manager 上有足够的空闲磁盘空间可用。

以下限制适用：

- 在以下情况下，不支持“使用已还原的数据库作为新的内部数据库”选项:
  - 如果正在考虑的备份是群集 Cell Manager 的 IDB 的备份，并且目标是独立的 Cell Manager。
  - 如果正在考虑的备份是独立 Cell Manager 的 IDB 的备份，并且目标是群集 Cell Manager。
- SG 群集配置不支持通过选项“启动数据库服务器”和“使用已还原的数据库作为新的数据库”将还原的 IDB 作为新的 IDB。可以使用下列方法之一:
  - 使用联机 IDB 还原进行还原，但不自动激活还原的 IDB。请参阅还原联机 IDB 但不自动激活还原的 IDB。
  - 使用基于 omnioffIr 命令的脱机恢复过程进行恢复。请参阅恢复 IDB。
- 要还原在重新安装 Data Protector 之前备份的 IDB，请删除 *<DP_SDATA>*/config/server/integ/config/idb/*.backupLog 文件 (如果有)，然后还原 IDB。

有关还原 IDB 的详细信息，请查看以下内容:

- 要从加密的 IDB 备份还原 IDB，还需要执行额外的步骤，然后才能进行实际还原过程。请参阅从加密备份准备 IDB 还原
- 有关使用 GUI 还原 IDB 并自动激活还原的 IDB 的信息，请参阅还原联机 IDB 并自动激活还原的 IDB。
- 有关使用 GUI 还原 IDB 但不激活还原的 IDB 的信息，请参阅还原联机 IDB 但不自动激活还原的 IDB。

从加密备份准备 IDB 还原

在加密 IDB 备份期间，加密密钥将自动导出到默认 Data Protector 导出加密密钥目录下的 IDB-ClientName-keys.csv 文件中。

还原 IDB 之前，进行如下操作：

1. 将 IDB-ClientName-keys.csv 文件传输到将执行 IDB 还原的 Cell Manager。
2. 通过运行以下命令导入文件中包含的密钥:

   omnikeytool -import CSVFile

Cell Manager 将使用联机 KMS 中的密钥对包含 IDB 备份的介质上的数据进行解密。在 SG 群集环境中，密钥文件的数量可能会有所不同，具体取决于进行 IDB 备份时处于活动状态的节点。每个文件名将基于承载它的节点。建议在尝试还原 IDB 之前导入所有此类密钥文件。

还原联机 IDB 并自动激活还原的 IDB

1. 在“上下文列表”中，单击 恢复。
2. 在“范围窗格”中，展开**恢复对象**，然后展开**内部数据库**。
3. 展开从中备份 IDB 的 Cell Manager 并单击**内部数据库**。
4. 在“内部数据库属性”页上，要还原内部数据库的基本部分，请将**还原内部数据库**选项保持选中状态。IDB 的基本部分是编目数据库 (CDB)、介质管理数据库 (MMDB) 和会话消息二进制文件 (SMBF)。指定还原期间用于内部数据库服务的临时端口，以及 IDB 的基本部分应还原到的位置。

   此外，决定是否使用存档的日志文件执行内部数据库恢复，以及是否应将还原的 IDB 作为单元的新内部数据库投入使用。
5. 选择**还原目录二进制文件**以还原 IDB 的 DCBF 部分，并选择其还原位置：

   > **注意:** 如果要将 DCBF 还原到其他位置，建议将 <DP_SDATA>/log/server/media.log 复制到一个临时位置。这将帮助您为相关 IDB 备份后创建的介质填充详细编目。如果 IDB 来自其他 Cell Manager 主机或重新安装了 Data Protector，则此方法不适用。
6. 指定是否 Data Protector 应将 IDB 还原到特定时间点，其中该时间不为上一次创建 IDB 备份映像的时间。在这种情况下，内部数据库的基本部分将还原到上一次的备份状态，然后再恢复到指定时间。
7. 在**配置文件**属性页上，进行有关 Cell Manager 配置数据还原的选择。如果选择该数据进行还原，还应指定其备份对象的版本、恢复位置并指定 Data Protector 如何处理仍存在于原始位置的配置文件。
8. 在**选项**属性页上，指定还原会话的可选 pre-exec 和 post-exec 命令。

9. 在**设备**属性页上，进行有关会话中使用哪些设备的选择。
10. 在**介质**属性页上，检查将用于还原 IDB 的备份介质。调整 Data Protector 将在会话期间考虑使用的优先级 (可选)。
11. 从“操作”菜单，选择**启动还原**，或在结果窗格中，单击**还原**。
12. 单击**完成**。
13. 如果还原失败，请根据显示的错误执行以下操作之一:
    - 如果还原失败并出现以下错误，则必须重置内部令牌，清除增量表并清除正在运行的会话:

      [Major] From: OB2BAR_POSTGRES_BAR@<Cell Manager> "DPIDB" Time: <Timestamp>
      Error running omnidbutil -reset_tokens.

      运行以下命令以执行所需的清理:

      - **Windows**：
        - *<DP_HOME>*\bin\omnidbutil.exe -reset_tokens.
        - *<DP_HOME>*\bin\omnidbutil.exe -force_purge_delta_tables
        - *<DP_HOME>*\bin\omnidbutil.exe -clear
      - **Linux**：
        - *<DP_HOME>*/sbin/omnidbutil -reset_tokens
        - *<DP_HOME>*/sbin/omnidbutil -force_purge_delta_tables
        - *<DP_HOME>*/sbin/omnidbutil -clear
    - 如果还原失败并出现以下错误，则必须清除增量表并清除正在运行的会话:

      [Major] From: OB2BAR_POSTGRES_BAR@<Cell Manager> "DPIDB" Time: <Timestamp>
      Error running omnidbutil -force_purge_delta_tables.

      运行以下命令以执行所需的清理:

      - **Windows**：
        - *<DP_HOME>*\bin\omnidbutil.exe -force_purge_delta_tables
        - *<DP_HOME>*\bin\omnidbutil.exe -clear
      - **Linux**：
        - *<DP_HOME>*/sbin/omnidbutil -force_purge_delta_tables
        - *<DP_HOME>*/sbin/omnidbutil -clear
    - 如果还原失败并出现以下错误，则必须清除正在运行的会话:

      [Major] From: OB2BAR_POSTGRES_BAR@<Cell Manager> "DPIDB" Time: <Timestamp>
      Error running omnidbutil -clear.

      运行以下命令以执行所需的清理:

      - **Windows**：
        - *<DP_HOME>*\bin\omnidbutil.exe -clear
      - **Linux**：
        - *<DP_HOME>*/sbin/omnidbutil -clear
14. 如果 Cell Manager 在 Windows 上运行，请在 IDB 还原完成后使用 omniinetpasswd 命令在 Cell Manager 的模拟数据库中为 PGOSUSER 实体重新创建用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。

    > **注意:** 从 <DP_CONFIG>\server\idb\idb.config 检索 PGOSUSER 值。

    - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
    - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*
15. 对于群集感知 Cell Manager，请在还原后将代理通信证书 (localhost_cert.pem) 和密钥 (localhost_key.enc) 文件从 *<DPDATA>*\config\server\sscertificates 目录复制到辅助节点 *<DPDATA>*\config\server\sscertificates 目录。
16. 如果 IDB 备份来自其他 Cell Manager，则在成功还原 IDB 后，检查配置的用户并使用 *<DP_HOME>*\bin\omniusers 命令删除属于原始 Cell Manager 的用户。
17. 如果 IDB 备份来自其他 Cell Manager，并且现在配置了群集感知 Cell Manager，则在还原后将 Data Protector 服务移动 (故障转移) 到那里后，在辅助节点上运行以下命令 -
    - **Windows**： *<DP_HOME>*\bin\omniusers -create_basic_cm_users
    - **Linux**： /opt/omni/bin/omniusers -create_basic_cm_users
18. 如果将详细编目 (DC) 和会话消息二进制文件还原到了不同的还原位置，则创建新 DC 目录，然后删除旧目录。运行 omnidbutil -remap_dcdir 命令以更新 DC 二进制文件的路径名。在这种情况下，您将丢失原始 IDB 备份后运行的备份的详细信息编目信息。上次安装中的 media.log 文件为您提供有关自上次 IDB 备份以来使用的介质的信息。您应该导入这些介质以填充受影响备份的详细信息编目信息。
19. 如果要将包含 CMMDB 或远程 MMDB 的 IDB 恢复到不同的磁盘布局，则需要在更新 IDB 之后运行以下命令。
    - **Windows**： <DP_HOME>\bin\omnidbutil.exe -cdbsync
    - **Linux:**< DP_HOME>/sbin/omnidbutil -cdbsync
20. (可选) 要将 IDB 移回原始位置，请在联机 IDB 还原到诸如 db80_restore 之类的目录后，在 Cell Manager 上执行以下步骤。
    1. 验证 IDB 还原后是否一切都按预期工作。重新连接 GUI。

2. 使用 omnidbcheck -extended 命令运行 IDB 一致性检查。
3. 使用 omnisv -stop 命令停止服务。
4. 在命令提示符下记录以下命令的输出:
   - **Windows**： dir *<DP_SDATA>*\server\db80\pg\pg_tblspc
   - **Linux**： ls -al /var/opt/omni/server/db80/pg/pg_tblspc
5. 重命名或删除预还原的文件夹 idb、 jce、 kcdb 和 pg (位于 *<DP_SDATA>*\server\db80 或 /var/opt/omni/server/db80
6. 将还原的文件夹 idb、 idb、 jce、 kcdb 和 pg 从 db80_restore 移动 (不复制) 到 *<DP_SDATA>*\server\db80 或 /var/opt/omni/server/db80.
   确保保留文件夹和文件的权限和所有权。
7. 在 pg_tblspc 中重新创建文件系统连接以指向移动的表空间。删除现有连接并重新创建它们，使用 dir 或 ls -al 命令验证结果:
   - mklink /J Link Target (Windows)
   - ln -sf TARGET LINK_NAME (Linux)
8. 在以下内容中，将 db80_restore 替换为 db80：
   - <DP_SDATA>\Config\Server\idb\idb.config 或 /etc/opt/omni/server/idb/idb.config
   - <DP_SDATA>\server\db80\pg\postmaster.opts 或 /var/opt/omni/server/db80/pg/postmaster.opts
   - <DP_SDATA>\server\db80\pg\postgresql.conf 或 /var/opt/omni/server/db80/pg/postgresql.conf
9. 运行以下 omnidbutil 命令以更改 IDB 服务相关文件中的路径:
   - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -sync_srv
   - **Linux**： /opt/omni/sbin/omnidbutil.exe -sync_srv
10. 从磁盘移动或删除剩余目录:
    - <DP_SDATA>\server\db80_restore 或 /var/opt/omni/server/db80_restore
    - meta_YYYY-MM-DD* 从 <DP_SDATA>\server\db80 或 /var/opt/omni/server/db80
    - msg_YYYY-MM-DD* 从 <DP_SDATA>\server\db80 or /var/opt/omni/server/db80
    - a uditing_YYYY-MM-DD* 从 <DP_SDATA>\log\server or /var/opt/omni/log/server
11. 使用以下命令启动服务 omnisv -start

重要说明:在时间点 IDB 还原会话后，将特定文件从 auditing_IDBRestoreSessionID_NNNNNNNNNN 目录复制到原始的 auditing 目录。这将使审计信息与还原的 IDB 的状态一致。应复制以下审计日志：

YYYY_MM_DD.med

YYYY_MM_DD.obj

YYYY_MM_DD.ses

以上文件名中， YYYY、 MM 和 DD 字符串对应于“内部数据库”属性页上“还原至”选项指定的日期。

注意: 还原后，您可能希望检查 IDB 一致性。

还原联机 IDB 但不自动激活还原的 IDB

此方法不能用于还原其他 Cell Manager 的 IDB。要还原 IDB，然后手动激活它，请执行以下操作:

还原联机 IDB 但不自动激活 IDB

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开**恢复对象**，然后展开**内部数据库**。
3. 展开从中备份 IDB 的 Cell Manager 并单击“内部数据库”。
4. 在“内部数据库”属性页上，选择“还原内部数据库”选项，以还原内部数据库的基本部分。IDB 的基本部分是编目数据库 (CDB)、介质管理数据库 (MMDB) 和会话消息二进制文件 (SMBF)。指定要在还原期间用于内部数据库服务的临时端口，以及 IDB 的基本部分应还原到的位置。
5. 取消选择“启动数据库服务器 (将执行恢复)”和“使用已还原的数据库作为新的内部数据库”。
6. 选择“还原编目二进制文件”以还原 IDB 的 DCBF 部分，并选择“还原到其他位置”。指定 Cell Manager 上要将 IDB 的 DCBF 部分还原到的目标目录。在调用还原前，请确保该目录为空并提供足够的可用存储空间。
7. 指定是否 Data Protector 应将 IDB 还原到特定时间点，其中该时间不为上一次创建 IDB 备份映像的时间。在这种情况下，内部数据库的基本部分将还原到上一次的备份状态，然后再恢复到指定时间。
8. 在**配置文件**属性页上，进行有关 Cell Manager 配置数据还原的选择。

   如果选择该数据进行还原，还应指定其备份对象的版本、恢复位置并指定 Data Protector 如何处理仍存在于原始位置的配置文件。

   选择“还原配置文件”以还原 Cell Manager 配置数据，然后选择“使用适用于选定数据库还原的备份版本”以使 Data Protector 能够自动选择并处理一个还原链，该还原链符合您为 IDB 的基本部分 (CDB、MMDB、SMBF) 选择的还原链。
9. 选择“还原到其他位置”以指定 Cell Manager 上应将 Cell Manager 配置数据还原到的目标目录。在调用还原前，请确保该目录为空并提供

足够的可用存储空间。

10. 在**选项**属性页上，指定还原会话的可选 pre-exec 和 post-exec 命令。
11. 在**设备**属性页上，进行有关会话中使用哪些设备的选择。
12. 在**介质**属性页上，检查将用于还原 IDB 的备份介质。调整 Data Protector 将在会话期间考虑使用的优先级 (可选)。
13. 从“操作”菜单，选择**启动还原**，或在结果窗格中，单击**还原**。
14. 单击“完成”。
15. 要手动激活还原的 IDB，请继续手动激活还原的 IDB。

手动激活还原的 IDB

1. 要停止 Data Protector 服务，请运行以下命令:

   ```
   omnisv stop
   ```

2. 如果在重新安装 DP 之后还原 IDB，请在重新安装 DP 之前将 media.log 文件从以下位置复制到一个临时位置。 这有助于将 IDB 恢复到最新可能的时间。请参阅通过导入介质更新 IDB。
   - **Windows**： <DP_SDATA>\server\media.log
   - **Linux**： /var/opt/omni/log/server/media.log
3. 在命令提示符下记录以下命令的输出。
   - **Windows**： dir <DP_SDATA>\server\db80\pg\pg_tblspc
   - **Linux**： ls -al /var/opt/omni/server/db80/pg/pg_tblspc
4. 记录以下文件夹权限，方法是使用 ls -l (Linux) 或 icacls.exe
   - **Windows**： <DP_SDATA>\server\db80
   - **Linux**：/var/opt/omni/server/db80
5. 对于重新安装 DP 后还原的 IDB，删除或重命名密钥库目录。
   - **Windows**： <DP_SDATA>\server\db80\keystore
   - **Linux**： /var/opt/omni/server/db80/keystore
6. 删除或重命名以下目录或文件 (如果存在)。
   在 **Windows** 中**:**
   - <DP_SDATA>\config\server
   - <DP_SDATA>\config\client\sscertificates
   - <DP_SDATA>\config\client\ssconfig (in a cluster-aware Cell Manager, it may not be available)
   - <DP_SDATA>\server\db80\idb
   - <DP_SDATA>\server\db80\jce
   - <DP_SDATA>\server\db80\kcdb
   - <DP_SDATA>\server\db80\pg
   - <DP_SDATA>\server\AppServer

   在 **Linux** 中**:**
   - /etc/opt/omni/server
   - /etc/opt/omni/client/sscertificates
   - /etc/opt/omni/client/ssconfig (在群集感知 Cell Manager 中，它可能不可用)
   - /var/opt/omni/server/db80/idb
   - /var/opt/omni/server/db80/jce
   - /var/opt/omni/server/db80/kcdb
   - /var/opt/omni/server/db80/pg
   - /var/opt/omni/server/db80/AppServer
7. 从还原位置复制目录，并相应替换以下目录。如果存在冲突，请选择覆盖。

   在 **Windows** 中**:**

   - <DP_SDATA>\config\server
   - <DP_SDATA>\config\client\sscertificates
   - <DP_SDATA>\config\client\ssconfig (在群集感知 Cell Manager 中，它可能不可用)
   - <DP_SDATA>\server\db80
   - <DP_SDATA>\server\AppServer

   在 **Linux** 中**:**
   - /etc/opt/omni/server
   - /etc/opt/omni/client/sscertificates
   - /etc/opt/omni/client/ssconfig (在群集感知 Cell Manager 中，它可能不可用)
   - /var/opt/omni/server/db80/
   - /var/opt/omni/server/db80/AppServer
8. 使用先前步骤中记录的权限，将其应用于以下目录。
   - **Windows**： <DP_SDATA>\server\db80
   - **Linux**： /var/opt/omni/server/db80
9. 修复链接，使其指向正确的位置。请参阅步骤 17 中记录的链接状态。删除以下目录中的现有链接，然后重新创建它们，使用 dir 或 ls -al command
   - **Windows**：
     <DP_SDATA>\server\db80\pg
     mklink /J Link Target (command)
   - **Linux**：
     /var/opt/omni/server/db80/pg
     ln -sf TARGET LINK_NAME (command)
10. 要修复配置文件以使其指向正确的位置，请打开 \ProgramData\OmniBack\server\db80\pg\postgresql.conf 文件，然后修改以下内容中 archive_command 的值:

    ```
    archive_command = 'copy "%p" "c:/IDB/idb/pg/pg_xlog_archive/%f"'
    ```

    更改为

archive_command = 'copy "%p" "c:/ProgramData/OmniBack/server/db80/pg/pg_xlog_archive/%f"'

11. 启动 Data Protector 服务，但应用程序服务器服务除外:
    - omnisv start
    - omnisv -stop_as
12. 使用以下命令在应用程序服务器配置中更新数据库凭据
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -update_as_security_domain
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -update_as_security_domain
13. 使用以下命令启动应用程序服务器服务：omnisv -start_as
14. 如果 Cell Manager 在 Windows 上运行，请在 IDB 还原完成后使用 omniinetpasswd 命令在 Cell Manager 的模拟数据库中为 PGOSUSER 实体重新创建用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。
    - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
    - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*

> **注意:** 从 <DP_CONFIG>\server\idb\idb.config 检索 PGOSUSER 值。

15. 使用以下命令清除正在运行的会话。如果命令失败，请在继续下一步之前运行 autovacuum 步骤:
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -clear
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -clear
16. 运行以下命令以重置内部令牌。
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -reset_tokens
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -reset_tokens
17. 运行以下命令以清除为报告服务器创建的增量表。
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -force_purge_delta_tables
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -force_purge_delta_tables
18. 运行以下命令以修复介质位置。
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -fixmpos
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -fixmpos
19. (如果 omnidbutil -clear 命令挂起，则视情况而定) 如果要将包含 CMMDB 或远程 MMDB 的 IDB 恢复到不同的磁盘布局，则运行以下命令以更新 IDB。
    - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -cdbsync
    - **Linux**： /opt/omni/sbin/omnidbutil.exe -cdbsync
20. (视情况而定) 在步骤 16 中，如果您存储了先前安装的 media.log 文件，请通过从日志文件导入介质来更新还原的 IDB。请参阅通过导入介质更新 IDB。
21. 如有必要，运行自动清理过程。
    1. 在仅 IDB 模式下启动 Data Protector。
       omnisv -start -idb_only
       - 如果 Cell Manager 在 Windows 群集中运行，仅启动 IP 资源、磁盘资源、IDB 资源和 IDB-CP 资源 (不要启动 AS 和 MCRS 资源)。
       - 使用以下内容 (一行) 创建文件 vacuum.sql ，执行清理过程:
         ==========
         vacuum full analyze verbose;
         ==========
       - 确保 Data Protector 未执行活动 (无会话、未运行/启动维护)
       - 退出所有 GUI 实例
       - 运行脚本:
         - **Windows**： *<DP_HOME>*\bin\omnidbutil.exe -run_script vacuum.sql -admin -detail
         - **Linux**： /opt/omni/sbin/omnidbutil -run_script vacuum.sql -admin -detail
       - 脚本运行时间随 IDB 核心大小的不同而异，通常少于 30 分钟
       - 处理各个表时，脚本会显示进度消息
    2. 停止 Data Protector 服务。
       omnisv -stop

> **注意:**还原后，您可能希望检查 IDB 一致性。

配置 IDB 报告

通过配置内部数据库报告，可以在需要执行某些 IDB 维护任务（如扩展 IDB 大小和减小 IDB 增大）时告知您。

IDB 报告

报告	告知您...
内部数据库大小报告	...IDB 特定部分的大小。

配置 IDB 通知

通过配置内部数据库通知，可以在需要执行某些 IDB 维护任务（如扩展 IDB 大小、检查 IDB 一致性等等）时告知您。

IDB 通知

通知	告知您...
IDB 空间不足	...如果 IDB 空间用尽。
IDB 限制	...如果任何 MMDB 或 CDB 部分达到其限制。
需要执行 IDB 备份	...如果 IDB 备份不够频繁或者连续增量 IDB 备份太多。

恢复 IDB

如果所有或某些 IDB 文件不可用或损坏，则需要恢复内部数据库。

IDB 问题分为三种级别，每种级别都有各自的修复方法：

- 解决由操作系统配置问题（如未装载文件系统、名称服务问题等等）导致的 IDB 问题。
- 忽略或删除 IDB 中有问题的非核心部分（二进制文件）。如果确认的 IDB 损坏级别为 minor（损坏不在 IDB 的核心部分），则可以执行此操作。
- 执行由 IDB 还原和自上次 IDB 备份以来更新 IDB 组成的完整恢复。如果确认的 IDB 损坏级别为 critical（损坏在核心部分），则必须采取此操作。

完整恢复（自上次 IDB 备份以来还原和更新 IDB）

完整恢复由两个阶段组成：

1. IDB 还原，此阶段使 IDB 恢复上一个（可用）一致状态。
2. 将 IDB 从上一个一致状态更新到上次 IDB 仍正常运行的时刻。

根据在发生问题之前为 IDB 恢复所做准备的充足程度（IDB 恢复文件、IDB 备份映像、原始备份设备和归档日志文件的可用性），恢复过程可能不同。如果上述各项都可用，则可以使用一种非常方便的 IDB 恢复方法，在指导下进行自动恢复。

相关主题

- IDB 恢复方法的概述
- IDB 损坏级别

相关任务

- 确认 IDB 损坏的级别

IDB 恢复方法的概述

可使用多种恢复方法恢复内部数据库。根据所确认的损坏级别，您的要求以及 IDB 恢复文件、原始备份设备和归档日志文件的可用性，恢复过程会有所不同。

最方便的完整恢复

此恢复方法指导您完成还原 IDB 和重放归档日志文件的过程。如果归档日志文件不可用，则通过导入自上一次 IDB 备份以来的所有介质，仍可以更新 IDB。

损坏级别	问题类型	当前情况	恢复过程
严重	缺少完整的 IDB，或损坏了核心部分。	IDB 恢复文件和用于 IDB 备份的原始设备可用。	执行指导下的自动恢复（恢复 IDB 和重放归档日志文件）（如果可能）。否则，按照“更多恢复方法”下给出的某种方法进行操作。

省略 (删除) 损坏的 IDB 部分

如果确认的损坏级别为 minor（损坏不在核心部分），则可以考虑省略（删除）IDB 的丢失或损坏部分，或改为执行完整 IDB 恢复。

损坏级别	问题类型	恢复过程
Minor	DC 二进制文件丢失或损坏。	处理 IDB DCBF 部分中的 Minor 损坏

更多恢复方法

以下这些恢复过程可适应多种特定的情况。它们假定要恢复完整 IDB，但因某些原因无法执行指导下的自动恢复方法。恢复由还原 IDB 和更新 IDB 组成。

还原

当前情况	注解	恢复过程（还原 IDB）
IDB 恢复文件可用，但已更改了用于 IDB 备份的原始设备。	此方法本质上与指导下的自动恢复方法相同，但接受的指导较少、更复杂和花费时间更多。	使用 IDB 恢复文件和更改的设备还原 IDB
IDB 恢复文件不可用。	此方法本质上与指导下的自动恢复方法相同，但接受的指导较少、更复杂和花费时间更多。	在无 IDB 恢复文件的情况下还原 IDB
要从特定 IDB 备份（不是最新的那个）恢复 IDB。	此方法并不提供 IDB 的最新状态作为结果。	从特定的 IDB 会话中还原 IDB
要恢复到不同的磁盘布局。	此方法等同于从 Data Protector 配置进行灾难恢复，这种情况下会丢失存档日志文件、IDB 恢复文件和 media.log 文件。它远比指导下的自动恢复更复杂，并且不提供 IDB 的最新状态作为结果。	将 IDB 还原到不同磁盘布局

自上一次 IDB 备份以来更新 IDB

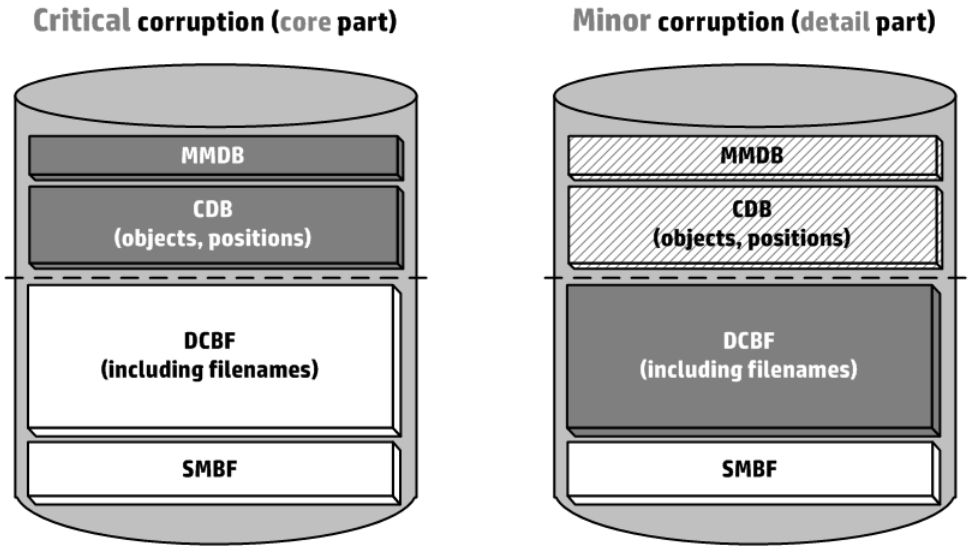
当前情况	恢复过程（更新 IDB）
归档日志文件不可用。	通过导入介质更新 IDB

IDB 损坏级别

数据库损坏: 严重和轻微。级别取决于 IDB 中发生损坏的部分。

可以使用 IDB 一致性检查确定 IDB 的哪个部分损坏。

根据损坏的级别，IDB 恢复过程有所不同。



相关任务

- 确认 IDB 损坏的级别

确认 IDB 损坏的级别

确认损坏的级别，以便选择相应的内部数据库恢复方法。

完成以下步骤:

1. 使用 omnidbcheck -extended 命令确认损坏的级别。

> **注意**扩展检查可能会花费相当长的一段时间。可以改为运行 omnidbcheck 命令的某些部分。例如，运行 omnidbcheck -connection 以确认 IDB 的连接是否正常工作。

确认损坏的级别之后，执行相应的恢复过程。

执行指导下的自动恢复 (还原 IDB 和重放存档的日志文件)

以下限制适用：

- 您不能使用 omnioffl r 命令将脱机 IDB 还原到其他磁盘或目录。
- 通用标准已认证的配置不支持将 IDB 还原到其他 Cell Manager。有关通用标准的详细信息，请参阅通用标准指南部分。
- 要还原在重新安装 Data Protector 之前备份的 IDB，请删除 *<DP_SDATA>*/config/server/integ/config/idb/*.backup lo g 文件 (如果有)，然后还原 IDB。

指导下的自动恢复是最方便的内部数据库恢复方法。如果 IDB 恢复文件和用于 IDB 备份的原始设备以及 IDB 备份介质都可用，则可以执行该方法。

该方法指导您还原 IDB 并重放上一次 IDB 备份以来的归档日志文件。如果存档日志文件不可用，仍可以通过导入介质更新上一次 IDB 备份的 IDB。

事务重放将更新 IDB 的核心部分。不更新二进制文件，并因此将丢失对二进制文件的更改。直到 IDB 损坏为止，以下各项才对从上一次 IDB 备份中运行的备份可用：

- 会话消息
- 浏览文件版本（可还原完整对象）。在备份使用的介质上执行导入目录以恢复更改。

以下先决条件适用:

- 根据内部数据库备份映像的大小，确保 Cell Manager 上有足够的空闲磁盘空间可用。
- 确保 Cell Manager 上的总 RAM 是发行说明中 Data Protector Cell Manager 安装要求中所述的两倍。如果 Cell Manager 是 UNIX 系统，请确保其内核参数 shmmax 设置为同一部分中所述的所需值的两倍。
- 在与 IDB 备份时相同的目录（在 Windows 系统中，必须分配相同驱动器号）上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 omnioffl r 命令的 -preview 选项查看要将文件还原到的位置。
- 在主机上重新安装 Cell Manager 之前，请确保将 IDB 恢复文件 (obrindex.dat) 和加密密钥文件 (用于加密的 IDB 备份) 从备份位置复制到主机上的临时位置 (例如：C:\temp)。

  要复制恢复文件，请执行以下操作:

  - **Windows** :
    copy <DP_DATA_DIR>\server\db80\logfiles\rlog\obrindex.dat C:\temp
  - **Linux** :
    cp /var/opt/omni/server/db80/logfiles/rlog/ obrindex.dat /temp

  要复制加密文件，请执行以下操作:

  - **Windows** :
    copy <DP_DATA_DIR>\Config\Server\export\keys\IDB-<hostname>-keys.csv C:\temp
  - **Linux** :
    cp /var/opt/omni/server/export/keys/IDB-<hostname>-keys.csv /temp
- 在 Cell Manager 和连接设备（首选用于 IDB 备份的设备）的系统上安装 Data Protector。
- 如果将 IDB 安装在 HPE Serviceguard 上，请在执行指导下的自动恢复之前将 DP 包置于维护模式。指导下的自动恢复完成后，请退出维护模式。
- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。
- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS_HPDP_AS、OBVS_HPDP_IDB 和 OBVS_HPDP_IDB_CP 群集组脱机。指导下的自动恢复完成后， OBVS_HPDP_AS 、 OBVS_HPDP_IDB 、 OBVS_HPDP_IDB_CP 和 OBVS_MCRS 群集组将自动联机。

完成以下步骤：

1. 运行以下命令将您保存在临时位置的 IDB 恢复文件 (obrindex.dat) 复制到新安装的 Cell Manager。
   - **Windows** :
     copy c:\temp\obrindex.dat \server\db80\logfiles\rlog\
   - **Linux** :
     cp /temp/obrindex.dat /var/opt/omni/server/db80/logfiles/rlog/
2. 对于加密的 IDB 备份，将您保存在临时位置的加密密钥文件复制到新安装的 Cell Manager
   - **Windows** :
     copy c:\temp\IDB-<hostname>-keys.csv <DP_Location>\server\export\keys
   - **Linux** : cp /temp/IDB-<hostname>-keys.csv /var/opt/omni/server/export/keys
3. 如果 Cell Manager 和介质代理位于不同的主机上，则在两台主机上都设置 omnirc 变量 OB2UNSECURE=1 。对于 Windows 系统，请在两台主机计算机上重新启动 INET 服务。
4. 运行 omnioffl r -idb -autorecover -force 命令。

> **注意**对于加密的 IDB 脱机还原，使用 -keyfile 选项。有关此问题的详细信息，请参阅 omnioffl r。

此命令读取 IDB 恢复文件，如果将 IDB 备份记录到文件，则它将停止服务，并就地启动 IDB 的还原。将使用 IDB 恢复文件中的数据自动生成所有选项。

还原完成后， omnioffl r 将检查并应用已存档的日志文件。

5. (视情况而定) 如果您已按照上一步中所指定的在 Cell Manager 主机和介质代理主机上将 omnirc 变量 OB2UNSECURE 设置为 1，则从两台主机删除之前设置的 omnirc 变量 OB2UNSECURE 。对于 Windows 系统，请在两台主机计算机上重新启动 INET 服务。
6. 如果 IDB 来自其他 Cell Manager，请如下运行 omnicellnamechange.pl 实用程序脚本:
   - 在 **Windows** 中**:** *<DP_HOME>*\bin\perl.exe <DP_HOME>\bin\omnicellnamechange.pl -newcmhost <newcm>
   - 在 **Linux** 中**:** /opt/omni/bin/perl *<DP_HOME>*\bin\omnicellnamechange.pl -newcmhost <newcm>
7. 如果安装了群集感知 Cell Manager，请在还原后将代理通信证书 (localhost_cert.pem) 和密钥 (localhost_key.enc) 文件从 *<DPDATA>*\config\server\sscertificates 目录复制到辅助节点 *<DPDATA>*\config\server\sscertificates 目录。
8. 如果 IDB 备份来自其他 Cell Manager，并且安装了支持群集的 Cell Manager，则在还原后将 Data Protector 服务移动到辅助节点上后，在辅助节点上运行以下命令
   - 在 **Windows** 中**:** *<DP_HOME>*\bin\omniusers -create_basic_cm_users
   - 在 **Linux** 中**:** /opt/omni/bin/omniusers -create_basic_cm_users
9. 如果 IDB 备份来自其他 Cell Manager，则在成功还原 IDB 之后，查看配置的用户，并使用 *<DP_HOME>*\bin\omniusers 命令删除属于 IDB 备份所在的 Cell Manager 的用户。
10. 如果重新安装 Windows Cell Manager，则必须在完成此 IDB 还原会话之后、执行下一次 IDB 备份之前重新创建 PGOSUSER 的用户信息。使用 omniinetpasswd 命令在 Cell Manager 上的模拟数据库中重新创建 PGOSUSER 的用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。
    - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
    - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*

> **注意:**可以从 *<DP_CONFIG>*\server\idb\idb.config 检索 PGOSUSER 值。

11. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \config\server\idb\idb.conf 以更正 "PGOSUSER" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。
12. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \server\db80\pg\pg_ident.conf 以更正 "SYSTEM-USERNAME" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。

使用 IDB 恢复文件和更改的设备还原 IDB

以下限制适用：

- 您不能使用 omnioffIr 命令将脱机 IDB 还原到其他磁盘或目录。
- 通用标准已认证的配置不支持将 IDB 还原到其他 Cell Manager。有关通用标准的详细信息，请参阅通用标准指南部分。
- 要还原在重新安装 Data Protector 之前备份的 IDB，请删除 *<DP_SDATA>*/config/server/integ/config/idb/*.backup log 文件 (如果有)，然后还原 IDB。

指导下的自动恢复是最方便的内部数据库恢复方法。如果 IDB 恢复文件和用于 IDB 备份的原始设备以及 IDB 备份介质都可用，则可以执行该方法。

该方法指导您还原 IDB 并重放上一次 IDB 备份以来的归档日志文件。如果存档日志文件不可用，仍可以通过导入介质更新上一次 IDB 备份的 IDB。

事务重放将更新 IDB 的核心部分。不更新二进制文件，并因此将丢失对二进制文件的更改。直到 IDB 损坏为止，以下各项才对从上一次 IDB 备份中运行的备份可用：

- 会话消息
- 浏览文件版本（可还原完整对象）。在备份使用的介质上执行导入目录以恢复更改。

以下先决条件适用:

- 根据内部数据库备份映像的大小，确保 Cell Manager 上有足够的空闲磁盘空间可用。
- 确保 Cell Manager 上的总 RAM 是发行说明中 Data Protector Cell Manager 安装要求中所述的两倍。如果 Cell Manager 是 UNIX 系统，请确保其内核参数 shmmax 设置为同一部分中所述的所需值的两倍。
- 在与 IDB 备份时相同的目录（在 Windows 系统中，必须分配相同驱动器号）上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 omnioffIr 命令的 -preview 选项查看要将文件还原到的位置。
- 在 Cell Manager 和连接设备（首选用于 IDB 备份的设备）的系统上安装 Data Protector。
- 如果将 IDB 安装在 HPE Serviceguard 上，请在执行指导下的自动恢复之前将 DP 包置于维护模式。指导下的自动恢复完成后，请退出维护模式。
- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。
- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS_HPDP_AS, OBVS_HPDP_IDB 和 OBVS_HPDP_IDB_CP 群集组脱机。指导下的自动恢复完成后， OBVS_HPDP_AS 、 OBVS_HPDP_IDB 、 OBVS_HPDP_IDB_CP 和 OBVS_MCRS 群集组将自动联机。

完成以下步骤：

1. 运行以下命令，创建含有还原作业选项的文本文件：
   omnioffIr -idb -autorecover -save C:\TEMP\restjob.txt -skiprestore -logview

   指定的 -logview 命令在会话 ID 旁列出第一个存档日志文件。请记住要还原的会话的第一个存档日志文件，因为您需要它才能在还原之后更新 IDB。例如，在输出 2013/02/09-2 AAAAAAH 中，要记住第一个存档日志文件 AAAAAAH 才能还原 2013/02/09-2 session.

   所创建的 restjob.txt 文件包含有关 (在执行 IDB 备份时) 介质最初所在的原始设备和插槽的信息。
2. 修改 restjob.txt 文件，指定介质当前所在的当前设备或插槽。
3. 用 omnioffIr -idb -read C:\TEMP\restjob.txt 命令运行还原。

   > **注意:** 对于加密的 IDB 脱机还原，使用 -keyfile 选项。有关此问题的详细信息，请参阅 omnioffIr。

   此命令指导您完成以下过程：还原 IDB 和重放从上一次 IDB 备份以来的存档日志文件。如果归档日志文件不可用，则通过导入自上一次 IDB 备份以来所使用的所有介质，仍可以更新 IDB。
4. 如果 IDB 来自其他 Cell Manager，请如下运行 omnicellnamechange.pl 实用程序脚本:
   - 在 **Windows** 中: *<DP_HOME>*\bin\perl.exe <DP_HOME>\bin\omnicellnamechange.pl -newcmhost <newcm>
   - 在 **Linux** 中: /opt/omni/bin/perl *<DP_HOME>*\bin\omnicellnamechange.pl -newcmhost <newcm>
5. 如果安装了群集感知 Cell Manager，请在还原后将代理通信证书 (localhost_cert.pem) 和密钥 (localhost_key.enc) 文件从 *<DPDATA>*\config\server\sscertificates 目录复制到辅助节点 *<DPDATA>*\config\server\sscertificates 目录。
6. 如果 IDB 备份来自其他 Cell Manager，并且安装了支持群集的 Cell Manager，则在还原后将 Data Protector 服务移动到辅助节点上后，在辅助节点上运行以下命令
   - 在 **Windows** 中: *<DP_HOME>*\bin\omniusers -create_basic_cm_users
   - 在 **Linux** 中: /opt/omni/bin/omniusers -create_basic_cm_users
7. 如果 IDB 备份来自其他 Cell Manager，则在成功还原 IDB 之后，查看配置的用户，并使用 *<DP_HOME>*\bin\omniusers 命令删除属于 IDB 备份所在的 Cell Manager 的用户。
8. 对于 Windows Cell Manager，在完成 IDB 还原会话后，使用 omniinetpasswd 命令在 Cell Manager 上的模拟数据库中重新创建 PGOSUSER 的用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。
   - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
   - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*

   注意: 可以从 *<DP_CONFIG>*\server\idb\idb.config 检索 PGOSUSER 值。
9. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \config\server\idb\idb.conf 以更正 "PGOSUSER" 参

数以指向当前的 Cell Manager IDB 应用程序服务器用户。

10. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \server\db80\pg\pg_ident.conf 以更正 "SYSTEM-USERNAME" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。

在无 IDB 恢复文件的情况下还原 IDB

以下限制适用：

- 您不能使用 omnioffl r 命令将脱机 IDB 还原到其他磁盘或目录。
- 通用标准已认证的配置不支持将 IDB 还原到其他 Cell Manager。有关通用标准的详细信息，请参阅通用标准指南部分。
- 要还原在重新安装 Data Protector 之前备份的 IDB，请删除 *<DP_SDATA>*/config/server/integ/config/idb/*.backup lo g 文件 (如果有)，然后还原 IDB。

以下先决条件适用:

- 在与 IDB 备份时相同的目录（在 Windows 系统中，必须分配相同驱动器号）上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 omnioffl r 命令的 -preview 选项查看要将文件还原到的位置。
- 在主机上重新安装 Cell Manager 之前，请确保将加密密钥文件 (用于加密的 IDB 备份) 从备份位置复制到主机上的临时位置 (例如: C:\tem p)。要复制加密文件，请执行以下操作:
  - **Windows**：
    copy <DP_DATA_DIR>\Config\Server\export\keys\IDB-<hostname>-keys.csv C:\temp
  - **Linux**：
    cp /var/opt/omni/server/export/keys/IDB-<hostname>-keys.csv /temp
- 如果可能，则将 media.log 文件从以前的安装移至安全位置。此文件将向您提供从上一次 IDB 备份以来有关所用介质的信息。如果归档日志文件不可用，则这对更新 IDB 很有用。
- 在 Cell Manager 和连接设备（首选用于 IDB 备份的设备）的系统上安装 Data Protector。
- 如果将 IDB 安装在 HPE Serviceguard 上，请在执行指导下的自动恢复之前将 DP 包置于维护模式。指导下的自动恢复完成后，请退出维护模式。
- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。
- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS_HPDP_AS, OBVS_HPDP_IDB 和 OBVS_HPDP_IDB_CP 群集组脱机。指导下的自动恢复完成后， OBVS_HPDP_AS 、 OBVS_HPDP_IDB 、 OBVS_HPDP_IDB_CP 和 OBVS_MCRS 群集组将自动联机。

要在 IDB 恢复文件不可用时还原内部数据库，请完成以下步骤:

此命令指导您完成以下过程：恢复 IDB 和重放从上一次 IDB 备份以来的归档日志文件。如果日志文件不可用，仍可以通过导入从上一次 IDB 备份以来的所有介质更新 IDB。

1. 对于加密的 IDB 备份，将您保存在临时位置的加密密钥文件复制到新安装的 Cell Manager
   - **Windows**：
     copy c:\temp\IDB-<hostname>-keys.csv <DP_Location>\server\export\keys
   - **Linux**： cp /temp/IDB-<hostname>-keys.csv /var/opt/omni/server/export/keys
2. 如果 Cell Manager 和介质代理位于不同的主机上，则在两台主机上都设置 omnirc 变量 OB2UNSECURE=1 。对于 Windows 系统，请在两台主机计算机上重新启动 INET 服务。
3. 使用 Data Protector GUI 配置设备。
4. 查找含有最新 IDB 备份的介质。
5. 将该介质插入设备中，然后使用以下命令显示介质的内容：

   omnimlist -dev device_name -slot SlotID

   对于 IDB 还原，需要介质 ID 和磁带客户机 ID 用于要还原的备份会话。
6. 使用以下命令显示有关设备配置的信息：

   omnidownload -dev device_name

   对于 IDB 还原，需要以下信息：
   - Mahost（介质代理主机）
   - 策略（数字）：可使用以下转换得到策略数字：1 表示独立设备、3 表示堆栈器设备、5 表示介质库设备、6 表示外部控制设备、8 表示 GRAU DAS 带库、9 表示 StorageTek ACS 带库以及 10 表示 SCSI 带库。
   - 介质类型（数字）：介质类型数字定义为 scsitab 文件中的介质类。有关位置，请参见对新设备的支持主题。
   - SCSI 地址
   - 机械手 SCSI 地址（仅当使用交换器库设备时）
7. 使用所得到的信息运行 omnioffl r 命令:

   omnioffl r -idb -policy PolicyNumber -type MediaTypeNumber [-ioctl RoboticsSCSIAddress] -dev SCSIAddress -mahost MAClientName -maid Medi umID -daid DiskAgentID -force

> **注意:** 对于加密的 IDB 脱机还原，使用 -keyfile 选项。有关此问题的详细信息，请参阅 omnioffl r。

例如，可以使用以下命令从介质 ID 为 0100007f:3a486bd7:0410:0001 且磁盘代理 ID 为 977824764 的备份会话还原 IDB，其中使用类型为 DLT、连接到系统 company.dot.com 且 SCSI 地址为 scsi0:1:2:0 的独立设备执行:

```
omnioffl r -idb -policy 1 -type 10 -dev scsi0:1:2:0 -mahost company.dot.com -maid 0100007f:3a486bd7:0410:0001 -daid 977824764 -force
```

8. (视情况而定) 如果您已按照上一步中所指定的在 Cell Manager 主机和介质代理主机上将 omnirc 变量 OB2UNSECURE 设置为 1，则从两台主机删除之前设置的 omnirc 变量 OB2UNSECURE。对于 Windows 系统，请在两台主机计算机上重新启动 INET 服务。
9. 如果 IDB 来自其他 Cell Manager，请如下运行 omnicellnamechange.pl 实用程序脚本:
   - 在 **Windows** 中: *<DP_HOME>*\bin\perl.exe <DP_HOME>\bin\omnicellnamechange.pl -newcmhost <newcm>
   - 在 **Linux** 中: /opt/omni/bin/perl *<DP_HOME>*\bin\omnicellnamechange.pl -newcmhost <newcm>
10. 如果安装了群集感知 Cell Manager，请在还原后将代理通信证书 (localhost_cert.pem) 和密钥 (localhost_key.enc) 文件从 *<DPDATA>*\config\server\sscertificates 目录复制到辅助节点 *<DPDATA>*\config\server\sscertificates 目录。
11. 如果 IDB 备份来自其他 Cell Manager，并且安装了支持群集的 Cell Manager，则在还原后将 Data Protector 服务移动到辅助节点上后，在辅助节点上运行以下命令
    - 在 **Windows** 中: *<DP_HOME>*\bin\omniusers -create_basic_cm_users
    - 在 **Linux** 中: /opt/omni/bin/omniusers -create_basic_cm_users
12. 如果 IDB 备份来自其他 Cell Manager，则在成功还原 IDB 之后，查看配置的用户，并使用 *<DP_HOME>*\bin\omniusers 命令删除属于 IDB 备份所在的 Cell Manager 的用户。
13. 如果重新安装 Windows Cell Manager，则必须在完成此 IDB 还原会话之后、执行下一次 IDB 备份之前重新创建 PGOSUSER 的用户信息。使用 omniinetpasswd 命令在 Cell Manager 上的模拟数据库中重新创建 PGOSUSER 的用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。
    - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
    - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*

> **注意:**可以从 *<DP_CONFIG>*\server\idb\idb.config 检索 PGOSUSER 值。

14. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \config\server\idb\idb.conf 以更正 "PGOSUSER" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。
15. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \server\db80\pg\pg_ident.conf 以更正 "SYSTEM-USERNAME" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。

从特定的 IDB 会话中还原 IDB

以下限制适用：

- 您不能使用 omnioffl r 命令将脱机 IDB 还原到其他磁盘或目录。
- 通用标准已认证的配置不支持将 IDB 还原到其他 Cell Manager。有关通用标准的详细信息，请参阅通用标准指南部分。
- 要还原在重新安装 Data Protector 之前备份的 IDB，请删除 *<DP_SDATA>*/config/server/integ/config/idb/*.backup lo g 文件 (如果有)，然后还原 IDB。

如果 IDB 恢复文件可用，则使用此过程可从最新备份以外的备份恢复内部数据库。

以下先决条件适用:

- 在与 IDB 备份时相同的目录（在 Windows 系统中，必须分配相同驱动器号）上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 omnioffl r 命令的 -preview 选项查看要将文件还原到的位置。
- 如果可能，则将 media.log 文件从以前的安装存储到安全位置。此文件将向您提供从上一次 IDB 备份以来有关所用介质的信息。如果归档日志文件不可用，则这对更新 IDB 很有用。
- 在 Cell Manager 和连接设备（首选用于 IDB 备份的设备）的系统上安装 Data Protector。
- 如果将 IDB 安装在 HPE Serviceguard 上，请在执行指导下的自动恢复之前将 DP 包置于维护模式。指导下的自动恢复完成后，请退出维护模式。
- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。
- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS_HPDP_AS, OBVS_HPDP_IDB 和 OBVS_HPDP_IDB_CP 群集组脱机。指导下的自动恢复完成后， OBVS_HPDP_AS 、 OBVS_HPDP_IDB 、 OBVS_HPDP_IDB_CP 和 OBVS_MCRS 群集组将自动联机。

完成以下步骤：

此命令指导您完成以下过程：恢复 IDB 和重放从上一次 IDB 备份以来的归档日志文件。如果归档日志文件不可用，则通过导入自上一次 IDB 备份以来所使用的所有介质，仍可以更新 IDB。

1. 使用以下命令检查所有备份：

   omnioffl r -idb -autorecover -logview -skiprestore

2. 通过运行以下命令，选择要从中还原的备份会话并执行 IDB 还原：

   omnioffl r -idb -autorecover -session SessionID -force

   > **注意:** 对于加密的 IDB 脱机还原，使用 -keyfile 选项。有关此问题的详细信息，请参阅 omnioffl r。

3. 如果 IDB 来自其他 Cell Manager，请如下运行 omnicellnamechange.pl 实用程序脚本:
   - 在 **Windows** 中**:** *<DP_HOME>*\bin\perl.exe <DP_HOME>\bin\omnicellnamechange.pl -newcmhost <newcm>
   - 在 **Linux** 中**:** /opt/omni/bin/perl *<DP_HOME>*\bin\omnicellnamechange.pl -newcmhost <newcm>
4. 如果安装了群集感知 Cell Manager，请在还原后将代理通信证书 (localhost_cert.pem) 和密钥 (localhost_key.enc) 文件从 *<DPDATA>*\config\server\sscertificates 目录复制到辅助节点 *<DPDATA>*\config\server\sscertificates 目录。
5. 如果 IDB 备份来自其他 Cell Manager，并且安装了支持群集的 Cell Manager，则在还原后将 Data Protector 服务移动到辅助节点上后，在辅助节点上运行以下命令
   - 在 **Windows** 中**:** *<DP_HOME>*\bin\omniusers -create_basic_cm_users
   - 在 **Linux** 中**:** /opt/omni/bin/omniusers -create_basic_cm_users
6. 如果 IDB 备份来自其他 Cell Manager，则在成功还原 IDB 之后，查看配置的用户，并使用 *<DP_HOME>*\bin\omniusers 命令删除属于 IDB 备份所在的 Cell Manager 的用户。
7. 对于 Windows Cell Manager，在完成 IDB 还原会话后，使用omniinetpasswd 命令在 Cell Manager 上的模拟数据库中重新创建 PGOSUSER 的用户信息。对于 Windows 群集，则需要在群集的所有节点上运行。
   - *<DP_HOME>*\bin\omniinetpasswd.exe -delete *<PGOSUSER>*
   - *<DP_HOME>*\bin\omniinetpasswd.exe -add *<PGOSUSER>*

   > **注意:**可以从 *<DP_CONFIG>*\server\idb\idb.config 检索 PGOSUSER 值。

8. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \config\server\idb\idb.conf 以更正 "PGOSUSER" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。
9. 如果 IDB 备份来自 Windows 上的其他 Cell Manager，则在成功还原 IDB 之后，编辑 \server\db80\pg\pg_ident.conf 以更正 "SYSTEM-USERNAME" 参数以指向当前的 Cell Manager IDB 应用程序服务器用户。

处理 DCBF 部分中的轻微 IDB 损坏

如果检测严重程度为“轻微”的内部数据库损坏，则它意味着某些 DC 二进制文件丢失或损坏。如果是这种情况，则不需要进行完整 IDB 恢复。可以通过从介质导入目录，方便地重新创建二进制文件。根据损坏类型选择恢复过程：

在 DC 二进制文件丢失的情况下进行恢复

组织 DC 二进制文件，以使对于每个介质都有一个二进制文件。如果某些 DC 二进制文件丢失，则某些介质的介质位置将指向不存在的文件。当浏览相关的文件系统时，就会显示错误消息。

完成以下步骤：

1. 从 omnidbcheck -bf 输出中，找出丢失的二进制文件的介质 ID。运行 omnimm -media_info medium-id 命令以获取介质的其他属性，如介质标签和介质池。
2. 运行 omnidbutil -fixmpos 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
3. 从介质导入编目，以重新创建二进制文件。

在 DC 二进制文件损坏的情况下进行恢复

如果 DC 二进制文件损坏，可以删除 DC 二进制文件并通过导入具有正确日志记录级别的介质来重新创建它们。删除文件所产生的唯一影响是某些介质位置将指向不存在的二进制文件，因此在浏览相关的文件系统时将显示错误消息。

完成以下步骤：

1. 从 omnidbcheck -dc 输出中，找出损坏的 DC 二进制文件的介质 ID。运行 omnimm -media_info medium-id 命令以获取介质的其他属性，如介质标签和介质池。
2. 找出受影响介质的 DC 二进制文件。DC 二进制文件的名称为：MediumID_TimeStamp.dat （在 MediumID 中），冒号“:”替换为“_”）。
3. 删除损坏的 DC 二进制文件。
4. 运行 omnidbutil -fixmpos 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
5. 从介质导入编目，以重新创建二进制文件。

通过导入介质更新 IDB

如果归档日志文件不可用，请通过导入上一次 IDB 备份使用的所有介质更新内部数据库。IDB 还原结束后即执行此操作。

完成以下步骤：

1. 启动 Data Protector 进程和服务。
2. 递增会话计数器。初始化和还原 IDB 后，计数器被设置为 0 。因此，任何新会话的会话 ID 都与那一天已启动的会话相同。

   以下命令将会话计数器设置为 200 ，对于大多数情况下此数值已足够:

   ```
   omnidbutil -set_session_counter 200
   ```

   如有必要，现在立即开始备份。
3. 导出和导入含有上一个 IDB 备份的介质。这样将产生有关上一个 IDB 备份的一致信息。
4. 导入（如果已在 IDB 中，则导出）上一个 IDB 备份和 IDB 恢复时使用的介质。有关使用的介质的列表，请参阅默认 Data Protector 服务器日志文件位置中的 media.log 文件。
5. 运行 omnidbcheck 命令。

此时应成功恢复完整 IDB。

设置用户

Data Protector 用户管理功能提供了一个安全层，可以防止未经授权的人员访问系统和数据。

安全基于与用户相关的安全概念。必须将要使用 Data Protector 的用户配置为 Data Protector 用户。具有丰富用户权限的用户组使您能够灵活地将安全要求映射到 Data Protector 用户配置中。

默认情况下，除备份所有者以外，备份的数据对其他用户隐藏。其他用户甚至看不到已经备份数据。如果愿意，可以通过适当的用户权限使数据对其他用户可见。

用户

要使用 Data Protector，您必须是 Data Protector 授权用户。因此，您需要一个 Data Protector 帐户，并限制对 Data Protector 和备份数据的未授权访问。在小型环境中，一个人足以胜任备份任务。Data Protector 管理员创建此帐户来指定用户登录名、用户可以从中登录的系统，以及 Data Protector 用户组成员身份。每当用户启动 Data Protector 用户界面或执行特定任务时，都会对该信息进行检查。

每个用户仅属于一个用户组。这可以定义用户的用户权限。

您可以配置 UNIX 和 Windows 用户：

UNIX

用户由登录名、UNIX 用户组和从中登录的系统定义。可以使用通配符。

Windows

用户由登录名、Windows 域或工作组以及从中登录的系统定义。可以使用通配符。

预定义用户 在初始安装之后，除了 admin 组以外，所有默认用户组均为空组。Data Protector 将以下用户添加到 admin 组:

Cell Manager	用户帐户	标注
Linux Cell Manager	Cell Manager 上的 root 用户 (root 、 *any group* 、 *Cell Manager host*)。	不应修改此用户帐户。CRS 后台程序和 Cell Manager 上的其他进程的正确操作需要此帐户。 最初仅允许此用户管理单元。要从任何其他客户机管理单元，请添加新用户。
Windows Cell Manager	在 Data Protector 安装期间指定的 CRS 服务帐户 (限于 Cell Manager 主机)。	CRS 服务帐户应当保留不变，除非修改 CRS 服务的登录参数。CRS 后台程序和 Cell Manager 上的其他进程的正确操作需要此帐户。
	安装 Cell Manager 的用户 (IDB AS 用户)。	此用户配置为 **IDB AS** 用户，并且可以从任何客户机管理该单元。建议在 Data Protector 安装完成之后修改此用户帐户。指定要从中管理单元的客户机，而不是允许从任何主机访问。如果要在此客户机上使用另一帐户，则添加此帐户，然后删除 **IDB AS** 用户，或仅从 Cell Manager 允许它。
	Cell Manager 上的本地系统帐户 (SYSTEM 、 NT AUTHORITY 、 *Cell Manager host*)。	在 CRS 服务配置为使用本地系统帐户登录时提供此帐户。

建议在环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。

> **重要说明** Admin 组的功能非常强大。Data Protector admin 用户组的成员在整个单元中有系统管理员功能。

用户组

用户组是具有相同权限的用户的集合。通过按照访问需要对用户分组，管理员可以简化用户配置。即，管理员可以将需要相同特定权限的用户放到同一组中。例如，用户可能需要监视单元中的会话、配置备份或还原文件的权限。

Data Protector 提供了默认用户组。可以使用提供的这些组、修改它们或者创建新组。

预定义用户组

为了简化配置，Data Protector 提供了三个具有以下用户权限的预定义用户组：

用户权限	管理员	操作员	用户
客户机配置	✓		
用户配置	✓		
设备配置	✓		
介质配置	✓	✓	
报告和通知	✓		
启动备份	✓	✓	
启动备份规范	✓	✓	
保存备份规范	✓		
作为 root 备份	✓		
切换会话所有权	✓	✓	
监控	✓	✓	
中止	✓	✓	
装载请求	✓	✓	
开始还原	✓	✓	✓
还原到其他客户机	✓		
从其他用户还原	✓	✓	
作为 root 还原	✓		
查看私有对象	✓	✓	
安全管理员	✓		
仪表板访问	✓	✓	
遥测订阅管理	✓		

在初始安装之后，除了 admin 用户组以外，所有预定义的组均为空组。

重要说明Admin 功能非常强大！Data Protector admin 用户组的成员在整个单元中有系统管理员权限。

在 Cell Manager 上设置的用户权限可确定 Data Protector Cell Manager GUI 或从中连接到 Cell Manager 的计算机的 GUI 上下文的可用性。例如，如果仅设置了“开始还原”用户权限，则在安装用户界面组件时仅有“还原”上下文可用。

用户权限

Data Protector 提供了一组丰富的用户权限来实现高级安全功能。可以使用以下用户权限：

- 客户机配置
- 用户配置
- 设备配置
- 介质配置
- 启动备份
- 启动备份规范
- 保存备份规范
- 作为 root 备份
- 切换会话所有权
- 监控
- 中止
- 装载请求
- 开始还原
- 还原到其他客户机
- 从其他用户还原
- 作为 root 还原
- 查看私有对象
- 安全管理员
- 仪表板访问
- 遥测订阅管理

Web 服务访问权限

Data Protector 使用 Web 服务进行内部通信和管理。默认情况下，所有用户都具有 Web 服务访问权限。

用户可以使用其 Web 用户名访问 Data Protector Web 服务，如 GUI (“用户”上下文，选择用户名以显示其属性) 和 CLI (omniusers -list) 中所列。

密码必须符合以下条件:

- 必须至少包含 8 个字符，最多包含 20 个字符
- 至少包含一个大写字母、一个小写字母和一个数字
- 至少包含以下特殊字符之一: 星号 (*)、句点 (.)、连字符 (-) 或下划线 (_)
- 不包含空格

从早期发布迁移到最新 Data Protector 版本时，具有 Web 访问权限的现有用户将作为两个用户迁移: 一个具有短名称，一个具有长名称。只有具有长名称的用户才能访问 Cell Manager GUI。

相关主题

- omniusers(1)

配置用户

可以执行以下任务:

添加用户

可将用户添加到现有的用户组中，从而对 Data Protector 配置用户。您最多可以添加 1000 个用户。

创建 LDAP 用户/用户组时，请考虑以下几点:

- 在 Data Protector 中配置 LDAP 用户和 LDAP 组时，请确保未将同一 LDAP 用户配置为单个实体，同时还要将其配置为 LDAP 组的成员。如果确实需要单独添加 LDAP 组的各个成员，则为避免此类冲突，管理员必须从 Data Protector 的配置中删除 LDAP 组。同样，如果要将一个 LDAP 组添加到 Data Protector 的配置中，则必须删除先前添加的组的各个成员。
- 将 LDAP 组添加到 Data Protector 时，如果该 LDAP 组的成员已作为 Data Protector 用户存在，则该用户将不再列为单个实体。
- 从 Data Protector 10.04 或更早版本升级时，需要将之前配置的所有 LDAP 用户再次添加为 Data Protector 用户。

需要具有用户配置权限才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要向其添加用户的用户组。
4. 单击**添加/删除用户**打开向导。
5. 在“添加/删除用户”对话框中，输入特定用户属性。在输入**名称**和**组/域**或者 **UNIX 组**时，确保输入与网络上现有用户相关的信息。
6. 按以下格式指定“密码”:
   - 必须至少包含 8 个字符，最多包含 20 个字符
   - 至少包含一个大写字母、一个小写字母和一个数字
   - 至少包含以下特殊字符之一: 星号 (*)、句点 (.)、连字符 (-) 或下划线 (_)
   - 不包含空格
7. 单击 **>>** 将此用户添加到用户列表。

   > **提示**还可以通过在用户列表中选择用户并单击 **<<** 来删除用户。

8. 单击**完成**退出向导。

用户即被添加到用户组，并具有此分配给此组的用户权限。

显示用户

使用此任务可以显示或查看特定用户属性。

需要成为 Data Protector 用户才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，双击要显示的用户。

特定用户属性即显示在结果区域中。

更改用户属性

在为 Data Protector 配置用户时，可以修改指定的用户属性。但通过将用户分配到另一个组会修改用户组，并因此修改用户权限。
具有 Web 访问权限的现有用户将在升级到最新 Data Protector 版本时作为两个用户迁移: 一个具有短名称，一个具有长名称。无法修改具有短名称的用户的属性。

需要具有用户配置权限，才能使用以下步骤更改用户属性:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要修改的用户。
5. 单击**属性**。

6. 输入要更改的属性。在修改**名称**和**组/域**或者 **UNIX 组**时，确保输入的信息与网络上的现有用户相关。
7. 单击“应用”。

将用户移动到另一个用户组

要更改单个用户的用户权限，请将该用户移动到不同用户组。

需要具有用户配置权限才能移动用户。执行以下步骤以移动用户:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要移动的用户。
5. 单击**移动**。
6. 在“目标组”列表中选择适当的用户组，并单击**确定**。

该用户即从原始用户组中删除，并添加到新用户组。新用户组的权限将分配给该用户。

删除用户

通过从配置用户的用户组删除用户，可以将该用户删除。

需要具有用户配置权限才能删除用户。执行以下步骤以删除用户:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要删除的用户并单击**删除**。
5. 确认操作。

用户即从用户组删除中，不能再用于 Data Protector。

> **提示**还可以在“添加/删除用户”对话框中删除用户。

重置用户密码

如果在用户创建期间未设置密码，则可以重置用户密码，以替换旧密码或指定密码。要更改用户密码，您必须具有以下用户权限:

- 要在不知道以前密码的情况下重置用户密码或重置其他帐户的密码，您需要具有用户配置权限。
- 如果您没有用户配置权限，则只能使用 omniusers -resetpass 命令重置自己的密码。如果之前未与该帐户关联，则该命令不需要旧密码。

执行以下步骤以重置用户密码:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 右键单击要重置密码的用户，然后单击“重置密码...”。
5. 在“密码”和“确认密码”字段中指定新密码。密码必须符合以下条件:
   - 必须至少包含 8 个字符，最多包含 20 个字符
   - 至少包含一个大写字母、一个小写字母和一个数字
   - 至少包含以下特殊字符之一: 星号 (*)、句点 (.)、连字符 (-) 或下划线 (_)
   - 不包含空格
6. 单击“确定”并在提示时确认重置密码。

清除用户密码

如果您具有以下用户权限，则可以清除或删除与用户关联的密码:

- 具有用户配置权限的管理员或用户可以清除所有用户的密码。
- 用户只能清除自己的密码。

执行以下步骤以使用 GUI 清除用户密码:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 右键单击要重置密码的用户，然后单击“清除密码...”。
5. 从“密码”字段中清除或删除密码。
6. 单击“确定”并在提示时确认清除密码。

> **重要说明**
>
> 禁止在用户管理上下文的“名称”、“域或组”和“客户机系统”字段中选择“<任意>”。要启用此选项，请在位于以下位置的全局选项

文件中将全局选项 EnableAnyOptionUserCtx 的值手动更改为 **1**:

- *Windows*： <PROGRAMDATA>\Config\Server\Options
- *Linux*: /etc/opt/omni/server/options 。

为用户管理上下文中的用户、组或客户机字段启用并使用“<任意>”选项，就会禁用或绕开安全功能，这会使系统面临更多的安全风险。使用此选项即表示您了解并同意承担所有相关风险，同样使 Micro Focus 免受损失。如果为用户管理上下文中的用户、组或客户机字段启用并使用“<任意>”选项，Micro Focus 建议客户采取相应的保护措施来防范与用户权限相关联的风险，Micro Focus 并不提供这些保护措施。若未实施相应的保护措施，您的系统可能面临更多的安全风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

配置用户组

可以执行以下任务:

添加用户组

默认 Data Protector 用户组通常就足够了。可以定义自己的用户组，从而根据需要在 Data Protector 环境中控制权限的分配。但是，在添加新组之前，通过更改现有组，检查是否可以满足要求。

必须具有“用户配置”权限才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，右键单击**用户**。
3. 单击**添加用户组**以打开向导。
4. 输入新组的名称和说明。
5. 单击“下一步”。
6. 设置新组的特定用户权限。
7. 单击**完成**退出向导。

新的空用户组将添加到 Data Protector 中。创建新的用户组后，您可以将角色分配给新创建的组。

> 您还可以为该新组分配与默认 admin 组相同的角色，并将用户添加到其中。但是，新创建的组中的用户将无法执行属于默认 admin 组的用户可执行的所有操作。例如，与新创建的组关联的用户不能删除 IDB 会话。

显示用户组

使用此过程可以查看特定用户组属性。

需要成为 Data Protector 用户才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击用户组。
4. 单击**属性**。

用户组的属性即显示在结果区域中。

更改用户权限

可以更改分配到任何用户组 (admin 用户组除外) 的用户权限，以便该组可以更好地满足您的要求。一个用户组必须至少分配一个用户权限。还可以修改组中每个用户的属性，例如用户所属的域，用户的真实姓名，以及用户所在的用户组。如果选择其中没有任何用户的组，则结果区域将显示该组的属性。如果选择其中有用户的组，则结果区域将列出该组中的用户。通过在要修改其属性的用户上单击，还可以修改用户组中每个用户的属性。无法更改 admin 用户组。

必须具有用户配置权限才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要修改的用户组。
4. 单击**属性**，然后单击**用户权限**选项卡。
5. 根据需要更改权限。要将所有用户权限分配到用户组，请单击**全选**。若须更改大量用户权限，请单击**取消全选**从用户组删除所有权限，然后将至少一个用户权限分配到组。
6. 单击“应用”。

指定的用户权限即分配到用户组和属于此组的所有用户。

删除用户组

可以删除不再需要的用户组 (admin 组除外)。无法删除 admin 用户组。

必须具有用户配置权限才能执行以下步骤:

1. 在“上下文列表”中，单击**用户**。

2. 在“范围窗格”中，展开**用户**。
3. 右键单击要删除的用户组。
4. 单击**删除**。

用户组及其所有用户即从 Data Protector 中删除。

Data Protector Inet 服务配置

在 Windows 系统上，通过 Data Protector Inet 服务启动备份和还原会话，并在默认情况下使用 Windows 本地用户帐户 system 运行。因此，可以使用相同的用户帐户进行备份或恢复会话。

集成

有些 Data Protector 集成要求使用 Windows 域用户帐户启动备份和还原会话。对于受支持的 Windows 操作系统，不允许执行此操作。因此，Data Protector 采用备用概念: 用户模拟。这意味着即使使用 Windows 本地用户帐户 SYSTEM 运行 Data Protector Inet 服务，该服务仍可以模拟 Windows 域用户帐户，因此可以使用该用户帐户启动集成代理。

要启用 Data Protector Inet 服务模拟，必须在备份规范或还原向导中指定 Windows 域用户帐户，且必须将用户帐户 (包括其密码) 保存在 Windows 注册表中。

使用 Windows 域用户帐户运行 Inet 服务

在某些情况下，Data Protector Inet 服务必须使用 Windows 域用户帐户运行:

群集环境

在群集中，必须为所有群集节点配置 Data Protector Inet 服务。这表示您需要将 Windows 域用户帐户作为 Inet 帐户使用。

使用 Windows 域用户帐户运行 Inet 服务时，您必须授予其以下 Windows 操作系统安全策略特权：

- Impersonate a client after authentication
- Replace a process level token

相关任务

- 为 Data Protector Inet 服务用户模拟设置用户帐户

为 Data Protector Inet 服务用户模拟设置用户帐户

对于在默认情况下使用 Windows 本地用户帐户 SYSTEM 运行的 Data Protector Inet 服务，可以将其指定为使用其他 Windows 域用户帐户启动会话。

以下先决条件适用:

- 授予用户适当的数据访问权限（例如应用程序数据）。
- 请确保将此用户添加到 Data Protector admin 或 operator 用户组。

使用 Data Protector GUI

要为 Data Protector Inet 服务用户模拟设置用户帐户，请完成以下步骤:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开 **Data Protector 单元**，然后展开**客户机**。
3. 右键单击客户机，然后单击**添加模拟**。
   要修改或删除用户，请分别单击**修改模拟**或**删除模拟**。
4. 在“选择客户机系统”页中，选择要配置 Data Protector Inet 服务用户模拟的客户机系统，然后单击“下一步”。
5. 在添加、删除或修改模拟页中，添加一个新的用户帐户，或者修改/删除现有用户帐户，然后单击**完成**。

需要时 Data Protector Inet 服务将使用保存于 Windows 注册表中的用户帐户。

使用 Data Protector CLI

- 要为某个 Data Protector 客户机上的用户模拟设置用户帐户，请使用 omniinetpasswd 命令。

登录到此客户机并运行: omniinetpasswd –add User@Domain Password

要为多个客户机上的用户模拟设置用户帐户，请使用 omnicc 命令。

登录到此客户机并运行:

omniinetpasswd –add User@Domain Password

- 要为多个 Data Protector 客户机上的用户模拟设置用户帐户，请使用 omnicc 命令。

登录到 Cell Manager 并运行： omnicc -impersonation -add_user -user User@Domain -host ClientName1 -host ClientName2 -host ClientName3 -passwd Password

设置 MoM

管理员可通过 Data Protector Manager-of-Managers (MoM) 概念管理大型环境 (也称为“企业备份环境”)，其中有多个 Data Protector 单元都集中来自单个点。

这种方式可以处理备份环境的几乎无限制增长：可以添加新单元，也可以将现有单元拆分为若干单元。

请注意，所有 MoM 客户机和 MoM Manager 都需要运行相同版本的 Data Protector。Manager-of-Managers 提供以下功能：

- 集中管理所有任务

  通过 Data Protector 可从一处配置、管理和控制企业备份环境。其中包括配置备份、还原、介质管理、监视和报告整个备份环境的状态。

- Centralized Media Management Database (CMMDB)

  （可选）环境中的所有单元都可以共享常用的中心数据库，以管理企业中的设备和介质。通过 CMMDB，可以在 MoM 环境中的若干单元之间共享高端设备和介质。这样使一个单元（使用 CMMDB）的所有设备都可由使用 CMMDB 的其他单元访问。

- 集中式许可证管理

  通过 Data Protector 可以配置整个 MoM 环境的集中式许可。所有 Data Protector 许可证都安装和保留在 MoM Manager 上。根据需要将许可证分发给特定的单元。

注意对于 Data Protector Express，不支持在 MoM 环境中跨 Cell Manager 重新分配套接字。

以下限制适用:

- MoM 环境中不支持调试日志收集。

CMMDB

在具有高端备份设备的大型多单元环境中，可能希望在几个单元之间共享设备和介质。通过对所有单元设置一个集中 MMDB 并对每个单元保留一个单独的 CDB，可以实现此目的。这样可以在保证多单元结构的安全功能的同时共享介质和设备。

如何共享介质

使用 CMMDB 时，介质只能归在这些介质上执行第一次备份的 Data Protector 单元拥有。介质所有者显示在介质视图中。当介质受到保护时，只能在介质上追加来自该单元的备份。每个其上数据受到保护的介质都具有相应信息，其中显示哪个单元当前拥有这些数据。保护到期后，介质即再次对其他单元可用。

如何初始化介质

如果磁带已由一个单元初始化，则只要磁带上没有任何受保护的数据，则任何其他单元都可以使用该磁带。如果库中加载了磁带但尚未将其初始化，则任何单元都可将其初始化（假定采用宽松策略，并且没有其他磁带可用）。介质分配规则以同样方式适用于共享磁带，但只有拥有可追加介质的单元才能追加这些介质。

重要说明请考虑以下几点：

- 集中式 MMDB 对许可有重大影响。MMDB 从本地变为远程之后，应立即从客户机单元中删除与从 MoM 管理器取得（验证）的库和设备关联的所有许可证。
- 企业环境中的单元必须能够访问 CMMDB 才能运行备份。例如，如果该单元与 MoM 单元之间发生网络故障，则会发生此情况。在 MoM 单元与其他 Data Protector 单元之间需要采用可靠的网络连接。
- 如果配置了 CMMDB，则无法使用自动复制同步功能。

相关主题

- 配置 MoM 环境
- 集中式许可

- 管理 MoM 环境

配置 MoM 环境

要配置 MoM 环境，必须:

- 为 MoM Manager 选择系统。所选择的系统必须是高度可靠的装有软件的 Data Protector Cell Manager。
- 在 MoM 单元上和每个预期的 MoM 客户机单元上安装必要的许可证。

MoM 环境配置过程由几个阶段组成。需要：

1. 设置 MoM 管理器 (将 Manager of Manager 用户界面组件推送到 MoM Cell Manager)。
2. 在 MoM Cell Manager 和 MoM 客户机 Cell Manager 之间建立安全通信。
3. 将 Data Protector 单元导入 MoM 环境。
4. 在 MoM 环境中每个单元上的 admin 用户组中创建将充当 MoM 管理员的 Data Protector 用户。
5. 重新启动 Data Protector 服务。

（可选）还可以配置集中式介质管理数据库，配置集中式许可，并分发 MoM 配置。

设置 MoM Manager

要设置企业环境，请将某个 Cell Manager 配置为 MoM Manager。

1. 在“上下文列表”中，单击**客户机**。
2. 在“操作”菜单中，单击“将 CM 配置为 Data Protector Manager-of-Managers Server”。
3. 重新启动 Data Protector 服务。
4. 通过在 Data Protector 程序组中选择“Data Protector Manager-of-Managers”启动 MoM 用户界面。

   或者，从 Data_Protector_home\bin 目录运行 mom 命令。有关 mom 命令的详细信息，请参阅 omnigui 手册页或《Data Protector 命令行界面参考》。

建立安全通信

通过运行以下命令在 MoM Cell Manager 和 MoM 客户机 Cell Manager 之间建立安全通信:

```
/opt/omni/bin/omnicc -secure_comm -configure_peer <FQDN of MoM Cell Manager>
```

向单元添加 MoM 管理员

MoM 管理员可以在企业环境中的所有单元中执行管理任务。

MoM 环境中每个 Cell Manager 上的 admin 用户组都需要包含特定用户。例如，可能包含称为 MoM_Admin 的用户。此用户将是 MoM 管理员。

执行以下步骤:

1. 使用 Data Protector Manager，以 admin 用户组成员的身份 (需要 User configuration 用户权限) 连接到 MoM 环境中的每个 Cell Manager。
2. 向 Data Protector admin 用户组添加将成为 MoM 管理员的用户。

将 Data Protector 单元导入 MoM 环境

将单元导入 MoM 环境中，即可用 MoM 管理器集中管理该单元。

群集客户机用其虚拟服务器名称向 MoM 管理器标识自身。如果在 MoM 环境中导入群集，则只需使用其虚拟服务器名称。

活动用户必须是要导入的单元的 Cell Manager 上 Admin 用户组的成员。完成以下步骤：

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 右键单击**企业客户机**，然后单击**导入 Cell Manager**。
3. 选择要导入的 Cell Manager，然后单击**完成**。

在 MoM 中重新启动 Data Protector 服务

配置 MoM 环境之后，将通知您重新启动 Data Protector 服务。

如果使用 Windows Service Control Manager 在 Cell Manager 上停止和启动服务，则系统将仅保留数据库日志的当前和以前的副本。使用 omnisv 命令将保存所有以前的数据库日志。

停止 **Data Protector** 服务

在以下位置停止 Data Protector 服务:

- 非群集环境中的 Cell Manager

  运行命令：omnisv -stop.

- Serviceguard 上的 Cell Manager

运行命令：cmhaltpkg PackageName ，其中 PackageName 是 Data Protector 群集包的名称。

此命令用于停止 Data Protector 包，并卸除 Data Protector 共享卷组。

- Symantec Veritas Cluster Server 上的 Cell Manager

  使 Data Protector 应用程序资源脱机。

- Microsoft 群集服务器上的 Cell Manager

  使 OBVS_HPDP_AS, OBVS_HPDP_IDB, 和 OBVS_HPDP_IDB_CP 群集组脱机 (在活动节点上使用 Cluster Administrator 实用程序)。

启动 Data Protector 服务

在以下位置启动 Data Protector 服务:

- 非群集环境中的 Cell Manager

  运行命令：omnisv -start

- Serviceguard 上的 Cell Manager

  使用 cmrunpkg -n NodeNamePackageName 命令重新启动 Data Protector 包。

- Symantec Veritas Cluster Server 上的 Cell Manager

  使 Data Protector 应用程序资源联机。

- Microsoft 群集服务器上的 Cell Manager

  使用 Cluster Administrator 实用程序使 OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP, and OBVS_MCRS 群集组联机。

配置 CMMDB

如果想拥有中心介质管理，则要设置 CMMDB。如果不设置 CMMDB，则每个单元将拥有自己的 IDB。

配置期间，有一个本地介质管理数据库将合并到 CMMDB 中（如果选择这样做）。可以决定每个单元将使用 CMMDB 还是其自身的本地 MMDB。

重要说明:

- 配置了 CMMDB 并开始使用它之后，即无法将其拆分回相应的本地 MMDB 中。不应尝试恢复 MMDB 的旧状态，而要从头创建新 MMDB。
- 全局选项 DeleteUnprotectedMediaFreq 的值会影响服务器上介质维护的频率，默认情况下设置为 **1**。根据您希望介质维护发生的频率来编辑此选项的值。
  - 对于具有 CMMDB 的 MoM 环境，取决于 CMMDB 服务器上设置的选项值，仅在 CMMDB 服务器上进行介质维护 (删除不受保护的介质)。
  - 对于没有 CMMDB (带有 MMDB) 的 MoM 环境，取决于每个 Cell Manager 服务器上设置的选项值，对所有 Cell Manager 进行介质维护。

如果要配置新单元（并且尚未配置设备和介质），则不需要合并数据库。只需要将单元与已配置了设备和介质的 CMMDB 合并。

要配置 CMMDB，请确保以下内容:

- 检查是否所有单元中的 Data Protector Cell Manager 都已安装了相同版本的 Data Protector，并且其正在运行。
- 确认在要添加到 CMMDB 的任何单元上没有运行备份、还原或介质管理会话。

配置阶段

- 在客户机单元上配置 CMMDB
- 在 MoM Manager 上配置 CMMDB

在客户机单元上配置 CMMDB

要在客户机单元上配置 CMMDB，请完成以下步骤:

1. 以 admin 用户组成员的身份登录客户机单元的 Cell Manager。
2. 创建包含 MMDB 服务器的名称（完全限定）的文件。在 Windows 系统中，以 Unicode 格式保存文件：

   Windows 系统： Data_Protector_program_data\Config\server\cell\mmdb_server

   UNIX 系统： /etc/opt/omni/server/cell/mmdb_server

3. 启用 MoM Manager 以建立单元连接，方法是修改 pg_hba.conf 文件，该文件位于内部数据库位置的 pg 目录中。

   在文本编辑器中打开该文件，并添加以下行：

   host hpdpidb hpdpidb_app MoM_Server_IP_Address/32 trust

添加到下行之后

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5
```

保存文件。

> **注意**如果 MoM 客户机上的 Cell Manager 是群集环境的一部分，则需要在 MoM 客户机的 Cell Manager 上的 pg_hba.conf 文件中指定所有群集节点的 IP 地址 (每个节点一个行项目) 或群集的子网。

在文本编辑器中打开该文件，并添加以下行：

```
host hpdpidb hpdpidb_app Cluster_Subnet trust
```

添加到下行之后

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5
```

保存文件。

4. 重新启动 Data Protector 服务。
5. 通过运行以下命令更新配置文件：

   ```
   omnicc -update_mom_server
   ```

对于要将其 MMDB 合并到 CMMDB 的所有客户机单元重复这些步骤。

在 MoM Manager 上配置 CMMDB

要在 MoM Manager 上配置 CMMDB，请执行以下步骤:

1. 运行以下命令，将本地 MMDB 合并到 CMMDB 中：

   ```
   omnidbutil -mergemmdb MoM_Client_Cell_Manager_Hostname
   ```

   确保 IDB 服务 (hpdp-idb) 端口 7112 在执行命令期间在 MoM Manager 和客户机 Cell Manager 上均打开。在合并完成后可关闭端口。

2. 运行以下命令，同步本地 CDB：

   ```
   omnidbutil -cdbsync MoM_Client_Cell_Manager_Hostname
   ```

3. 编辑介质池和设备的重复名称。如果两个单元上都存在默认池，则对于默认池始终会发生这种重复现象。重复名称的名称中附加有 "_N"，其中，N 表示数字。在这种情况下，手动更改使用这些设备的备份规范以使用新设备名称。
4. *如果在合并之前已在客户机 Cell Manager 上配置了密码，则应用。*编辑从客户机 Cell Manager 合并的“StoreOnce 备份系统”和“数据域提升”类型的“备份到磁盘”设备，以再次配置其密码。此步骤是必需的，因为这些密码是使用在客户机 Cell Manager 中生成的密钥加密的，这些密钥在 MoM Cell Manager 中不再有效。

对于要将其 MMDB 合并到 CMMDB 的所有客户机单元重复这些步骤。

相关主题

- 有关 DeleteUnprotectedMediaFreq 全局选项的详细信息，请参阅最常用的全局选项。

集中式许可

集中式许可意味着在 MoM 管理器上配置所有许可证，并且可以根据需要将这些许可证分配给特定单元。集中式许可简化了许可证管理。MoM 管理员对 MoM 环境中的所有单元执行许可管理，其中包括分发和移动许可证。

设置集中式许可为可选操作。作为替代，也可以在每个 Cell Manager 上安装单独的许可证。这些许可证仅限安装它们的单元使用，并且所有许可管理任务都必须在本地执行。

设置集中式许可

设置集中式许可可简化企业环境中的许可证管理。

如果要将现有 Data Protector 单元合并到 MoM 环境中，则向 *Password Delivery Center* 发送请求，以将许可证从现有 Cell Manager 移至新的 MoM Manager。

1. 登录 MoM Manager，然后创建 licdistrib.dat 文件:

   Windows 系统： Data_Protector_program_data\Config\server\cell\licdistrib.dat

   UNIX 系统： /etc/opt/omni/server/cell/licdistrib.dat
2. 登录 MoM 环境中的每个 Cell Manager，然后用 MoM Manager 的名称创建 lic_server 文件:

   Windows 系统： Data_Protector_program_data\Config\server\cell\lic_server

   UNIX 系统： /etc/opt/omni/server/cell/lic_server
3. 在做出更改的每个 Cell Manager 上停止并重新启动 Data Protector 服务。
4. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
5. 在范围窗格中，右键单击要更改的许可信息所在的 Cell Manager，然后单击**配置许可**以打开向导。此时将显示对所选 Cell Manager 可用的许可证的类型和数量。

   > **注意**用虚拟主机名标识群集客户机。
6. 单击**远程**选项，将许可从本地更改为远程。此时“已用”列更改为“已分配”。
7. 修改许可证配置。修改过程中只有“已分配”列可用。
   - 要释放（丢弃）许可证类型，因此增加可用许可证的数量，请在“已分配”列中减去其相应的数字。
   - 要分配许可证类型，请在“已分配”列中增加其相应的数字。
8. 单击**完成**应用配置。
9. 对于要为其设置集中式许可的所有 Cell Manager 重复上述步骤。
10. 使用 omnisv -stop 和 omnisv -start 命令停止并重新启动 Data Protector 进程。

    如果在 Serviceguard 上配置了 Cell Manager，则运行 cmhaltpkg PackageName 命令停止 Data Protector 包，然后运行 cmrunpkg -n NodeNamePackageName 将其启动，其中， PackageName 是 Data Protector 群集包的名称。

    如果在 Symantec Veritas Cluster Server 上配置了 Cell Manager，则使 Data Protector 应用程序资源脱机，然后使 Data Protector 应用程序资源联机。

在做出更改的每个 Cell Manager 上，停止并重新启动 Data Protector 服务之后，更改即生效。

> **注意**Data Protector 每小时用 MoM Manager 检查一次许可证配置。当通信出现问题或 MoM Manager 不可用，将该许可状态保持 72 小时。如果此后 72 小时内未解决问题，则使用本地许可证。

停用集中式许可

可以停用集中式许可并将其转换为本地许可。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 在范围窗格中，右键单击要停用其集中式许可的 Cell Manager，然后单击**配置许可**以打开向导。此时将显示对所选 Cell Manager 可用的许可证的类型和数量。

   > **注意**用虚拟主机名标识群集客户机。

3. 单击**本地**选项，将许可从远程更改为本地。
4. 单击**完成**应用配置。
5. 对于要停用其集中式许可的所有 Cell Manager 重复上述步骤。
6. 登录 MoM Manager，然后装载位于默认 Data Protector 服务器配置目录的 cell 目录。
7. 例如，将 licdistrib.dat 文件重命名为 licdistrib.old.

在进行更改的 MoM Manager 和所有 Cell Manager 上使用 omnisv -stop 和 omnisv -start 命令停止并重新启动 Data Protector 服务后，更改将生效。

如果在 Serviceguard 上配置了 Cell Manager，则运行 cmhaltpkg PackageName 命令停止 Data Protector 包，然后运行 cmrunpkg -n NodeNamePackageName 将其启动，其中， PackageName 是 Data Protector 群集包的名称。

如果在 Symantec Veritas Cluster Server 上配置了 Cell Manager，则使 Data Protector 应用程序资源脱机，然后使 Data Protector 应用程序资源联机。

管理 MoM 环境

通过 MoM 管理器可以从一处配置、管理和控制企业备份环境。

在 MoM 用户界面中，可以导入和导出单元，在各单元之间移动客户机，以及将 MoM 配置分发到环境中的其他单元。

用本地管理员的相同方式在 MoM Manager 上执行其他任务。按照标准过程配置备份和还原、管理特定单元的设备和介质、配置 Data Protector 用户和用户组、添加客户机、监视正在运行的会话和备份环境的状态以及配置报告和通知。

注意只能从相应的 Cell Manager 而非 MoM Manager 配置连接到单独单元中客户机的设备。只能从 MoM Manager 配置直接连接到 Cell Manager 的设备。

导入单元

将单元导入 MoM 环境中，即可用 MoM 管理器集中管理该单元。

群集客户机用其虚拟服务器名称向 MoM 管理器标识自身。如果在 MoM 环境中导入群集，则只需使用其虚拟服务器名称。

活动用户必须是要导入的单元的 Cell Manager 上 Admin 用户组的成员。执行以下步骤：

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 右键单击**企业客户机**，然后单击**导入 Cell Manager**。
3. 选择要导入的 Cell Manager，然后单击**完成**。

导出单元

导出单元将从 MoM 环境中删除该单元。

群集客户机用其虚拟服务器名称向 MoM 管理器标识自身。如果在 MoM 环境中导出群集，则只需使用其虚拟服务器名称。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 在范围窗格中，右键单击要导出的 Cell Manager，然后单击**导出 Cell Manager**。
3. 确认选择。

在单元间移动客户机系统

通过 Data Protector 可以在单元之间移动系统。在此过程中，Data Protector 执行以下操作：

- 检查是否在任何备份规范中配置了要移动的客户机，并从初始 Cell Manager 上配置的备份规范中删除属于此客户机的所有备份客户机，同时其他客户机的备份对象保留原样。因此，Data Protector 确保将客户机移至另一个单元之后，备份规范中没有剩余的孤立备份对象。
- 检查系统上是否配置了任何设备，并且指导您完成将设备移至另一个系统的步骤。
- 检查此系统上的设备中是否有已使用的介质，并且指导您完成移动介质的步骤。

完成以下步骤：

1. 运行以下命令，在要移动的客户机上配置目标 Cell Manager 证书:

   omnicc -secure_comm -configure_peer <target CM hostname> [-accept_host]

2. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
3. 展开要移至另一个单元的客户机系统所在的 Cell Manager。
4. 右键单击该客户机系统，然后单击**将客户机系统移至其他单元**以打开向导。

5. 选择目标 Cell Manager。
6. 单击**完成**移动客户机。

停用集中式许可

Data Protector 允许您在 MoM 环境中的所有 Cell Manager 上创建常用用户类规范、Holidays 文件设置、全局选项设置和保管。

在 MoM Manager 上创建所需的用户类规范、假期文件设置和全局选项设置，然后完成以下步骤。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 右键单击**企业客户机**，然后单击**分发配置**。
3. 在“分发配置”对话框中，选择配置类型以及要向其分发所选配置的 Cell Manager。
4. 单击**完成**分发配置。

配置 Data Protector 用户

可将用户或用户组添加到 MoM 环境，就像对单个 Cell Manager 那样。确保满足以下条件:

- 所有 Cell Manager 中已添加 MOM 服务器用户，并为 MoM 服务器用户设置了密码。
- 所有相应的 Cell Manager 用户均已添加至 MOM 服务器客户机，并在 MoM 服务器中设置了其密码。

要使用新用户更新所有 Cell Manager，请完成以下过程:

1. 在 Data Protector Manager-of-Managers 中，在上下文列表中单击**用户**。
2. 选择要向其添加用户的 Cell Manager。
3. 在“编辑”菜单中，如果要添加新用户，则单击**添加**，然后选择**用户**；如果要添加新用户组，则选择**用户组**。
4. 输入所需的信息，然后单击**完成**。

将用户添加至其他单元

可以将现有用户添加到 MoM 环境中的其他单元。该用户将自动添加到目标 Cell Manager 上与其在源 Cell Manager 上所处相同的用户组。

> **注意**如果目标 Cell Manager 上不存在用户在源 Cell Manager 上所在的组，则无法将该用户添加到目标单元。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“用户”。
2. 在范围窗格中，展开 Cell Manager，然后展开该用户所在的组。
3. 右键单击该用户，然后单击**向其他单元添加用户**以打开向导。
4. 选择目标 Cell Manager。
5. 单击**完成**退出向导。

从单元中删除用户

可以从 MoM 环境的单元中删除用户。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“用户”。
2. 在范围窗格中，展开 Cell Manager，然后展开该用户所在的组。
3. 右键单击该用户，然后单击**从单元中删除用户**以打开向导。
4. 选择要从中删除用户的 Cell Manager。
5. 单击**完成**退出向导。

管理特定单元的设备和介质

可以配置企业环境中任何单元的设备和介质。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 选择要管理的介质或设备所在的单元。
3. 在**工具**菜单中，单击**设备和介质管理**。

   此时将打开 Data Protector Manager，并显示“设备和介质”上下文。
4. 像本地管理员那样配置设备和介质。

> **注意**只能从相应的 Cell Manager 而非 MoM Manager 配置连接到单独单元中客户机的设备。只能从 MoM Manager 配置直接连接到 Cell Manager 的设备。

管理特定单元的 IDB

可以管理企业环境中任何单元的 IDB。

1. 在 Data Protector Manager-of-Managers 的上下文列表中，单击“客户机”。
2. 选择要管理的 Cell Manager。
3. 在**工具**菜单中，单击**数据库管理**。在“内部数据库”上下文中，像本地管理员那样执行数据库管理任务。

设备

Data Protector 定义具有 Data Protector 使用情况属性的物理设备，并对其进行建模。多个 Data Protector 设备定义可以引用同一个物理设备。通过此设备概念，可方便灵活地配置设备，并在备份规范中使用这些设备。

什么是备份设备？

一种物理设备，被配置为与可从存储介质读取数据和向其写入数据的 Data Protector 配合使用。例如，此设备可以是独立的 DDS/DAT 驱动器或库。

有关 Data Protector 支持的设备列表，请参阅《Data Protector 设备支持矩阵》。可使用 scsitab 文件配置不受支持的设备。

某些备份设备（如磁带驱动器）受特定 Data Protector 许可证管辖。

配置备份设备

完成准备部分之后，可以配置备份设备，使其与 Data Protector 配合使用。

建议让 Data Protector 自动配置备份设备。Data Protector 可以自动配置最常用的备份设备（包括库）。虽然仍需要为备份会话准备介质，但 Data Protector 可确定设备的名称、策略、介质类型、介质策略和设备文件或 SCSI 地址，并且还可配置驱动器和插槽。

也可以手动配置备份设备。配置备份设备的方式取决于设备类型。

可使用未在发行说明中列为受支持设备的设备。将使用 scsitab 文件配置不支持的设备。

> **注意**外部控制是控制 Data Protector 未知的库的一种方法。如果 Data Protector 不支持某个特定设备，则用户可以编写相应的脚本/程序，以运行机械手控制，将介质从特定插槽加载到指定的驱动器中。通过引用特殊脚本，可以将库配置为外部控制。

备份设备的类型

Data Protector 支持以下可配置的设备类型（取决于已安装的组件）：

- 独立
- 备份到磁盘设备
- SCSI 库
- 堆栈器
- 箱盒设备
- 介质库
- 独立文件设备
- 文件库设备
- 外部控制
- ADIC/GRAU DAS 库
- StorageTek ACS 库

独立

独立设备是包含一个驱动器的简单设备，该驱动器一次从一个介质读取或写入一个介质（如 DDS 或 DLT）。这些设备用于小规模备份。介质充满后，操作员必须手动将其替换为新介质，备份才能继续。因此，独立设备不适合大规模的无人看管备份。

备份到磁盘设备

“备份到磁盘”(B2D) 设备是基于磁盘的存储设备，与 Data Protector 介质库或文件库设备相比，可提供附加功能，如通过多个主机 (*网关*) 进行访问，或重复数据删除 (具体取决于设备类型)。

SCSI 库

SCSI 库设备是大型备份设备，也称为自动加载器。这些设备由设备存储库中的大量介质磁带盒组成，并且可以有多个驱动器，一次处理多个介质。大多数库设备在驱动器变脏时还可以自动清洗驱动器。

典型的库设备中，每个驱动器和库的一个机械手机构（可将介质从插槽移至驱动器，然后将其移回）有一个对应的 SCSI ID（Windows 系统）或设备文件（UNIX 系统）。（例如，一个由四个驱动器组成的库拥有五个 SCSI ID，四个用于驱动器，一个用于机械手装置）。

介质存储在设备存储库的插槽中。Data Protector 向每个插槽分配一个数字，从一开始。管理库时，要使用其数字引用插槽。

驱动器索引标识驱动器在库中的机械位置。索引编号与机械手控制紧密相关。库机械手只了解驱动器索引编号，而没有有关驱动器 SCSI 地址的信息。驱动器索引是一个顺序整数（从 1 开始），必须与驱动器的 SCSI 地址相结合。SCSI 库、Commandview TL 的许多 Web 界面或 SCSI 库的控制面板将从“0”开始对驱动器编号。驱动器 "0" 在 Data Protector 设备配置中无效，第一个驱动器必须始终为 "1"。

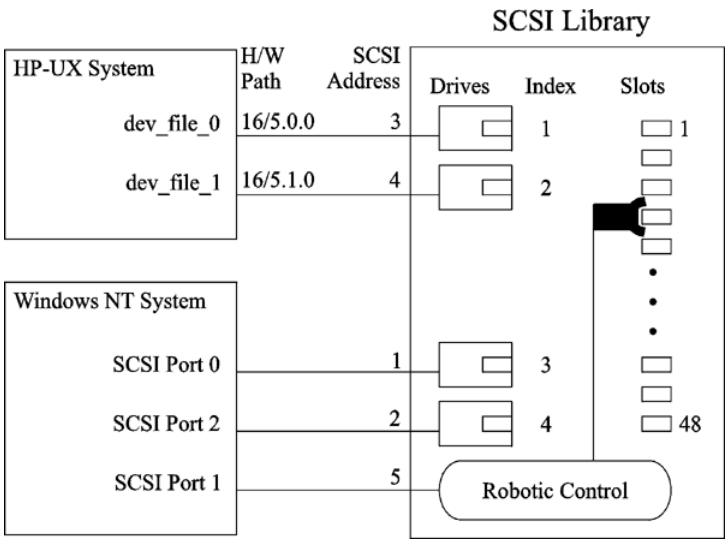
例如，对于四个驱动器的库，驱动器索引为 1、2、3 和 4。如果库中只有一个驱动器，则驱动器索引为 1。

驱动器索引必须与相应的 SCSI 地址匹配。这意味着需要配置各对内容：

SCSI address_A 对应于索引 1，SCSI address_B 对应于索引 2，以此类推。

配置箱盒设备时，还要指定此类型的设备。

驱动器索引到 SCSI 地址的映射



堆栈器

堆栈器是一个单独的设备，通常其中只有一个驱动器。它顺序而非随机加载介质，因此建议使用宽松介质分配策略。堆栈器从“堆栈”（其存储库）中提取介质，并将介质插入其驱动器中。这种交换始终仅限于弹出已在驱动器中的介质以及插入来自堆栈的下一个介质。自动完成加载，但必须手动加载第一个介质。磁带已满后将弹出，并自动加载下一个磁带。堆栈器箱盒中的所有磁带用完后，必须手动卸载箱盒，然后插入下一个箱盒。仍然必须将第一个磁带手动加载到驱动器中。

如果没有介质，则不会中止备份或还原会话，而是将发出一个装载请求。如果在一个超时周期内不更改堆栈器箱盒，则将不会中止整个会话。

箱盒设备

箱盒设备将许多介质组成一个单位，称为箱盒。通过箱盒，可以比使用许多单独的介质更方便地处理大量数据。箱盒中每个介质上的操作都由 Data Protector 完全控制。可以将 XP DAT 24x6 配置为箱盒设备。

介质库

介质库是一种库设备。它可以包含光盘或文件介质。如果设备用于容纳文件介质，则将其称为文件介质库设备。在初始配置期间定义设备将容纳的介质类型。

如果要在 UNIX 上运行光盘介质库，则需要为每个交换器插槽或盘面配置一个 UNIX 设备文件。

独立文件设备

独立文件设备是指定目录中的一个文件，您向该文件备份数据而非写入磁带。

文件库设备

文件库设备由一组目录组成，您向这组目录备份数据而非写入磁带。

外部控制

外部控制是控制 Data Protector 未知的库的一种方法。如果 Data Protector 不支持某个特定设备，则用户可以编写相应的脚本/程序，以运行机械手控制，将介质从特定插槽加载到指定的驱动器中。通过引用特殊脚本，可以将库配置为外部控制。

ADIC/GRAU DAS 库

ADIC/GRAU DAS 库是一种大型的库 (silo)。它用于备份数据量极大，且存储数据所需的介质数量也很大的复杂环境中。它可以处理成百上千个磁带。通常，ADIC/GRAU DAS 库可以容纳多种类型的备份驱动器和数千个介质插槽，所有这些都由内部机械手装置提供服务，并通过特殊的库控制单元进行控制。可以将库中的一组专用介质分配给应用程序，以便可以在 Data Protector 与其他应用程序之间共享该库。

可以从 Data Protector 用户界面执行所有介质操作。对于采用可识别格式的介质，Data Protector 以介质类型的形式显示该格式，如 tar。对于采用无法识别格式的介质，介质类型为 foreign。

介质管理数据库跟踪所有 Data Protector 和非 Data Protector 介质，无论驻留 (介质在设备存储库中) 还是非驻留 (介质不在设备存储库中)，同时提供成熟的覆盖保护。Data Protector 不会覆盖采用可识别格式的含数据介质。但是，无法保证使用相同介质的某些其他应用程序不会覆盖磁带上的 Data Protector 数据。建议 Data Protector 所使用的介质不要由任何其他应用程序使用，反之亦然。

介质的实际位置由 DAS 服务器维护，该服务器使用其 volser 跟踪该位置。在存储库中到处移动介质时，并非每次都向该介质分配相同的物理插槽。因此，处理介质时不能依赖于插槽号，而是要依赖于条形码 (volser)。

使用驱动器所设置的次数之后，ADIC/GRAU DAS 库可以自动清洗其驱动器。但是，建议不要这么做，因为驱动器清洗将中断当时正在运行的会话，从而导致该会话失败。如果要使用库的清洗功能，则必须确保在没有 Data Protector 会话运行时执行驱动器清洗。

> **重要说明**必须为每种介质类型创建一个逻辑 Data Protector 库。虽然 ADIC/GRAU 或 STK ACS 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。

StorageTek ACS 库

StorageTek Automated Cartridge System (ACS) 库是一种机械手库 (silo)。它用于备份数据量极大，且存储数据所需的介质数量也很大的复杂环境中。它可以处理数百个磁带。可以将设备中的一组专用介质分配给应用程序，以便可以在 Data Protector 与其他应用程序之间共享该库。

通常，此类设备有多种类型的备份驱动器和数千个介质插槽，所有这些都由内部机械手机构提供服务，并且通过 ACS Library Server (ACSLS) 软件进行控制。由 Data Protector 发起的与介质和与设备相关的操作通过用户界面传递到 ACSLS，后者随后直接控制机械手，并执行介质的移动和加载。

正确安装和配置库后，通过 Data Protector 可在备份和还原会话期间轻松地处理介质。可以从 Data Protector 用户界面执行所有介质操作。对于采用可识别格式的介质，Data Protector 以介质类型的形式显示该格式，如 tar。对于采用无法识别格式的介质，介质类型为 foreign。

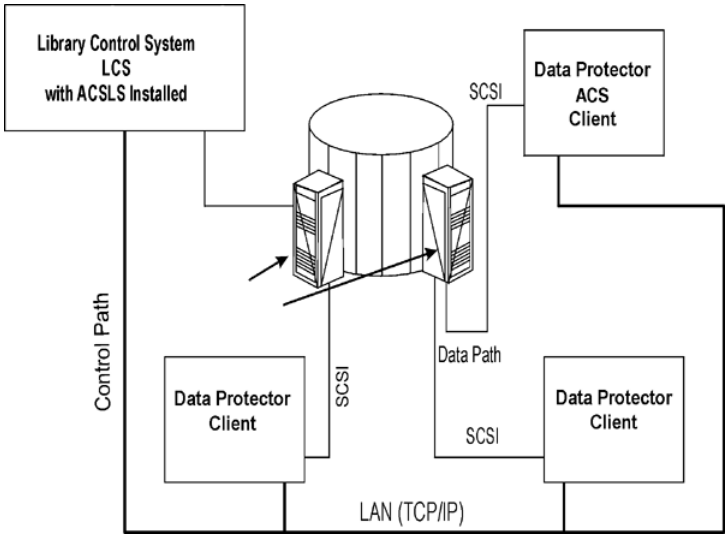
介质管理数据库跟踪所有 Data Protector 和非 Data Protector 介质，无论驻留 (介质在设备存储库中) 还是非驻留 (介质不在设备存储库中)，同时提供成熟的覆盖保护。Data Protector 不会覆盖采用可识别格式的含数据介质。但是，无法保证使用相同介质的某些其他应用程序不会覆盖磁带上的 Data Protector 数据。建议 Data Protector 所使用的介质不要由任何其他应用程序使用，反之亦然。

介质的实际位置由 ACS 服务器维护，该服务器使用其 volser 跟踪该位置。在存储库中到处移动介质时，并非每次都向该介质分配相同的物理插槽。因此，处理介质时不能依赖于插槽号，而是要依赖于条形码 (volser)。

使用驱动器所设置的次数之后，StorageTek ACS 库可以自动清洗其驱动器。但是，建议不要这么做，因为库驱动器清洗将中断当时正在运行的会话，从而导致该会话失败。如果要使用库的清洗功能，则必须确保在没有 Data Protector 会话运行时执行驱动器清洗。

重要说明必须为每种介质类型创建一个逻辑 Data Protector 库。虽然 ADIC/GRAU 或 STK ACS 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。

Data Protector 与 StorageTek ACS 库的集成



Data Protector 重复数据删除存储

Data Protector 重复数据删除存储是一种新的基于软件的重复数据删除存储设备。它执行重复数据删除，并仅存储非重复数据和对重复数据块的引用。这确保了高效利用存储空间和网络带宽。它提供源端、目标端和服务器端重复数据删除。这种新设备旨在提供 PB 级的容量。截至目前，它已通过高达 250 TB 的测试，可以安装在物理机和虚拟机上的标准 Windows Server 2016/2019 和 Linux 系统 (RHEL、SLES) 上。

重复数据删除服务器提供三种类型的重复数据删除:

- **服务器端重复数据删除**: 当您启用此选项时，重复数据删除将在安装了 MA 的系统上进行。此后，只有经过重复数据删除的数据才会传输到安装了重复数据删除存储组件的系统 (备份存储所在的重复数据删除服务器)。
- 目标端重复数据删除: 当您禁用服务器端重复数据删除选项时，将启用此选项。数据从安装了 MA 的系统传输到安装了重复数据删除存储组件的系统 (连接备份存储的重复数据删除服务器)，然后在该重复数据删除服务器上进行重复数据删除。
- 源端重复数据删除: 只有在同一客户机系统上安装了 MA 和 DA 时，才能启用此选项。在此客户机上执行重复数据删除，并且将经过重复数据删除的数据传输到安装了重复数据删除存储组件的客户机。

云存储支持

Data Protector 重复数据删除存储支持以下常用公共供应商所提供的扩展云存储支持:

- Amazon S3
- Azure
- Google Cloud
- S3 兼容云目标

每个带有云存储的重复数据删除存储都有一个本地缓存，可以实现更快的数据传输。

先决条件

完成以下先决条件:

- 确保重复数据删除服务器已将重复数据删除存储组件与磁盘代理一起安装。
- dedupe_store（重复数据删除服务器）系统上的总可用 RAM 应大于或等于 32 GB。建议保留 64 GB RAM 以获得最佳性能。
- 每个重复数据删除存储需要 8 GB RAM。但是，加密的重复数据删除存储需要 16 GB RAM。
- 根据所选的重复数据删除类型，介质代理系统应具有 16 GB RAM，以防重复数据删除在该主机上不起作用。
- 重复数据删除存储要求重复数据删除服务器中的每个存储都有一个服务器端口。默认情况下，它占用 6442 端口及更高端口。
- 重复数据删除存储至少需要一个服务器端口，默认情况下使用端口 6442。如果您选择为每个存储配置一个端口，则它将使用端口 6442 或更高端口号。
  要更改 Data Protector 使用的端口号范围，请在重复数据删除服务器上相应地设置 omnirc 选项 OB2PORTRANGE 。请参阅 Omnirc 选项。

限制

请考虑以下限制和注意事项:

- 仅在 Windows 2016、2019、Rhel 7.x 及更高版本和 SLES 12 (64 位) 及更高版本上支持重复数据删除存储。
- dedupe_store（重复数据删除服务器）系统上的总可用 RAM 应大于或等于 32 GB，建议保留 64 GB RAM。
- 对于要启动的每个 sdfs 卷，在 dedupe_store 系统上应该至少提供 8 GB 可用内存。建议保留 32 GB。
- 您不能选择源端网关进行对象复制。您可以：
  - 手动将读取源设备替换为非源端网关。网关必须与源端网关属于相同的 B2D 设备。
  - 在非源端网关的“属性”窗口中，转到“策略”选项卡并选择“网关”。 它可用作对象副本的源网关。Data Protector 会自动将源端网关替换为此网关。
- 您创建的存储只能通过手动登录重复数据删除服务器来删除。
- 备份到任何云存储设备时，建议对加密存储和非加密存储使用不同的容器。对两者使用相同的容器可能会导致备份失败。
- 删除重复数据删除存储中未受保护或过期的介质后，大约 2-3 GB 的残留数据不会被删除，将保留在设备上。

> 重要说明: 底层目标存储系统应具有高冗余级别以确保数据保护。

配置设备

完成以下步骤以配置 Data Protector 重复数据删除存储组件:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”选为“重复数据删除存储”。要创建 NDMP 设备，请选择“重复数据删除存储 (NDMP)”。
5. 单击“下一步”。
6. “重复数据删除服务器”下拉列表列出了所有安装了重复数据删除软件的虚拟机。
7. 在“重复数据删除存储”文本框中，可以输入重复数据删除存储名称，或单击“选择/创建存储”。此时将显示“选择/创建存储”窗口。可以选择现有重复数据删除存储，或创建一个新的存储。
8. 如果您选择从现有存储中选择，请选择“选择现有存储”。从列表中选择一个现有存储，然后单击“添加”。如果您选择创建新的重复数据删除存储，请选择“新建存储”选项。“新建存储”部分被激活。

9. 在“存储名称” 对话框中，输入存储名称。
10. 在“重复数据删除目录” 对话框中，输入您要创建存储的路径。您还可以浏览并选择一个目录，或者通过在路径中输入目录名称来创建一个新目录。
11. 单击“确定” 以创建本地重复数据删除设备。如果要创建云设备，请单击“云支持” 复选框。此时将显示“云选项” 对话框。输入详细信息，然后单击“确定” 。有关此对话框中选项的详细信息，请单击“帮助” 。
12. 单击“添加”以添加网关。此时将显示“添加网关”窗口。提供“网关名称”，然后单击“确定”。添加网关时，可以选择所需的重复数据删除类型。默认情况下，启用服务器端重复数据删除。要启用目标端重复数据删除，请通过取消选中“高级设置” 下的框来禁用服务器端重复数据删除。
13. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

备份

Data Protector 重复数据删除存储支持“完整”、“差异” 和“增量” 备份类型。您可以通过在创建备份规范时启用源端重复数据删除网关来执行源端重复数据删除备份。禁用此选项会自动启用目标端重复数据删除。

完成以下步骤以创建重复数据删除备份规范:

1. 添加新的重复数据删除设备。请参阅“配置设备”。
2. 创建以该设备为目标的备份规范。有关创建备份规范的步骤，请参阅创建备份规范。或者，要启用源端重复数据删除，请在创建备份规范时选择源端重复数据删除选项。

   在“源”页面选择备份对象时，Data Protector 将禁用所有未配置源端网关的客户机。通过在“显示”下拉列表中选择“源端重复数据删除”，您可以过滤客户机列表。

   或者，选择备份规范，打开“选项” 窗格，并选择“源端重复数据删除”。
3. 在“目标”页面，选择将用于备份的网关。单击“属性”以查看和修改网关选项。请注意，可通过指定选项“每个网关的并行流的最大数量”覆盖设备配置期间设置的值。

> **注意:** 选择源端重复数据删除时，您只能备份支持源端网关的客户机中的对象，而且只能选择带有源端网关的设备。

还原

Data Protector 重复数据删除存储支持使用所有三个文件冲突处理选项 (“保持最新”、“不覆盖”、“覆盖”) 还原到原始位置和还原到新位置。

StoreOnce 软件重复数据删除

本节提供安装 StoreOnce 软件重复数据删除组件时的主要安装任务和特定要求概述。

确保已在支持的系统上安装 Data Protector Cell Manager、用户界面客户机和安装服务器。

重要说明: 在停止后台程序 (Linux) 或服务 (Windows) 或重新启动服务器之前，必须手动停止 StoreOnce 软件服务器上的所有存储。否则可能会导致存储崩溃和数据丢失。您可以使用 StoreOnceSoftware 实用程序停止存储。建议使用 --force 选项及时停止存储。运行以下命令来停止存储:

```
StoreOnceSoftware --stop_store --name=StoreName --force
```

防火墙配置

确保已为传入的连接打开以下端口：

- 9387/tcp – 命令端口（针对 StoreOnce 软件系统和 StoreOnce 备份系统）。
- 9388/tcp – 数据端口（针对 StoreOnce 软件系统和 StoreOnce 备份系统）。

必须在防火墙中打开端口 9387 和 9388，将目标设备与任何网关分开。(Windows 系统: 端口在安装过程中打开，UNIX 系统: 端口必须手动打开。)有关 Data Protector 端口的详细信息，请参阅《Data Protector 帮助》索引: “端口范围”。

StoreOnce 软件服务器上的防病毒使用

本节列出了您正在 StoreOnce 软件服务器上使用或计划使用的防病毒产品的一些注意事项。

- 由于复杂的文件结构，不应对 StoreOnce 软件根目录执行计划扫描或实时扫描。
- 扫描属于 StoreOnce 软件内务管理过程的文件夹中的文件可能会导致 StoreOnce 软件失败。
- 将任何文件移动到隔离位置，或在病毒扫描程序在 StoreOnce 库文件夹结构中识别出安全风险时删除文件，可能会损坏存储区，使其无法使用。

建议

- 禁用实时病毒扫描。
- 将 StoreOnce 软件根目录添加到病毒扫描程序的“排除列表”中。
- 通过执行 --get_server_properties 命令来定期查看存储区根信息。

安装过程

在所有将成为网关的系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，其中包括将启用源端重复数据删除的客户机。

StoreOnce 软件重复数据删除的其他步骤

在将托管 StoreOnce 存储区的系统上安装 Data Protector StoreOnce 软件重复数据删除组件。

StoreOnce 软件重复数据删除组件可以本地安装或远程安装。

远程安装 Data Protector StoreOnce 软件重复数据删除组件

1. 通过 Data Protector 用户界面组件连接到任何客户机。
2. 打开 Data Protector GUI，在“上下文”列表中，选择“客户机”。
3. 将 Data Protector StoreOnce 软件重复数据删除组件添加到备份客户机：
   - 如果备份客户机不是 Data Protector 单元的一部分，则使用 Data Protector 添加客户机功能。
   - 如果备份客户机已经是 Data Protector 单元的一部分，则使用 Data Protector 添加组件功能。

成功安装后，StoreOnce 软件重复数据删除组件列在安装的组件列表中。

在可以使用 StoreOnce 软件重复数据删除之前，必须配置存储的根目录。

本地安装 Data Protector StoreOnce 软件重复数据删除组件

Windows 系统：
在本地安装 Data Protector 期间，请在“组件”列表中选择 the StoreOnce Software Deduplication 组件。

Linux 系统：
运行 omnisetup.sh –install StoreOnceSoftware 。

设置 StoreOnce 软件服务/后台程序

Windows 系统：
成功安装后，StoreOnceSoftware 可执行文件将作为服务启动 (请参阅“任务管理器”中的“服务”选项卡)。服务名称为 Data Protector StoreOnceSoftware，描述为 StoreOnce Software Deduplication ，启动类型为“自动”。

Linux 系统：
要安装 StoreOnceSoftware 后台程序，使其在系统重新启动后自动启动，请将文件 StoreOnceSoftwared 复制到 /etc/init.d 目录并将其包含在启动脚本中。也可以使用命令手动启动或停止后台程序：

```
/opt/omni/lbin/StoreOnceSoftwared start
```

和

```
/opt/omni/lbin/StoreOnceSoftwared stop
```

从系统中删除 StoreOnce 软件重复数据删除组件时，会自动停止进程，并从 /etc/init.d/ 目录中删除文件 StoreOnceSoftwared 。在 Linux 服务器上运行 StoreOnce 软件后台程序时，将在 /tmp 文件夹下创建临时文件，如 Global\DeduplicationDaemon:9387.mutex 。为了正常运行后台程序，需要保留这些文件，不应将其删除。

安装的目录结构

Windows 系统：
安装组件包括以下文件：

文件名(F)	文件位置
StoreOnceSoftware.exe	Data_Protector_home\bin
system.db	Data_Protector_program_data\Config\client\ StoreOnceSoftware

Linux 系统：
成功安装后，StoreOnceSoftware 作为后台进程 (后台程序) 启动。重新启动后，可以自动启动。

安装组件包括以下文件：

文件名(F)	文件位置
StoreOnceSoftware	/opt/omni/lbin
StoreOnceSoftwared	/etc/init.d/ /opt/omni/lbin
system.db	/etc/opt/omni/client/StoreOnceSoftware

故障诊断

本节提供使用 Data Protector StoreOnce 软件集成时的日志和事件报告、警告、诊断及问题解决信息。

磁盘空间不足警告

为避免存储区所在的磁盘空间不足，当达到预定义阈值时，将写入警告消息（Windows 系统上的事件日志或 Linux 系统上的 Syslog）。阈值的默认值是存储区容量的 10%。默认值可以使用 omnirc 选项进行修改。在对存储执行任何进一步读取/写入操作之前，或者如果 StoreOnce 软件实用程序重新启动，警告消息每天发出一次。在会话开始和结束时，警告还显示在备份会话消息中。磁盘空间不足警告消息是：

```
You are running out of disk space on Deduplication Store root directory: [path]. The threshold x% is reached. Please free space or add more disks. [warning] 。
```

system.db 文件的备份

system.db 数据库文件包含根目录信息及有关存储的信息。该文件位于 DataProtector_Program_Data\OmniBack\Config\client\StoreOnceSoftware 下。如果该文件被删除或丢失，则无法访问存储区和已备份的数据。为避免出现此情况，每次更改数据库时，会将 system.db 文件的备份复制到 .\Store_Root\StoreOncelibrary\system.db.bak 。可通过将备份文件复制到原始位置，进行重命名，然后重新启动 StoreOnceSoftware 实用程序，还原 system.db 文件。

确保根目录下的文件受到保护（RAID 或备份）。

下方列出了 StoreOnce 软件实用程序报告的常见问题和错误。错误通常与操作环境和重复数据删除存储区的目录结构相关。

StoreOnce 软件实用程序未能找到存储区的根目录。

问题
Accessing the system.db file: The system.db file is inaccessible (for example, permission denied, or disk full).
操作
更改权限，释放磁盘空间，或使数据库可访问。对于重复数据删除存储的根目录，数据库文件（system.db）包含空值或无值。

StoreOnce 软件实用程序未能启动。

问题
访问 system.db 文件: 存储的根目录中缺少 system.db 文件。
操作
还原或重新创建 system.db 文件。请参见上一问题。

在存储区的启动过程中，记录了错误。无法访问存储区。

问题
启动存储: 无法访问存储目录。
操作
使存储区的目录可访问，检查权限并验证根目录是否存在。

已成功启动存储区，但没有找到项目。

问题
启动存储: 缺少存储目录。
操作
还原根目录和根目录下的存储区。

记录了错误。无法访问存储区。

问题
启动存储: 存储较脏，无法恢复。
操作
还原根目录和根目录下的存储区。

停止存储区时报告错误。

问题
停止存储: 项目打开 (例如，备份或还原会话正在运行)。
操作
在停止 StoreOnce 软件实用程序之前，检查所有操作是否均已完成。

关闭过程中报告了错误。恢复可能发生在下一次启动时。

问题
停止存储: 无法停止内务管理实用程序。
操作
检查所有操作是否均已完成，然后停止 StoreOnce 软件实用程序。恢复可能发生在下一次启动时。

当可用磁盘空间不足时，将记录警告消息。

问题
由于磁盘空间和内存不足，StoreOnce 软件服务/后台程序在 Windows 事件日志或 Linux syslog 中记录了警告和错误消息。 当系统达到剩余可用虚拟内存的 25% 时，记录了警告消息，当只剩下剩余可用虚拟内存的 20% 时，记录了错误消息，服务/后台程序开始拒绝读取和写入操作。
操作
释放系统资源。释放磁盘空间或内存后，服务/后台程序将停止拒绝操作。

Data Protector 显示警告“存储区不存在”，并且备份会话失败。

问题
使用 StoreOnce 备份系统设备执行备份会话时，Data Protector 显示类似以下的警告，并且会话异常结束： [Warning] From: BSM@computer.company.com "CS2BackupTmp" Time: 6/18/2012 1:34:08 PM Got error: " Store does not exist. " when contacting " DeviceName" B2D device! 如果 B2D 设备上已删除此存储或已修改此存储的访问权限，则可能会出现此问题。
操作
• 检查存储区是否存在，或是否已修改此存储区的任何权限。 • 如果已正确设置存储区，则检查 Data Protector 中的设备设置。右键单击设备，选择“属性”，并在“设备 - 存储和网关”页面检查“客户机 ID”。

B2D 设备的状态更新按指定时间间隔执行。

问题
已超出备份大小软配额或存储区大小软配额，但 Data Protector 没有报告任何警告。
操作
无。下一个备份会话将正确报告警告。

StoreOnce 和 DDBoost 重复数据删除设备

Data Protector 支持 HPE (使用 Catalyst 的 StoreOnce) 和 Dell EMC (使用 Boost 的数据域) 的重复数据删除产品。StoreOnce Catalyst 和 DDBoost 是指在前一个产品中管理重复数据删除的软件，在以下材料中互换使用。

本节包含示例环境和配置过程。

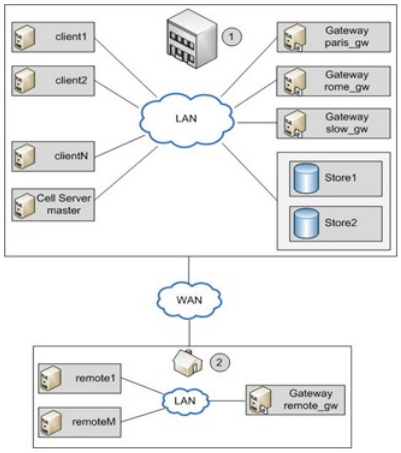
多接口支持

Data Protector 提供多接口支持，IP 和 FC 连接可导致相同的 Catalyst 或 Boost 存储区。Data Protector 支持与同一 Catalyst/DDBoost 存储区建立 IP 以及光纤通道连接，而无需配置单独的存储区。可同时通过这两种接口访问存储。例如，有时本地客户机可通过光纤通道访问单个 Catalyst/DDBoost 存储以执行较快的备份，而远程客户机可通过 WAN 访问同一存储以执行较慢的备份。

请注意，如果配置使用同一 StoreOnce 存储的多个 Data Protector 设备，将引发介质管理问题。

使用 B2D 设备的配置示例

下图提供中央办公室/远程办公室配置的典型使用模型。



项目	描述
1	中央办公室。该 LAN 位于中央办公室。通过 WAN 连接到远程办公室的 LAN。
2	远程办公室。该 LAN 位于远程办公室。

Data Protector Cell Manager 安装在主机 *master* 的中央办公室中。中央办公室有多个客户机：*client1 到 clientN*（非网关客户机）、*paris_gw, rome_gw* 和 *slow_gw*（网关客户机）。此外，在中央办公室配置了两个对象存储区（Store1 和 Store2）。

远程办公室包括客户机 *remote1* 至 *remoteM* 和 *remote_gw*。远程办公室的所有客户机属于与中央办公室的客户机相同的 Data Protector 单元。远程办公室通过较慢的 WAN 网络连接至中央办公室。

> 注意**:** 网关只是安装有介质代理组件的客户机。将它们视为网关客户机。客户机若要成为网关，则必须是 64 位系统。

配置 B2D 设备时，您必须指定某些参数，如存储区的名称和位置、网关、网络路径。在上述示例中，您想要使用存储区 Store1（通过 StoreOnce 软件重复数据删除访问），以用于在您的环境中备份客户机。为此，您可将 B2D 设备配置为将 Store1 用作存储库。您还决定，客户机*paris_gw*、*rome_gw* 和 *slow_gw* 将用作中央办公室的其他 Data Protector 客户机的网关。此外，请注意以下事项：

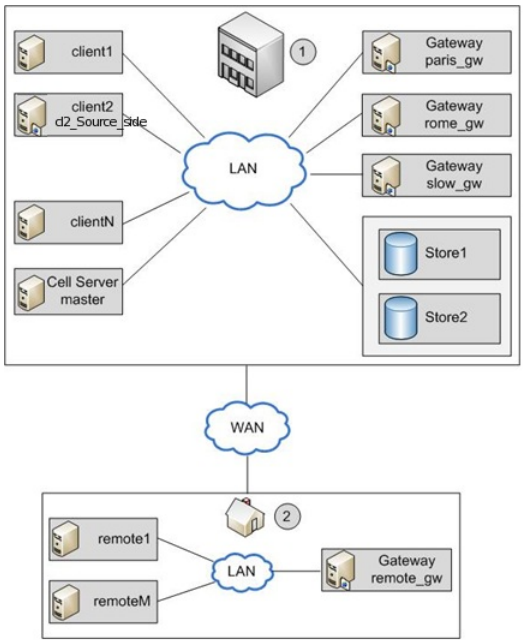
- 并发可指定多个并行写入到设备的磁盘代理。多个磁盘代理并行读取数据（从磁盘），为介质代理提供连续的数据流。 借助 StoreOnce 软件重复数据删除，每个介质代理的磁盘代理并发设置为 1（这样可以改善重复数据删除比率）。
- Data Protector 支持备份到未加密存储区和已加密存储区。可在创建存储区时启用加密功能。注意，存储区一经创建，就不能将其从已加密状态更改为未加密状态，反之亦然。
- 每个设备只能配置一个存储区。
- 存储区由包含重复数据删除系统和存储名称相关信息的网络路径 (UNC) 表示。(注意: 在 B2D 设备的上下文中，重复数据删除系统指重复数据删除存储所在的托管计算机的名称。)

源端重复数据删除

如果各个客户机的备份数据量有限，则上述场景适用。然而，为减少网络流量，您可以配置源端网关。

例如，在我们的场景中，client2 系统上有许多重复的数据，但系统负载属于中度。为减少网络负载，您可以启用 B2D 设备的源端重复数据删除。如果您在 client2 的备份规范中也启用了源端重复数据删除，则将在 client2 上自动创建源端网关，介质代理将仅通过网络发送删除重复的数据。

同样，如果您为其他客户机启用源端重复数据删除，也将在这些客户机上自动创建源端网关。



添加 B2D 设备的步骤与添加设备类型的步骤类似。

备份

在备份规范中指定 B2D 设备可告知 Data Protector 执行重复数据删除类型备份。重复数据删除进程在后台运行，删除重复的数据写入到 StoreOnce 软件系统或 StoreOnce 备份系统。

您执行与传统备份相同的重复数据删除类型备份：

1. 添加新的 B2D 设备（在此例中，通过指定 StoreOnce 软件重复数据删除或 StoreOnce 备份系统）。
2. 创建以该设备为目标的备份规范。请参阅《Data Protector 帮助》索引: “创建, 备份规范”。或者，要启用源端重复数据删除，请在创建备份规范时选择源端重复数据删除选项。

   在“源”页面选择备份对象时，Data Protector 将用阴影表示所有未配置源端网关的客户机。通过在“显示”下拉列表中选择**源端重复数据删除**，您可以过滤客户机列表。

   或者，选择备份规范，打开“选项”窗格，并选择**源端重复数据删除**。
3. 在“目标”页面，选择将用于备份的网关。单击**属性**以查看和修改网关选项。请注意，可通过指定选项“每个网关的并行流的最大数量”覆盖设备配置期间设置的值。

> 注意**:** 选择源端重复数据删除时，您只能备份支持源端网关的客户机中的对象，而且只能选择带有源端网关的设备。如果取消选择该选项，Data Protector 将自动选择 B2D 设备的所有网关，而非源端网关，并显示警告消息。

> 重要说明**:** 如果您在现有备份规范中启用源端重复数据删除，则取消选中且不备份无法执行源端重复数据删除的客户机。

还原

使用与传统还原操作相同的方法还原备份的数据。虽然与传统还原进程相比，从重复数据删除存储区中检索数据的后台进程明显不同，但不执行任何特殊任务。检索进程的主要操作包括，将待还原数据加载到内存，从索引表读取参考信息，并使用该信息*再水合*备份数据。

源端重复数据删除

如果执行备份时已启用源端重复数据删除且在不支持源端网关的客户机上执行还原，则将使用普通网关。

CoFC 的 StoreOnce Catalyst 配置

以下信息不旨在决定基于光纤通道的 Catalyst (CoFC) 的 StoreOnce Catalyst 客户机配置。有关最新且最详细的信息，请参阅 HPE StoreOnce 文档。

Windows 客户机

通过光纤通道备份运行 Catalyst 需要管理员权限。基于光纤通道的 StoreOnce Catalyst 表示**处理器**的一种设备类型。对设备进行分区或更改每

个启动器端口的设备数量后，请执行以下操作：

1. 转到 **Windows 设备管理器**，右键单击**其他设备**。
2. 选择**扫描硬件更改**，以检测新设备。

Linux 客户机

基于光纤通道的 StoreOnce Catalyst 表示处理器的一种设备类型。在 Linux 上，设备文件在 /dev/sg* 中进行创建。默认情况下，只有根用户才能访问 /dev/sg* 设备。对于非根用户，使用 Linux udev 规则提供备份用户权限，以访问设备文件。

要创建 udev 规则，请执行以下操作：

1. 在每个备份服务器的以下位置，创建 udev 文件：
   /etc/udev/rules.d/70-cofc.rules
2. 在文件中添加以下规则：
   KERNEL=="sg[0-9]*", ATTRS{vendor}=="HP*", ATTRS{model}=="StoreOnce CoFC*", ATTRS{rev}=="CAT1", GROUP="##CORRECT_USER_GROUP##"
   其中， ##CORRECT_USER_GROUP## 替换为将执行备份和还原的 Linux 用户组。例如， dba/oracle 。
3. 扫描设备文件更改，以更新权限。
   lsscsi --generic 命令可用于确定哪些 /dev/sg* 设备文件属于基于光纤通道的 Catalyst。

AIX 客户机

在 StoreOnce 软件 3.14 版本之前，只能通过请求使用 AIX 上基于光纤通道的 StoreOnce Catalyst。在 StoreOnce 版本低于 3.14 的 AIX 客户机上，如果您需要基于光纤通道的 Catalyst，请联系 StoreOnce 支持。基于光纤通道的 StoreOnce Catalyst 代表 AIX 上的顺序的一种设备类型。这些设备文件在 /dev/rmt* 位置进行创建。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

1. 执行 storeonce-cofc-passthrough-install.sh 脚本。
2. 以根用户身份执行 cfgmgr 命令，以扫描设备文件中的更改。
3. 默认情况下，只有根用户才能访问 /dev/rmt* 设备文件。作为根用户运行备份需要其他权限。

> **注意:** 该安装脚本是 HPE StoreOnce 的一部分，不是 Data Protector 的一部分。请联系 HPE 支持人员。

HP-UX 客户机

基于光纤通道的 StoreOnce Catalyst 表示处理器的一种设备类型。在 HP-UX 上，设备文件在 /dev/pt/ptX 位置进行创建。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

1. 扫描设备文件更改。
2. 以根用户身份执行 ioscan -fnC /dev/pt 命令。
   默认情况下，只有根用户才能访问 /dev/pt/ptX 设备。对于非根用户，使用 chmod o+rwx /dev/pt/pt* 命令提供备份用户权限，以访问设备文件。
3. 要获得 /dev/pt/ptX 设备文件的权限，请使用基于光纤通道的 Catalyst 命令：
   /usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid | grep StoreOnce
4. 在相应设备上使用 chmod o+rwx 命令。

Solaris 客户机

基于光纤通道的 StoreOnce Catalyst 表示处理器的一种设备类型。在 Solaris 上，设备文件在 /dev/scsi/processor/* 位置进行创建。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

1. 扫描设备文件更改。
2. 如果您是根用户，请执行以下命令：
   1. add_drv -vi scsiclass,03 sgen
   2. update_drv -vai scsiclass,03 sgen
3. 默认情况下，只有根用户才能访问 /dev/scsi/processor/* 设备。对于非 root 用户，使用以下命令提供备份用户权限以访问设备文件:
   1. chmod -R o+rwx /dev/scsi/processor/*
4. 要获得 /dev/scsi/processor/* 设备文件的权限，请使用基于光纤通道的 Catalyst 命令:
   1. for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep "Vendor|Product"; echo; done
5. 在适当的设备上使用 chmod -R o+rwx 命令。

与 B2D 设备相关的 omnirc 选项

可以使用其他选项配置介质代理上的 omnirc 文件。使用该文件设置端口号和磁盘空间阈值警告等参数。

omnirc 选项	默认值	使用情况
OB2_STOREONCESOFTWARE_COMMAND_PORT	9387	该选项更改用于介质代理和 StoreOnce 软件实用程序之间的命令通信的端口。
OB2_STOREONCESOFTWARE_DATA_PORT	9388	该选项更改用于介质代理和 StoreOnce 软件实用程序之间的数据通信的端口。
OB2_STOREONCESOFTWARE_SESSION_IDLE_TIMEOUT	300	StoreOnce 软件后台程序定期检查空闲连接并终止这些连接。该选项指定闲置秒数，之后，连接被视为空闲。范围最小值 10 秒
OB2_STOREONCESOFTWARE_DISK_SPACE_THRESHOLD	10	该选项将设置可用磁盘空间的阈值。范围 1％-95％
OB2_STOREONCESOFTWARE_MINIMUM_DISK_SPACE	1000	该选项控制 StoreOnce 软件需要保留的最小磁盘空间（以 MB 为单位）。如果达到该最小值，向任何存储写入数据的操作将失败。最少：500 MB
OB2_STOREONCESOFTWARE_DISABLE_IPV6_LISTEN	0	默认情况下，StoreOnce 软件后台程序侦听双堆栈套接字（相同端口上的 IPv6 和 IPv4）。如果设置为 1，IPv6 被禁用。该选项适用于 RPC 和 IpcServer 侦听端口。
OB2D2D_COMMAND_PORT	9387	该选项更改用于介质代理和 StoreOnce 备份系统之间的命令通信的端口。
OB2D2D_DATA_PORT	9388	该选项更改用于介质代理和 StoreOnce 备份系统实用程序之间的数据通信的端口。
OB2D2D_NUM_OF_LBWTHREADS	4	定义在介质代理客户机上执行重复数据删除时用于重复数据删除计算的线程数量。如果您具备更强大的网关，您可以将该数字增加至 8 个线程。必须在每个网关上单独设置该选项。
OB2D2D_BANDWIDTH_BUFF_SIZE	10	设置在介质代理客户机上执行重复数据删除时的缓冲区大小。当介质代理通过 LAN 与 D2D 设备通信时，默认设置合适。当 WAN 网络用于通信时，更合适的值是 20 MB。必须在每个网关上单独设置该选项。
OB2SCRIPTOUTPUTTIMEOUT	不适用	它定义备份磁盘代理使用的超时 (分钟)。对象 pre-exec 或 post-exec 脚本必须至少每 OB2SCRIPTOUTPUTTIMEOUT 分钟发送一些输出，否则将中止磁盘代理。

云设备 - Azure

云设备用于实现从 Data Protector 到 Microsoft Azure 对象存储的备份和对象复制。云 (Azure) 设备使用 Azure 凭据进行配置，并将数据发送到云。

先决条件

满足以下要求。

Data Protector 先决条件

要将 Data Protector 与 Azure 设备一起使用，需满足以下先决条件:

- 确保已在支持的系统上安装 Data Protector 的 Cell Manager、用户界面客户机和安装服务器，以及最新的常规补丁版本包。
- 在将成为云 (Azure) 网关的 Windows 和 Linux 系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，其中包括将启用云 (Azure) 设备的客户机。
- 对于需要配置代理服务器才能连接到 Web 的介质代理系统，需要在 **omnirc**文件中设置 **omnirc**变量 OB2_CLOUD_DEVICE_PROXY=*proxy_server.port_number*> 。

> **注意**
>
> 介质代理具有内置重试机制，可处理不同错误情况。因此，用户操作有时可能需要一段时间才能完成。

Azure 设备先决条件

要使用 Azure 设备，必须满足以下先决条件:

- 您必须拥有 Microsoft Azure 帐户。
- 您必须拥有 Microsoft Azure 在创建 Microsoft Azure 存储帐户时生成的两个存储访问密钥。

  为帐户生成了两个访问密钥。创建相关的 Data Protector 设备时，在提供凭据的过程中需要这些密钥。
- 必须准确设置系统时间，以确保网关主机和 Microsoft Azure 之间正确同步。

限制

以下是云 (Azure) 设备的限制：

- 在云 (Azure) 设备中选择或创建容器时，需遵循以下限制：
  - 只能为每个设备分配一个容器。
  - 多个设备无法使用相同的容器。
  - 将容器分配给设备之后，不能进行更改。
- 云 (Azure) 设备 blob 大小限制
  Data Protector 介质作为数据和元数据的一个或多个 blob，上载到云 (Azure) 设备。云 (Azure) 的 blob 大小限制为 195 GB，而 Data Protector 介质的大小没有上限。然而，为遵守该限制，一个 Data Protector 介质可跨多个 blob，每个 blob 的大小上限为 75 GB。每个 blob 存储的确切数据量是数据可压缩程度的函数。

配置云 (Azure) 设备的建议

以下是配置云 (Azure) 设备的建议：

- 备份文件系统规范时，请使用数据源的本地云 (Azure) 设备网关，因为这将减少对象复制操作期间的网络负载。
- 由于在默认情况下，到云 (Azure) 的对象复制作业经过加密，因此在为复制操作生成数据的初始备份规范中，应关闭加密。如果加密开启，数据会加密两次，消耗额外的 CPU 资源，对象复制数据变得不可压缩。因此，传输到云 (Azure) 的数据量增加，延长了复制时间。
- 将数据复制到云 (Azure) 设备时，请将大数据集分解成多个备份规范，以便能够并行启用多个复制会话。从而增加整体带宽。
- 建议不要在云 (Azure) 设备上进行合并，因为这需要大量带宽以及关联成本。

为云 (Azure) 设备做准备

要将对象复制操作配置到云 (Azure) 设备，必须执行以下任务。

1. 配置备份规范，将数据备份到本地备份设备。
2. 登录 Microsoft Azure 门户，并获取使用 Microsoft Azure 存储帐户所需的访问密钥。
3. 在 Data Protector 中配置云 (Azure) 设备。
4. 分别使用本地备份设备和云 (Azure) 设备作为源设备和目标备份设备，配置对象复制会话。

创建“复制到云 (Azure) 设备”对象操作之后，本地备份设备中存储的数据可复制到云 (Azure) 设备。默认情况下，会对发送到云 (Azure) 的数据进行压缩和加密。

5. 从云 (Azure) 设备还原数据。要还原数据，您可以：
   - 创建从云 (Azure) 设备到本地备份设备的对象复制，并从本地备份设备还原到客户机。
   - 回收并导出本地介质，然后直接从云 (Azure) 设备还原到客户机。
   - 通过指定要用于还原的云 (Azure) 设备，直接从云 (Azure) 中还原，即使存在本地版本也如此。
   - 将介质位置优先级设置为云 (Azure) 介质，而非本地介质。

配置云 (Azure) 设备

要配置“接口类型”为“云 (Azure)”的“备份到磁盘”设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Azure)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 指定要使用的“存储帐户名称”。
7. 指定“访问密钥 1”和“访问密钥 2”信息。

   如果将对象从本地设备复制到云，并复制回同一设备以备恢复，则本地设备和云设备的块大小必须匹配。

8. 单击“选择/创建容器”以获取已创建的所有容器列表并显示它们。此时将显示“选择容器”窗口。选择现有的容器或创建新的容器以上载数据。
9. 单击“添加”以添加网关。
10. 单击**检查**验证网关是否已连接到云 (Azure)。如果连接成功，则状态显示为“正常”。
11. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

云设备 - Amazon S3

云 (Amazon S3 API 兼容) 设备用于启用从 Data Protector 到 Amazon S3 和兼容对象存储的备份和对象复制。云 (Amazon S3 API 兼容) 设备使用与相关对象存储相关联的凭据进行配置。Amazon S3 API 兼容接口类型包括 Amazon S3、Ceph 和 Scality 设备。

先决条件

满足以下先决条件。

Data Protector 先决条件

要将 Data Protector 与 Amazon S3 API 兼容设备一起使用，请满足以下先决条件:

- 确保已在支持的系统上安装 Data Protector 的 Cell Manager、用户界面客户机和安装服务器，以及最新的常规补丁版本包。
- 请确保在将成为云 (Amazon S3) 网关的 Windows 和 Linux 系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，包括将启用云 (Amazon S3 API 兼容) 设备的客户机。
- 对于需要配置代理服务器才能连接到 Web 的介质代理系统，需要在 **omnirc**文件中设置 **omnirc**变量 OB2_CLOUD_DEVICE_PROXY=*proxy_server:port_number*> 。

> **注意**
>
> 介质代理系统具有内置重试机制，用于处理不同的错误情况。因此，用户操作有时可能需要一段时间才能完成。

AWS S3 先决条件

要使用 AWS S3 目标，必须满足以下先决条件:

- 必须拥有 AWS 账户。有关详细信息，请参阅 Amazon S3。
- 必须拥有 AWS 账户的访问密钥 ID 和密码访问密钥。创建 Data Protector Amazon S3 设备时，在提供凭据的过程中需要这些密钥。
- 必须准确设置系统时间，才能确保网关主机和 Amazon S3 之间正确同步。

Ceph/Scality 先决条件

要使用 Ceph/Scality 目标，必须满足以下先决条件:

- 可使用 Data Protector 配置支持 AWS 签名版本 4 的 Ceph 和 Scality 版本。
- 必须拥有 Ceph/Scality 存储的身份验证凭据。创建 Data Protector Amazon S3 API 兼容设备时，在提供凭据的过程中需要这些值。
- 必须准确设置系统时间，才能确保网关主机和对象存储之间正确同步。
- 必须配置兼容 S3 API 的 Ceph 对象网关/Scality S3 连接器 (http 或 https)。

限制

使用云 (Amazon S3 API 兼容) 设备时，以下限制适用:

- 云 (Amazon S3 API 兼容) 设备对象大小限制:
  Data Protector 介质将作为数据和元数据的一个或多个对象，上载至云 (Amazon S3 API 兼容) 设备。一个 Data Protector 介质可以跨越多个对象，每个对象的最大大小为 50 GB。每个对象存储的确切数据量是数据可压缩程度的函数。
- 云 (Amazon S3 API 兼容) 设备对象复制适用于以下各项:
  - 源设备: 文件库设备和 StoreOnce 设备。
- 在云 (Amazon S3 API 兼容) 设备中选择或创建散列存储时，需要遵循以下限制:
  - 只能向每个设备分配一个散列存储。
  - 多个设备不能使用同一散列存储。
  - 向设备分配散列存储之后，不能进行更改。

配置云 (Amazon S3 API 兼容) 设备的建议

以下是配置云 (Amazon S3 API 兼容) 设备的建议:

- 备份或复制数据时，请使用源的本地云 (Amazon S3 API 兼容) 设备网关，因为此举可减少操作期间的网络负载。
- 默认会加密到云 (Amazon S3) 的对象复制作业，因此在为复制操作生成数据的初始备份规范中，应关闭加密。如果加密开启，数据会加密两次，消耗额外的 CPU 资源，对象复制数据变得不可压缩。因此，传输至云 (Amazon S3) 的数据量会增加，从而延长复制时间。
- 在将数据复制到云 (Amazon S3 API 兼容) 设备之前，请将大型数据集拆分成多个备份规范。此举使得多个复制会话能够并行运行，从而增加操作的可用总带宽。

- 建议不要在云 (Amazon S3 API 兼容) 设备上进行合并，因为这需要大量带宽以及关联成本。

为云 (Amazon S3 API 兼容) 设备做准备

可执行直接备份到云目标，也可以创建本地备份，然后对云目标执行对象复制操作。建议执行本地备份，然后执行对象复制操作。

执行以下步骤以配置对云 (Amazon S3 API 兼容) 设备的对象复制操作:

1. 配置备份规范，将数据备份到本地备份设备。

   对于直接备份，请将本地备份设备替换为 Amazon S3 兼容目标。

2. 登录 Amazon S3 门户，然后获取使用 Amazon S3 帐户所需的访问密钥。
3. 在 Data Protector 中配置云 (Amazon S3) 设备。
4. 分别使用本地备份设备和云 (Amazon S3 API 兼容) 设备作为源设备和目标备份设备，配置对象复制会话。

   创建“复制到云 (Amazon S3 API 兼容)”设备对象操作之后，可将本地备份设备中存储的数据复制到云 (Amazon S3 API 兼容) 设备。默认情况下，会对发送至云 (Amazon S3) 的数据进行压缩和加密。

5. 从云 (Amazon S3 API 兼容) 设备还原数据。要还原数据，您可以：
   - 创建从云 (Amazon S3 API 兼容) 设备到本地备份设备的对象复制，然后从本地备份设备还原到客户机。
   - 回收并导出本地介质，然后直接从云 (Amazon S3 API 兼容) 设备还原到客户机。
   - 通过指定要用于还原的云 (Amazon S3 API 兼容) 设备，直接从云 (Amazon S3) 还原，即使存在本地版本也如此。
   - 将介质位置优先级设置为云 (Amazon S3) 介质，而非本地介质。

   对于直接备份，可执行直接还原操作。

配置云 (Amazon S3 API 兼容) 设备

要配置“接口类型”为“云 (Amazon S3 API 兼容目标)”的“备份到磁盘”设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 API 兼容目标)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“S3 目标类型”。
   - 如果要创建指向 Amazon S3 的设备，请选择“AWS S3”。
   - 如果要创建指向内部部署目标的设备 (Amazon S3 API 兼容)，请选择“Ceph/Scality”。
7. 指定网关。
   - **AWS S3**: 选择散列存储可用的“S3区域”，或要创建散列存储的区域。
   - **Ceph/Scality**: 对于内部部署目标，输入网关 URL。

   如果将对象从本地设备复制到云，并复制回同一设备以备恢复，则本地设备和云设备的块大小必须匹配。

8. 指定“访问密钥 ID”和“密码访问密钥”信息。
9. 单击“选择/创建散列存储”以获取已创建的所有散列存储列表并显示它们。此时将显示“选择散列存储”窗口。

   选择现有散列存储或新建散列存储以上载数据。

10. 单击“添加”以添加网关。
11. 单击“检查”以验证网关是否已连接到云 (Amazon S3/Ceph/Scality)。如果连接成功，则状态显示为“正常”。
12. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

云设备 - Amazon S3 Glacier 和 S3 Glacier Deep Archive

Amazon S3 Glacier 和 S3 Glacier Deep Archive 是 Data Protector 支持的存档云 B2D 设备。您可以使用它们长期备份大量数据，这些数据不需要经常还原或查看。Data Protector 支持将数据备份和还原到这些设备。数据可以备份到:

- 保管库
- 散列存储

先决条件

满足以下先决条件。

Data Protector 先决条件

要将 Data Protector 与 Amazon S3 Glacier 设备一起使用，需满足以下先决条件:

- 确保已在支持的系统上安装 Data Protector 的 Cell Manager、用户界面客户机和安装服务器，以及最新的常规补丁版本包。
- 请确保在将成为云 (Amazon S3 Glacier) 网关的 Windows 系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，包括将启用云 (Amazon S3 Glacier) 设备的客户机。
- 确保在 **omnirc** 文件中将 **omnirc** 变量 OB2_CLOUD_DEVICE_PROXY 设置为 <proxy_server:port_number> 。

> **注意**
>
> 如果 **omnirc** 变量 OB2_CLOUD_DEVICE_PROXY 不设置为 <proxy_server:port_number> ，则 Amazon S3 Glacier 和 DeepArchive 设备创建无法完成，备份失败。

AWS S3 Glacier 先决条件

要使用 AWS S3 Glacier 和 AWS S3 Glacier Deep Archive，必须满足以下先决条件:

- 必须拥有 AWS 账户。有关详细信息，请参阅 Amazon S3。
- 必须拥有 AWS 账户的访问密钥 ID 和密码访问密钥。创建 Data Protector Amazon S3 Glacier 设备时，在提供凭据的过程中需要这些密钥。
- 必须准确设置系统时间，才能确保网关主机和 Amazon S3 之间正确同步。
- 必须拥有“Amazon Glacier 存储完全访问 (列出/读取和写入)”权限，才能从 AWS S3 Glacier 执行备份和还原。
- 必须拥有“Amazon S3 完全访问 (列出/读取和写入)”权限，才能从 AWS S3 Glacier Deep Archive 执行备份和还原。

配置云 (Amazon S3 Glacier) 设备

要配置“接口类型”为“云 (Amazon S3 Glacier)”的“备份到磁盘”设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 Glacier)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“Glacier 区域”。
7. 提供 Glacier 帐户的“访问密钥 ID”和“密码访问密钥”。
8. 单击“选择/创建保管库”。此时将显示“选择保管库”窗口。可以选择现有保管库，或创建一个新保管库。单击**确定**。
9. 单击“添加”以添加网关。此时将显示“添加网关”窗口。提供“网关名称”，然后单击“确定”。
10. 单击“检查”以验证网关是否已连接到云 (Amazon S3 Glacier)。如果连接成功，则状态显示为“正常”。
11. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

配置云 (Amazon S3 Glacier Deep Archive) 设备

要配置“接口类型”为“云 (Amazon S3 Glacier Deep Archive)”的“备份到磁盘”设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 Glacier Deep Archive)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“S3 区域”。
7. 提供 Glacier 帐户的“访问密钥 ID”和“密码访问密钥”。
8. 单击“选择/创建散列存储”。此时将显示“选择散列存储”窗口。可以选择现有散列存储，或创建一个新散列存储。单击**确定**。
9. 单击“添加”以添加网关。此时将显示“添加网关”窗口。提供“网关名称”，然后单击“确定”。
10. 单击“检查”以验证网关是否已连接到云 (Amazon S3 Glacier Deep Archive)。如果连接成功，则状态显示为“正常”。
11. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

设备性能

由于设备向磁带写入数据（或从中读取数据）时可保持的速度不同，设备类型和型号会影响性能。

数据传输率还取决于是否使用硬件压缩。可以达到的压缩率取决于要备份的数据的性质。在大多数情况下，使用带硬件压缩的高速设备能提高性能。但是，仅在设备流畅通无阻时才使用此类高速设备。

在备份会话的开始和结束时，备份设备需要些时间以执行回绕介质和装载或卸载介质等操作。

库提供了自动化的优势：必须在备份时加载新的或可重用的介质，并且必须在还原时快速访问介质，但由于库访问是自动化的，因此该过程更快。

基于磁盘的设备使用起来比传统设备快。使用基于磁盘的设备时不需要装载和卸载介质，并且访问基于磁盘的设备中的数据时速度更快，因此减少了备份和还原所需的时间长度。

设备性能优化

可用的选项如下：

块大小

可将所有逻辑设备配置为以特定大小单位处理数据。不同设备有不同的默认块大小，这些大小可以使用（成功完成所有会话），但可能不是最佳选择。通过调整块大小，可以增强 Data Protector 会话的性能。

最佳的块大小值取决于所处环境：

- 硬件（设备、网桥、交换机等等）
- 固件
- 软件（操作系统、驱动程序、防火墙等等）

要获得最佳结果，请首先通过安装最新的驱动程序和固件优化环境、优化网络等等。

确定最佳块大小

要确定最佳的块大小，请通过用不同的块大小值运行常规的 Data Protector 任务（备份、还原、复制等等）执行不同的测试，并度量性能。

> **注意**更改设备块大小后，就无法再用此设备（用旧的块大小）还原旧的备份。
>
> 因此，请将旧的逻辑设备和介质池保留原样，以便能够从旧介质还原数据，并创建各种块大小值的新逻辑设备和介质池用于测试目的。或者，了解如何在执行还原时更改块大小。还原对话框将提示您块大小。

以下限制适用：

- 灾难恢复：要能够执行脱机 EADR/OBDR 恢复（增强型自动灾难恢复，一键式灾难恢复），请使用默认的块大小备份数据。
- 带库：如果在同一库中使用类似技术的若干驱动器类型，则这些驱动器的块大小必须相同。
- SCSI 适配器：检查设备所连接的主机 SCSI 适配器是否支持所选的块大小。
- 对象副本功能：目标设备的块大小必须等于或大于源设备。
- 对象合并功能：目标设备的块大小必须等于或大于源设备。
- 镜像：设备的块大小在镜像链中不得递减。用于写入镜像 1 的设备的块大小必须等于或大于用于备份的设备；用于写入镜像 2 的设备的块大小必须等于或大于用于写入镜像 1 的设备，以此类推。

更改块大小

可以在特定设备的“高级选项”对话框的“大小”选项卡中设置块大小。

相关主题

- 块大小
- 设备和介质的高级选项
- 设置设备和介质的高级选项

支持新设备

scsitab 文件是机器可读格式的 Data Protector 支持矩阵，包含有关所有受支持设备的信息。Data Protector 介质代理使用 scsitab 文件确定是否支持给定设备或库。该文件还提供有关设备及其特定参数的信息。

重要说明不支持修改 scsitab 文件。

要使用未在发行说明中列为受支持设备的设备，请从以下 Data Protector 网站下载 scsitab 文件的最新软件包: https://software.microfocus.com/en-us/products/data-protector-backup-recovery-software/overview。

下载 scsitab 软件包之后，请按照软件包随附的安装过程进行操作。

scsitab 文件位于设备所连接的系统的以下位置:

Windows 系统： Data_Protector_home\scsitab

HP-UX、Solaris 和 Linux 系统： /opt/omni/scsitab

其他 UNIX 系统： /usr/omni/scsitab

如果在配置设备时仍收到相同的错误，请与支持人员联系，以获取何时将支持该设备的信息。

准备备份设备

准备备份设备包括将设备连接到系统或在 SAN 环境中连接到 SAN 和了解要使用哪些（正常工作的）关联的设备文件（SCSI 地址）。

介质代理（常规介质代理或 NDMP 介质代理）必须安装在每个连接了备份设备的系统中或在 SAN 环境中安装在控制 SAN 上备份设备的系统中。

1. 将备份设备连接到计算机系统或在 SAN 环境中连接到 SAN。
2. 继续准备：

   Windows 系统：

   为连接到 Windows 系统的设备指定 SCSI 地址语法。

   UNIX 系统：

   为连接到 UNIX 系统的设备查找或创建设备文件名。
3. 如果有若干设备要使用同一个介质，则必须确保写入密度和块大小设置完全相同。
4. 引导系统以使系统识别出该设备。
5. 对于某些备份设备，必须执行额外的步骤。

准备备份设备之后，配置该设备与 Data Protector 配合使用。准备要与备份配合使用的介质。

- 在 SAN 环境中
- 文件设备
- 箱盒
- SCSI 库、介质库、外部控制
- Windows 机械手驱动程序

在 SAN 环境中

请执行以下操作：

1. 核实需要访问共享库的所有系统中存在的机械手设备文件名都相同。如果要使用间接库访问功能，则忽略此步骤。

   HP-UX 和 Solaris 系统：

   如有必要，通过硬链接或软链接达到设备文件标识的要求。

   Windows 系统：

   使用 libtab 文本文件覆盖默认 SCSI 设备标识，然后将机械手控制设备重新分配给在其他主机上定义的逻辑驱动器。

   应在介质代理客户机的 Data_Protector_home 目录中创建 libtab 文件，作为采用以下语法的文本文件 (允许在逻辑驱动器名称中使用空格):

   hostnamecontrol_device_filedevice_name

   例如

   computer.company.com scsi2:0:4:0 DLT_1

文件设备

对要用作设备的文件禁用 Windows 压缩选项。可以使用 Windows 资源管理器执行此操作：

1. 右键单击文件，单击**属性**，然后清除**属性**下的**压缩**选项。

箱盒

1. 创建一个支持箱盒的介质池，然后再配置箱盒设备。该设备必须支持箱盒（例如 12000e）。

SCSI 库、介质库、外部控制

1. 决定库中的哪些插槽要用于 Data Protector。配置库时，将需要指定这些插槽。

Windows 机械手驱动程序

在 Windows 系统中，将为启用的磁带库自动加载机械手驱动程序。要在 Windows 系统中将库机械手与 Data Protector 配合使用，请禁用相应的 Windows 驱动程序。

1. 在控制面板中，双击**管理工具**。
2. 双击**计算机管理**，然后单击**设备管理器**。
3. 展开**介质更换器**。
4. 右键单击介质更换器并选择**禁用**。
5. 重新启动系统以应用更改。机械手现在准备好，可以用 Data Protector 进行配置。

在 Windows 系统中创建 SCSI 地址

SCSI 地址语法取决于连接到 Windows 系统的物理设备（磁光或磁带）的类型。设备必须已连接到系统（并已通电），然后再启动系统。

提示可以使用 Data Protector 自动检测 SCSI 地址。

磁光设备

如果系统连接了磁光设备，则 SCSI 地址语法为 N:B:T:P:L（N 为可移动驱动器的装载点、B 为总线编号、T 为 SCSI 目标 ID、P 为路径、L 为 LUN)。

在**控制面板**中打开 **SCSI 适配器**，然后双击目标设备的名称。再单击**设置**以打开设备属性页。此时将显示所有必要的信息。

磁带设备

如果系统连接了磁带设备，则 SCSI 地址语法取决于是否加载了本机磁带驱动程序。地址语法还取决于系统。有关创建目标 SCSI 地址的说明，请参见以下各部分：

- 无本机磁带驱动程序的 Windows

  如果卸载了本机磁带驱动程序，则 SCSI 地址语法为 P:B:T:L（P 为 SCSI 端口、B 为总线编号、T 为 SCSI 目标 ID、L 为 LUN)。查找所连接磁带驱动器的属性可收集这些信息。

  在**控制面板**中打开 **SCSI 适配器**，然后双击目标设备的名称。再单击**设置**以打开设备属性页。此时将显示所有必要的信息。

- 使用本机磁带驱动程序的 Windows

  如果加载了本机磁带驱动程序，则 SCSI 地址语法为 tapeN（N 为驱动器实例编号)。只能使用驱动器实例编号创建磁带驱动器文件，例如，如果 N 等于 0，则为 tape0。

  1. 在 Windows“控制面板”中，双击**管理工具**。
  2. 在“管理工具”窗口中，双击**计算机管理**。展开**可移动存储**，然后展开**物理位置**。
  3. 右键单击磁带驱动器并选择**属性**。

     如果加载了本机磁带驱动程序，则设备文件名会显示在“常规”属性页中。否则，可在“设备信息”属性页中找到相关信息。

在 UNIX 系统中查找设备文件名

需要了解设备文件名以便配置连接到 UNIX 系统的设备。

设备文件的创建过程取决于特定的 UNIX 操作系统供应商。对于 HP-UX 和 Solaris 平台上的设备，请参见以下各节。对于其他 UNIX 平台上的设备，请查询各自供应商的信息。

在 HP-UX 中查找设备文件名

在完成以下步骤之前，请使用 /usr/sbin/ioscan -f 命令检查是否已正确连接设备:

1. 在 HP-UX 系统中启动 **System Administration Manager (SAM)** 应用程序。
2. 单击**外围设备**，然后单击**磁带驱动器**。
3. 单击目标设备。
4. 在“操作”菜单中，单击“ShowDevice 文件”。此时将显示设备文件名。使用语法为 *BEST 的文件名。对于非重绕设备，使用语法为 ‘BESTn’ 的文件名。

如果不显示任何设备文件名，则需要创建这些文件名。

在 Solaris 中查找设备文件名

要在 Solaris 上查找设备文件名，请执行以下步骤:

1. 按 **Stop** 和 **A** 停止客户机系统。
2. 在 ok 提示符下，使用 probe-scsi-all 命令检查是否正确连接设备。

   这样可提供有关所连接 SCSI 设备的信息，这些信息应包括所连接备份设备的设备 ID 字符串。
3. 在 ok 提示符下，输入 go 恢复正常运行。
4. 列出 /drv/rmt 的内容，如果使用多驱动器库，则还要列出 /drv 目录:
   - /drv/rmt 目录应包含备份设备的驱动器的设备文件名。
   - 如果使用多驱动器库设备，则 /drv 目录应包含机械手的设备文件名。

如果不显示任何设备文件名，则需要创建这些文件名。

在 UNIX 系统中创建设备文件

如果在系统初始化（引导过程）期间没有创建对应于特定备份设备的设备文件，则必须手动创建这些设备文件。管理库控制设备（库机械手）所需的设备文件就是这种情况。

设备文件的创建过程取决于特定的 UNIX 操作系统供应商。对于 HP-UX 和 Solaris 平台上的设备，请参见以下各节。对于其他 UNIX 平台上的设备，请查询各自供应商的信息。

在 HP-UX 系统上创建设备文件

在完成以下步骤之前，请使用 /usr/sbin/ioscan -f 命令检查是否正确连接设备:

1. 在 HP-UX 系统中启动 **System Administration Manager (SAM)** 应用程序。
2. 单击**外围设备**，然后单击**磁带驱动器**。
3. 单击目标设备。
4. 在“操作”菜单中，单击**创建设备文件**，然后单击**创建默认设备文件**。

在 Solaris 系统中创建设备文件

首先必须更新客户机的设备和驱动程序配置文件，如果使用库设备则安装另一个驱动程序，并在客户机上创建新的设备文件，然后才能在 Solaris 客户机上使用新的备份设备。

1. 按 **Stop** 和 **A** 停止客户机系统。
2. 在 ok 提示符下，运行 probe-scsi-all 命令，以检查客户机系统上的可用 SCSI 地址，然后为要连接的设备选择地址 (适用于单驱动器设备)。在多驱动器设备的情况下，将需要为每个驱动器选择一个 SCSI 地址，还要为机械手机构选择一个。
3. 在 ok 提示符下，输入 go 恢复正常运行。
4. 关闭客户机系统，并将其断电。
5. 在备份设备上设置所选的 SCSI 地址。
6. 如有必要，在将 SCSI 设备连接到相关客户机系统时，关闭系统，并将其断电。
7. 将备份设备连接到客户机系统
8. 首先给备份设备通电，然后再给客户机系统通电（如果之前断电）。

9. 按 **Stop** 和 **A** 再次停止系统。
10. 在 ok 提示符下，运行 probe-scsi-all 命令。

    这样可提供有关所连接 SCSI 设备的信息，包括新连接的备份设备的正确设备 ID 字符串。
11. 在 ok 提示符下，输入 go 恢复正常运行。
12. 编辑配置文件 st.conf，并为驱动器添加所需的设备信息和 SCSI 地址。
13. 如果要将多驱动器设备与库机械手机构相连，则还要执行以下步骤。
    1. 将 sst 驱动程序复制到客户机上，然后进行安装。
    2. 将配置文件 sgen.conf (Solaris 10) 复制到相关客户机系统上，然后进行编辑并针对机械手装置添加一个条目。
    3. 编辑 /etc/devlink.tab 文件，然后针对机械手装置设备文件添加一个条目。
14. 根据需要更新驱动程序和配置文件后，为客户机系统创建新的设备文件：
    1. 从 /drv/mnt/ 目录中删除所有现有设备文件。
    2. 运行命令 shutdown -i0 -g0 ，关闭系统。
    3. 运行命令 boot -rv ，重新启动系统。
    4. 重启完成之后，列出 /dev 目录的内容以检查所创建的设备文件。机械手装置的设备文件应位于 /dev 目录中，而驱动器的设备文件应位于 /dev/rmt 目录中。

自动检测设备文件名和 SCSI 地址

可以自动检测连接到 Windows、HP-UX 或 Solaris 平台的大多数设备的设备文件名（SCSI 地址）。

对于现有的 Data Protector 设备定义

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中，右键单击设备，然后单击**属性**。
4. 单击**驱动器**选项卡。
5. 使用下拉列表可自动检测设备的 SCSI 地址（设备文件名）。

创建 Data Protector 设备定义时

1. 按照配置设备的过程操作。
2. 在向导中，当提示指定设备文件名（SCSI 地址）时，使用下拉列表选择可用设备。

自动检测库的设备文件名和 SCSI 地址

可以自动检测连接到 Windows、HP-UX 或 Solaris 平台的库机械手的设备文件名（SCSI 地址）。

对于已配置的库

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中，右键单击库，然后单击**属性**。
4. 单击**控制**选项卡。
5. 在库的机械手 SCSI 地址区域中，使用下拉列表选择库机械手的可用文件名（SCSI 地址）。

配置库时

1. 按照用于配置库机械手的过程操作。
2. 在向导中，当提示指定 SCSI 地址（文件名）时，使用下拉列表选择库机械手的可用文件名（SCSI 地址）。

配置备份设备

完成准备部分之后，可以配置备份设备，使其与 Data Protector 配合使用。

建议让 Data Protector 自动配置备份设备。Data Protector 可以自动配置最常用的备份设备（包括库）。虽然仍需要为备份会话准备介质，但 Data Protector 可确定设备的名称、策略、介质类型、介质策略和设备文件或 SCSI 地址，并且还可配置驱动器和插槽。

也可以手动配置备份设备。配置备份设备的方式取决于设备类型。

可使用未在发行说明中列为受支持设备的设备。将使用 scsitab 文件配置不支持的设备。

相关任务

- 准备备份设备
- 自动配置备份设备
- 配置独立设备
- 配置备份到磁盘设备
- 配置文件库设备
- 配置堆栈器设备
- 配置介质库设备 (光盘库)
- 配置 SCSI 库或箱盒设备
- 配置 ADIC/GRAU DAS 库设备
- 配置 StorageTek ACS 库设备
- 配置 SAN 环境中的设备

库管理控制台

当前许多磁带库都集成了管理控制台，使您可以在远程执行库的配置、管理和监视任务。库管理控制台是库的 Web 界面，该界面就像普通网页一样显示在 Web 浏览器中。磁带库配备此类 Web 控制台后，即可从任何远程系统执行各种任务。例如，可以设置库配置参数、将磁带加载到库驱动器中以及检查库的当前状态。可远程执行的任务范围取决于管理控制台的实施，它独立于 Data Protector。

每个库管理控制台都有自己的 URL（Web 地址），这是管理控制台界面的入口点。在 Web 浏览器的地址栏中键入此 URL 即可访问控制台界面。

Data Protector 中对库管理控制台的支持

库配置包含表示库管理控制台 URL 的参数。可以在库配置或重新配置过程中指定**管理控制台 URL**。

通过扩展 Data Protector GUI 功能，简化了对管理控制台界面的访问。可调用 Web 浏览器，然后从 Data Protector GUI 中加载控制台界面。根据操作系统，将使用系统默认 Web 浏览器（在 Windows 系统中）或 Data Protector 配置中指定的 Web 浏览器（在 UNIX 系统中）。

重要说明使用库管理控制台之前，请考虑某些可通过控制台执行的操作可能会妨碍介质管理操作和/或备份和还原会话

不支持输入空格和双引号作为管理控制台 URL 的一部分；而应输入安全的 URL 代码。下表中显示了不受支持的字符及其安全 URL 代码等效字符。

字符	安全 URL 代码
空格	%20
双引号 (")	%22

访问库管理控制台界面

在配置库的过程中，需要指定库管理控制台的有效 URL。完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示已配置设备的名称的列表。
3. 右键单击所需的库，然后单击**管理控制台**。等待 Web 浏览器启动并加载控制台界面。

通过在“操作”菜单中单击**管理控制台**，也可以访问所选库的管理控制台。

重要说明通过管理控制台可访问的库配置参数可能与作为 Data Protector 中库配置一部分的参数相关。因此，每次通过管理控制台修改库配置时，必须检查和 (可选) 调整 Data Protector 中的库配置，反之亦然。

还应避免多个管理员使用库管理控制台界面的多个实例同时操作库的情况。

相关任务

- 访问库管理控制台界面
- 配置介质库设备 (光盘库)
- 配置 SCSI 库或箱盒设备
- 配置 StorageTek ACS 库设备
- 配置 ADIC/GRAU DAS 库设备
- 手动配置 SAN 环境中的设备

自动配置备份设备

将备份设备连接到要配置的系统并且存在正常工作的设备文件（SCSI 地址）之后，可以配置该备份设备与 Data Protector 配合使用。自动配置表示 Data Protector 将为您创建设备定义。

Data Protector 可以检测和自动配置连接到 SAN 中一个或几个系统的最常用备份设备。以后可以修改自动配置的设备的属性，以使其适合您的特定需要。

以下操作系统中可以进行自动配置：

- Windows
- HP-UX
- Solaris
- Linux

> **注意**如果在可移动存储服务运行时自动配置库，则将无法正确组合驱动器和机械手（更换器）。

要自动配置的每个客户机系统必须装有介质代理。

设备自动配置

执行以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**自动配置设备**以打开向导。
3. 选择含有要配置的设备的客户机系统，然后单击**下一步**。
4. 选择系统上要配置的备份设备。单击“下一步”。
5. 要启用对已更改 SCSI 地址的自动发现，请选择**自动发现已更改的 SCSI 地址**，然后单击**完成**。对于箱盒设备，在自动配置后将介质池更改为支持箱盒的一个池。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。

SAN 环境中的设备自动配置

Data Protector 提供 SAN 环境中的设备自动配置，此环境中不同客户机使用一个库中的磁带驱动器。Data Protector 自动配置功能可在多个客户机系统上自动配置设备和库。

Data Protector 确定设备的名称、锁名称、策略、介质类型、介质策略和设备文件或 SCSI 地址，并配置驱动器和插槽。

> **注意**将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。
>
> - 如果要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
> - 如果要将设备添加到现有库，或者可以删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者可以手动将驱动器添加到库中。

以下限制适用：

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

要在 SAN 环境中自动配置设备，请执行以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**自动配置设备**以打开向导。
3. 选择要配置的客户机系统。在 Microsoft 群集服务器环境中，选择虚拟服务器。

   单击“下一步”。
4. 选择系统上要配置的设备和库。
5. 配置库时，选择控制主机，即库对多个客户机可见时将控制库机械手的客户机。如果可看到库的系统之间有 Cell Manager，则默认情况下选择它。可以在以下两个视图之间切换：
   - 按设备分组

     显示所有设备和库的列表。展开库或设备，然后选择要从中配置库或设备的客户机系统。
   - 按主机分组

     显示连接了设备的客户机的列表。展开要从中配置设备或库的客户机。
6. （可选）要启用多路径设备，请选择**自动配置多路径设备**。单击“下一步”。
7. 要启用对已更改 SCSI 地址的自动发现，请选择**自动发现已更改的 SCSI 地址**。
8. 单击**完成**。此时将显示所配置设备的列表。

可以扫描设备以验证配置。

配置独立设备

将备份设备连接到系统并且存在正常工作的设备文件（SCSI 地址）之后，可以配置该备份设备与 Data Protector 配合使用。

建议让 Data Protector 自动配置备份设备。

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. （可选）选择**多路径设备**。
6. 如果*未*选择**多路径设备**选项，则从“客户机”下拉列表中选择客户机（备份系统）的名称。
7. 在“设备类型”列表中，选择“独立设备”设备类型，然后单击“下一步”。
8. 输入物理设备的 SCSI 地址（Windows 系统）或设备文件名（UNIX 系统），然后单击**添加**。

   对于多路径设备，从下拉列表中选择客户机，然后输入该设备的设备文件名。单击**添加**，将路径添加到所配置路径的列表中。

   > **提示**可以输入多个地址以创建设备链。
   >
   > 向设备链添加设备的顺序决定了 Data Protector 使用这些设备的顺序。
   >
   > 当设备链中的所有介质都装满后，Data Protector 将发出装载请求。将第一个设备中的介质替换为新介质，格式化新介质，然后确认装载请求。Data Protector 可以立即使用已识别且不受保护的介质。还可以使用空白介质。

9. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击“下一步”。
10. 在“介质类型”列表中，对要配置的设备选择介质类型。
11. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
12. 单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。如果正确配置了设备，则 Data Protector 将可以在插槽中加载、读取和卸载介质。

配置备份到磁盘设备

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。Data Protector 支持各种 B2D 设备，以支持本地、远程和云备份方案。

要添加 B2D 设备 (定位到现有存储)，请继续执行以下步骤。

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 指定设备名称及其说明（可选）。
4. 选择**备份到磁盘**设备类型，然后选择**接口类型**：**StoreOnce 备份系统**、**数据域提升**、**StoreOnce 软件**、**云 (Azure)**、**云 (Amazon S3)**、**云 (Amazon S3 Glacier)**、**云 (Amazon S3 Glacier Deep Archive)** 或**智能缓存**。
5. 配置设备的步骤因所选的接口类型而异。
   - 配置 StoreOnce Catalyst
   - 配置 StoreOnce 软件重复数据删除
   - 配置数据域提升
   - 配置智能缓存
   - 配置云 (Azure)
   - 配置云 (Amazon S3)
   - 配置云 (Amazon S3 Glacier)
   - 配置云 (Amazon S3 Glacier Deep Archive)

多接口支持

Data Protector 提供多接口支持。Data Protector 支持与同一 StoreOnce Catalyst/DDBoost 存储建立 IP 以及光纤通道连接，而无需配置单独的存储。可同时通过这两种接口访问存储。例如，有时本地客户机可通过光纤通道访问单个 Catalyst/DDBoost 存储以执行较快的备份，而远程客户机可通过 WAN 访问同一存储以执行较慢的备份。在 Solaris 环境中或 FC 配置为重复数据删除目标的标识符时，此功能不可用。此选项仅适用于 StoreOnce 备份系统和 DD Boost。

重要说明添加 StoreOnce 或 DDBoost 设备时，强烈建议使用 IP 地址或主机名，以利用多接口功能。

配置备份到磁盘设备 - StoreOnce

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。

如果要配置 StoreOnce 软件重复数据删除设备，则需要执行一些其他步骤。请参阅配置备份到磁盘设备 - StoreOnce 软件。

注意Data Protector 最多支持八个成员的联合存储。可以在 StoreOnce 中更改存储中的成员数。要反映此更改，可以使用 Data Protector GUI 或 CLI 手动刷新 Data Protector 缓存。有关详细信息，请参阅刷新存储的缓存。所有联合成员均必须联机，联合存储才能发挥作用。

要添加 StoreOnce 备份系统或 StoreOnce 软件 B2D 设备（定位到现有存储），请按以下步骤操作：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 指定设备名称及其说明（可选）。
4. 选择**备份到磁盘**设备类型，然后选择接口类型：“StoreOnce 备份系统”或“StoreOnce 软件”。
5. （可选）在**管理控制台 URL** 文本框中输入设备管理控制台的有效 URL。单击“下一步”。
6. 对于 StoreOnce 备份系统设备，请输入**客户机 ID** 和密码（可选）以访问存储。可在密码中使用以下字符: [a-z][A-Z][0-9][_-.+()\{\}:#$*;=?@[]^|~]?
7. 在“重复数据删除系统”框中，输入重复数据删除系统的 IP 地址、主机名、完全限定域名 (FQDN) 或光纤通道 (FC) 地址 (重复数据删除存储所在的宿主计算机)。

   或单击**选择服务集**，查询并检索重复数据删除系统的地址。

   注意对于 StoreOnce 软件重复数据删除，支持 IPv4 或 IPv6 地址或者 FQDN。但是，对于 StoreOnce 备份系统接口，如果使用最新的 StoreOnce Catalyst 版本，则支持 IPv4 或 IPv6 地址、FQDN 或 FC 全局标识符。

   如果使用 FC 连接到 StoreOnce 备份系统，请指定设备的 FC 地址。确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

8. 单击**选择/创建存储**按钮，选择现有的联合或非联合存储，或者创建非联合存储。从列表中选择存储名称。

   要创建加密存储，请选择**已加密存储**选项。单击**确定**。

   > 只能在创建存储区时启用加密功能。存储一经创建，就无法将其从已加密状态转换成未加密状态，反之亦然。StoreOnce 软件重复数据删除设备不支持存储加密。
   > 不能使用 Data Protector GUI 创建联合存储。需要使用 StoreOnce 管理控制台创建它们。

9. （可选）选择**源端重复数据删除**以启用源端重复数据删除。此时将打开“源端重复数据删除属性”窗口。查看属性并在需要时进行修改。默认情况下，源端网关将命名为 DeviceName_Source_side 。注意，只能为每个设备创建一个源端网关。如果在备份规范中启用了源端重复数据删除，则在备份的系统上此（虚拟）网关将被自动扩展。

   > **注意**对于联合存储，所有写入操作均在低带宽模式中执行（服务器端重复数据删除）。即使网关配置为目标端重复数据删除（高带宽模式），它也会自动切换到低带宽模式。

10. 选择一个网关，然后单击**添加**以显示“属性”对话框。根据需要更改任意网关属性，然后单击**确定**添加网关。如果使用 FC 连接到 StoreOnce 备份系统，请确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

    > **注意**连接到 Data Protector 网关的联合成员必须是联合存储的成员。如果使用 StoreOnce 缩小了联合成员，请使用刷新存储的缓存中提到的步骤，将 Data Protector 网关调整为连接到其他联合成员。

    要查看网关属性，请选择所需的网关然后单击**属性**。要设置其他网关选项，请单击**设置**选项卡，再单击**高级**打开“高级”属性窗口。

    在“高级属性”窗口中，要限制每个网关上的流数，请选择“每个网关的并行流的最大数量”。可以指定最多 100 个流。如果未选择此选项，则不限制流数。注意，还可以在创建备份规范时设置此选项。在这种情况下，B2D 设备创建过程中指定的值将被覆盖。

    要限制网关所使用的网络带宽，请选择**限制网关网络带宽(Kbps)** 并输入以每秒千位 (kbps) 为单位的限制。

    要启用服务器端重复数据删除，请选择**服务器端重复数据删除**。

    如果已配置 IP 地址或 FQDN 作为重复数据删除目标，则**使用 FC** 和**回退至 IP** 选项可用，并且它们默认处于选中状态。

11. 要验证连接，请单击**检查**。

12. 单击**下一步**进入“设置”窗口，在此窗口中可以指定以下选项：

    - 每个存储的最大连接数量
    - 备份大小软配额 (GB)
    - 存储大小软配额 (GB)
    - **催化剂项目大小阈值(GB)**：为 StoreOnce Software Deduplication 和 StoreOnce 备份系统设备定义催化剂项目的阈值大小。如果当前的催化剂项目超过此大小，您将无法再向其中附加更多对象。默认情况下，催化剂项目的大小是无限制的。
    - **每个催化剂项目单个对象**：选中后，对于 StoreOnce Software Deduplication 和 StoreOnce 备份系统设备，每个催化剂项目启用一个对象。

13. 单击**下一步**以显示“摘要”窗口，其中包括已配置 B2D 存储的详细信息。此外，对于联合存储，它还包括所有联合成员及其状态（联机或脱机）的列表。

14. 检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

刷新联合 StoreOnce 商店的缓存

使用 StoreOnce 3.12 及更高版本，可以在联合存储中添加或删除联合成员。要反映此更改，可以使用 Data Protector GUI 或 CLI 手动刷新 Data Protector 缓存。

使用 Data Protector GUI 刷新缓存

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，展开**设备**。
3. 右键单击所需的 StoreOnce 设备，然后单击**属性**。
4. 单击**存储和网关**选项卡，然后单击**选择/创建存储**。如有必要，更改目录路径，使其包括当前活动的联合成员的地址。
5. 选择与此 StoreOnce 设备关联的同一存储，然后单击**确定**。
6. 单击“应用”。

使用 Data Protector CLI 刷新缓存

1. 请执行以下命令：

   omnidownload –library <DPDeviceName> -file <DPDeviceOutputFile>

2. 编辑 DPDeviceOutputFile。

   如果设备未联合，请删除以下行：

   B2DTEAMEDSTORE 1

   B2DTEAMEDMEMBERS

   “<teamed.device.one>”

   “<teamed.device.two>”

   ...

   如果设备已联合，请在替换适当的成组设备 IP 地址后，将这些行添加到 DPDeviceOutputFile。如有必要，更改目录路径，使其包括当前活动的联合成员的地址。

   > **注意:** 地址和格式应该与 StoreOnce 成组策略文件中的地址和格式完全匹配。例如，如果成组策略文件包括 IPv6 地址，则必须也在此文件中添加相同地址。

3. 使用以下命令保存修改后的文件：

   omniupload –modify_library <DPDeviceName> -file <DPDeviceOutputFile>

配置备份到磁盘设备 - StoreOnce 软件

如果您正在配置 StoreOnce Software Deduplication 设备，需要额外的步骤。

- 配置重复数据删除存储的根目录
- 创建存储

配置重复数据删除存储的根目录

本节描述了如何配置存储的根目录。此操作必须在安装软件后、创建第一个重复数据删除存储前完成。

如果存储共享相同的根目录，一个 StoreOnce Software Deduplication 系统可以托管多个重复数据删除存储。每个存储的操作独立于其他存储，即，重复数据删除仅发生在一个存储内，每个存储有其自己的索引表。虽然所有存储在相同进程下运行，但可以单独启动/停止 (这并不表示以物理方式启动/停止存储，有关详细信息，请参阅 *《重复数据删除白皮书 -附录 A: StoreOnceSoftware 实用程序》*)。如果操作停止（脱机），则不能在存储上完成。

不能以物理方式分隔共享相同根目录的存储。该设计确保在所有磁盘上统一加载，并提供更好的性能。

安装成功后，StoreOnceSoftware 实用程序以正在运行但等待配置存储根目录的模式启动。在配置根目录之前，无法添加 B2D 设备，无法创建存储。

可通过以下方式配置存储根目录：

- GUI: 遵循添加设备的步骤，出现提示时，指定根目录 (有关详细信息，请参阅下文)。
- CLI: 使用命令 StoreOnceSoftware --configure_store_root (请参阅《重复数据删除白皮书 - *附录 A: StoreOnceSoftware 实用程序》*)。

> **注意**: 根目录必须已经存在 (在服务器上)，必须具有写入权限才能对其进行配置。这是因为 (GUI) 配置过程要求您指定其位置。

使用 GUI 配置根目录的过程与创建存储类似，但包括一些额外步骤。配置好根目录后，不再需要这些额外步骤。要配置根目录（同时创建存储），请按如下方式继续操作：

1. 按照添加设备的过程操作：
   1. 在“设备和介质”上下文中，右键单击**设备 > 添加设备**。
   2. 指定设备名称，添加说明，选择设备类型**备份到磁盘**，然后选择接口 **StoreOnce Software Deduplication**。
   3. （可选）在**管理控制台** URL 文本框中输入设备管理控制台的有效 URL。
   4. 单击**下一步**以显示可指定存储和网关列表的屏幕。
   5. 对于 StoreOnce 备份系统设备，请输入**客户机 ID** 和**密码**（可选）以访问存储。
2. 在“重复数据删除系统”框中，输入重复数据删除存储所在的宿主计算机的主机名、IP 地址或完全限定域名 (FQDN)。
3. 选择一个网关，单击**添加**以显示属性对话框，然后单击**确定**以添加该网关。
4. 单击**检查**。“根目录未配置”消息随即显示。
5. 在对话框中，指定根目录路径（例如，C:\Volumes\StoreOnceRoot），所有存储都将驻留在该路径下，然后单击**确定**。（注意：无法浏览到有效的根目录)。
6. 如果根目录存在，对话框关闭，设备配置继续。StoreOnceSoftware 实用程序在指定的根目录中创建子目录（存储）。如果根目录不存

在，将显示错误消息。
7. 继续执行添加设备的过程。

配置根目录和创建存储时，注意以下几点：

- 不要使用安装操作系统 (OS) 的相同磁盘。
- 使用专用（独有）存储磁盘。
- 在每个卷上，Data Protector 支持最多 32 个存储。

> 在 Windows 系统上，要改进性能，请将以下选项应用于将放置存储根的 NTFS 卷：
> 使用以下命令，在卷上禁用短（类似于 DOS）文件名的创建： fsutil behavior set Disable8dot3 Volume 1
> 使用以下命令，增加 NTFS 内部日志文件大小： Chkdsk Volume /L:131072

创建存储

创建存储之前，确保存储的根目录已配置，并且物理存储磁盘（LUN 设备）已格式化且已装载到 StoreOnce Software Deduplication 系统。LUN 设备可位于本地磁盘或磁盘阵列 (SCSI 或光纤通道接口) 或相同 LAN 的 NAS 设备 (iSCSI 接口)。使用 iSCSI 接口时，可靠的网络连接必须提供不超过 2 毫秒的延迟和至少 1 GB/秒的吞吐量。

可通过以下方式创建存储：

- GUI: 遵循添加设备的步骤，出现提示时，指定存储的名称 (有关详细信息，请参阅下文)。
- CLI: 使用命令 StoreOnceSoftware --create_store。

创建存储的过程与添加设备类似，但包括一些额外步骤。要创建存储，请执行以下操作：

1. 按照添加设备的过程操作：
   1. 在“设备和介质”上下文中，右键单击**设备 > 添加设备**。
   2. 指定设备名称，添加说明，选择设备类型**备份到磁盘**，然后选择接口 **StoreOnce Software Deduplication**。
   3. 单击**下一步**以显示可指定存储和网关列表的屏幕。
2. 选择重复数据删除系统，并为存储指定名称。存储名称的最大长度为 80 个字符（仅字母数字字符）。
   1. 选择一个网关，单击**添加**以显示属性对话框，然后单击**确定**以添加该网关。
   2. 单击**检查**验证连接。如果存储不存在，则会创建。（注意：单击“下一步”时，还会验证连接。）
   3. 继续执行添加设备的过程。

如果您指定的存储名称不正确，将无法通过 GUI 更改。再次运行该过程，并以正确名称创建存储。使用 CLI 删除名称错误的存储（假设数据未写入）。

配置备份到磁盘设备 - 数据域提升

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。

以下先决条件适用:

- 要支持在数据域设备之间进行复制，必须在数据域设备上启用虚拟合成和分布段处理 (DSP)。
  - 可以使用 Data Domain System Manager (DDEM) 或 ssh 启用它。要使用 ssh 配置它，请连接到数据域设备，然后运行以下命令:

```
ddboost option show ddboost option set virtual-synthetics enabled ddboost option set distributed-segment-processing enabled
```

- 要支持复制，必须在具有相同管理角色的源设备和目标设备上配置同一数据域提升用户名和密码。在源和目标数据域系统上需要复制许可证。有关详细信息，请参见您的数据域文档。
- 如果通过相同或不同的备份应用程序为多个存储单元 (LSU) 配置了数据域系统，建议在 Data Protector 使用的存储单元上启用软**或**硬配额。这样可以正确报告“高级备份到磁盘”许可证要求。

以下限制适用：

- 执行交互复制时，只能选择一个会话进行复制。
- 如果修改加密强度的默认值，则不支持 Data Protector 操作。

> 提到数据域提升设备时，使用“存储单元”一词，而非“存储”。

要添加 DDBoost B2D 设备（以现有存储为目标），执行以下操作：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。

3. 指定设备名称及其说明（可选）。
4. 选择**备份到磁盘**设备类型，然后选择**接口类型**：**数据域提升**。
5. （可选）在**管理控制台 URL** 文本框中输入设备管理控制台的有效 URL。单击“下一步”。
6. 输入**用户名**和**密码**。可在密码中使用以下字符: [a-z][A-Z][0-9][_-.+(){}:#$*;=?@[]^|~]?
7. 输入存储单元名称（假设存储单元已经存在）。
8. 在**重复数据删除系统**文本框中，输入重复数据删除系统的主机名、IP 地址或 FC 地址（重复数据删除存储单元所在的宿主计算机）。

   > 建议您使用 IP 地址或 FQDN 以利用多接口功能。要了解此功能的相关内容，请参阅多接口支持。

9. （可选）选择**源端重复数据删除**以启用源端重复数据删除。此时将打开“源端重复数据删除属性”窗口。查看属性并在需要时进行修改。默认情况下，源端网关将命名为 DeviceName_Source_side 。注意，只能为每个设备创建一个源端网关。如果在备份规范中启用了源端重复数据删除，则在备份的系统上此（虚拟）网关将被自动扩展。
10. 选择一个网关，然后单击**添加**以显示“属性”对话框。根据需要更改任意网关属性，然后单击**确定**添加网关。

    要查看网关属性，请选择所需的网关然后单击**属性**。要设置其他网关选项，请单击**设置**选项卡，再单击**高级**打开“高级”属性窗口。

    要限制每个网关上的流数，请选择**每个网关的并行流的最大数量**。可以指定最多 100 个流。如果未选择此选项，则不限制流数。注意，还可以在创建备份规范时设置此选项。在这种情况下，B2D 设备创建过程中指定的值将被覆盖。

    要限制网关所使用的网络带宽，请选择**限制网关网络带宽(Kbps)** 并输入以每秒千位 (kbps) 为单位的限制。

    如果已配置 IP 地址或 FQDN 作为重复数据删除目标，则**使用 FC** 和**回退至 IP** 选项可用，并且它们默认处于选中状态。

    要启用服务器端重复数据删除，请选择**服务器端重复数据删除**。
11. 要验证连接，请单击**检查**。
12. 单击**下一步**进入“设置”窗口，在此窗口中可以指定以下选项：
    - **每个存储单元的最大连接数量**：定义限制物理连接的最大读写流的中值。
    - **备份大小软配额(GB)**：输入备份大小软配额 (GB)
    - **存储大小软配额(GB)**：如果已创建存储单元，或者如果已手动为整个数据域操作系统 (DD OS) 启用配额并在创建存储单元时指定配额，则支持该设置。
    - **存储介质项目大小阈值(GB)**：定义数据域提升设备的存储项的阈值大小。如果当前的存储项超过此大小，您将无法再向其中附加更多对象。默认情况下，存储项的大小是无限制的。
    - **每个存储介质项单个对象**：选中后，对于数据域提升设备，每个存储项启用一个对象。
13. 单击**下一步**以显示“摘要”窗口，其中包括已配置 B2D 存储单元的详细信息。
14. 检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

在 AIX 系统上配置数据域提升

要在 AIX 系统上配置通过光纤通道 (FC) 协议的数据域提升，您必须安装 AIX DDdfc 设备驱动程序。驱动程序文件名为 DDdfc.1.0.0.x.bff，其中 x 是版本号。

1. 作为 root 用户，登录 AIX 客户机。
2. 输入 `# smitty install` 命令。
3. 选择**安装和更新软件**。
4. 选择**安装软件**。
5. 输入路径 /usr/omni/drv 以安装 DDdfc.1.0.0.x.bff 文件，其中，x 是版本号。
6. 按 **F4**，选择想要安装的 DDdfc.1.0.0.x 版本。
7. 按 **Tab**，将“仅预览？”行的值切换至“否”。
8. 按 **Enter**，接受信息并安装驱动程序。

配置备份到磁盘设备 - 智能缓存

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。

以下先决条件适用:

- 在磁盘上的所需位置中为智能缓存设备手动创建目录。
  - 您可以在 Windows 和 Linux 的本地驱动器上创建智能缓存设备 (例如介质代理上的 c:\SmartCache 或 /SmartCache) 或 Linux 系统的 NFS 装载文件系统。
  - 在 Windows 上，确保“智能缓存主机凭据” 用户在用于智能缓存的目录上具有“完全控制” (文件系统权限) 。这是从智能缓存设备进行粒度恢复操作所必需的。
  - 您也可以在网络驱动器上创建智能缓存设备。要指定网络驱动器，请使用以下格式： \\hostname\share_name 。“浏览驱动器”对话框中没有显示主机名以及共享名称和网络驱动器。必须输入 UNC 名称的路径。这需要将介质代理上的 Data Protector Inet 帐户从系统帐户更改为具有网络共享访问权限的特定用户帐户。

- 对于 Linux 操作系统，必须在智能缓存客户机上安装和运行 Samba 服务器，这是因为 Data Protector 在恢复期间使用 Samba 服务器创建共享。要验证 Samba 服务器是否正在运行，请执行以下命令： ps -ef | grep smbd 。Samba 服务器的默认安全模式为*用户级*。如果更改了默认模式，则必须使用以下命令将其更新为*用户级*： [global] security = user 。
- 确保 Samba 共享具有读写权限。如果已在 Linux 系统中部署增强安全机制的 Linux (SELinux) 内核安全模块，请执行 # setsebool -P samba_export_all_rw on 命令来启用对 Samba 共享的读写权限。
- 在 Samba 服务器中，必须使用以下命令将介质代理主机的用户添加到 Samba 密码数据库： smbpasswd –a <user> 。可以使用以下命令验证用户是否已添加到密码数据库： pdbedit -w -L 。
- 必须定期清理 Samba 配置文件 (smb.conf)。这可确保以前的 Samba 共享配置信息被删除。
- 必须将整个文件系统专用于一个智能缓存设备。此文件系统不应由其他应用程序使用，也不应由其他智能缓存/备份到磁盘设备共享。
- 仅可将单个介质池与一个智能缓存设备相关联。

以下限制适用：

- 智能缓存仅在 Windows x64 和 Linux x64 平台上可用。
- 智能缓存仅可用作 VMware 备份的目标。
- 在 Linux 操作系统上，如果已安装 NDMP 介质代理，则不支持备份到智能缓存。
- 不支持已编码或 AES 256 位已加密的 VMware 备份到智能缓存设备。
- 不支持源到智能缓存设备的已编码或 AES 256 位已加密的对象复制。但是，支持在具有硬件加密的磁带设备中进行对象复制。
- 每个智能缓存设备仅支持一个装载点。
- 智能缓存设备不支持导出和导入介质。
- 如果在复原文件系统 (ReFS) 卷或网络共享 (CIFS/NFS) 上创建智能缓存设备，请在同一主机上安装 VMware Granular Recovery Extension 代理组件 (用于恢复)，否则非暂存恢复将失败。
- 在 StoreOnce 系统上，智能缓存设备配置不支持 CIFS。

完成以下步骤：

1. 在 Data Protector 的上下文列表中，单击“设备和介质”。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 指定设备名称及其说明（可选）。
4. 选择**备份到磁盘**设备类型，然后选择**智能缓存**接口类型。
5. 在“客户机”下拉列表中，选择设备所在的系统。单击“下一步”。
6. 输入需要访问共享的用户的用户名和密码。
7. 指定智能缓存设备的目录。单击**添加**。
8. 要更改目录的默认属性，请选择该目录，然后单击**属性**。
9. 单击**下一步**以显示“摘要”窗口。检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

配置备份到磁盘设备 - 云 Azure

在 Data Protector 中，配置“备份到磁盘”设备，并将“接口类型”设置为: “云 (Azure)”。

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在**设备名称**字段指定设备名称，可选填**说明**字段。
4. 选择**备份到磁盘**设备类型，然后选择**接口类型**：“云 (Azure)”。单击“下一步”。

   默认情况下会输入**管理控制台 URL**。
5. 在字段中输入**存储帐户名**、**密钥**和**密钥 2** 的信息。单击**添加**添加网关以向云 (Azure) 发送数据。此时将显示“选择容器”窗口。
6. 选择现有的容器或创建新的容器以上载数据。可以通过默认值添加网关。

   对象复制的块大小存在限制。如果将对象从本地设备复制到云，并复制回同一设备以备恢复，则本地设备和云设备的块大小必须匹配。
7. 单击**检查**验证网关是否已连接到云 (Azure)。如果连接成功，则“状态”显示为**正常**。设备已创建且可供使用。

配置备份到磁盘设备 - 云 Amazon S3

在 Data Protector 中，配置“备份到磁盘”设备，并将“接口类型”设置为: 云 (Amazon S3)。执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 API 兼容目标)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“S3 目标类型”。
   - 如果要创建指向 Amazon S3 的设备，请选择“AWS S3”。
   - 如果要创建指向内部部署目标的设备 (Amazon S3 API 兼容)，请选择“Ceph/Scality”。
7. 指定网关。
   - **AWS S3**: 选择散列存储可用的“S3区域”，或要创建散列存储的区域。
   - **Ceph/Scality**: 对于内部部署目标，输入网关 URL。

   如果将对象从本地设备复制到云，并复制回同一设备以备恢复，则本地设备和云设备的块大小必须匹配。

8. 指定“访问密钥 ID”和“密码访问密钥”信息。
9. 单击“选择/创建散列存储”以获取已创建的所有散列存储列表并显示它们。此时将显示“选择散列存储”窗口。

   选择现有散列存储或新建散列存储以上载数据。

10. 单击“添加”以添加网关。
11. 单击“检查”以验证网关是否已连接到云 (Amazon S3/Ceph/Scality)。如果连接成功，则状态显示为“正常”。
12. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

配置备份到磁盘设备 - 云 Amazon S3 Glacier

在 Data Protector 中，配置“备份到磁盘”设备，并将“接口类型”设置为: 云 (Amazon S3 Glacier)。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 Glacier)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“Glacier 区域”。
7. 提供 Glacier 帐户的“访问密钥 ID”和“密码访问密钥”。
8. 单击“选择/创建保管库”。此时将显示“选择保管库”窗口。可以选择现有保管库，或创建一个新保管库。单击**确定**。
9. 单击“添加”以添加网关。此时将显示“添加网关”窗口。提供“网关名称”，然后单击“确定”。
10. 单击“检查”以验证网关是否已连接到云 (Amazon S3 Glacier)。如果连接成功，则状态显示为“正常”。
11. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

配置备份到磁盘设备 - 云 Amazon S3 Glacier Deep Archive

在 Data Protector 中，配置“备份到磁盘”设备，并将“接口类型”设置为: 云 (Amazon S3 Glacier Deep Archive)。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”字段中，指定设备名称，然后添加“描述”。
4. 选择“备份到磁盘”设备类型，然后将“接口类型”设置为“云 (Amazon S3 Glacier Deep Archive)”。
5. 单击“下一步”。默认情况下会列出管理控制台 URL。
6. 在“云连接设置”下，选择“S3 区域”。
7. 提供 Glacier 帐户的“访问密钥 ID”和“密码访问密钥”。
8. 单击“选择/创建散列存储”。此时将显示“选择散列存储”窗口。可以选择现有散列存储，或创建一个新散列存储。单击**确定**。
9. 单击“添加”以添加网关。此时将显示“添加网关”窗口。提供“网关名称”，然后单击“确定”。
10. 单击“检查”以验证网关是否已连接到云 (Amazon S3 Glacier Deep Archive)。如果连接成功，则状态显示为“正常”。
11. 单击“下一步”。将显示“摘要”页。单击“完成”完成向导。

配置文件库设备

请注意，文件库设备所在的磁盘必须在介质代理的本地。否则，设备性能可能会降低。

确保满足以下条件:

- 文件库设备所在的磁盘必须在文件库设备所在的文件系统中可见。
- 文件库设备所在的磁盘上必须存在其中要创建文件库设备的内容的目录。
- 如果要在 Windows 系统上创建文件库设备，需为要用作文件库设备的文件禁用 Windows 压缩选项。

以下限制适用：

- 文件库设备可以包括一个或多个目录。但只有一个目录可以位于文件系统上。
- 可用于配置文件库类型设备的目录的路径名长度不能超过 46 个字符。

要配置文件库设备，请执行以下任务:

1. 在希望文件库设备所在的磁盘上为该设备创建一个目录，例如： c:\FileLibrary 。

   > **注意**可以在本地或网络驱动器（或 UNIX 系统中由 NFS 装载的文件系统）上创建文件库设备。可以按 \\hostname\share_name 形式指定网络驱动器。

   “浏览驱动器”对话框中输入路径的地方没有显示主机名以及共享名和网络驱动器。需要自行输入 UNC 名称或网络驱动器的路径。

   在 **Windows** 操作系统上，要获取访问文件库设备所在的共享磁盘的正确权限，请更改介质代理上的 Data Protector Inet 帐户 (通过向其授予本地客户机系统和远程共享磁盘的访问权限)。此外，确保它是特定用户帐户，而非系统帐户。设置 Inet 帐户后，即可配置和使用共享磁盘上的文件库设备。

   > **重要说明**不要从磁盘删除为文件库创建的目录。如果删除了该目录，则将丢失文件库设备中的任何数据。

2. 在 Data Protector Manager 上下文列表中，单击“设备和介质”。
3. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
4. 在“设备名称”文本框中，键入文件库设备的名称。
5. 在“说明”文本框中，键入库的说明（可选）。
6. 在“设备类型”下拉列表中，选择**文件库**。
7. 在“客户机”下拉列表中，选择设备所在的系统。单击“下一步”。
8. 指定希望库所在的目录或一组目录。单击**添加**。
9. 要更改目录的默认属性，请选择该目录，然后单击**属性**。
10. 输入文件库设备的写入程序数量。默认为所添加的目录的数量。如果所添加的写入器多于设备中的目录数，则可能将提高设备性能。这一点取决于硬件配置。需要在环境中测试这一点。单击“下一步”。
11. 文件库设备的“介质类型”为“文件”。要在此文件库中启用虚拟完整备份，请选择**使用分布式文件介质格式**。单击“下一步”。
12. 查看文件库设备配置的摘要。单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。设备名称还显示在向其分配该设备的介质池中。

直到第一次使用该设备，该设备中才会显示文件仓库。第一次使用该设备之后，可以扫描该设备以验证配置。

默认情况下，由文件库使用的介质池的介质使用策略为不可追加。建议使用此策略，因为这样可使您从文件库中受益，如自动重用过期的介质。此外，要使用文件库执行对象复制或对象合并，必须采用不可追加的介质使用策略。

将介质从文件库导入其他主机

以下限制适用：

- 只能将数据从位于不同主机上的文件库中的介质导入目标系统上的文件介质库。
- 无法从使用分布式文件介质格式的文件库导入或导出介质。要清理已备份的分布式文件库，请参阅无法清理分布式文件库。

完成以下步骤：

1. 将要发送到不同主机的数据从文件库复制到目标主机上的目录（例如通过 FTP）。
2. 在目标主机上将包含源数据的文件介质库中创建一个插槽。

3. 选择这个新插槽。
4. 从刚复制的文件将数据导入目标主机。

配置设备的多条路径

SAN 环境中的设备通常连接到若干客户机，因此可以通过若干路径访问该设备，这些路径包括客户机名称和 SCSI 地址（UNIX 系统中的设备文件）。Data Protector 可以使用这些路径中的任意一种。您可以将所有物理设备路径配置为单个逻辑设备 — *多路径设备*。

例如，连接到 client1 的磁带设备配置为 /dev/rs1 和 /dev/rs2 ，在 client2 上配置为 /dev/r1s1 ，在 client3 上配置为 scsi1:0:1:1 。因此，可以通过四条不同的路径访问该设备： client1:/dev/rs1 、 client1:/dev/rs2 、 client2:/dev/r1s1 和 client3:scsi1:0:1:1 。因此，多路径设备包含指向此磁带设备的所有四个路径。

为何使用多条路径

如果使用以前版本的 Data Protector，只能从一个客户机访问设备。为解决此问题，必须为使用锁名称的物理设备配置多个逻辑设备。因此，如果使用锁名称来配置从不同系统对单个物理设备的访问，就不得不在每个系统上配置所有设备。例如，如果有 10 台客户机与单个设备连接，则必须用相同的锁名称配置 10 台设备。而使用当前版本的 Data Protector 简化了这一配置过程，您可以为所有路径配置单个多路径设备。

多路径设备可提高系统的复原能力。Data Protector 将尝试使用所定义的第一个路径。如果某台客户机上的所有路径都不可访问，Data Protector 会尝试使用下一台客户机上的路径。只有当所有列出的路径都不可用时，才会中止会话。

路径选择

备份会话期间，按设备配置期间定义的顺序选择设备路径，但如果在备份规范中选择了首选客户机则例外。在这种情况下，首先使用首选客户机上的路径。

还原会话期间，按以下顺序选择路径：

1. 还原对象的目标客户机上的路径，如果*所有*对象都还原到同一目标客户机
2. 过去用于备份的路径
3. 其他可用路径

对于配置了多个路径的设备，首选本地路径。如果没有本地路径可用，则以预定义顺序使用任何可用路径。

如果启用了直接库访问功能，则无论配置了什么顺序，都会首先使用本地路径（目标客户机上的路径）进行库控制。

Data Protector 备份会话管理器 (BSM) 在多路径 SAN 环境中尽可能使用本地设备。可使用 LANfree 全局选项调整此行为。可使用 LANfree 全局选项调整此行为。

LANfree 全局选项具有两个可能的值:

- 0 – 是默认值。对于 Data Protector 8.11 之前的较早版本，无需进行任何更改。
- 1 – 适用于具有以下特点的多路径环境：Data Protector 选择生成对象的主机，而不是从多路径列表中选择首选主机或第一个主机。

  下文介绍 LANfree 全局选项设置为 1 时多路径设备分配的实际改进。

  - Data Protector 会为具有已配置到某主机的路径的设备首选该主机，数据将源自该主机。
  - Data Protector 在生成数据的主机上为已配置主机路径的设备启动新介质代理 (MA)。即使已通过可用的并发插槽为目标设备启动远程 MA，也会执行此操作。

在以下情况下，Data Protector 可能还无法对设备使用本地路径：

- 如果用户已指定负载均衡（MIN 或 MAX 参数），则 BSM 可选择并锁定任何不属于生成数据主机本地的设备。
- 如果控制多路径设备的 MA 在一个主机上执行，而对象来自具有设备路径的其他主机，则 Data Protector 不会将 MA 迁移到本地主机，但会通过 LAN 将数据传送到已启动的 MA。已达到负载均衡的 MAX 值时，便会发生这种情况。
- 设置 IgnoreObjectLocalityForDeviceSelection 全局选项之后，将禁用 LANfree 设置。默认情况下，未设置 IgnoreObjectLocalityForDeviceSelection 。

在以下情况下，用户可能需要添加额外的设备路径，才能实现无 LAN 备份：

- 当备份客户机具有多个网络接口和主机名时。在这种情况下，根据 DNS 配置，Data Protector 备份可能会经过多个接口。然后，建议为每个接口添加本地路径。
- 当对属于 Windows 群集资源的 Windows 文件服务器执行文件系统备份时。在此类设置中，每个 Windows 群集资源均应有自己的主机

名，应为这些主机名创建单独的设备路径条目。

向后兼容

升级期间不会重新配置使用先前版本的 Data Protector 配置过的设备，无需任何更改即可与在先前版本的 Data Protector 中一样使用这些设备。为了利用新增的多路径功能，请将设备重新配置为多路径设备。

限制

以下限制适用：

- NDMP 设备和介质库不支持多路径。
- 多路径设备不支持设备链。

设置设备和介质的高级选项

配置新设备时或更改设备属性时，可以设置设备和介质的高级选项。是否有这些选项取决于设备类型。

配置备份时也可以设置其中某些选项。一般而言，备份规范中设置的设备选项优先于为设备设置的选项。

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，展开**设备**。
3. 右键单击要更改其选项的设备（库设备情况下为驱动器），然后单击**属性**。
4. 单击**设置**选项卡，然后单击**高级**按钮打开“高级选项”页：**设置**、**大小**和**其他**。
5. 指定所需的选项，然后单击**确定**应用更改。

配置 VTL 设备

要配置 VTL 设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**环境**，然后右键单击**设备**，并单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入 VTL 的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. （可选）选择**多路径设备**。
6. 在“设备类型”列表中，选择 **SCSI 库**。然后，在“接口类型”列表中自动选择 **SCSI**。
7. 如果*未*选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。
8. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。单击“下一步”。
9. 指定有关库 SCSI 地址和驱动器处理的所需信息，然后单击**下一步**。
10. 指定要与 Data Protector 配合使用的插槽，然后单击“下一步”。
11. 选择将与设备配合使用的介质类型。
12. 单击**完成**退出向导。

注意如果在 RedHat Linux (RHEL) 7.1 系统上使用 VTL 设备，则必须手动加载通用 SCSI 驱动程序。可通过执行命令 modprobe -vs sg 完成此操作。还建议将此命令添加到 RHEL init scripts 或 cron job，以确保在系统启动时启动此命令。

配置堆栈器设备

将备份设备连接到系统并且存在正常工作的设备文件（SCSI 地址）之后，可以配置该备份设备与 Data Protector 配合使用。

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. （可选）选择**多路径设备**。
6. 如果未选择**多路径设备**选项，则选择客户机的名称。
7. 单击“下一步”。
8. 在“设备类型”列表中，选择“堆栈器”设备类型，然后单击“下一步”。
9. 在“数据设备”文本框中，输入物理设备的 SCSI 地址（Windows 系统），输入设备文件名（UNIX 系统），或使用下拉箭头自动检测驱动器地址或文件名。

   对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
10. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
11. 单击“下一步”。
12. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
13. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
14. 单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。如果正确配置了设备，则 Data Protector 将可以在插槽中加载、读取和卸载介质。

堆栈器设备介质管理

配置堆栈器设备之后，请考虑管理此类设备中的介质有一些具体问题。例如，对于堆栈器设备中的每个介质，必须单独运行扫描、验证或格式化操作。应正确加载介质才能运行 Data Protector 会话。

管理堆栈器设备介质

使用堆栈器设备时，必须对每个介质单独运行扫描、验证和格式化操作。使用**在操作完成之后弹出介质**选项以自动加载每个介质（仅应手动加载第一个介质）。堆栈器按顺序加载介质，因此建议采用宽松介质分配策略。

1. 手动加载第一个介质。
2. 在 Data Protector Manager 中，单击“设备和介质”。
3. 在范围窗格中，展开“设备”。
4. 右键单击堆栈器设备，然后单击以下某项：
   - **格式**
   - **验证**
   - **扫描**
5. 按照向导操作。在最后一页中，选择**在操作完成之后弹出介质**选项。单击**完成**。

   此时将自动加载下一个磁带。
6. 重复步骤 4 和 5，直到所有磁带加载完毕为止。
7. 用尽堆栈器箱盒中的所有磁带后，手动卸载箱盒，然后插入下一个箱盒。

如果未正确加载介质，则 Data Protector 将中止介质会话。

配置介质库设备（光盘库）

将备份设备连接到系统并且存在正常工作的设备文件（SCSI 地址）之后，可以配置该备份设备与 Data Protector 配合使用。

配置介质库设备

要配置介质库设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. 在“设备类型”列表中，选择**介质库**设备类型。
6. 在“客户机”列表中，选择客户机的名称。
7. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
8. 单击“下一步”。
9. 为介质库指定一组文件/磁盘。使用短划线一次输入多个文件或磁盘（例如 /tmp/FILE 1-3），然后单击“添加”。对于磁光介质库，磁盘名称必须以 A/a 或 B/b 结尾。单击“下一步”。
10. 在“介质类型”列表中，对要配置的设备选择介质类型。
11. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

配置介质库设备中的驱动器

要配置介质库中的驱动器，请完成以下步骤:

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明（可选）。
3. 指定所选介质类型的介质池。可以从“介质池”列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。单击“下一步”。
4. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
5. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

配置 SCSI 库或箱盒设备

将备份设备连接到系统并且存在正常工作的设备文件（SCSI 地址）之后，可以配置该备份设备与 Data Protector 配合使用。

除了配置箱盒设备时必须指定设置了**箱盒支持**选项的介质池外，库和箱盒设备的配置过程相同。

建议让 Data Protector 自动配置备份设备。

配置 SCSI 库机械手

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. （可选）选择**多路径设备**。
6. 在“设备类型”列表中，选择 **SCSI 库**设备类型。
7. 在“接口类型”列表中，选择 **SCSI** 接口类型。
8. 如果*未*选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。
9. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
10. 单击“下一步”。
11. 输入库机械手的 SCSI 地址，或使用下拉箭头自动检测驱动器地址或文件名

    对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
12. 在“繁忙驱动器处理”列表中，选择在驱动器繁忙时 Data Protector 应采取的操作。
13. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
14. （可选）选择 **SCSI 保留/释放(机械手控制)**。单击“下一步”。
15. 指定设备的插槽。使用短划线输入插槽范围，然后单击**添加**。例如，输入 1-3，然后单击**添加**可同时添加插槽 1、2 和 3。请勿使用字母或以零开头。单击“下一步”。
16. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
17. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

配置库中的驱动器

完成以下步骤：

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明（可选）。
3. （可选）选择**多路径设备**。
4. 如果*未*选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。

   > **提示**可以配置库，以使每个驱动器从运行 Data Protector 介质代理的不同系统接收数据。这样可以提高高端环境中的性能。从“客户机”下拉列表中，选择要与每个驱动器配合使用的客户机系统。

   单击“下一步”。
5. 在“数据驱动器”文本框中，输入数据驱动器的 SCSI 地址或文件名。

   对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。

6. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
7. 在“驱动器索引”文本框中，输入库中驱动器的索引。单击“下一步”。
8. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。建议使用默认的介质池。

   > **注意**不必将所有驱动器都配置为用于 Data Protector。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。

   指定箱盒设备的介质池时，请选择设置了**箱盒支持**选项的池。

   单击“下一步”。
9. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
10. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。如果正确配置了设备，则 Data Protector 将可以在插槽中加载、读取和卸载介质。

配置 SAN 环境中的设备

SAN 环境的规模可以从一个客户机使用一个库到若干客户机使用若干库不等。客户机可以采用不同的操作系统。从 Data Protector 的角度看，配置 SAN 环境的目标是:

- 在要共享库机械手的每个主机上，为每个主机创建一个库机械手。如果只有一个主机控制机械手，则仅为默认的机械手控制主机创建库定义。
- 在要参与共享库中同一（磁带）驱动器的每个主机上：
  - 为要使用的每个设备都创建设备定义。
  - 如果另一个主机也将使用（物理）设备（共享设备），则使用锁名称。
  - （可选）如果要使用直接访问，则选择此功能。如果使用此功能，请确保在该主机上设置了 libtab 文件。

注意事项

- Microsoft 群集服务器：确保两个群集节点上的驱动器硬件路径相同：配置设备后，即执行故障转移核实这一点。

配置方法

有三种配置方法，具体采用哪一种取决于参与 SAN 配置的平台：

- 使用 GUI 自动配置设备
- 使用 CLI 自动配置设备（sanconf 命令）
- 在 UNIX 系统中手动配置

使用 GUI 自动配置设备

可以使用 Data Protector 自动配置功能在 SAN 环境中的多个主机上自动配置设备和库。以下操作系统中提供自动配置功能：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

限制

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

Data Protector 可发现连接到环境的备份设备。对于库设备，Data Protector 确定插槽数、介质类型和属于库的驱动器。然后，Data Protector 设置逻辑名称、锁名称、介质类型、设备的设备文件或 SCSI 地址以及驱动器和插槽，从而配置设备。

> **注意**将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。
>
> - 要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
> - 要将设备添加到现有的库，或者删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者手动将驱动器添加到库中。

使用 sanconf 命令自动配置设备

可使用 sanconf 命令配置 SAN 环境中的设备和库。 sanconf 命令是一个实用程序，可简化 Data Protector 单元的 SAN 环境中以及具有 Centralized Media Management Database (CMMDB) 的 MoM 环境中库的配置。它通过从多个客户机收集有关驱动器的信息并将这些驱动器配置为一个库，可自动配置 SAN 环境中的库。在 MoM 环境中， sanconf 还可以配置使用 CMMDB 的任何 Data Protector 单元中的任何库 (如果运行 sanconf 的单元使用 CMMDB)。 sanconf 以下操作系统中提供 ：

- Windows
- HP-UX
- Solaris

sanconf 命令可以检测和配置连接到在以下操作系统中运行的客户机的受支持设备:

- Windows
- HP-UX
- Solaris
- Linux
- AIX

使用此命令，可以：

- 扫描指定的 Data Protector，同时收集有关连接到 SAN 环境中客户机的驱动器和机械手控制的 SCSI 地址的信息。
- 使用在扫描 Data Protector 客户机期间收集的信息，配置或修改给定客户机的带库或驱动器的设置。
- 从库中删除所有或指定客户机上的驱动器。

设备锁定

sanconf 命令自动为配置的驱动器创建锁名称。锁名称由驱动器供应商 ID 字符串、产品 ID 字符串和产品序列号组成。

还可以手动添加锁名称。锁名称对于每个逻辑设备都是唯一的。

不得更改由 sanconf 命令创建的锁名称。手动创建并且表示已由 sanconf 配置的物理驱动器的所有其他逻辑驱动器也必须使用由 sanconf 创建的锁名称。

限制

- 有关 sanconf 适用的库的完整列表，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。
- sanconf 不提供以下功能：
  - 将备用驱动器放入驱动器插槽中。
  - 混合驱动器类型；例如，DLT、9840 和 LTO 驱动器的组合。
  - 配置当前不可用的客户机。只有在使用包括通过扫描客户机收集的信息的配置文件执行库的配置时，才能配置此类客户机。

建议

对于系统中的特定设备仅配置一个驱动程序。

检测永久性设备路径中的设备

Data Protector 查找存在于标准路径 (特定于操作系统的格式) 中的设备。可以通过重新启动操作系统 (例如: Linux OS) 来更改这些设备的路径。如果设备位于其他路径中，则 Data Protector 将无法检测到设备。要避免出现这种情况，请在 /opt/omni/ 文件夹下创建一个名为 .paths 的文件。将永久性设备路径添加到此文件。例如：

```
/dev/tape/by-id/scsi-35001438024a3452e /dev/tape/by-id/scsi-35001438024a3458d-nst /dev/tape/by-id/scsi-35001438024a34592-nst
/dev/tape/by-id/scsi-35001438024a34597-nst /dev/tape/by-id/scsi-35001438024a3459c-nst
```

将此 /opt/omni/.paths 文件与 /dev/tape/by-id 结合使用。

在 UNIX 系统中手动配置

手动配置 SAN 环境中连接到 UNIX 系统的共享设备时，必须：

- 为要使用的每个设备都创建设备定义。
- 使用锁名称。
- （可选）如果要使用直接访问，则选择此功能。如果这样做，则必须确保正确配置了该主机上的 libtab 文件。

手动配置 SAN 环境中的设备

以下过程表示若干系统使用驱动器和机械手、若干应用程序 (不只是 Data Protector) 使用驱动器以及所有系统都发送机械手控制命令 (直接库访问)。以下任务还提供用于不同环境的替代步骤。

要控制机械手，可以使用 SAN 中的任意客户机。首先需要在充当默认机械手控制系统的客户机上配置库机械手控制。无论哪个客户机请求介质移动，都将使用此客户机管理介质移动。这样做是为了放置多个主机同时请求介质移动时机械手出现冲突。只有在主机故障并启用了直接访问时，由请求介质移动的本地主机执行机械手控制。

必须在需要与共享库通信的每个客户机上都安装 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)。

配置 SAN 环境中的库

如果希望由群集管理机械手控制，则需要确保：

- 每个群集节点上都存在机械手控制。
- 库机械手配置中使用了虚拟群集名称。
- 常用机械手和设备文件名使用 mksf 命令或 libtab 文件进行安装。

执行以下步骤配置 SAN 环境中的库:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. （可选）在“说明”文本框中，输入说明。
5. （可选）选择**多路径设备**。
6. 在“设备类型”下拉列表中，选择 **SCSI 库**设备类型。
7. 在“接口类型”下拉列表中，选择 **SCSI** 接口类型。
8. 如果未选择**多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
9. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
10. 单击“下一步”。
11. 输入库机械手的 SCSI 地址，或使用下拉箭头自动检测驱动器地址或文件名。

    对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击**添加**，将路径添加到所配置路径的列表中。
12. 在**繁忙驱动器处理**列表中，选择**弹出介质**。
13. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击“下一步”。
14. 指定设备的插槽。使用短划线一次输入多个插槽，然后单击**添加**。例如，输入 1-3，然后单击**添加**可同时添加插槽 1、2 和 3。单击“下一步”。
15. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
16. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。按照向导操作，如下方的任务中所述。

配置库中的驱动器

在从中要使用每个驱动器的每个客户机上配置这些驱动器。完成以下步骤：

1. 在“设备名称”文本框中，输入驱动器的名称。

   建议使用以下命名约定：

   - LibraryLogicalName_DriveIndex_Hostname ，例如 SAN_LIB_2_hotdog（对于非多路径设备）
   - LibraryLogicalName_DriveIndex ，例如 SAN_LIB_2（对于多路径设备）
2. （可选）在“说明”文本框中，输入说明。
3. （可选）选择**多路径设备**。
4. 如果未选择**多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
5. 单击“下一步”。
6. 在“数据驱动器”文本框中，输入数据驱动器的 SCSI 地址或文件名

   对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击**添加**，将路径添加到所配置路径的列表中。
7. 在“驱动器索引”文本框中，输入库中驱动器的索引。
8. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击“下一步”。
9. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。

   可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。
10. 单击**高级**按钮。在**设置**选项卡中，选择**使用直接库访问**选项。

    如果只希望由一个系统发送用于启动 Data Protector 的机械手控制命令，请勿选择“使用直接库访问”选项。用 Data Protector 配置库/驱动器时选择的客户机系统将控制库机械手。
11. 对于多路径驱动器*不必* 执行此步骤。单击“下一步”。
    - 如果 Data Protector 是唯一一个访问驱动器的应用程序，则单击“其他”选项卡，选择“使用锁名称”选项，然后输入名称。记住该名称，因为在另一个客户机上配置相同驱动器时将需要该名称。建议使用以下命名约定：

LibraryLogicalName_DriveIndex ，例如 SAN_LIB_D2

- 如果 Data Protector 不是访问驱动器的唯一应用程序，则选择“使用锁名称”选项，并确保操作规则一次只能从一个应用程序提供所有设备的独占访问。
- 如果只有一个系统使用该驱动器，则不要选择**使用锁名称**选项。

12. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
13. 单击**完成**退出向导。

驱动器由若干系统和若干应用程序 (不仅由 Data Protector) 使用。使用设备锁定 (定义“锁名称”)，并确保操作规则要求同时只能从一个应用程序中独占访问所有设备

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

配置 SAN 环境中的 libtab 文件

libtab 文件用于映射库机械手控制访问权限，以便也可以在“请求直接访问的系统”上运行，因为此处的本地控制路径可能与默认库机械手控制系统上使用的路径不同。

所有需要“直接访问”库机械手并且与配置为默认库机械手控制系统的系统不同的 Windows 和 UNIX 客户机都需要有一个 libtab 文件。

完成以下步骤：

1. 在所有请求直接访问的系统的以下目录中以纯文本格式创建 libtab 文件:

   Windows 系统： Data_Protector_home\libtab

   HP-UX 和 Solaris 系统： /opt/omni/.libtab

   其他 UNIX 系统： /usr/omni/.libtab

2. 在 libtab 文件中提供以下信息:

   FullyQualifiedHostnameDeviceFile | SCSIPathDeviceName

   - FullyQualifiedHostname 是请求直接访问控制库机械手的客户机的名称。如果客户机是群集的一部分，则应使用节点名称。
   - DeviceFile | SCSIPath 是此客户机上库机械手驱动程序的控制路径。
   - DeviceName 是此客户机上使用的设备定义的名称。

   对于请求直接访问的每个设备都需要有一行。

如果系统是群集的一部分，则 FullyQualifiedHostname 必须是虚拟服务器名称，并且 DeviceFile | SCSIPath 必须指向群集节点 (物理系统)。

配置 ADIC/GRAU DAS 库设备

Data Protector 提供专用的 ADIC/GRAU 库策略，用于将 ADIC/GRAU 库配置为 Data Protector 备份设备。

装有介质代理软件并通过 DAS 服务器访问库机械手的每个系统都称为 DAS 客户机。

以下内容可能会提供其他信息：

- ADIC/GRAU 功能需要持有特定的 Data Protector 许可证。
- 由于此库管理由不同应用程序使用的介质，因此必须配置希望将哪些介质和驱动器与 Data Protector 配合使用，以及要跟踪哪些介质。
- Data Protector 自行保持独立的介质分配策略，并且不使用暂存池。

配置阶段

1. 连接库驱动器
2. 准备安装介质代理
3. 安装介质代理
4. 配置 ADIC/GRAU DAS 库设备
5. 配置 ADIC/GRAU DAS 库设备中的驱动器

连接库驱动器

要连接库设备，请完成以下步骤:

1. 将库驱动器和机械手物理连接到要安装介质代理软件的系统。
2. 配置 ADIC/GRAU 库。请参见 ADIC/GRAU 库随附的文档获取相关说明。

为安装介质代理做准备

请遵循以下步骤:

1. 如果 DAS 服务器基于 OS/2，则在配置 Data Protector ADIC/GRAU 备份设备之前，请创建或更新 DAS 服务器计算机上的 C:\DAS\ETC\CONFIG 文件。

   在此文件中，必须定义所有 DAS 客户机的列表。对于 Data Protector，这意味着必须定义已安装介质代理的所有 Data Protector 客户机。

   每个 DAS 客户机都用唯一的客户机名称（无空格）进行标识，例如 OMNIBACK_C1 。在此示例中， C:\DAS\ETC\CONFIG 文件的内容应类似于此：

   ```
   client client_name = OMNIBACK_C1,

   # hostname = AMU,"client1"

   ip_address = 19.18.17.15,

   requests = complete,

   options = (avc,dismount),

   volumes = ((ALL)),

   drives = ((ALL)),

   inserts = ((ALL)),

   ejects = ((ALL)),

   scratchHPools = ((ALL))
   ```

   必须在所有 Data Protector 介质代理客户机上将这些名称配置为 omnirc 选项 DAS_CLIENT 。 omnirc 文件是 Data_Protector_home 目录（Windows 系统）中的文件 omnirc ，或文件 .omnirc （UNIX 系统）。例如，在 IP 地址为 19.18.17.15 的系统上，omnirc 文件中相应的行为 DAS_CLIENT=OMNIBACK_C1 。
2. 了解如何静态或动态配置了 ADIC/GRAU 库插槽分配策略。有关如何检查所用分配策略的类型的信息，请参见 AMU Reference Manual 。

   静态策略对于每个 volser 具有专用的插槽，而动态分配策略则随机分配插槽。根据已设置的策略相应地配置 Data Protector。

   如果已配置了静态分配策略，则将以下 omnirc 选项添加到控制库机械手的系统中：

OB2_ACIEJECTTOTAL = 0

请注意，这适用于 HP-UX 和 Windows。

有关配置 ADIC/GRAU 库的进一步问题，请与 ADIC/GRAU 支持人员联系或查阅 ADIC/GRAU 文档。

安装介质代理

可以在将物理连接到 ADIC/GRAU 库中备份驱动器的系统中和在将通过 DAS 服务器访问库机械手的系统中安装常规介质代理或 NDMP 介质代理。

需要特殊的许可证，具体取决于含介质的存储库的大小或 ADIC/GRAU 库中使用的驱动器数和插槽数。

确保满足以下条件:

- ADIC/GRAU 库必须已配置且正在运行。有关如何配置 ADIC/GRAU 库，请参见 ADIC/GRAU 库随附的文档。
- DAS 服务器正常运行，并且已正确配置 DAS 客户机。

  需要用 DAS 软件控制 ADIC/GRAU 库。该软件由一个 DAS 服务器和多个 DAS 客户机构成。有关 DAS 软件的详细信息，请参见 ADIC/GRAU 库随附的文档。
- 安装介质代理之前，必须获取以下信息:
-
  - DAS 服务器的主机名。
  - 含有驱动器相应 DAS 名称的可用驱动器列表。

    如果已定义 ADIC/GRAU 系统的 DAS 客户机，则运行以下命令以获取此列表：

    dasadmin listd2 [client] 或

    dasadmin listd [client] 其中，[client] 是要显示为其保留的驱动器的 DAS 客户机。

    dasadmin 命令位于 OS/2 主机上的 C:\DAS\BIN 目录中，即装有 DAS 客户机的目录中：

    Windows 系统： %SystemRoot%\system32

    UNIX 系统： /usr/local/aci/bin
  - 含有相应格式规范的可用插入/弹出区域的列表。

    可以在 OS/2 主机上 AMS（AML 管理软件）的图形配置中获得此列表：

    在“管理”菜单中，单击**配置**以启动配置。双击 **I/O** 打开 EIF-Configuration 窗口，然后单击**逻辑范围**。在文本框中，将会列出可用的“插入/弹出区域”。

    请注意，一个 Data Protector 库设备只能处理一种介质类型。记住哪种介质类型属于每个指定的“插入/弹出区域”非常重要，因为稍后将需要该数据来为 Data Protector 库配置“插入/弹出区域”。
  - **Windows 系统：**Windows 系统：驱动器的 SCSI 地址列表，例如 scsi4:0:1:0 。
  - **UNIX 系统：**驱动器的 UNIX 设备文件的列表。

    在系统上运行 ioscan -fn 系统命令以显示所需的信息。

执行以下任务:

1. 使用 Data Protector 图形用户界面和安装服务器，将介质代理组件分发到客户机。
2. 为客户机界面安装 ADIC/GRAU 库。

   Windows 系统：
   - 将 aci.dll、winrpc32.dll 和 ezrpc32.dll 库复制到 Data_Protector_home\bin 目录。（这三个库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上或 AMU-PC 上的 C:\DAS\AMU\ 目录中可以找到它们。）
   - 将这三个库也复制到 %SystemRoot%\system32 目录。
   - 将 Portinst 和 Portmapper 服务复制到 DAS 客户机上。（这些必需文件是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上可以找到它们。）
   - 在“控制面板”中，转至**管理工具**、**服务**，然后启动 portinst 来安装 portmapper 。
   - 重新启动 DAS 客户机以启动 portmapper 服务。
   - 在“控制面板”中，转到**管理工具**、**服务**，检查 portmapper 和 rpc 服务是否正在运行。

HP-UX、Linux 和 AIX 系统：

将共享库 libaci.sl （HP-UX 系统）、libaci.so （Linux 系统）或 libaci.o （AIX 系统）复制到目录 /opt/omni/lib （HP-UX 和 Linux 系统）或 /usr/omni/lib （AIX 系统）。您必须具有访问该目录的权限。确保共享库已为每个人（root、组和其他人）读取并执行了权限。（libaci.sl 和 libaci.o 共享库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。在安装介质上可以找到它们。）

3. 正确安装 DAS 软件之后，执行 devbra -dev 命令，检查库驱动器是否正确连接到系统。此命令位于默认的 Data Protector 管理命令目录中。

   此时将显示包含相应设备文件/SCSI 地址的库驱动器的列表。

配置 ADIC/GRAU DAS 库设备

当 ADIC/GRAU 库物理连接到系统并且装有介质代理后，可以从 Data Protector GUI 中配置 ADIC/GRAU 库设备。然后，DAS 客户机将在特定的介质管理操作（查询、放入、弹出）期间访问 ADIC/GRAU 机械手。

完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**。
3. 在“设备名称”文本框中，键入设备的名称。
4. 在“说明”文本框中，（可选）键入说明。
5. （可选）选择**多路径设备**。
6. 在“设备类型”列表中，选择 **GRAU DAS 库**。
7. 如果未选择**多路径设备**选项，则选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称。
8. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
9. 单击“下一步”。
10. 在“DAS 服务器”文本框中，键入 DAS 服务器的主机名。

    对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
11. 在“繁忙驱动器处理”列表中，选择在驱动器繁忙时 Data Protector 应采取的操作，然后单击“下一步”。
12. 指定库的导入和导出区域，然后单击**添加**。单击“下一步”。
13. 在“介质类型”列表中，为设备选择相应的介质类型。
14. 单击**完成**退出向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

配置 ADIC/GRAU DAS 库设备中的驱动器

完成以下步骤:

1. 在“设备名称”文本框中，键入驱动器的名称。
2. 在“说明”文本框中，（可选）键入说明。
3. （可选）选择**多路径设备**。
4. 如果未选择**多路径设备**选项，则选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称。
5. 单击“下一步”。
6. 在“数据驱动器”文本框中，指定设备的 SCSI 地址。

   对于多路径设备，还要选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称，然后单击**添加**，将路径添加到所配置路径的列表中。
7. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
8. 在“驱动器名称”文本框中，指定在安装介质代理期间获取的 ADIC/GRAU 驱动器名称。单击“下一步”。
9. 选择驱动器的**默认介质池**。
10. 单击**高级**以设置驱动器的高级选项，例如**并发**。单击**确定**。单击“下一步”。
11. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。

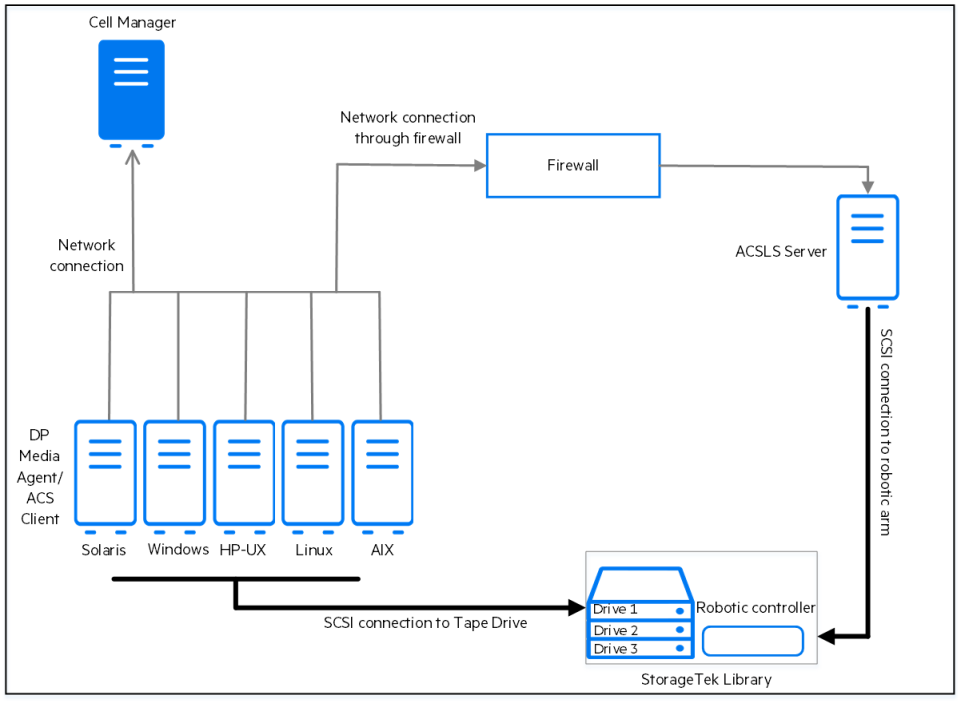
12. 单击**完成**退出向导。

配置 StorageTek ACS 库设备

Data Protector 提供专用的 StorageTek Automated Cartridge System (ACS) 库策略，用于将 StorageTek ACS 库配置为Data Protector 备份设备。ACS 库软件 (ACSLS) 控制 StorageTek ACS 磁带库。ACS 库通过直通端口 (PTP) 连接和控制。ACSLS 通过网络上的命令处理来访问和管理存储在一个或多个 ACS 中的信息。

Data Protector ACS 集成

以下是 Data Protector ACS 设置的示例。您安装和配置 ACSLS 的系统称为 ACSLS 服务器。装有介质代理并通过 ACSLS 访问库机械手的每个系统都称为 Data Protector 介质代理或 ACS 客户机。



请注意以下各项:

- StorageTek 功能需要持有特定的 Data Protector 许可证。
- 由于此库管理由不同应用程序使用的介质，因此必须配置希望将哪些介质和驱动器与 Data Protector 配合使用，以及要跟踪哪些介质。
- Data Protector 自行保持独立的介质分配策略，并且不使用暂存池。

配置步骤

1. 安装 ACSLS 服务器
2. 连接库驱动器
3. 安装介质代理
4. 配置 ACS 客户机以跨防火墙与 ACSLS 通信 (*可选*)
5. 配置 StorageTek ACS 库设备
6. 配置 StorageTek ACS 库设备中的驱动器

安装 ACSLS 服务器

安装和配置 ACSLS。有关安装 ACSLS 的详细说明，请参阅 docs.oracle.com 上的 StorageTek ACSLS 文档。

连接库驱动器

完成以下步骤：

1. 将库驱动器和机械手物理连接到要安装介质代理的系统。
2. 配置 StorageTek ACS 库。请参见 STK ACS 库随附的文档获取相关说明。

   有关受支持的 StorageTek 库的详细信息，请参阅 Data Protector 设备支持矩阵。

安装介质代理

可以在将物理连接到 StorageTek 库中备份驱动器的系统中和在将通过 ACSLS 访问库机械手的系统中，安装常规介质代理或 NDMP 介质代理。

> **注意**需要特殊的许可证，具体取决于含介质的存储库的大小或 StorageTek 库中使用的驱动器数和插槽数。

确保满足以下条件:

- StorageTek 库已配置且正在运行。有关配置 StorageTek 库的信息，请参阅 StorageTek 库随附的文档。
- 开始安装介质代理之前，需要获取以下信息:
  - 运行 ACSLS 的主机的 hostname 。
  - 要用于 Data Protector 的 ACS 驱动器 ID 的列表。登录正在运行 ACSLS 的主机，并执行以下命令以显示该列表：

    rlogin “ACSLS hostname” -l acssa

    输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：

    ACSSA> query drive all

    ACS 驱动器的格式规范必须为以下格式：

    ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
  - 请确保将用于 Data Protector 的驱动器处于 online 状态。如果某个驱动器不处于 online 状态，则在 ACSLS 主机上使用以下命令更改状态：

    vary drive drive_id online
  - 可用的 ACS CAP ID 和 ACS CAP 格式规范的列表。登录正在运行 ACSLS 的主机，并执行以下命令以显示该列表：

    rlogin “ACSLS hostname” -l acssa

    输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：

    ACSSA> query cap all

    ACS CAP 的格式规范必须为以下格式：

    ACS CAP: ID:#,#,# (ACS num, LSM num, CAP num)
  - 确保将用于 Data Protector 的 CAP 处于 online 状态，并处于 manual 工作模式。

    如果 CAP 不处于 online 状态，则使用以下命令更改状态：

    vary cap cap_id online

    如果 CAP 未处于 manual 操作模式，则使用以下命令更改模式：

    set cap manual cap_id
  - **Windows 系统：**Windows 系统：驱动器的 SCSI 地址列表，例如 scsi4:0:1:0 。
  - **UNIX 系统：**驱动器的 UNIX 设备文件的列表。

    在系统上运行 ioscan -fn 系统命令以显示所需的信息。

要安装介质代理，请完成以下步骤:

1. 使用 Data Protector GUI 和适用于 Windows 的安装服务器将介质代理组件分发到客户机。
2. 在可访问库中机械手的所有库主机（介质代理客户机）上启动 ACS ssi 后台程序。

   Windows 系统：

   安装 LibAttach 服务。有关详细信息，请参见 ACS 文档。请确保在 LibAttach 服务配置期间输入相应的 ACSLS 主机名。成功配置之后，将自动启动 LibAttach 服务，并且在每次系统重新启动之后也会自动启动该服务。

   > 注意**:** 安装 LibAttach 服务之后，检查 libattach\bin 目录是否已自动添加到系统路径。如果未添加，则手动添加它。

   HP-UX 和 Solaris 系统：

   请执行以下命令：

   /opt/omni/acs/ssi.sh start ACS_LS_hostname

   AIX 系统：

   请执行以下命令：

   /usr/omni/acs/ssi.sh start ACS_LS_hostname
3. 从默认 Data Protector 管理命令目录中执行 devbra -dev 命令，以检查库驱动器是否正确连接到介质代理客户机。

   此时将显示包含相应设备文件/SCSI 地址的库驱动器的列表。

配置 ACS 客户机以跨防火墙与 ACSLS 通信

如果要配置用于与 ACSLS 通信的防火墙，请遵循以下过程。如果不需要防火墙配置，则可以直接继续进行配置 StorageTek ACS 库设备过程。

要在防火墙后支持 ACSLS，请在 ACS 客户机上进行以下更改:

1. 登录 ACS 客户机计算机并将目录更改为 /opt/omni/acs 。
2. 如下编辑 ssi.sh 脚本:
   - 将 SI_UDP_RPCSERVICE="TRUE "; export CSI_UDP_RPCSERVICE 更改为 CSI_UDP_RPCSERVICE="FALSE "; export CSI_UDP_RPCSERVICE 。
   - 添加这些行:
     - SSI_INET_PORT=30031; export SSI_INET_PORT
     - CSI_HOSTPORT=30031; export CSI_HOSTPORT
3. 通过运行以下命令，停止然后再启动现有 SSI 实例:
   ssi.sh stop
   ssi.sh start

配置 StorageTek ACS 库设备

当 StorageTek 库物理连接到系统并且装有介质代理后，可以从 Data Protector GUI 中配置 StorageTek 库设备。然后，ACS 客户机将在特定的介质管理操作（查询、放入、弹出）期间访问 StorageTek 机械手。
完成 Data Protector GUI 中的以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**。
3. 在“设备名称” 文本框中，键入设备的名称。
4. 在“说明” 文本框中，(可选) 键入说明。
5. （可选）选择**多路径设备**。
6. 在“设备类型” 列表中，选择“StorageTek ACS 库”。
7. 如果未选择**多路径设备**选项，则选择将访问 StorageTek 机械手的介质代理客户机。
8. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
9. 单击“下一步”。
10. 在“ACSLM 主机名” 文本框中，键入 ACS 服务器的主机名。

    对于多路径设备，还要选择客户机名称，然后将路径添加到所配置路径的列表中。
11. 在“繁忙驱动器处理”列表中，选择在驱动器繁忙时 Data Protector 应采取的操作，然后单击“下一步”。
12. 指定库的 **CAPs**，然后单击**添加**。单击“下一步”。
13. 在“介质类型” 列表中，为设备选择相应的介质类型。
14. 单击**完成**退出向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

配置 StorageTek ACS 库设备中的驱动器

完成 Data Protector GUI 中的以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**。
3. 在“设备名称” 文本框中，键入驱动器的名称。
4. 在“说明” 文本框中，(可选) 键入说明。
5. （可选）选择**多路径设备**。
6. 如果未选择**多路径设备**选项，则选择将访问 StorageTek 机械手的介质代理客户机。
7. 单击“下一步”。
8. 在“数据驱动器” 文本框中，指定设备的 SCSI 地址。

   对于多路径设备，还要选择将访问 StorageTek 机械手的介质代理客户机，然后单击**添加**，将路径添加到所配置路径的列表中。
9. 在“驱动器索引” 文本框中，指定在安装介质代理期间获取的 StorageTek“驱动器索引”。驱动器索引为由逗号分隔的四个数字的组合。单击“下一步”。
10. 选择驱动器的**默认介质池**。
11. 单击**高级**以设置驱动器的高级选项，例如**并发**。单击**确定**。单击“下一步”。
12. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
13. 单击**完成**退出向导。

管理备份设备

使用备份设备适用于多种任务，如扫描设备以确认设备中的介质、通过指定虚拟锁名称锁定设备、执行计划的介质弹出、自动或手动清洗不洁驱动器、重命名备份设备以及响应装载请求以确认设备中有所需的介质。

Data Protector 还为设备和介质提供一组对设备和介质管理有益的高级选项，具体有哪些选项取决于设备类型。

此外，在同一库中可以使用多种驱动器类型，但必须了解所用介质的特性。

当某个设备因某种原因无法运行时，可以禁止使用该设备进行备份，并自动使用设备列表中另一个可用的设备。如果不想再使用某个设备，可以从 Data Protector 配置中将其删除。

相关主题

- 设备和介质的高级选项
- 有多种驱动器类型的库
- 关于扫描
- 驱动器清洗
- 计划弹出介质
- 设备锁定
- 禁用备份设备
- 重命名备份设备
- 删除备份设备
- 响应装载请求

高级选项

Data Protector 为设备和介质提供一组高级选项。是否有这些选项取决于设备类型。例如，用于配置库的选项比独立设备的选项多。

配置新设备时或更改设备属性时，可以设置这些选项。一般而言，这些选项适用于各自设备。还可以优化所列出的一组选项以适合特定的备份规范。一般而言，这些选项优先于为设备设置的选项。配置或更改备份规范时，可以访问这些选项。

高级选项 - 设置

并发

选项

- CRC 检查
- 检测不洁驱动器
- 基于驱动器的加密
- 会话后弹出介质
- 重新扫描
- 使用直接库访问 (特定于 SAN 的选项)

高级选项 - 大小

- 块大小(KB)
- 磁盘代理缓冲区
- 段大小(MB)(S)

高级选项 - 其他

装载请求

- 延迟(分钟)(D)
- 脚本

设备锁名称

- 使用锁名称

相关任务

- 设置设备和介质的高级选项
- 更改备份设备选项

驱动器类型

在同一个库中可以使用多种相似技术的驱动器类型，如 DLT 4000/7000/8000（DDS 系列中也是如此）。如果要在任意驱动器中使用介质，但无法确保所有介质上都采用常用格式，则这可能会产生问题。例如，还原时 DLT-4000 无法读取用 DLT-8000（最高密度）写入的磁带。压缩和非压缩介质也无法互换使用。

通过设置相同的密度或为每个驱动器类型创建不同的介质池可以避免这些种类的问题。

相同的密度设置

此方法在所有介质上都使用一种常用格式，这种格式允许在任意驱动器中互换地使用所有介质。对于 Windows 系统中使用的设备，需要查看有关如何使用特定的写入密度的驱动器文档。在 UNIX 系统上，创建设备文件名时或通过选择相关的设备文件名并在设备定义中使用这些设备文件名，可以设置驱动器的密度。必须将密度设置为相同的值。例如，在 DLT 4000 和 DLT 7000 的情况下，应设置 DLT 4000 密度。还必须确保所使用设备的块大小设置相同。必须在格式化介质时在设备定义中使用此设置。当所有介质的密度设置都相等时，还可以根据需要使用自由池。在还原期间，可以在任意驱动器中使用任意介质。

每个驱动器类型都有不同的介质池

此方法明确地将一组驱动器使用的介质与另一组驱动器使用的介质相隔离，从而可以更好地优化驱动器和介质的使用情况。可以对不同组的驱动器配置不同的介质池。这样可以对不同的驱动器类型使用不同的密度设置。例如，创建一个 DLT-4k-pool 和一个 DLT-8k-pool。必须在格式化介质时在设备定义中使用此设置。例如，必须由 DLT-8000 以最高密度设置格式化 DLT-8000-highest-density 的池中的介质。

自由池支持

不能用一个自由池“跨越”上述池。这样无法在设备中正确识别“其他”池中的介质，而是会将其视为陌生介质。在用不兼容的方式写入相同介质类型 (DLT) 时，自由池的概念仅适用于*每种驱动器类型一个池*（如 DLT-8k-pool）。还原期间，必须了解来自某个池的介质只能与相关设备配合使用。

相关任务

- 配置 SCSI 库或箱盒设备
- 在 UNIX 系统中创建设备文件
- 创建介质池
- 创建自由池
- 修改介质池

扫描介质

扫描将检查插入驱动器中的介质的格式，显示设备存储库的内容，并更新 IDB 中的这些信息。

- 在独立设备中，扫描驱动器中的介质。
- 在带库设备中，扫描所选插槽中的介质。
- 在支持条码的带库设备中，扫描使用条码的介质。
- 在文件库设备中，更新 IDB 中有关文件仓库的相应信息。
- 对于 ADIC/GRAU DAS 或 STK ACS 库，Data Protector 将查询 ADIC/GRAU DAS 或 STK ACSLM Server，然后根据从服务器返回的信息同步 IDB 中的相应信息。

何时使用扫描

要更新有关设备中介质的 Data Protector 信息时即可扫描设备。如果手动更改介质的位置，则必须扫描设备。手动更改位置（插槽、驱动器）将使 IDB 中的信息产生不一致的现象，因为 Data Protector 无法获知手动更改。扫描将 MMDB 与所选位置（例如库中的插槽）实际存在的介质进行同步。

确保单元中所有介质的条码标签都唯一。如果在扫描期间检测到已有的条码，则以逻辑方式移动 IDB 中已有的介质。

如果已将一个文件仓库移至另一个位置，则在文件库设备中执行扫描。

限制

如果在存储库中对 ADIC/GRAU 库配置了多于 3970 个 volser，则无法成功完成 volser 扫描。解决此问题的方法是配置多个逻辑 ADIC/GRAU 库，以便将大型存储库中的插槽隔离为多个较小的存储库。

重要说明对于 ADIC/GRAU DAS 和 STK ACS 库，当为同一个物理库配置了多个逻辑库时，建议不要查询 DAS 或 STK ACSLM Server。请手动添加 volser。但是，对于 ADIC/GRAU DAS 库，当不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上进行 Data Protector 查询操作。

相关主题

- 用于 ADIC/GRAU DAS 或 STK ACS 库的查询操作
- 扫描设备
- 扫描库设备中的介质
- 扫描库设备中的驱动器
- 激活条形码读取器支持
- 扫描库设备的条形码
- 查询 ADIC/GRAU DAS 和 StorageTek ACSLM 主机
- 手动添加 Volser

清洗驱动器

Data Protector 提供了多种清洗不洁驱动器的方法：

- 库内置的清洗机构

  某些磁带库具有一种功能，可在驱动器请求清洗磁头时自动清洗驱动器。库检测到不洁驱动器时，将自动加载清洗磁带，并且不向 Data Protector 通知此操作。这将中断任何活动的会话，从而导致其失败。由于这种由特定硬件管理的清洗过程与 Data Protector 不兼容，因此建议不要采用此过程。请改用由 Data Protector 管理的自动驱动器清洗。

- 由 Data Protector 管理的自动驱动器清洗

  Data Protector 可使用清洗磁带自动清洗大多数设备。对于 SCSI 库和箱盒设备，可以定义在哪些插槽中放置磁头清洁磁带。不洁驱动器发送清洗请求，然后 Data Protector 使用清洗磁带清洗该驱动器。此方法可防止因驱动器不洁而使会话失败（前提是有合适的介质可用于备份）。支持条码的库和不支持条码的库都支持自动驱动器清洗。

- 手动清洗

  如果未配置自动驱动器清洗，则需要手动清洗不洁驱动器。如果 Data Protector 检测到不洁驱动器，则会话监视器窗口中会显示清洗请求。然后您必须手动将清洗磁带插入驱动器中。

使用一种特殊的磁带清洗卡盒（含有略带摩擦性的磁带）清洗磁头。加载后，驱动器即识别这种特殊的磁带卡盒，然后开始清洗磁头。

限制

- Data Protector 不支持用诊断供应商的特殊 SCSI 命令通过在一个特殊的清洗磁带存放插槽中存放的清洗磁带执行驱动器清洗。无法使用普通的 SCSI 命令访问这些特殊的清洗磁带存放插槽，因此这些插槽无法用于由 Data Protector 管理的自动驱动器清洗。请配置标准插槽以存放清洗磁带。
- 磁头清洁磁带的检测和使用取决于运行介质代理的系统平台。
- 如果配置由 Data Protector 管理的自动驱动器清洗，则不应使用另一种设备管理应用程序，因为这可能会导致意外的结果。这是因为读取 cleanme 请求时会清除此请求，具体取决于特定设备类型和供应商。
- 不支持用共享的清洗磁带自动清洗逻辑库的驱动器。需要为每个逻辑库都配置其特定的清洗磁带。

自动清洗的条件

- 在不支持条码的库中，Data Protector 设备定义中已配置了清洗磁带插槽，并且该插槽中含有清洗磁带卡盒。清洗磁带库插槽必须与其他库插槽一同进行配置。
- 在支持条码的库中，必须激活条码支持才能启用自动驱动器清洗。清洗磁带的条形码标签以 CLN 作为前缀，从而使 Data Protector 能够自动识别清洗磁带条形码。
- 所配置的驱动器启用了检测不洁驱动器选项。

Data Protector 收到驱动器需要清洗的通知时，将自动加载清洗磁带，清洗驱动器，然后恢复会话。将在 cleaning.log 文件中记录所有清洗活动，该文件位于 Data Protector 服务器日志文件目录中。

配置驱动器清洗

Data Protector 可检测不洁驱动器，并可（在 Windows 和 HP-UX 系统上）自动清洗大多数使用清洗磁带的驱动器（假定设备提供此功能）。对于 SCSI 库和箱盒设备，可以定义放置清洗磁带的插槽。对于不支持条码的库也支持自动驱动器清洗。

需要满足以下先决条件: 激活条码支持以启用自动磁带清洗。磁带条码的前缀为“CLN”，使 Data Protector 能够自动识别清洗磁带条码。

启用不洁驱动器检测

Data Protector 通过不洁驱动器检测可以识别由驱动器发出的事件。对所有设备类型（独立和库）都必须执行此步骤。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击要更改的设备，然后单击**属性**。
3. 单击“设置”，然后单击“高级”以显示“高级选项”对话框。
4. 单击“设置”，选择“检测不洁驱动器”选项，然后单击“确定”。
5. 单击**应用**以启用不洁驱动器检测。

为清洗磁带配置插槽

在库或箱盒设备内为清洗磁带配置插槽之后，Data Protector 便能够自动对此类别的设备执行清洗操作。如果在独立设备上检测到不洁驱动器迹象，则 Data Protector 发出磁头清洁磁带的装载请求。

不能为启用了条码读取器支持的库配置清洗插槽。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击某个 SCSI 库设备，然后选择**属性**。
3. 单击**存储库**。
4. 选择**清洁插槽**选项，然后在下拉列表中选择一个现有的插槽以放置磁头清洁磁带。
5. 单击**应用**确认。

为清洗配置驱动器之后，可以测试该驱动器。

测试驱动器清洗配置

可以测试是否已成功配置驱动器清洗。此测试由两个单独的阶段构成：

为测试驱动器清洗配置做准备

完成以下步骤：

1. 登录到装有驱动器的介质代理的系统。
2. 更改为默认 Data Protector 临时文件目录。
3. 在 Windows 系统中创建名为 simtab 的 ASCII 文件，或在 UNIX 系统中创建名为 .simtab 的 ASCII 文件。创建此文件时请考虑以下几点：

- 字段分隔符应为单个 ASCII 字符（制表符或分号）。
- 逻辑设备名称不能加引号，并且不能包含空格（例如 "test drive"）

simtab/.simtab 文件的内容应为：CLEANME file_name drive_name ，其中 file_name 是将用于模拟不洁驱动器的文件的名称，而 drive_name 是要测试的驱动器的名称。可以为各种驱动器添加多个条目。请勿指定带有文件名的路径。

测试驱动器清洗配置

完成以下步骤：

1. 在默认的 Data Protector 临时文件目录中，创建一个空文件用于模拟不洁驱动器。将其命名为其在 simtab 或 .simtab 文件中的相同名称。
2. 使用要测试的驱动器启动备份。

Data Protector 的行为如同所选驱动器不洁一样，然后执行清洗操作。要停止模拟特定驱动器的不洁驱动器行为，请删除相应的“不洁文件”。

相关任务

- 激活条形码读取器支持
- 配置驱动器清洗
- 测试驱动器清洗配置

弹出介质

Data Protector 可以使用报告功能配合一个脚本执行计划的介质弹出。

必须在 Cell Manager 上创建程序或脚本才能执行弹出，并且还必须在 Cell Manager 上安装任何适用的解释程序。

可以设置和计划报告组，以使其创建报告，并将该报告作为输入发送给脚本。此类报告组应包括仅列出要弹出的介质的报告（例如，可以使用“介质报告”列表）。启动报告组（作为日程计划或“结束会话”等通知的结果）后，Data Protector 将启动脚本，并使用报告结果作为输入。脚本使用 Data Protector omnimm CLI 命令，分析报告并执行指定介质的弹出。

默认情况下，如果需要从邮件插槽中取出介质，以使弹出操作可以继续（例如，如果要弹出的介质多于库中的空邮件插槽），则将在事件日志查看器中通知您。如果经过默认时间后没有从邮件槽中取出介质，并且仍有介质要弹出，则 omnimm 命令将中止该操作。可以在 omnirc 文件中更改默认的时间范围。

锁定装置

通过将设备配置为不同的设备名称，即可多次为同一物理设备配置不同特征。因此，可以将一个物理设备配置为多个 Data Protector 备份设备，并且一个设备即可用于多个备份会话。内部锁定逻辑设备可防止两个 Data Protector 会话同时访问相同的物理设备。例如，如果一个备份会话正在使用某个特定设备，则所有其他备份/还原会话必须等待此设备空闲，然后再开始使用此设备。开始备份或还原会话时，Data Protector 将锁定用于该会话的设备、驱动器和插槽。

执行介质操作（如初始化、扫描、验证、复制或导入）的介质会话也会锁定设备。在此期间，没有其他操作可以锁定和使用该设备。如果介质会话无法获取锁定，则操作失败，必须以后再重试操作。

备份或还原会话发出装载请求时将释放锁定，从而使您只能执行介质管理操作。仍将保留设备，以使任何其他备份或还原会话都不能使用设备。此外，首次介质操作期间不允许在同一驱动器上进行其他介质管理操作。确认装载请求后，备份或还原会话将再次锁定设备，并继续会话。

由于内部锁定在逻辑设备上而非物理设备上进行，因此如果在一个备份规范中指定一个设备名称，而在另一个备份规范中对同一物理设备指定另一个设备名称，则会发生冲突。根据备份计划，Data Protector 可能会尝试同时在若干备份会话中使用同一物理设备，这样可能会导致冲突。在其他操作（如备份和还原、备份和扫描等等）中使用两个设备名称时也可能会发生此情况。要防止 Data Protector 可能尝试同时在若干备份会话中使用相同物理设备时发生冲突，请在设备配置中指定虚拟锁名称。然后，Data Protector 使用此锁名称检查设备是否可用，从而防止冲突。对于同一物理设备，必须在所有备份设备配置中使用相同的锁名称。

注意“设备流”报告中有关物理设备的信息取自当前配置的设备，并且可能与实际使用该设备时的相应信息不同（例如，最近更改了设备逻辑名称，但内部数据库中的某些会话仍然包含以前的设备名称）。

“设备流”报告始终显示当前信息 - 含当前逻辑设备名称的当前物理表示形式。

锁定备份设备

要防止 Data Protector 可能尝试同时在若干备份会话中使用相同物理设备时发生冲突，请在设备配置中指定虚拟锁名称。对于同一物理设备，必须在所有备份设备配置中使用相同的锁名称。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中，右键单击要指定其锁名称的设备，然后单击**属性**。
4. 在“设置”属性页中，单击**高级**。
5. 在“高级选项”对话框中，单击**其他**。选择**使用锁名称**选项，键入所选的锁名称，然后单击**确定**。
6. 单击**应用**确认。

禁用备份设备

如果禁用某个备份设备，则所有后续备份都跳过该设备。如果已选择负载均衡，则改用备份规范的设备列表中定义的下一个可用设备。还会禁用与已禁用设备使用相同锁名称的所有设备。

这样您可以避免备份因设备受损或处于维护模式而失败，同时使其他设备可用于（和配置为）备份。

设备受损或处于维护模式时禁用备份设备很有用。

要禁用备份设备，请执行以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击要禁用的设备，然后单击**属性**。
4. 单击**设置**选项卡，然后选择**禁用设备**选项。
5. 单击“应用”。

此时即禁用设备。要允许设备进行备份，请取消选中**禁用设备**选项。

自动禁用备份设备

可以配置 Data Protector 以自动禁用已发生一定数量未知错误的设备。要确定该阈值，可将 SmDeviceErrorThreshold 全局选项设置为 SmDeviceErrorThreshold=MaxNumberOfUnknownErrors 。

要在对设备做出安排后允许该设备进行备份，请右键单击该设备，然后单击**启用设备**。

重命名备份设备

重命名备份设备时，该设备不再以其旧名称用于备份或还原。

重要说明请确保从使用该设备的所有备份规范中删除了该设备的旧名称。否则，Data Protector 将尝试备份到不存在的设备或从该设备还原，并因此会话将失败。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击设备的名称，然后单击**属性**。
4. 在“常规”属性页中，修改“设备名称”文本框中的名称。
5. 单击“应用”。

此时所配置设备的列表中将以新名称显示该设备。

删除备份设备

从 Data Protector 配置中删除备份设备时，该设备就不再用于备份或还原。

重要说明请确保从使用该设备的所有备份规范中删除了该设备的旧名称。否则，Data Protector 将尝试备份到不存在的设备或从该设备还原，并因此会话将失败。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击要删除的设备，然后单击**删除**。确认操作。

此时即从所配置设备的列表中删除了该设备。

提示如果不再将某个备份设备与 Data Protector 配合使用，则可能要从系统中删除介质代理软件组件。可使用“客户机”上下文完成此操作。

响应装载请求

对装载请求作出响应可确认所需的介质位于设备中。必须了解如何选择介质进行备份。

您必须已经添加到 Admin 用户组中或者获授予“监视”用户权限才能完成以下步骤:

1. 在上下文列表中，选择**监视**。
2. 将所需的介质插入设备中。如果有库设备，则不必使用由装载请求所请求的插槽。
3. 在结果区域中，双击含有装载请求状态的会话以显示有关会话的详细信息。
4. 选择具有装载请求状态的设备。
5. 在**操作**菜单中，选择**确认装载请求**，或右键单击含有装载请求状态的设备，然后选择**确认装载请求**。

此时会话和设备的状态变为“正在运行”。

在 SAN 中使用 Data Protector

存储区域网络 (SAN) 是专用于数据存储的网络，以高速光纤通道技术为基础。通过 SAN 可进行从应用程序服务器到某个单独网络的卸载存储操作。Data Protector 支持此技术，使多个主机可以共享通过 SAN 连接的存储设备，从而形成多系统对多设备的连接。通过多次定义同一物理设备达到此目的，例如，在需要访问该设备的每个系统上都定义一次。

在 SAN 环境中使用 Data Protector 时，必须考虑以下几点：

- 每个系统都可以有其（伪）本地设备，但通常都在若干系统之间共享设备。这一点适用于单独的驱动器以及库中的机械手。
- 必须小心谨慎，以防多个系统同时写入相同设备。需要在所有系统之间同步对设备的访问。使用锁定机制实现这一点。
- SAN 技术对于管理多个系统中的库机械手是一种极好的方式。只要发送到机械手的请求在所涉及的全部系统之间同步，这种方式就能直接管理机械手。

FC-AL 和 LIP

在光纤通道仲裁环路 (FC-AL) 中使用磁带设备可能会导致一些有可能中止备份会话的异常现象。出现此问题是因为只要连接/断开新 FC 链路以及只要重新引导连接到 FC-AL 的系统，FC-AL 就会执行环路初始化协议 (LIP)。FC-AL 的这种重新初始化将使正在运行的备份中止。应重新启动此类被终止的作业。

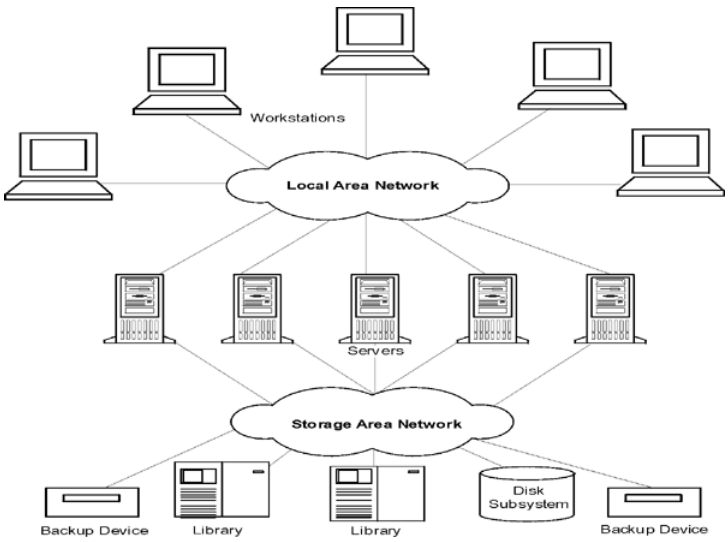
FC-AL 环路上发生 LIP 时，任何具有活动 I/O 进程的实用程序都会出现 I/O 错误。对于尝试使用共享磁带的备份实用程序，I/O 错误会导致当前备份会话失败：

- 倒回和卸载磁带
- 备份会话中止

建议采取以下措施：

- 备份会话正在运行时，不要添加新设备或从仲裁环路取下设备。
- 备份会话正在运行时，不要接触 FC 组件。静电会导致 LIP。
- 请勿在 Windows 中使用 discovery 或在 HP-UX 系统中使用 ioscan，因为这些命令还会导致 LIP。

SAN 中多系统对多设备的连接示例



相关主题

- SAN 环境中的设备锁定
- 间接和直接库访问
- 关于配置设备的多个路径
- 共享设备和 Serviceguard
- 配置 SAN 环境中的设备
- 准备备份设备

SAN 环境中的设备锁定

Data Protector支持 SAN 概念，使多个系统能够共享 SAN 环境中的备份设备。相同设备可由多个应用程序共享。该设备还可由 Data Protector 环境中的多个系统共享。锁定的用途是确保一次只有一个系统与在若干系统之间共享的设备进行通信。

锁定 Data Protector 专用的设备

如果只有 Data Protector 这一个应用程序使用驱动器，但需要从若干系统中使用这个驱动器，则可以使用设备锁定机制。

如果 Data Protector 是若干系统中唯一一个使用机械手控制的应用程序，则 Data Protector 从内部处理这种情况，假定库控制位于与需要控制它的所有系统相同的单元中。在这种情况下，由 Data Protector 内部控制管理对设备访问的所有同步。

锁定由多个应用程序使用的设备

如果多个系统正在使用 Data Protector 访问同一物理设备，则必须使用设备锁定机制。

如果 Data Protector 和至少一个其他应用程序要从几个系统中使用相同设备，则每个应用程序都必须使用相同（常规）的设备锁定机制。此机制必须在若干应用程序中都正常发挥作用。Data Protector 当前不支持此模式。如果必须这样，则操作规则必须保证一次只从一个应用程序中独占访问所有设备。

相关任务

- 锁定备份设备

库访问

配置具有 SCSI 库设备或 silo 库（ADIC/GRAU 和 StorageTek）的Data Protector 时，有以下两种方式可供客户机系统访问库机械手：

间接库访问

间接库访问时，只有一个系统（默认机械手控制系统）发送从 Data Protector 发起的机械手控制命令。任何其他请求机械手功能的系统将请求转发到机械手控制系统，此系统随后将实际命令发送到机械手。在 Data Protector 中为所有来自 Data Protector 的请求透明完成此操作。

直接库访问

直接库访问时，每个系统都直接向库机械手发送控制命令。因此，每个系统都不依赖于任何其他系统即可发挥作用。

由于直接库访问时有多个系统向同一个库发送命令，因此必须协调此通信的顺序。

在 Data Protector 中，每个库定义都与控制库机械手的主机关联（默认情况下）。如果另一个主机请求移动某个介质，则 Data Protector 将首先访问库定义中指定的系统以执行介质移动。如果该系统不可用，并且设置了 libtab 文件，则可以从本地主机直接访问库机械手。所有这些都在 Data Protector 中透明完成。

如果为多路径设备启用了直接库访问功能，则无论配置了什么顺序，都会首先使用本地路径（目标客户机上的路径）进行库控制。对于多路径设备，忽略 libtab 文件。

相关主题

配置 SAN 环境中的设备

SAN 环境的规模可以从一个客户机使用一个库到若干客户机使用若干库不等。客户机可以采用不同的操作系统。从 Data Protector 的角度看，配置 SAN 环境的目标是:

- 在要共享库机械手的每个主机上，为每个主机创建一个库机械手。如果只有一个主机控制机械手，则仅为默认的机械手控制主机创建库定义。
- 在要参与共享库中同一（磁带）驱动器的每个主机上：
  - 为要使用的每个设备都创建设备定义。
  - 如果另一个主机也将使用（物理）设备（共享设备），则使用锁名称。
  - （可选）如果要使用直接访问，则选择此功能。如果使用此功能，请确保在该主机上设置了 libtab 文件。

注意事项

- Microsoft 群集服务器：确保两个群集节点上的驱动器硬件路径相同：配置设备后，即执行故障转移核实这一点。

配置方法

有三种配置方法，具体采用哪一种取决于参与 SAN 配置的平台：

- 使用 GUI 自动配置设备
- 使用 CLI 自动配置设备（sanconf 命令）
- 在 UNIX 系统中手动配置

使用 GUI 自动配置设备

可以使用 Data Protector 自动配置功能在 SAN 环境中的多个主机上自动配置设备和库。以下操作系统中提供自动配置功能：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

限制

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

Data Protector 可发现连接到环境的备份设备。对于库设备，Data Protector 确定插槽数、介质类型和属于库的驱动器。然后，Data Protector 设置逻辑名称、锁名称、介质类型、设备的设备文件或 SCSI 地址以及驱动器和插槽，从而配置设备。

> **注意**将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。
>
> - 要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
> - 要将设备添加到现有的库，或者删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者手动将驱动器添加到库中。

使用 sanconf 命令自动配置设备

可使用 sanconf 命令配置 SAN 环境中的设备和库。 sanconf 命令是一个实用程序，可简化 Data Protector 单元的 SAN 环境中以及具有 Centralized Media Management Database (CMMDB) 的 MoM 环境中库的配置。它通过从多个客户机收集有关驱动器的信息并将这些驱动器配置为一个库，可自动配置 SAN 环境中的库。在 MoM 环境中， sanconf 还可以配置使用 CMMDB 的任何 Data Protector 单元中的任何库 (如果运行 sanconf 的单元使用 CMMDB)。 sanconf 以下操作系统中提供 ：

- Windows
- HP-UX
- Solaris

sanconf 命令可以检测和配置连接到在以下操作系统中运行的客户机的受支持设备:

- Windows
- HP-UX
- Solaris
- Linux
- AIX

使用此命令，可以：

- 扫描指定的 Data Protector，同时收集有关连接到 SAN 环境中客户机的驱动器和机械手控制的 SCSI 地址的信息。
- 使用在扫描 Data Protector 客户机期间收集的信息，配置或修改给定客户机的带库或驱动器的设置。
- 从库中删除所有或指定客户机上的驱动器。

设备锁定

sanconf 命令自动为配置的驱动器创建锁名称。锁名称由驱动器供应商 ID 字符串、产品 ID 字符串和产品序列号组成。

还可以手动添加锁名称。锁名称对于每个逻辑设备都是唯一的。

不得更改由 sanconf 命令创建的锁名称。手动创建并且表示已由 sanconf 配置的物理驱动器的所有其他逻辑驱动器也必须使用由 sanconf 创建的锁名称。

限制

- 有关 sanconf 适用的库的完整列表，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。
- sanconf 不提供以下功能：
  - 将备用驱动器放入驱动器插槽中。
  - 混合驱动器类型；例如，DLT、9840 和 LTO 驱动器的组合。
  - 配置当前不可用的客户机。只有在使用包括通过扫描客户机收集的信息的配置文件执行库的配置时，才能配置此类客户机。

建议

对于系统中的特定设备仅配置一个驱动程序。

检测永久性设备路径中的设备

Data Protector 查找存在于标准路径 (特定于操作系统的格式) 中的设备。可以通过重新启动操作系统 (例如: Linux OS) 来更改这些设备的路径。如果设备位于其他路径中，则 Data Protector 将无法检测到设备。要避免出现这种情况，请在 /opt/omni/ 文件夹下创建一个名为 .paths 的文件。将永久性设备路径添加到此文件。例如：

```
/dev/tape/by-id/scsi-35001438024a3452e /dev/tape/by-id/scsi-35001438024a3458d-nst /dev/tape/by-id/scsi-35001438024a34592-nst
/dev/tape/by-id/scsi-35001438024a34597-nst /dev/tape/by-id/scsi-35001438024a3459c-nst
```

将此 /opt/omni/.paths 文件与 /dev/tape/by-id 结合使用。

在 UNIX 系统中手动配置

手动配置 SAN 环境中连接到 UNIX 系统的共享设备时，必须：

- 为要使用的每个设备都创建设备定义。
- 使用锁名称。
- （可选）如果要使用直接访问，则选择此功能。如果这样做，则必须确保正确配置了该主机上的 libtab 文件。

手动配置 SAN 环境中的设备

以下过程表示若干系统使用驱动器和机械手、若干应用程序 (不只是 Data Protector) 使用驱动器以及所有系统都发送机械手控制命令 (直接库访问)。以下任务还提供用于不同环境的替代步骤。

要控制机械手，可以使用 SAN 中的任意客户机。首先需要在充当默认机械手控制系统的客户机上配置库机械手控制。无论哪个客户机请求介质移动，都将使用此客户机管理介质移动。这样做是为了放置多个主机同时请求介质移动时机械手出现冲突。只有在主机故障并启用了直接访问时，由请求介质移动的本地主机执行机械手控制。

必须在需要与共享库通信的每个客户机上都安装 Data Protector 介质代理 (常规介质代理或 NDMP 介质代理)。

配置 SAN 环境中的库

如果希望由群集管理机械手控制，则需要确保：

- 每个群集节点上都存在机械手控制。
- 库机械手配置中使用了虚拟群集名称。
- 常用机械手和设备文件名使用 mksf 命令或 libtab 文件进行安装。

执行以下步骤配置 SAN 环境中的库:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. （可选）在“说明”文本框中，输入说明。
5. （可选）选择**多路径设备**。
6. 在“设备类型”下拉列表中，选择 **SCSI 库**设备类型。
7. 在“接口类型”下拉列表中，选择 **SCSI** 接口类型。
8. 如果未选择**多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
9. （可选）在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
10. 单击“下一步”。
11. 输入库机械手的 SCSI 地址，或使用下拉箭头自动检测驱动器地址或文件名。

    对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击**添加**，将路径添加到所配置路径的列表中。
12. 在**繁忙驱动器处理**列表中，选择**弹出介质**。
13. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击“下一步”。
14. 指定设备的插槽。使用短划线一次输入多个插槽，然后单击**添加**。例如，输入 1-3，然后单击**添加**可同时添加插槽 1、2 和 3。单击“下一步”。
15. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
16. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。按照向导操作，如下方的任务中所述。

配置库中的驱动器

在从中要使用每个驱动器的每个客户机上配置这些驱动器。完成以下步骤：

1. 在“设备名称”文本框中，输入驱动器的名称。

   建议使用以下命名约定：

   - LibraryLogicalName_DriveIndex_Hostname ，例如 SAN_LIB_2_hotdog（对于非多路径设备）
   - LibraryLogicalName_DriveIndex ，例如 SAN_LIB_2（对于多路径设备）
2. （可选）在“说明”文本框中，输入说明。
3. （可选）选择**多路径设备**。
4. 如果未选择**多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
5. 单击“下一步”。
6. 在“数据驱动器”文本框中，输入数据驱动器的 SCSI 地址或文件名

   对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击**添加**，将路径添加到所配置路径的列表中。
7. 在“驱动器索引”文本框中，输入库中驱动器的索引。
8. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击“下一步”。
9. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。

   可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。
10. 单击**高级**按钮。在**设置**选项卡中，选择**使用直接库访问**选项。

    如果只希望由一个系统发送用于启动 Data Protector 的机械手控制命令，请勿选择“使用直接库访问”选项。用 Data Protector 配置库/驱动器时选择的客户机系统将控制库机械手。
11. 对于多路径驱动器*不必* 执行此步骤。单击“下一步”。
    - 如果 Data Protector 是唯一一个访问驱动器的应用程序，则单击“其他”选项卡，选择“使用锁名称”选项，然后输入名称。记住该名称，因为在另一个客户机上配置相同驱动器时将需要该名称。建议使用以下命名约定：

LibraryLogicalName_DriveIndex ，例如 SAN_LIB_D2

- 如果 Data Protector 不是访问驱动器的唯一应用程序，则选择“使用锁名称”选项，并确保操作规则一次只能从一个应用程序提供所有设备的独占访问。
- 如果只有一个系统使用该驱动器，则不要选择**使用锁名称**选项。

12. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
13. 单击**完成**退出向导。

驱动器由若干系统和若干应用程序 (不仅由 Data Protector) 使用。使用设备锁定 (定义“锁名称”)，并确保操作规则要求同时只能从一个应用程序中独占访问所有设备

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

配置 SAN 环境中的 libtab 文件

libtab 文件用于映射库机械手控制访问权限，以便也可以在“请求直接访问的系统”上运行，因为此处的本地控制路径可能与默认库机械手控制系统上使用的路径不同。

所有需要“直接访问”库机械手并且与配置为默认库机械手控制系统的系统不同的 Windows 和 UNIX 客户机都需要有一个 libtab 文件。

完成以下步骤：

1. 在所有请求直接访问的系统的以下目录中以纯文本格式创建 libtab 文件:

   Windows 系统： Data_Protector_home\libtab

   HP-UX 和 Solaris 系统： /opt/omni/.libtab

   其他 UNIX 系统： /usr/omni/.libtab

2. 在 libtab 文件中提供以下信息:

   FullyQualifiedHostnameDeviceFile | SCSIPathDeviceName

   - FullyQualifiedHostname 是请求直接访问控制库机械手的客户机的名称。如果客户机是群集的一部分，则应使用节点名称。
   - DeviceFile | SCSIPath 是此客户机上库机械手驱动程序的控制路径。
   - DeviceName 是此客户机上使用的设备定义的名称。

   对于请求直接访问的每个设备都需要有一行。

如果系统是群集的一部分，则 FullyQualifiedHostname 必须是虚拟服务器名称，并且 DeviceFile | SCSIPath 必须指向群集节点 (物理系统)。

备份到磁盘

Data Protector 备份到磁盘可将数据保存到磁盘而非磁带。Data Protector 写入位于一个或多个磁盘上的目录。将数据写入位于磁盘上目录中的文件。

磁盘备份比备份到磁盘速度快，因为无须执行任何机械过程（如加载磁带）即可进行备份。此外，磁盘存储正在变得日益廉价。

许多处理业务关键数据的应用程序都需要在完成每个事务后即备份该事务。基于磁盘的备份意味着可以在整个工作日不断写入磁盘。

什么是基于磁盘的备份设备？

概念上，基于磁盘的备份设备类似于磁带驱动器或磁带堆栈。此类设备有一个或多个目录，等同于磁带驱动器中的存储库。正在进行备份时，基于磁盘的备份设备将数据写入文件仓库，如同这些仓库将文件写入磁带一样。由于基于磁盘的备份设备将数据写入位于磁盘上的文件，因此这些设备也称为“文件设备”。

如何配置基于磁盘的设备？

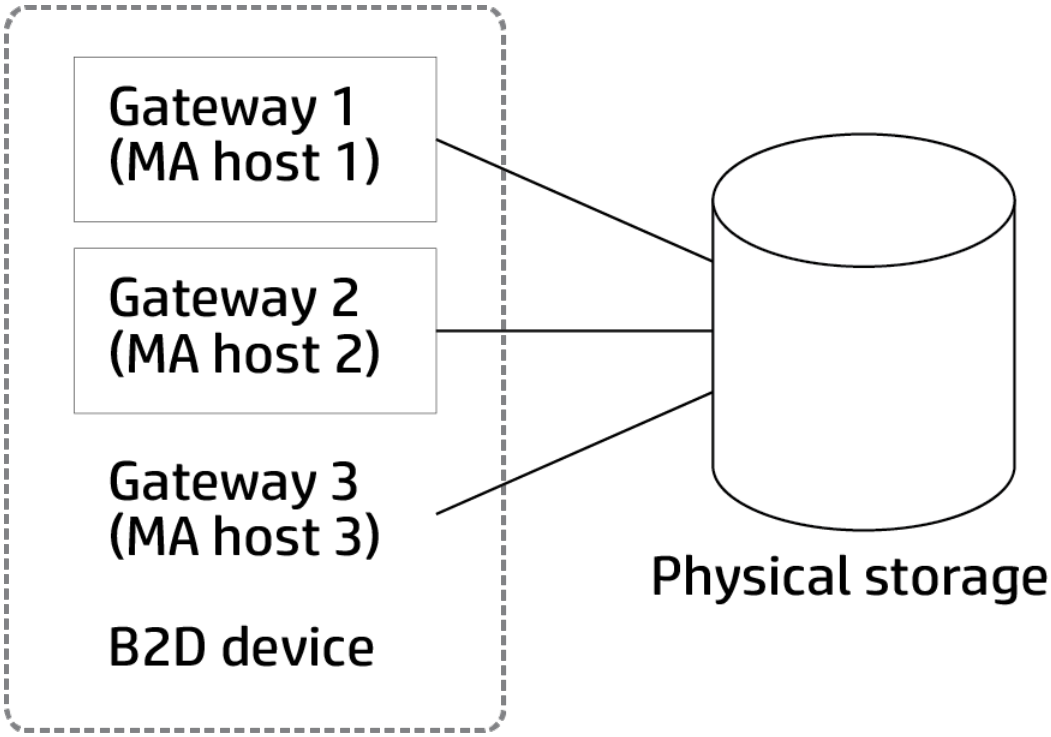
使用 Data Protector GUI 配置基于磁盘的备份设备。这些设备使用所有 Data Protector 介质管理以及备份和还原设施。

备份到磁盘设备

备份到磁盘 (B2D) 设备是将数据备份到物理磁盘存储的设备。B2D 设备支持多主机配置。这表示可以通过多个主机（称为网关）访问单个物理存储。每个网关都表示一个安装有介质代理组件的 Data Protector 客户机。物理存储还可以分区为表示特定存储部分的各个存储区（这类似于对硬盘进行分区）。物理存储上的每个存储区只能通过一个 B2D 设备进行访问。但是，多个 B2D 设备可以访问相同物理存储上的不同存储区。

尽管类似于其他基于库的设备，但是 B2D 设备的行为方式不同，因为网关可实现更大灵活性。与库驱动器不同，每个网关都表示一个主机，在该主机上可以同时启动多个介质代理（采用单个或多个会话）。

B2D 设备（逻辑视图）



可以在特定网关上启动的介质代理数由以下各项定义：

- 网关限制。每个 B2D 网关都受限于最大数量的并行流。
- 存储区上的连接限制。配置 B2D 设备时，在 GUI 中指定此限制。如果该值保留为未选中状态，则 Data Protector 使用可用的最大值。
- 物理存储单元的物理连接限制。此值从物理存储区检索得到。
- 根据当前操作，每个 Session Manager 会尝试针对以下输入参数平衡网关上的介质代理数：

- 要备份的对象数
- 对象位置
- 物理连接限制。

B2D 设备使用特殊数据格式进行快速读/写访问，这与传统 Data Protector 磁带格式不兼容。该数据格式会在您选择 B2D 设备时自动设置。

限制:

- 使用 B2D 设备执行备份时，仅“不记录任何内容”和“全部记录”日志级别适用。

重复数据删除

重复数据删除是一种数据压缩技术，通过不备份重复数据来减小备份数据的大小。重复数据删除过程将数据流分割为可管理的数据区块（或块）。这些数据区块的内容随后会相互进行比较。如果发现相同区块，则会将它们替换为指向唯一区块的指针。换句话说，如果发现 20 个相同区块，则只保留（并备份）一个唯一区块，其他 19 个区块都会替换为指针。备份数据会写入基于磁盘的目标设备（称为重复数据删除存储）。进行还原操作时，唯一区块会进行复制并插入指针所指示的正确位置。对于重复数据删除类型的还原操作，还原过程有时称为备份数据的“再水合”。

何时使用重复数据删除功能

通常，在备份可能包含同一个 1 MB 图形文件附件的 100 个实例的电子邮件系统时，会使用重复数据删除。如果该系统是使用传统备份技术备份的，则该附件的所有 100 个实例都会进行备份。这需要大约 100 MB 的存储空间。但是，借助重复数据删除，实际上只存储该附件的一个实例。所有其他实例都引用到存储的唯一副本。在此示例中，*重复数据删除率*大约为 100:1。虽然此示例称为文件级别重复数据删除，但是可用于演示使用备份到磁盘设备和重复数据删除的优点。

重复数据删除功能的优点

通常，重复数据删除可提高备份服务的整体速度并降低总存储成本。重复数据删除可显著减少所需磁盘存储空间量。因为重复数据删除是基于磁盘的系统，所以还原服务级别要高得多，会减少磁带（或其他介质）处理错误。

重复数据删除技术

市场上提供了多种重复数据删除技术。这些技术通常分为基于硬件的解决方案和基于软件的解决方案。这些解决方案可以进一步细分，例如分为文件级别（单实例化）或块级别重复数据删除。

Data Protector 以下重复数据删除后端：

StoreOnce 软件重复数据删除

Data Protector 的 StoreOnce 软件重复数据删除提供基于软件的块级别重复数据删除解决方案。

使用 StoreOnce 软件重复数据删除时，请注意以下事项：

- 重复数据删除仅备份到基于磁盘的设备。它不能用于可移动介质，如磁带驱动器或库。
- 因为 Data Protector 使用仅限软件的方法进行重复数据删除（即，使用 StoreOnce 软件重复数据删除时），所以除了标准硬盘，无需特定硬件来存储备份数据。
- StoreOnce 软件重复数据删除使用基于哈希的分块技术，将数据流分割为可调大小的数据区块。
- 在重复数据删除过程中，重复数据会删除，仅存储数据的一个副本，以及指向唯一副本的引用链接。重复数据删除能够减少所需存储容量，因为仅存储唯一数据。
- 在备份规范中指定备份到磁盘目标设备可告知 Data Protector 执行重复数据删除类型备份。

StoreOnce 备份系统设备

StoreOnce 备份系统设备是支持重复数据删除的磁盘到磁盘 (D2D) 备份设备。

重复数据删除设置

Data Protector 支持各种重复数据删除设置：

- 源端重复数据删除 (1) — 数据在源端（备份的系统）进行重复数据删除。

  对于源端重复数据删除 (1)，介质代理会与磁带客户机一起安装在进行备份的客户机上，因而客户机会成为网关（源端网关）。重复数据删

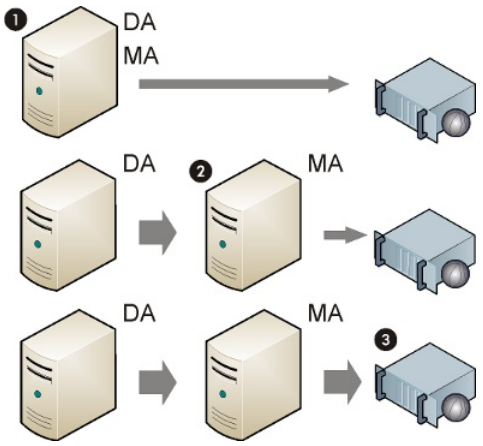
除由介质代理在客户机自身上执行，因此只有删除了重复数据的数据才会发送到目标设备，从而可减少总体网络流量。并发流的数量受限于负载均衡设置。在介质代理完成本地对象备份之后，新的介质代理会在下一个客户机系统上启动。请注意，备份的系统必须支持重复数据删除。

- 服务器端重复数据删除 (2) — 数据在介质代理系统（网关）上进行重复数据删除。

  对于服务器端重复数据删除，重复数据删除由介质代理在单独的介质代理客户机（网关）上执行。这样可减少备份的系统和目标设备上的负载，但是不会减少磁盘代理与介质代理之间的网络流量。

- 目标端重复数据删除 (3) — 数据在目标设备（StoreOnce 备份系统或 StoreOnce 软件系统）上进行重复数据删除。

  重复数据删除过程在目标设备上进行。它从安装在客户机（网关）上的介质代理接收要备份的数据。目标端重复数据删除不会减少介质代理与重复数据删除系统之间的网络流量。



相关主题

- 备份设备的类型
- 关于文件库设备
- 关于文件介质库设备
- 关于独立文件设备
- 准备备份设备
- 配置独立文件设备
- 配置文件介质库设备
- 配置文件库设备
- 配置备份到磁盘设备

文件库设备

文件库设备是位于由您定义的内部或外部硬盘驱动器上某个目录中的一种设备。文件库设备由一组目录组成。向该设备进行备份时，将自动在这些目录中创建文件。文件库目录中包含的文件称为文件仓库。

Data Protector 没有设置文件库设备的最大容量。设备大小的唯一限制由目录所在文件系统的最大大小决定。例如，Linux 中运行的文件库设备的最大大小将是可以在文件系统上保存的最大大小。

首次配置文件库设备时，要指定该设备中每个文件仓库的容量。使用设备期间随时都可以使用文件库属性重置文件仓库的调整大小属性。

文件库设备可以位于本地或外置硬盘驱动器上，只要 Data Protector 了解其路径即可。配置文件库设备时要指定路径。

如何维护基于磁盘的设备？

如果所使用的所有基于磁盘的设备都已装满，则在继续用该设备进行备份之前，将需要执行以下操作之一：

- 开始将数据移至磁带，以释放文件设备或一个或多个文件插槽。
- 循环回收文件仓库。
- 向文件设备添加新文件仓库。

文件仓库

文件仓库是包含从备份到文件库设备的数据的那些文件。

- **创建文件仓库**

  使用文件库设备启动第一个备份时，Data Protector 会在设备中自动创建文件仓库。Data Protector 为使用该设备进行的每个数据备份会话创建一个文件仓库。如果要备份的数据量大于默认最大文件仓库大小，则 Data Protector 将为一个备份会话创建多个文件仓库。

- **文件仓库名称**

  每个文件仓库的名称都是由系统自动生成的一个唯一标识符。

  Data Protector 还向文件仓库添加一个介质标识符。这样将文件仓库标识为介质池中的介质。添加到介质的标识符有助于在执行还原时标识特定的备份会话。查看文件仓库属性时，可以看到该标识符。

  请注意，如果已回收文件仓库，则尽管文件仓库图标在 GUI 中仍可见，但文件仓库名称可能从 GUI 中消失。

- **文件仓库大小**

  最初创建文件库设备时定义文件仓库的大小。在此过程中，要指定该设备的所有大小属性，包括文件仓库的最大大小。文件仓库的大小属性尽管仅输入一次，但适用于全局的每个文件仓库。如果在一个会话中要备份的数据大小大于最初指定的文件仓库大小，则 Data Protector 自动创建更多文件仓库，直到为文件库设备分配的磁盘空间用尽为止。

  默认文件仓库大小为 5 GB。可以增加此值（最多 2 TB），但性能可能会降低一些。

- **文件仓库空间消耗**

  Data Protector 自动创建文件仓库，直到对于设备没有磁盘空间可用为止。最初设置设备时，在设备属性中定义必须为文件库设备保持可用的空间量。

- **磁盘已满处理**

  如果对文件库设备可用的总磁盘空间低于用户指定的水平，则发出通知。

- **每个磁盘的设备数**

  文件库设备可以包括一个或多个目录。但只有一个目录可以位于文件系统上。

  在文件仓库位于多个磁盘上的情况下，建议不要将来自两个不同文件库设备的文件仓库放置在一个磁盘上。这是由于如果属性不同，可能会在 Data Protector 中产生冲突（例如，如果在一个文件库设备上将文件仓库的剩余磁盘空间指定为 20 MB，而在其他文件库设备上指定为 10 MB）。

设置文件库设备属性

可以在文件库设备初始配置期间设置文件库设备属性，也可以在设备运转之后更改这些属性。

属性初始设置

要设置设备目录属性，请完成以下步骤:

1. 在文件库设备配置期间，选择文件库设备目录，然后单击**属性**。
2. 指定设备的大小属性。单击**确定**。
3. 单击**下一步**，并继续配置文件库设备。

更改设备属性

要更改设备属性，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，然后单击要更改的文件库设备的名称。
3. 右键单击文件库设备名称，然后单击**属性**。
4. 单击**存储库**选项卡。在列表中选择文件库路径。
5. 单击**属性**。指定设备的所有大小属性，单击**确定**。

更改设备属性之后，Data Protector 将“属性”对话框中指定的属性应用于文件库设备中创建的每个文件仓库。后续设备属性更改之前创建的任何文件仓库的属性将不受影响。

删除文件库设备

文件库设备不得包含任何受保护数据，然后才能删除该设备。这意味着必须更改文件库中包含的每个文件仓库的数据保护级别，然后才能删除该设备。删除在以下阶段发生:

1. 检查数据保护
2. 回收文件仓库
3. 删除导出的文件仓库图标
4. 删除文件库设备

检查数据保护

要检查数据保护，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，选择要删除的文件库设备的名称，并打开该文件库中的“目录”文件夹。
3. 在结果区域中找到“保护”列。检查哪些文件仓库的保护级别为永久。

回收文件仓库

通过回收和删除文件仓库或整个文件库设备，可释放磁盘空间。

可以循环回收单独的文件仓库或文件库中的所有文件仓库。这意味着可以在下一次备份中恢复和使用由回收项占据的磁盘空间。通过删除不受保护的文件仓库和创建新文件仓库可达到此目的。完成以下步骤；

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开文件库设备的文件仓库。
3. 在结果区域中，通过单击单独的仓库，选择要循环回收的文件仓库。
4. 右键单击所选的仓库，然后单击**导出**。

导出文件仓库将可从 IDB 删除有关该文件仓库的信息。Data Protector 不再识别存在文件仓库。但仍保留仓库信息，如果需要恢复文件仓库，则以后还可以导入这些信息。

5. 右键单击所选仓库，然后单击**回收**。
6. 对文件库中数据保护级别为“完整”的每个文件仓库重复此操作。

将文件仓库标为回收后，由 Data Protector 为其自动生成的名称即消失，而只有文件仓库图标在 Data Protector GUI 中可见。可以删除导出的文件仓库图标。

删除导出的文件仓库图标

导出文件仓库后，其名称即消失，而只有仓库图标在 Data Protector Manager 中可见。完成以下步骤：

1. 在结果区域中，选择要删除的图标。
2. 右键单击所选图标，然后单击**删除**。
3. 对每个要删除的导出文件仓库图标重复此操作。

这样将从 GUI 删除图标，但不会从 IDB 中物理删除该文件。

删除文件库设备

要删除文件库设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，选择要删除的文件库设备的名称。
3. 右键单击该文件库设备，然后单击**删除**。

现在将从 IDB 中删除该文件库设备。

相关主题

- 配置文件库设备
- 释放介质
- 将介质从文件库导入到另一个主机

介质库设备

介质库是一种库设备。它可以包含光盘或文件介质。如果设备用于容纳文件介质，则将其称为文件介质库设备。在初始配置期间定义设备将容纳的介质类型。如果要在 UNIX 上运行光盘介质库，则需要为每个交换器插槽或盘面配置一个 UNIX 设备文件。

介质库文件设备

文件介质库设备在逻辑上等同于磁带堆栈。它包含多个插槽，初始设备配置期间用户定义其大小。手动配置此设备。使用文件介质库时，可更改该属性。如果用于包含文件介质，则该设备写入磁盘而非磁带。文件介质库设备以文件的形式保存数据；每个此类文件都等同于磁带设备中的一个插槽。

此设备的最大建议数据存储容量仅由正在运行文件介质库的操作系统在文件系统中所能存储的数据量限制。文件介质库设备中每个插槽的最大容量为 2 TB。但是，通常建议将插槽大小对于 Windows 保持在 100 MB 到 50 GB 之间（在 Windows 系统上），对于 UNIX 保持在 100 MB 到 2 TB 之间（在 UNIX 系统上）。例如，如果有 1 TB 数据要备份，则可以采用以下设备配置：

Windows 系统：1 个文件介质库设备，其中具有 100 个文件插槽，每个插槽 10 GB

UNIX 系统：1 个文件介质库设备，其中具有 250 个文件插槽，每个插槽 4 GB

要提高介质库文件设备的性能，建议每个磁盘仅有一个设备，并且每个设备仅有一个驱动器。还应避免 Data Protector 正在备份/还原时其他应用程序从磁盘传输大量数据或将大量数据传输到磁盘。

建议对于 Windows 和 UNIX 采用的插槽大小

可用磁盘空间	插槽数	插槽大小
1 TB	100	10
5 TB	250	20
10 TB	250	40

维护文件介质库设备

如果所使用的所有文件介质库设备都已装满，则在继续用该设备进行备份之前，将需要执行以下操作之一：

- 开始将数据移至磁带，以释放文件设备或一个或多个文件插槽。
- 循环回收介质库插槽。
- 向文件设备添加新的介质库插槽。

配置文件介质库设备

建议将所创建的设备置于 IDB 所在磁盘以外的磁盘上。这样可确保有足够的磁盘空间供数据库使用。将设备数据库和 IDB 放置在不同的磁盘上还能提高性能。

配置阶段

- 配置文件介质库设备
- 配置文件介质库设备中的驱动器

配置文件介质库设备

配置文件介质库设备时，请考虑以下事项:

- 请勿使用现有设备的名称配置这些设备，因为现有设备将被覆盖。
- 请勿使用相同的设备名称用于配置多个设备，因为每次访问设备时都会覆盖设备名称。

- 在 Windows 系统中，必须对要用作设备的文件禁用 Windows 压缩选项。
- 必须已在磁盘上创建设备所在的目录，然后再创建设备。

要配置文件介质库设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. 在“设备类型”列表中，选择**介质库**设备类型。
6. 在“客户机”列表中，选择客户机的名称。
7. 在“管理控制台 URL”文本框中，输入库管理控制台的有效 URL 地址（可选）。
8. 单击“下一步”。
9. 为介质库指定一组文件/磁盘。使用短划线一次输入多个文件或磁盘 (例如 /tmp/FILE 1-3)，然后单击“添加”。对于磁光介质库，磁盘名称必须以 A/a 或 B/b 结尾。单击“下一步”。
10. 在“介质类型”列表中，对要配置的设备选择**文件**。
11. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

配置文件介质库设备中的驱动器

要在文件介质库设备中配置驱动器，请完成以下步骤:

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明（可选）。
3. 指定所选介质类型的介质池。可以从“介质池”列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。单击“下一步”。
4. （可选）选择**设备可用于还原**和/或**设备可用作进行对象复制的源设备**，并指定**设备标记**。
5. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

回收文件介质库插槽

对文件介质库中的每个文件插槽都设置了数据保护，因此通过将其保护设置为**无**可以循环回收单个插槽。因此，拥有多个小型插槽可以提高灵活性，并使数据保护和空间保留管理更高效。回收文件介质库设备中的插槽将去除其数据保护，这样即可重新使用插槽进行备份。后续的备份会话中将覆盖插槽中的数据。

> **重要说明**如果使用此方法，则介质上的现有数据将被覆盖并丢失。

要回收文件介质库插槽，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开文件介质库设备插槽。
3. 在结果区域中，选择要循环回收的插槽。
4. 右键单击所选插槽，然后单击**回收**。

相关任务

- 添加插槽

独立设备

有两种类型的独立设备:

- 独立物理设备
- 独立文件设备

独立物理设备

独立设备是包含一个驱动器的简单设备，该驱动器一次从一个介质读取或写入一个介质（如 DDS 或 DLT）。这些设备用于小规模备份。介质充满后，操作员必须手动将其替换为新介质，备份才能继续。因此，独立设备不适合大规模的无人看管备份。

独立文件设备

独立文件设备是指定目录中的一个文件，您向该文件备份数据而非写入磁带。此设备以文件的形式保存数据；每个此类文件都等同于磁带设备中的一个插槽。独立文件设备适用于较小的备份。

文件设备的最大容量为 2 TB。但是，通常建议将独立文件设备大小对于 Windows 系统保持在 100 MB 到 50 GB 之间，对于 UNIX 系统保持在 100 MB 到 2 TB 之间。Data Protector 从不测量文件系统上的可用空间量；对于文件大小限制，它采用默认或指定容量。对于文件设备不能使用压缩文件。可通过设置 FileMediumCapacity 全局选项来更改默认文件大小。

独立文件设备的默认最大大小为 100 MB。如果要备份比这更大的文件，可通过设置 FileMediumCapacity 全局选项更改默认文件大小。

例如，如果最大值为 20GB (20Gb = 20000 MB)，则按如下设置 FileMediumCapacity 全局选项:

```
# FileMediumCapacity=MaxSizeInMBytes
```

```
FileMediumCapacity=20000
```

首次格式化介质时指定文件设备的容量。重新格式化介质时，可以指定新大小；但是，将使用最初指定的大小。只能通过从系统中删除文件才能更改文件设备的容量。

指定的大小应至少比文件系统中的最大可用空间小 1 MB。文件设备达到其大小限制时，Data Protector 将发出装载请求。

要提高独立文件设备的性能，建议每个磁盘仅有一个设备，并且每个设备仅有一个驱动器。还应避免 Data Protector 正在备份/还原时其他应用程序从磁盘传输大量数据或将大量数据传输到磁盘。

文件可以位于本地或外置硬盘驱动器上，只要 Data Protector 了解其路径即可。配置文件设备时要指定路径。

配置独立文件设备

建议将所创建的设备置于 IDB 所在磁盘以外的磁盘上。这样可确保有足够的磁盘空间供数据库使用。将设备数据库和 IDB 放置在不同的磁盘上还能提高性能。

请考虑以下几点：

- 请勿使用现有设备的名称配置这些设备，因为现有设备将被覆盖。
- 请勿使用相同的设备名称用于配置多个设备，因为每次访问设备时都会覆盖设备名称。

- 在 Windows 系统中，必须对要用作设备的文件禁用 Windows 压缩选项。
- 必须已在磁盘上创建设备所在的目录，然后再创建设备。

要配置独立文件设备，请完成以下步骤:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. 在“客户机”列表中，选择客户机的名称。
6. 在“设备类型”列表中，选择“独立设备”设备类型，然后单击“下一步”。
7. 在文本框中，输入文件设备的路径名和文件名，例如 c:\My_Backup\file_device.bin 。
8. 单击**添加**，然后单击**下一步**。
9. 在“介质类型”列表中，选择**文件**介质类型。
10. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
11. 单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。

此时已将设备指定为 Data Protector，但磁盘上尚未实际存在该设备。必须格式化该设备，然后才能将其用于备份。

相关主题

- 要修改现有全局选项的值或添加新选项，请参阅自定义全局选项。

设置备份

备份是在备份介质上创建系统数据副本的过程。该副本的存储和保留是供将来万一发生原始数据损坏时使用。

备份会话以备份规范为基础，而且能够以交互方式启动。在备份会话期间，Data Protector 读取备份对象，通过网络传输其数据，然后将其写入设备中的介质。

重要说明请确保备份的数据前后一致。例如，可能会在备份之前关闭应用程序，或将其置于“备份”模式以避免备份期间数据发生更改。如果所备份的数据前后不一致，则在还原和尝试使用数据时可能会遇到意外的结果。

Data Protector 备份的高级功能包括：

- 自动平衡设备的使用情况（负载均衡）
- 备份共享磁盘
- 安排无人看管备份
- 同时进行完全备份和增量备份以节省时间和介质
- 允许以多种不同的方式组织备份
- 使用对象镜像功能同时备份到多个位置

Data Protector 帮助中提供的过程假定您使用根据可供备份或模板使用的数据类型所设置的默认备份视图（按类型）。

有关如何备份 Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、Informix Server、IBM DB2 UDB 或 Sybase 等数据库应用程序的信息，请参阅《Data Protector 集成指南》。

设置备份视图

可以根据需要设置备份视图。默认备份视图是**按类型**。

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，选择一个可用视图。

根据已选的视图显示“备份”上下文。

备份类型

Data Protector 通过以下备份类型:

- 文件系统备份
- 基于块的备份

文件系统备份

Data Protector 提供两种基本的文件系统备份类型：完整备份和增量备份。这些备份类型适用于整个备份规范，并仅适用于文件系统对象。

要组合使用完整和增量备份，请确保备份对象拥有完全相同的：

- 客户机名称
- 驱动器/装载点
- 描述
- 所有者（适用于私有对象）

如果执行交互式备份，则会提示您选择备份类型。安排备份时，在计划向导中指定备份类型。例如，可以创建一个日程安排，对相同的备份规范在周六执行完整备份，在所有工作日执行 Incr1 备份。

完整备份

完整备份始终备份所选的全部对象，即使从上一次备份以来没有更改也是如此。对象的第一个备份始终是完整备份。如果备份时不存在具有相同所有权的受保护完整备份（适用于专用对象），则任何后续备份都将以完整备份的形式执行。

增量备份

增量备份备份自上次仍受保护的（完整或增量）备份以来的更改。必须存在对象的完整备份（客户机名称、装载点、说明和所有者完全相同），然后才能对该对象进行增量备份。

增量备份的类型

Data Protector 提供不同类型的增量备份。

- 增量

  简单的增量备份基于仍受保护的上次备份，后者可以是完整备份或增量备份。

- 增量 1-9

  分级增量备份取决于低一级别仍受保护的上一次备份。例如，1 级增量备份保存自上次完整备份以来的所有更改，而 5 级增量备份保存自上次 4 级增量备份以来的所有更改。Incr1-9 备份永不引用现有的 Incr 备份。

- 差异

  在 Incr1 备份的某些应用程序集成中使用的术语。差异备份将保存从上次完整备份以来所做的所有更改。

高级备份解决方案

Data Protector 还提供高级备份解决方案，如增强型增量备份和合成备份。

完整备份和增量备份 - 比较

提高备份性能的基本方法是减少所备份数据的量。规划完整备份和增量备份时，应充分利用时间和资源。通常不需要在同一天对所有系统都执行完整备份。

请考虑以下有关备份类型的内容：

	完整备份	增量备份
资源	需要比增量备份更多的时间，并且需要更多介质空间。	仅备份自上次备份以来发生的更改，这样需要的时间和介质空间较少。
设备处理	如果使用只有一个驱动器的独立设备，则在备份不适合单个介质时需要手动更换介质。	但备份不大可能需要额外的介质。
还原	可实现简单且快速的还原。	由于所需的介质较多，因此还原需要较长时间。
对 IDB 的影响	占据 IDB 中的更多空间。	占用 IDB 中的空间较少。

注意必须设置适当的数据保护以确保所有需要的完整备份和增量备份可供还原。如果数据保护设置得不正确，则可能会覆盖某些介质，这会导致还原链中断。

传统增量备份

在运行备份对象的增量备份之前，Data Protector 将备份对象中的树与此对象的有效还原链中的树进行比较。如果树不匹配（例如，选中了备份对象中上次备份时尚不存在的其他目录进行备份，或者存在备份对象相同、树不同的多个备份规范），将自动执行完整备份。这可确保备份中包括全部所选文件。

检测更改

对于传统的增量备份，确定某文件自上次备份以来有没有更改的主要标准是该文件的修改时间。但是，有一些情况下此标准无效。例如，如果将某个文件重命名、移至新位置或改变了其部分属性，其修改日期不会更改。因此，在增量备份中并不总是备份该文件。而是在下次完整备份中备份此类文件。

增量备份中是否备份名称、位置或属性发生更改的文件，还取决于备份规范中以下选项的设置。首选设置可改善对更改的检测。

Windows 系统: 不使用存档属性

默认情况下，不选择此选项（使用存档属性）。这是首选设置。

UNIX 系统: 不保留访问时间属性

默认情况下，不选择此选项（保留访问时间属性）已首选此选项。

您可以使用 Windows NTFS 更改日志提供程序执行传统增量备份。在此情况下，将使用 Windows 更改日记生成自上次完整备份以来已修改的文件的列表，而不执行文件树遍历。使用更改日志提供程序可提高增量备份的总体性能，方式与其提高增强型增量备份性能的方式相同。如果由于某种原因而无法使用更改日志提供程序，则会执行常规的传统增量备份。

要可靠地检测和备份重命名和移动过以及属性发生更改的文件，请使用增强型增量备份。

增强型增量备份

对于传统的增量备份，确定某文件自上次备份以来有没有更改的主要标准是该文件的修改时间。但是，有一些情况下此标准无效。例如，如果将某个文件重命名、移至新位置或改变了其部分属性，其修改日期不会更改。因此，在增量备份中并不总是备份该文件。而是在下次完整备份中备份此类文件。

增强型增量备份能可靠检测和备份重命名过的、移动过的和属性更改过的文件。

能否检测到某些更改（如权限或 ACL 的更改）还取决于备份规范中以下选项的设置。首选设置可使增强型增量备份最大程度地检测到更改。

- **Windows 系统:** 不使用存档属性

  默认情况下，不选择此选项（使用存档属性）。这是首选设置。

- **UNIX 系统:** 不保留访问时间属性

  默认情况下，不选择此选项（保留访问时间属性）该选项在被选中时为首选设置。

部分选择备份的树变更时，使用增强型增量备份就无需对整个备份对象进行完整备份。例如，如果自上次备份以来选择了其他目录进行备份，则将执行该目录（树）的完整备份，而对剩余部分进行增量备份。

此外，还可以使用 Windows NTFS 更改日志提供程序，执行增强型增量备份。在此情况下，将使用 Windows 更改日记生成自上次完整备份以来已修改的文件的列表，而不执行文件树遍历。使用更改日志提供程序可提高增量备份的总体性能，尤其是在文件众多但其中仅有一小部分文件发生变化的环境中。

为什么使用增强型增量备份

使用增强型增量备份是为了：

- 确保对名称、位置或属性发生更改的文件进行增量备份。
- 在仅所选的某些树发生更改时消除不需要的完整备份。
- 实现后续的对象合并（合成备份）。

对磁盘空间消耗的影响

增强型增量备份在所备份的每个客户机上使用一个小数据库。会对每个文件系统装载点都创建数据库。增强型增量备份存储库位于以下目录中：

- **Windows 系统：** Data_Protector_home\enhincrdb\MountPointDir

  要从装载点获取装载点目录 (MountPointDir)，可通过将任何 ":" (冒号) 和 "\\" (反斜杠) 字符(冒号) 和 "\" (反斜杠) 字符替换为 "_" (下划线) 字符，并删除结尾的 ":" 或 "\"。

- **HP-UX 和 Linux 系统：** /var/opt/omni/enhincrdb

对客户机上磁盘空间的影响通常小于选择进行备份的文件大小的 1%。确保定期清除增强型增量备份数据库。可以通过设置 OB2_ENHINC_DELETE_INTERVAL 和 OB2_ENHINC_DELETE_THRESHOLD omnirc 选项来执行此操作。

磁带客户机并发

多个磁盘代理可能会同时访问增强型增量备份数据库。要避免可能出现的备份问题，请通过设置以下 omnirc 选项来配置磁盘代理行为:

- OB2_ENHINC_LOCK_TIMEOUT
- OB2_ENHINC_SQLITE_MAX_ROWS
- OB2_ENHINC_MAX_MEMORY_LIMIT

以下限制适用：

- 仅目录级别支持增强型增量备份。如果逐个选择文件进行备份，则将不使用增强型增量模式。
- 使用增强型增量模式时，硬链接检测被禁用。

使用更改日志提供程序的增量备份

传统的增强型增量备份通过执行文件树遍历来生成要备份的文件列表。这个过程可能会占用相当长的时间，尤其是目录结构很大且包含大量文件的情况。Windows NTFS 更改日志提供程序（基于 Windows 更改日记）解决此问题的方式为向更改日记查询发生更改的文件的列表，而非执行文件树遍历。更改日记能够可靠地检测并记录对 NTFS 卷上文件和目录所做的全部更改，因此 Data Protector 可使用它作为一种跟踪机制，以生成自上次完整备份以来已修改的文件的列表。这对于具有大型文件系统但在两次备份之间仅有少量文件发生更改的环境大有裨益。在这种情况下，可以用短得多的时间完成确定哪些文件发生更改的过程。

每个 NTFS 卷都有自己的更改日记数据库。对文件或目录做出一次更改，就会向日记追加一条记录。记录中标明了更改的文件名、时间和类型。请注意，日记中并不保留发生更改的实际数据。如果日记文件变得过大，则系统会清除日记开头处最旧的记录。如果已从更改日记中清除了备份所需的数据，则 Data Protector 将执行完整备份，并发出无法使用更改日记的警告。

在使用更改日志提供程序的增量备份中是否备份某个文件，取决于在备份规范中是否设置了如有可能，请使用本机文件系统更改日志提供程序选项。如果指定了此选项，则 Data Protector 尝试使用“更改日记”。如果“更改日记”处于不活动状态，则 Data Protector 会发出一个警告。如果在增强型增量备份过程中发生这种情况，则改为执行完整备份。如果在传统增量备份过程中发生这种情况，则改为执行常规增量备份。自动设置不保留访问时间属性和不使用归档属性选项，并且不能禁用这两个选项。

Data Protector 仅支持使用 Windows NTFS 的更改日志提供程序进行增量备份。

在使用更改日志提供程序运行增量备份之前，请确保满足以下条件:

- 使用 omnicjutil -query 命令在所需卷上激活更改日记。如果更改日记未处于活动状态，请通过运行 omnicjutil - start 启动它。有关 omnicjutil 命令的详细信息，请参阅位于此 Mount_point/DOCS/C/MAN 目录的安装包中的《Data Protector 命令行界面参考》。
- 至少存在一个完整备份 (在备份规范中选择了“如有可能，请使用本机文件系统更改日志提供程序”选项)，然后再使用更改日志提供程序启动增强型增量备份。

性能损失和磁盘空间消耗

要达到更改日志提供程序的最佳性能，请在启动备份（备份类型为 Incr）时使用增量备份。也支持 Incr1-9，但性能可能会降低一些。

打开后，更改日记会消耗一些 CPU 时间和磁盘空间。所消耗的磁盘空间限制为 4 GB。可以设置更改日记的最大大小，以及当日记达到其最大大小时对其要截断的大小。有关详细信息，请参阅《Data Protector 命令行界面参考》。

要优化更改日志提供程序的性能，可使用 OB2_CLP_MAX_ENTRIES omnirc 选项指定更改日志提供程序在内存中可容纳的条目数。有关详细信息，请参阅《Data Protector 故障诊断指南》。

在以下情况下，Data Protector 执行完整备份，并忽略在备份规范中设置更改日志提供程序选项：

- 如果在客户机系统上更改日记不活动。
- 如果已从更改日记清除了所需的数据。
- 如果更改日记 ID 与原先不同（这意味着另一个应用程序已删除然后又重新创建了更改日记）。

默认情况下，首次执行更改日志提供程序时，它不会创建增强型增量存储库。这意味着更改日志提供程序首次发生错误时将执行完整备份，而此过程将创建增强型增量存储库。可通过 OB2_CLP_CREATE_EI_REPOSITORY omnirc 选项更改此行为。有关详细信息，请参阅《Data Protector 故障诊断指南》。

注意事项

- Data Protector 对更改日记没有独占访问权限。这意味着，通过激活或取消激活更改日记，其他应用程序也会影响 Data Protector。如果在给定卷上禁用更改日记，则不会向日记中记录任何文件和目录更改。默认情况下，NTFS 卷禁用了其更改日记，因此必须使用 cjutil 或 omnicjutil 命令显式将其激活。同时，任何其他应用程序都可以随时激活或禁用卷的日记。有关更改日记的详细信息，请参见 Windows 文档。

  默认情况下，更改日记在受支持的 Windows 版本上处于活动状态。

- 在文件系统上只有少量更改的环境下，使用更改日志提供程序大有裨益。如果要备份包含许多更改（例如，含有创建并在创建不久后删除的许多临时文件）的文件系统，则对树进行普通遍历更快。

- Windows 更改日记 API 不提供有关属性的详细信息。所有属性更改都组合在一起。使用 API 时，无法确定更改日记中的条目是由要清除的

存档属性还是上次访问时间中的更改所引起。

更改日志提供程序不清除存档属性。备份文件之后，Data Protector 的正常行为是清除存档属性。因此，使用更改日志提供程序时，将自动选中**不使用存档属性**选项。

备份文件之后，Data Protector 的正常行为是重置上次访问时间（因为备份过程总是会更改上次访问时间）。更改日志提供程序不会将其重置，因此将自动选中**不保留访问时间属性**选项。

自动选择这两个选项的原因是为了避免多次备份相同文件的情况。如果清除了存档属性或重置了上次访问时间，则在更改日记中显示一个条目，并在下次会话中备份文件，即使尚未更改文件也是如此。

- 需要使用 cjutil - query 命令不时地监视 NextUsn 数字，并在 NextUsn 接近 MaxUsn 数字时重新启动更改日记。
- 如果已更改了备份规范，则完整地备份所有新树。这意味着对所有新树执行普通树遍历，而对旧树使用更改日志提供程序。
- 如果重命名备份空间下的目录，则将对该目录执行普通树遍历。

合成备份

合成备份是一种高级备份解决方案，无需运行定期的完整备份。在初始完整备份之后，只需要运行增量备份，然后与完整备份合并为一个新的合成完整备份。此过程可以无限重复，不再需要运行完整备份。在还原速度方面，此类备份与传统的完整备份相当。

Data Protector 用一种名为对象合并的操作执行合成备份。

如何执行合成备份

合成备份过程由以下步骤组成：

1. 在用于完整备份和增量备份的备份规范中，启用增强型增量备份选项。
2. 执行完整备份。
3. 配置后续的增量备份，使其写入一个文件库或 B2D 设备（智能缓存除外）
4. 当存在至少一个增量备份时，执行对象合并。执行对象合并的频率取决于备份策略。

虚拟完整备份

虚拟完整备份是一种更高效的合成备份类型。此解决方案用指针合并数据，而非复制数据。因此，合并所用时间更短，并且避免了对数据不必要的复制。

该过程与常规合成备份基本相同，但有以下额外要求：

- 所有备份（完整备份、增量备份和所产生的虚拟完整备份）均必须写入一个文件库。
- 文件库必须使用分布式文件介质格式。

> **注意**通过虚拟完整备份，可以减少空间消耗，因为对象共享相同的数据块。但是，如果数据块损坏，可能会影响多个对象。为提高可靠性，请将文件库放置在 RAID 磁盘上。

基于块的备份过程

通过基于块的备份选项，您能够在块级别执行备份。

要创建基于块的备份规范，请完成以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型（例如**文件系统**），然后单击**添加备份**。
4. 在“创建新备份”对话框中，选择一个可用的模板以及备份类型，然后根据需要选择其他选项。单击**确定**打开向导。
5. 在“源属性”页上，从“文件系统备份”下拉列表中选择“基于块的备份”选项。
6. 在“所有系统”下拉列表中，选择以下某选项: “所有系统”、“选定的系统”和“Windows 系统”。
7. 展开包含要备份的对象的系统，选择所需的对象。

   展开系统时仅显示受支持的 **NTFS** 对象。至少选择一个要继续的对象，然后单击“下一步”。
8. 在“目标”属性页中，选择要用于备份的设备。

   展开主机时仅显示受支持的设备。至少选择一个设备以继续。

   还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击“添加镜像”和“删除镜像”按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。

   > **提示**如果备份经过负载均衡，则可以设置 Data Protector 使用设备的顺序。右键单击所选设备，然后单击“给设备排序”。

   单击“下一步”。
9. 在“选项”属性页中，可以设置备份选项。可用的备份选项取决于所备份的数据类型。例如，所有可用于文件系统备份的备份选项并不可用于磁盘映像备份或基于块的备份。单击“下一步”。
10. 在“调度程序”页面上，可以根据需要计划备份，然后单击“下一步”。
11. 在“备份摘要”页中，检查备份规范的摘要。建议首先保存备份规范，然后再开始预览。

    对于基于块的备份，“手动添加”选项不可用。

    单击“下一步”。
12. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。
    - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
    - 如果保存并计划所配置的备份，请首先保存备份规范，然后打开“调度程序”页面，在其中可以指定必须运行此保存的备份规范的日期和时间。
    - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

> **提示**通过复制现有规范，然后修改某个副本，可以创建多个备份规范。

有关备份规范的详细信息，请参阅标准备份过程。

标准备份过程

标准备份过程由以下几个部分组成：

- 选择要备份的数据。
- 选择要将这些数据备份到的位置。
- 选择要额外创建多少备份副本（镜像）。
- 开始或安排备份会话。

与此同时，创建备份规范。通过设置各种选项（使用默认值或将其设置为满足特定需要）定义如何备份的详细信息。

要更改这些预定义的设置，请指定：

- 目标备份规范中所有对象的备份选项，如 pre-exec 和数据保护
- 希望执行备份的日期和时间

执行标准备份过程时，请考虑以下事项:

- 需要在要备份的每个系统上都安装磁盘代理，除非使用 NFS（在 UNIX 系统中）或执行网络共享备份（在 Windows 系统中）备份这些系统。
- 至少需要在 Data Protector 单元中配置一个备份设备。
- 需要将介质做好备份的准备。
- 需要具有执行备份的相应用户权限。

对于每个文件系统，可以限制对特定的几个目录树进行备份。对于每个目录树，可以：

- 排除任何子树或文件
- 备份符合特定通配符模式的文件
- 跳过符合特定通配符模式的文件

例如，软件应用程序永久使用某些文件。应从文件系统备份中排除这些文件，并应以特殊方式备份这些文件。

创建备份规范

备份规范定义要备份的客户机、磁盘、目录和文件；要使用的磁带设备或驱动器；其他备份副本（镜像）的数量；备份选项；以及时间安排信息（希望何时执行备份）。备份规范可以像将一个磁盘备份到独立 DDS 驱动器一样简单，也可以像指定将 40 台大型服务器备份到含有 8 个驱动器的磁带库一样复杂。

- Data Protector GUI 可显示的备份规范数量是有限的。可显示的备份规范数量取决于备份规范的参数大小（名称、组、所有权信息以及备份规范是否为负载均衡的信息）。此大小不应超过 80 KB。

要创建备份规范，请完成以下步骤:

> **重要说明**在 UNIX 系统中，如果要执行即时恢复，请选择要备份的卷组中的所有文件系统。否则，将无法使用 Data Protector GUI 进行即时恢复，或者（如果使用 Data Protector CLI 执行即时恢复）会损坏数据。

单击“下一步”。

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型（例如**文件系统**），然后单击**添加备份**。
4. 在**创建新备份**对话框中，选择一个可用的模板以及备份类型，然后根据需要指定其他选项。单击**确定**打开向导。
5. 在零宕机时间备份的情况下，此时将显示“配置”页。配置集成，然后单击**下一步**。
6. 在集成备份的情况下，选择客户机和应用程序数据库。单击“下一步”。
7. 在“源”属性页中，展开包含要备份的对象的系统，然后选择要备份的内容。
8. 在“目标”属性页中，选择将用于备份的设备。

   还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。无法使用 ZDB 到磁盘或 NDMP 来镜像备份的对象。

   > **提示**如果备份经过负载均衡，则可通过右键单击选定设备，然后单击“对设备进行排序”，设置 Data Protector 使用设备时采用的顺序。

单击“下一步”。

9. 在“选项”属性页中，可以设置备份选项。可用的备份选项取决于所备份的数据类型。例如，磁盘映像备份或基于块的部分并不具有文件系统备份所具有的所有备份选项。单击“下一步”。
10. 在“备份摘要”页中，检查备份规范的摘要。建议首先保存备份规范，然后再开始预览。预览不可用于 Data Protector 内部数据库备份、特定 Data Protector 应用程序集成的备份会话以及零宕机时间备份 (ZDB)。

    单击“下一步”。
11. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。此时会发生以下情况：
    - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
    - 如果保存并计划所配置的备份，请首先保存备份规范，然后打开“调度程序”页面，在其中可以指定必须运行此保存的备份规范的日期和时间。
    - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

提示通过复制现有规范，然后修改某个副本，可以创建多个备份规范。

修改备份规范

可以修改已配置和保存的备份规范。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“源”属性页以及其他属性页（“目标”、“选项”和“日程”）中修改备份规范，然后单击**应用**。
   如果是基于块的备份，则备份类型一旦创建便无法修改。

修改备份后，即可在**操作**菜单中预览或开始该备份。

注意预览不可用于 Data Protector 内部数据库备份、特定 Data Protector 应用程序集成的备份会话以及零宕机时间备份 (ZDB)。

提示修改备份规范、执行备份然后选择对象进行还原时，仅选择上一个版本中备份的文件和目录进行还原。要更改备份版本，请右键单击对象，然后单击**选择版本**。

预览和启动备份

可以预览备份以验证您的选择。预览不从选择进行备份的磁盘中读取数据，也不将数据写入为备份配置的设备中的介质。但是，预览将检查通过所使用的基础架构进行的通信，并确定数据大小和目标处是否有介质。向 Data Protector 提供所有备份的信息之后，可以启动现有的（已配置和保存）备份。以下限制适用：

- 预览不可用于 Data Protector 内部数据库备份以及特定 Data Protector 应用程序集成的备份会话。
- 预览不可用于零宕机时间备份 (ZDB)。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 选择要启动或预览的备份规范。
4. 在**操作**菜单中，如果要预览备份，则单击**预览备份**，或单击**启动备份**以启动该备份。
5. 在“预览或启动备份”对话框中，选择备份类型（完整或增量；对于特定集成还有某些其他备份类型）和网络负载。只能在完整模式下预览文件系统备份。

   在 ZDB 到磁盘 + 磁带或 ZDB 到磁盘（启用了即时恢复）的情况下，指定分割镜像/快照备份选项。
6. 单击**确定**预览或启动备份。

此时“会话信息”消息将显示备份的状态。

提示配置新备份时，可以在备份向导的结尾处启动交互式备份或交互式预览。

中止备份

中止备份会话可终止备份会话。仅对中止会话之前备份的数据将存在备份副本。要中止备份，请完成以下步骤:

1. 在“操作”菜单中，单击**中止**，以中止备份会话。

   如果在中止备份会话时该会话仍在确定您选择进行备份的磁盘大小，则不会立即中止该会话。确定大小后即中止备份。

提示可以中止 Data Protector 监视器上下文中一个或多个当前正在运行的会话。

重新启动失败的备份

在备份会话期间，某些系统因其关闭、有某些临时网络连接性问题等等而不可用。这些情况导致无法备份某些系统或只能备份一部分，换句话说，某些对象失败。解决了妨碍的问题后，可以重新启动出现问题的会话。此操作只会重新启动失败的对象。 当重新启动失败的对象时，备份会使用新的会话 ID 重新启动。

对于失败的文件系统和 Oracle Server 集成备份会话，您还可以使用恢复会话功能从会话失败的点开始继续备份。

以下限制适用：

- 无法重新启动以交互方式运行（意味着它们是基于未保存的备份规范）的失败会话。
- 无法同时重新启动多个会话。

重要说明重新启动失败的备份会话之前不要更改备份规范。否则将无法重新启动所有对象。

要完成以下步骤，必须位于 Data Protector Admin 用户组中，或具有 Data Protector“监视”用户权限。

1. 如果您使用的是普通 Cell Manager，在上下文列表中单击**内部数据库**。

   如果您使用的是管理器的管理器，在上下文列表中选择**客户机**，然后展开**企业客户机**。选择会话出现问题的 Cell Manager。从“工具”菜单中选择**数据库管理**，从而打开一个新 Data Protector GUI 窗口，并显示“内部数据库”上下文。

2. 在范围窗格中，展开**内部数据库**，然后单击**会话**。

   此时将在结果区域中显示会话的列表。每个会话的状态显示在“状态”列中。

3. 右键单击失败、中止或完成但发生过失败或出现错误的会话，然后选择**重新启动失败的对象**以备份失败的对象。

4. 单击**是**确认。

复制备份规范

可通过完成以下步骤复制已配置并保存的备份规范:

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 在结果区域中，右键单击要复制的备份规范，然后单击**复制为**。此时将打开“将备份复制为”对话框。
4. 在“名称”文本框中，输入所复制的备份规范的名称。（可选）从“组”下拉列表中，选择所复制的备份规范所属的备份规范组。
5. 单击**确定**。

此时将在范围窗格中和结果区域中的新名称下显示所复制的备份规范。

删除备份规范

可以删除已配置和保存的备份规范。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 右键单击要删除的备份规范，然后单击**删除**。确认选择。

此时即从范围窗格的备份上下文中删除备份规范。

高级备份任务

可以用多种方式控制备份。Data Protector 提供一组适用于 Windows 和 UNIX 系统的高级备份任务。

高级备份任务包括指定默认情况下不使用的某些选项或采取某些不遵循标准备份过程的操作。

- 需要在要备份的每个系统上都安装磁盘代理，除非使用 NFS（在 UNIX 系统中）或执行网络共享备份（在 Windows 系统中）备份这些系统。
- 至少需要在单元中配置一个备份设备。
- 需要将介质做好备份的准备。
- 需要具有执行备份的相应用户权限。
- 在进行之前必须考虑标准备份过程。

以下是高级备份任务:

选择网络共享磁盘进行备份

可以备份 Windows 共享磁盘上的数据。必须使用常规 Data Protector 磁带客户机才能通过共享磁盘备份其他远程系统。

使用共享磁盘方法进行备份是对无法以其他方式备份的系统进行备份的一种解决方法。建议不要将此方法作为主要备份方法。

在以下条件下，备份位于网络中共享的 Windows 系统上的文件系统：

- 如果系统不是 Data Protector 单元的一部分，并且未安装 Data Protector 磁盘代理。
- 如果您想要备份 Data Protector 不直接支持的平台。

> **提示:**为了减少网络负载，磁带客户机客户应也是介质代理客户。否则，数据将在网络上传输两次。

以下限制适用：

- 备份共享磁盘并不备份所有文件属性。只能备份共享主机上可见的内容。可以还原数据，但可能会缺少某些文件/目录属性。
- 不支持使用 VSS 功能备份在网络共享卷上存储其数据的写入程序。此外，在 Windows Server 2012 上，也不支持在启用了磁盘代理和使用卷影复制选项的情况下备份网络共享或远程网络文件夹。

在选择网络共享磁盘进行备份之前，请执行以下操作:

- 必须更改磁带客户机上的 Data Protector Inet 帐户，以便获得正确的权限以访问要备份的共享磁盘。此帐户必须具有同时访问本地客户机系统和远程共享磁盘的权限。
- 设置 Inet 服务的用户帐户后，即可备份共享磁盘，如同其位于本地系统上一样。

在受支持的 Windows 系统中:

必须添加一个对要备份的共享磁盘具有访问权限的用户帐户。此帐户必须是本地系统帐户。

必须满足这一先决条件，然后才能更改磁带客户机上的 Data Protector Inet 帐户。在将运行磁带客户机的 Data Protector 客户机上运行以下命令：

```
omniinetpasswd -add User@Domain [Password]
```

确保已使用“备份”向导映射共享驱动器。

使用 Windows GUI，因为 UNIX GUI 中不支持浏览 Windows 系统。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型（例如**文件系统**），然后单击**添加备份**。
4. 在**创建新备份**对话框中，选择一个可用的模板，然后单击**确定**打开向导。
5. 在“源”属性页中，从下拉列表中选择**网络共享备份**（当 GUI 在 Windows 系统中运行时可用）。
6. 单击**映射网络共享**以打开**浏览网络共享**窗口。

7. 在“客户机系统”下拉列表中，选择具有将用于备份的磁带客户机的客户机系统。
8. 在“共享目录”框中，选择或指定共享磁盘，然后单击**确定**。如果要选择更多磁盘，请使用**应用**。
9. 在“源”属性页中，选择或指定要备份的共享文件系统。单击“下一步”。
10. 在“目标”属性页中，选择将用于备份的设备。

    还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。无法使用 ZDB 到磁盘或 NDMP 备份功能镜像对象备份。

    > **提示:**如果备份经过负载均衡，则可通过右键单击选定设备，然后单击“对设备进行排序”，设置 Data Protector 使用设备时采用的顺序。

    单击“下一步”。
11. 在“选项”属性页中，可以设置备份选项。可用的备份选项取决于所备份的数据类型。例如，磁盘映像备份并不具有文件系统备份所具有的所有备份选项。

    在受支持的 Windows 系统中:

    a. 在“备份规范选项”下，单击**高级**按钮。
    b. 在“备份选项”对话框中的“所有权”下，输入对将备份的共享磁盘具有访问权限的用户帐户的相关信息。
    c. 单击**确定**。
12. 单击“下一步”。
13. 在“备份摘要”页中，检查备份规范的摘要。建议首先保存备份规范，然后再开始预览。单击“下一步”。
14. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。此时会发生以下情况：
    - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
    - 如果保存并计划所配置的备份，请首先保存备份规范，然后打开“调度程序”页面，在其中可以指定必须运行此保存的备份规范的日期和时间。
    - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

对于所备份的每个磁盘都启动一个磁带客户机。如果同时启动过多备份，则这样可能会降低备份性能。

仅选择特定文件进行备份

可通过使用通配符，仅备份特性文件或符合特定条件的文件。

> **注意**Data Protector NDMP 服务器集成不支持此功能。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 选择具有目标对象的备份规范。
4. 单击**备份对象摘要**选项卡。
5. 在“备份对象摘要”页中，右键单击某个备份对象，然后单击**属性**。
6. 单击**树/筛选器**选项卡，然后单击**筛选器**按钮。
7. 在“仅”文本框中，输入要用于仅备份特定文件的标准，然后单击**添加**按钮。

   如果要使用更多标准，则重复此步骤。
8. 单击**确定**。

备份时跳过文件

通过使用通配符，可以使符合特定标准的文件跳过备份。

> **注意**Data Protector NDMP 服务器集成不支持使文件跳过备份。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 选择具有目标对象的备份规范。
4. 单击**备份对象摘要**选项卡。
5. 在“备份摘要”页中，右键单击某个备份对象，然后单击**属性**。
6. 单击**树/筛选器**选项卡，然后单击**筛选器**按钮。
7. 在“跳过”文本框中，输入要用于跳过某些文件（如 *.tmp）的标准，然后单击**添加**按钮。

   如果要使用更多标准，则重复此步骤。
8. 单击**确定**。

选择用于启动备份的快捷方式的位置

可以在磁盘上创建所选备份规范的快捷方式，以后可以使用该快捷方式运行备份，而无需使用 Data Protector GUI。双击它打开命令提示符，然后针对选定备份规范运行 omnib 命令。

在 Windows 系统上仅支持用于启动备份的快捷方式。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。
3. 右键单“击所选备份规范”，然后单击**选择快捷键的位置**。此时将显示“另存为”对话框。
4. 输入名称并选择快捷键的位置，然后单击**保存**。

用于启动所选备份的快捷方式将出现在磁盘上所选位置。

使用多个磁盘代理进行备份

备份大型对象时，可使用多个磁带客户机加快备份的速度。

以下内容可能会提供其他信息：

- 在备份规范中，必须手动定义将使用新的磁带客户机备份哪些目录/文件。应小心操作以避免相同数据发生重叠。
- 如果多个磁带客户机同时访问同一磁盘，则从磁盘检索数据的性能将下降。使用磁盘阵列时，这一点可能有所不同。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型（例如**文件系统**），然后单击**添加备份**。
4. 在“创建新备份”对话框中，选择一个可用的模板，然后单击**确定**打开向导。
5. 在“源”属性页中，如果要使用磁带客户机备份目录/文件，则请勿选择位于同一逻辑磁盘或装载点上的目录/文件。但是，可以选择用一个磁带客户机备份目录/文件。单击“下一步”。
6. 在“目标”属性页中，选择将用于备份的设备。单击“下一步”。

   还可以指定是否要在备份会话期间额外创建备份的其他副本（镜像）。通过单击**添加镜像**和**删除镜像**，指定要创建的镜像数和将做此用途的设备。用于创建对象镜像的设备不得与用于备份的设备相同。ZDB 到磁盘和 NDMP 备份不支持对象镜像。
7. 在“选项”属性页中，根据需要指定其他选项，然后单击**下一步**。
8. 在“备份摘要”页中，单击**手动添加**。
9. 在“选择备份对象”对话框中，选择要备份的对象类型（例如 **Windows 文件系统**）。单击“下一步”。
10. 在“常规选择”对话框中，选择要备份的客户机系统和装载点。还必须输入说明。单击“下一步”。
11. 在“树/筛选器选择”对话框中，指定要备份或从备份中排除的目录/文件。将使用一个磁带客户机备份此处选择的内容。单击“下一步”。
12. 在“常规”、“高级”和“Windows 特有对象选项”对话框中，根据需要指定其他选项，然后单击**下一步**，并在最后一个对话框中单击**完成**。
13. 对于要使用另一个磁带客户机备份的装载点上的目录/文件重复第 9-13 步。
14. 在“备份摘要”页中，查看备份规范的摘要，然后单击**下一步**。
15. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。

管理小型重复备份

需要对大量小型对象执行重复进行的备份时，需要运行大量备份会话。在每个备份会话期间，驱动器中将加载然后卸载介质。这样的备份不仅缓慢，还会造成介质质量变差。要更节省地使用介质并节省时间，建议创建一个文件库设备，然后使用它向磁盘而非磁带执行重复进行的小规模备份。然后可以使用对象副本功能将数据从磁盘移至磁带介质。

使用这种方法后，备份将执行得更快，而介质将使用得更节省，因为在对象复制会话中对于介质只会加载和卸载一次。

要对大量小型对象执行频繁备份，请执行以下任务：

1. 配置一个文件库设备。将每个写入程序的块大小设置为第二阶段中将使用的设备的块大小。
2. 为所有小型对象创建一个备份规范。在备份的第一步中使用所创建的文件设备。
3. 执行或计划备份。
4. 使用对象副本功能将所备份的数据移至磁带。

磁盘映像备份

可以在 UNIX 和 Windows 平台上执行磁盘映像备份。

磁盘的磁盘映像备份是一种高速备份，其中 Data Protector 备份磁盘、磁盘分区或逻辑卷，但不跟踪这些数据源上存储的文件和目录结构。Data Protector 存储字符级别的磁盘映像结构。

可以对磁盘的特定部分或整个磁盘执行磁盘映像备份。

> **注意:**在 Windows 系统中，使用 VSS 写入程序执行磁盘映像备份。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。这在备份系统卷时尤其重要。默认情况下会启用磁盘映像的 VSS 备份。要自定义 VSS 磁盘映像备份，请使用以下 **omnirc** 选项：OB2_VSS_RAW_BACKUP 、 OB2_VSS_RAW_BACKUP_ALLOW_FALLBACK 和 OB2_VSS_SNAPSHOT_TIMEOUT 。

何时使用磁盘映像备份？

- 当小文件众多而又需要高速备份时。
- 为灾难恢复或在重要软件更新之前需要对磁盘进行完整备份时。在 Windows 系统中，可以在准备到 EADR 和 OBDR 时使用磁盘映像备份。
- 无法进行磁盘对磁盘的直接连接以及要将文件系统复制到另一个磁盘时。后者必须与原始磁盘相同。

如何指定磁盘映像的某个部分？

- 在 UNIX 系统中：
  - 要指定磁盘映像的某个部分，请使用以下格式： /dev/rdsk/Filename ，例如： /dev/rdsk/c2t0do
  - 要指定原始逻辑卷的某个部分，请使用以下格式： /dev/vgNumber/rlvolNumber ，例如： /dev/vg01/rlvol1
- 在 Windows 系统上：

  可以用两种方式指定磁盘映像的某个部分：第一种方式选择特定卷，第二种方式选择整个磁盘。在零宕机时间备份的情况下，请使用第二种方式：
  - \\.\DriveLetter ，例如： \\.\E:

    > **注意**当为卷名称指定了驱动器号时，卷在备份过程中不会锁定。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

  - \\.\PHYSICALDRIVE# ，其中 # 是要备份的磁盘的当前编号。例如： \\.\PHYSICALDRIVE3

从何处查找磁盘映像的某个部分？

- 在 UNIX 系统中：

  通常在 /dev/rdsk 目录中列出各个磁盘映像分区。可在 /dev/vgNumber 中找到原始逻辑卷。在 HP-UX 系统中，可在 /dev/vgNumber 中找到原始逻辑卷。原始逻辑卷的第一个字母是 r ，例如 /dev/vg01/rlvol2 。
- 在 Windows 系统上：

  可通过从控制面板中单击**管理工具**，然后依次单击**计算机管理**、**存储**、**磁盘管理**找到磁盘的当前编号（以及驱动器号）。

> **注意**在 Windows 系统中，如果重新启动系统，表示磁盘的数字可能会发生变化。

磁盘发现的客户机备份

对于执行磁盘发现的客户机备份，要指定客户机作为数据源。如果随后装载另一个磁盘，则备份中将加入该磁盘。在文件系统备份中必须指定备份规范中尚未指定的任何新加磁盘或新装载的文件系统，相比之下，如果使用磁盘发现，则不必这样做。

Data Protector 在备份时与客户机联系，并查找与该系统连接的磁盘上的所有文件系统。然后将每个检测到的文件系统（还包括 Windows 系统中的 CONFIGURATION）作为常规文件系统进行备份。此时将生成每个文件系统对象的说明，并将文件系统装载点追加到客户机备份的说明中。

使用磁盘发现进行备份时，Data Protector 仅备份真实磁盘。因此，在 UNIX 系统中，Data Protector 不发现 NFS、CD 装载的文件系统和可移动装载点。此外，在 Windows 系统中，Data Protector 也不发现 CD 和具有可移动介质的驱动器。

何时使用磁盘发现

此备份类型在配置快速变化的动态环境中尤为有用。建议在以下条件下采用：

- 如果所备份的工作站具有频繁装载或卸除的较小磁盘。
- 如果希望在不考虑装载了多少个文件系统的情况下将装载点后的数据备份到一个目录中。例如 /home/data ，其中， /home/data/disk1 和 /home/data/newdisk/disk2 可以频繁装载或卸除且彼此独立。
- 如果备份整个系统为灾难恢复做准备。

备份规范

创建将定义磁盘发现备份的备份规范时，单击客户机系统名称旁而非系统磁盘（卷）旁的复选框。选择客户机系统后，即可在“备份对象摘要”属性页中检查所配置的备份类型。在“类型”标签下，应看到“客户机系统”。

Web 服务器备份

要备份 Web 服务器，请使用标准备份过程以备份文件、目录和客户机。此外，还需要考虑以下各项：

- 执行客户机备份时，Data Protector 备份整个 Web 服务器，但不备份其他客户机/服务器上存储的数据。要备份其他客户机/服务器上的数据，还需要选择这些数据进行备份。
- 执行文件系统备份时，需要了解 Web 服务器及其各自客户机的所有文件和目录的位置。始终包括 Web 配置文件和根目录。
- Data Protector 以静态状态备份所有文件。如果备份期间文件发生更改，则不备份更改。

如果 Web 服务器上含有 Oracle 或 Informix Server 等数据库，则要使用该数据库特有的备份过程。

启用网络唤醒支持

如果 Windows 系统支持网络唤醒，则可以使用 Data Protector 网络唤醒支持。

当 Backup Session Manager 未能连接到配置为使用网络唤醒支持的客户机时，它会根据网络唤醒协议发送唤醒请求，并重试连接到该客户机。这样可以完全利用桌面系统的节能功能，否则节能功能将妨碍备份过程。

可以为配备与网络唤醒兼容的 LAN 接口 (如 NightDIRECTOR 序列) 的计算机启用网络唤醒支持。BIOS 设置中有网络唤醒 (WOL) 选项。

在 Windows 客户机上安装磁盘代理并将其添加到单元时，将自动发现客户机的 MAC 地址。也可以手动更改 MAC 地址。

要启用网络唤醒支持，请完成以下步骤:

1. 在“上下文列表”中，单击**客户机**。
2. 在范围窗格中，浏览所需的客户机，右键单击该客户机，然后单击**属性**。
3. 单击**高级**选项卡。
4. 选择启用 Magic Packet 选项。如果需要，则更改 MAC 地址。
5. 单击“应用”。

备份模板

Data Protector 备份模板可帮助您简化对（许多）备份规范和相关选项的处理。模板对于备份规范有一组明确指定的选项，可使用这些选项作为创建和修改备份规范的基础。

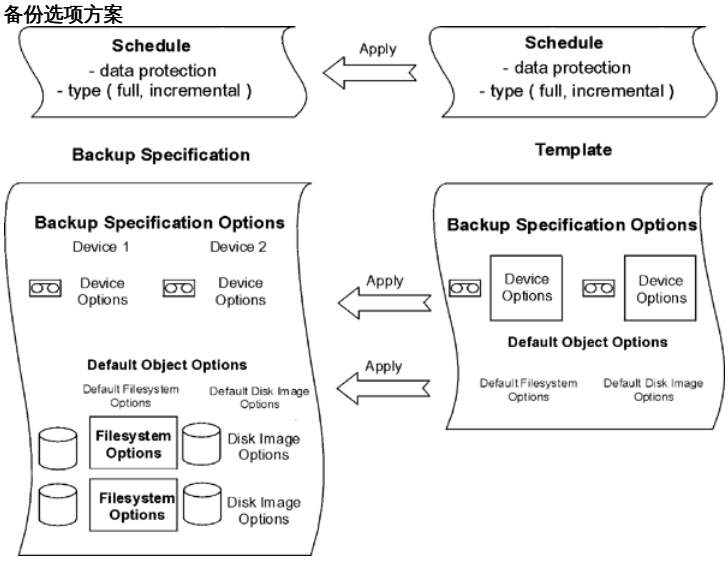
模板的用途是以用法相同的不同对象（设备选项或/和文件系统选项等特定区域的常见选项设置）配置多个备份规范。

Data Protector 为不同类型的数据（文件系统、Exchange 等等）提供默认模板，不必指定对象、设备、选项和日程。在空白备份模板（如空白文件系统备份、空白 Informix 备份等等）中，未选择任何对象或设备。备份规范选项和对象选项的默认值为 Data Protector，并且没有任何备份计划。

模板的创建和修改方式类似于备份，但备份模板中不选择对象等元素。随后可以向现有备份规范应用模板，或者可以在创建新备份时使用该模板。如果随后更改模板，则要使更改生效，必须再次应用该模板。

提示将光标移至模板上方时将显示一个弹出窗口，其中含有模板的说明。

备份选项方案



新建备份模板

可以为具有特殊需要的环境创建包含特殊设置的新备份模板。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**模板**。
3. 右键单击要创建的模板类型（例如**文件系统**），然后单击**添加模板**打开向导。
4. 按照向导操作，确定要使用的备份设备、要设置的备份选项以及计划。

创建新备份规范时或将模板应用于一个或多个备份规范时，有新模板可用。

计划备份模板

要计划备份模板，请使用以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“模板”，然后展开要计划的模板的类型 (例如，“文件系统”)。将显示所有已保存模板。
3. 右键单击要计划的模板，然后单击“编辑计划...”。计划向导随即打开。

要计划模板，请按照向导中的步骤执行操作。有关如何创建计划的详细信息，请参阅创建计划。

修改备份模板

可以修改备份模板。如果希望备份规范根据模板更改，则必须重新应用它，因为备份规范不会自动更新。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**模板**，然后展开要修改的模板类型（例如**文件系统**）。此时将显示该类型的所有已保存模板。
3. 右键单击要修改的模板，然后单击**属性**。
4. 在模板的属性页中，修改已选的模板，然后单击**应用**。

修改备份模板之后，可以将其应用于备份规范，或将其用于创建新备份规范。

复制备份模板

可通过完成以下步骤复制备份模板:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“模板”，然后展开备份模板的相应类型 (例如，“文件系统”)。此时将显示所保存的全部备份模板。
3. 在结果区域中，右键单击要复制的模板，然后单击**复制为**。此时将打开“将备份复制为”对话框。
4. 在“名称”文本框中，输入所复制的模板的名称。（可选）从“组”下拉列表中，为所复制的模板选择一个不同的组。
5. 单击**确定**。

此时将在范围窗格中和结果区域中显示所复制的备份模板。

删除备份模板

可通过完成以下步骤删除备份模板:

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开“模板”，然后展开备份模板的相应类型 (例如，“文件系统”)。此时将显示所保存的全部备份模板。
3. 右键单击要删除的模板，然后单击**删除**。确认选择。

此时即删除备份模板。

将备份模板应用于备份规范

可以将模板应用于一个或若干备份会话。在这种情况下，可以选择应该应用哪些选项组。

> **注意**如果将备份模板应用于现有的备份规范，并选择文件系统选项和/或计划选项，则模板中的保护设置将替换备份规范各个相应部分中以前的数据保护设置。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击某个保存的备份规范，然后单击**应用模板**。
4. 在“应用模板”对话框中，选择要应用于备份规范的模板。

> **注意**选择选项 **1** 可应用基本调度程序模板，选择 **2** 可应用基于 Web 的调度程序模板。默认选择为 **1**。

> **提示**可以取消选择模板中的某些选项（**树**、**备份选项**、**设备**等等），这样就不会将其应用于所选的备份规范。

> **注意**要将模板应用于集成备份规范，不应在结果区域中打开要应用的备份规范。如果首先单击备份规范将其打开，然后尝试将模板应用于此备份规范，则**应用模板**选项将不可用。

5. 单击**确定**将模板应用于备份规范。

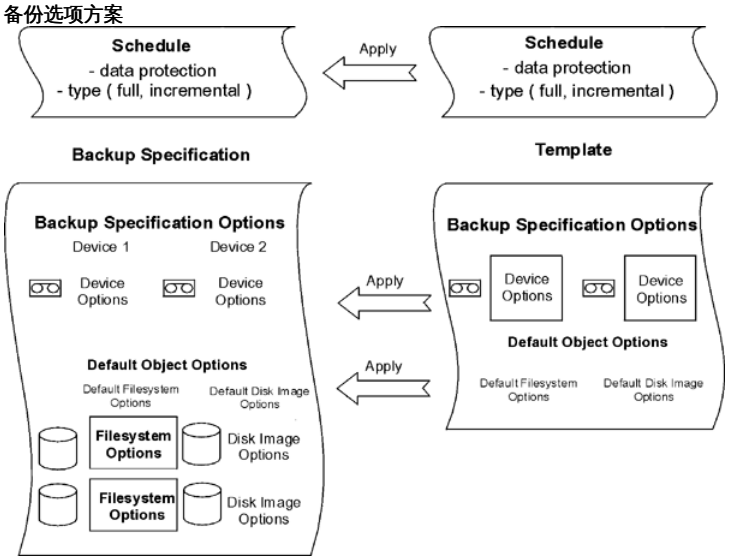
应用模板选项后，仍可修改备份规范并更改任何设置。

备份选项

Data Protector 提供一组全面的备份选项，通过这些选项可以对备份进行微调。所有这些选项都有适合大多数情况的默认值（选择或不选择）。

是否具有备份选项取决于要备份的数据类型。例如，磁盘映像备份并不具有文件系统备份所具有的所有备份选项。特定备份类型的上下文相关帮助中介绍了 Exchange、SQL 等的选项属性页中公共和特定的应用程序选项。

备份选项方案



可用的备份选项

备份数据时有下面的一组选项可用：

- 备份规范选项

  这些选项适用于整个备份规范，无论备份对象的类型是什么。

- 文件系统选项

  这些选项适用于文件系统备份的每个对象。还可以更改特定对象的选项。特定的对象设置优先于默认设置。

- 磁盘映像选项

  这些选项适用于磁盘映像备份的每个对象。还可以更改特定对象的选项。特定的对象设置优先于默认设置。

- 设备选项

  这些选项定义备份设备的行为。如果未设置设备选项，则从设备定义中读取相应的值。

- 计划选项

  对于每次单独的或定期的计划备份，都可以指定备份类型（完整或增量；对于特定集成还有某些其他备份类型）、网络负载和数据保护。对于ZDB，可以选择 ZDB 到磁盘 + 磁带或 ZDB 到磁盘（如果启用了即时恢复）。在计划向导中指定的数据保护优先于备份规范中任何其他地方的保护设置。

最常用选项

以下列出了根据特定备份策略经常要修改的选项。

- 数据保护
- 编目保护
- 日志记录
- 负载均衡
- 所有权

数据保护: 在介质上将数据保留多长时间

配置保护策略对于数据安全和成功管理环境至关重要。必须根据公司的数据保护策略指定在介质上将备份数据保留多长时间。例如，可能决定数据在三周后到期，然后可以用后续备份覆盖这些数据。

可以在不同的位置指定数据保护。此选项有不同的组合，具体取决于正在运行交互式备份、启动已保存的备份规范还是安排备份。默认值为永久。

交互式备份

配置交互式备份时，可以更改整个备份的默认数据保护。此外，还可以为各个备份对象指定不同的数据保护期。在备份对象级别上指定的保护优先于默认的保护设置。

使用已保存的备份规范进行备份

使用 GUI 启动已保存的备份时将应用数据保护，如针对交互式备份所述。

使用 CLI 启动已保存的备份时，也可以指定数据保护。这将优先于备份规范中的所有数据保护设置。

计划的备份

可以为每个单独或定期计划的备份指定不同的保护期。计划向导中指定的数据保护优先于备份规范中的所有其他数据保护设置。如果保持默认保护，则将应用数据保护，如针对交互式备份所述。

编目保护: 在 IDB 上将数据保留多长时间

可以单独设置编目保护和数据保护。当数据保护结束并且重写介质时，无论编目保护设置是什么，都将删除对象的目录。

编目保护与日志记录级别一起，对 IDB 的增大、浏览数据进行还原的方便程度以及备份性能有着重要影响。请定义适合您所在环境的编目保护策略，这一点很重要。如果将日志记录级别设置为无日志，则编目保护无效。

如果编目保护为永久，则只有在导出或删除介质时才会删除 IDB 中的信息。在这种情况下，IDB 的大小线性增长，直到数据保护期限到期为止，即使单元中的文件数没有发生变化时也是如此。

默认值为**与数据保护相同**。这意味着只要有介质可供还原，就可以浏览并选择文件或目录。

由于操作系统限制，可以设置的最后保护日期为 2038 年 1 月 18 日。

到期的编目保护

目录保护到期后，并不会立即从 IDB 中删除信息。Data Protector 每天自动删除一次这些信息。由于 IDB 中的信息是按介质排列的，因此只有在介质上所有对象的编目保护都到期时，才会删除这些信息。

当编目保护到期时，仍能进行还原，但必须手动指定文件名。

编目保护和备份

编目保护设置对备份性能没有任何影响。

编目保护和还原

编目保护到期时，会像使用无日志选项备份数据那样还原数据。

日志记录: 更改有关 IDB 中存储的数据的详细信息

Data Protector 日志记录级别决定在备份期间写入 IDB 的关于文件和目录的详细信息量。有如下四个日志记录级别：

- 全部记录
- 记录文件
- 日志目录
- 不记录任何内容

建议在同一个单元中使用不同的日志记录级别。一个单元通常由每日生成大量文件的邮件（或类似）服务器、将所有信息存储在少量文件中的数据库服务器以及一些用户工作站组成。由于这些系统的变化情况不尽相同，因此很难提供一种适合所有系统的设置。建议使用以下日志记录级别设置创建多种备份规范:

- 对于电子邮件服务器，使用日志目录选项。
- 对于数据库服务器，使用无日志选项，因为浏览各个文件对此情况无意义。
- 对于工作站，使用日志文件选项，以使您可以搜索并还原不同版本的文件。
- 通过全部记录选项，可以查看修改时间和 ACL 等文件属性。

日志记录级别和备份速度

无论所选的日志记录级别是什么，备份速度都大致一样。

日志记录级别和浏览还原

信息存储详细程度的变化会影响还原期间使用 Data ProtectorGUI 浏览文件的信息量。如果设置了**无日志**选项，则无法浏览数据；如果设置了**日志目录**选项，则可以浏览目录；如果设置了**日志文件**选项，则可以浏览完整数据，但不会显示文件属性（大小、创建日期和修改日期等）。

如果知道要还原的文件的名称，则无论生效的日志记录级别是什么，都始终可以手动指定它们而不是通过浏览来寻找它们。

日志记录级别和还原速度

以**全部记录 (Log All)**、**记录目录 (Log Directories)** 或**记录文件 (Log Files)** 日志记录级别运行的对应备份会话对还原速度的影响大致相同。

如果备份会话使用**无日志**日志记录级别运行，则还原速度可能在还原单个文件时降低。在这种情况下，Data Protector 必须从对象的开头起读取所有数据，然后再查找要还原的文件。

在进行完整系统还原的情况下，无论如何都要读取整个备份对象，因此日志记录级别的影响不大。

负载均衡：使备份设备的使用情况保持均衡

要将大量对象备份到许多可用设备，并希望 Data Protector 使所有设备始终处于繁忙状态时，可使用负载均衡选项。应使用负载均衡最大限度地降低不可用的设备对备份的影响。

要备份少量对象时、在简单设备（如 DDS）上备份对象时、要手动选择对象将备份到的设备时或要了解将在哪些介质对象上备份时，请清除负载均衡选项。

将对象分配到在负载均衡备份规范中指定的设备列表中的某个可用设备。启动第一个设备，并使用其并发定义所选择的对象数。启动下一个设备并选择对象，直到列表中再也没有对象或已运行了最大数量的设备为止。

如果某个设备变为不可用，则在失败时仅中止备份到该设备的对象。实际备份的是失败时间之前备份到设备的所有对象。如果在备份规范中指定了任何其他设备，并且尚未使用最大数量的设备，则将启动新设备。设备在遇到以下情况时可能会变为不可用：

- 在备份期间失败
- 在备份期间停止
- 正由另一个会话使用
- 完全无法启动

根据以下标准访问要备份的对象：

- 位于连接到备份设备的客户机上的对象具有更高的优先级。
- 通过选择对象，使每个客户机的磁盘代理数尽可能保持较低水平。
- 对象大小在向设备分配对象方面不起作用。

应用模板中的设备选项时应考虑以下规则：

- 如果模板中未选择负载均衡选项，则设备不与备份规范一起使用。
- 如果同时在模板和备份规范中选择了负载均衡选项，则应用设备选项。
- 如果仅在模板中选择了负载均衡选项，则只有在备份规范没有设备时才会应用设备选项。

所有权: 谁可以还原

谁是备份会话的所有者？

每个备份会话和在会话中备份的所有数据都会指定有一个所有者。所有者可以是启动交互式备份的用户、运行 CRS 进程时使用的帐户，或在备份规范选项中指定为所有者的用户。

如果用户未修改某个现有备份规范即启动它，则不会将备份会话视为交互式会话。

如果用户启动了经过修改的备份规范，则除非以下情况属实，否则该用户即为所有者：

- 用户具有切换会话所有权用户权限。
- 备份规范（其中指定用户名、组名或域名以及系统名称）中明确定义了备份会话所有者。

如果在 Lunux Cell Manager 上计划了备份，则除非以上情况属实，否则会话所有者为 root:sys 。

如果在 Windows Cell Manager 上计划了备份，则除非以上情况属实，否则会话所有者为安装期间指定的用户。

为什么更改备份所有者？

如果管理员配置并安排了备份规范，并且允许操作员运行该备份规范，但操作员无法修改或保存该备份规范，则可能要更改备份所有者。如果对所有对象都设置了私有备份选项，则操作员将无法还原任何内容，但仍可管理备份和重新启动失败的会话。

如果更改了备份配置但未保存，则将备份视为交互式备份，并且不更改所有者。如果以交互方式启动增量备份，并且您不是完整备份的所有者，则将进行另一次完整备份而非增量备份。

谁可以还原私有对象？

除非将对象标为公共，否则只有以下用户可以还原该对象:

- Admin 和 Operator 用户组的成员。
- 具有“启动还原”用户权限的备份会话所有者。可能需要其他用户权限，如“还原到另一个客户机”。
- 具有查看私有对象用户权限的用户。

也可以将查看和还原私有对象的权限授予 admin 或 operator 以外的组。

备份规范选项

这些选项适用于整个备份规范，无论备份对象的类型是什么。

基本选项为负载均衡。默认情况下，在“创建新备份”对话框中启用此选项。如果这里禁用了此选项，则以后可以在备份规范的“目标”属性页的“备份”选项卡中选择此选项。

备份规范选项的类别为：

- 常规备份规范选项
- 群集备份规范选项 (仅用于群集用途)
- P9000 XP 磁盘阵列系列备份规范选项 (仅适用于 P9000 XP 磁盘阵列系列)

常规备份规范选项

- 描述
- 在客户机上
- Post-exec
- Pre-exec
- 重新连接已断开的连接
- 所有权

群集备份规范选项

会话自动重新启动

如果在备份期间发生了群集感知 Data Protector 的故障转移，则所有正在运行和挂起的备份会话将失败。以下选项定义了 Data Protector 在故障转移之后的行为：

- 故障转移时不重新启动备份
- 重新启动所有对象的备份
- 重新启动失败对象的备份

中止会话和中止 ID 参数

当 Data Protector 之外的某些群集感知应用程序在 Data Protector 之外的节点上运行，并且故障转移到该节点 (Data Protector 正在运行) 时，可以控制此系统上的负载。以下选项与 omniclus 命令一起用于定义 Data Protector 在故障转移之后的行为。

- 不检查已用的会话时间
- 小于此时间则中止
- 大于此时间则中止
- 不检查中止 ID
- 检查中止 ID

P9000 XP 磁盘阵列系列备份规范选项

- 客户机系统

  只有在保存了备份规范之后才能修改这组选项。

  - 应用程序系统
  - 备份系统
- 镜像类型
  - Business Copy P9000 XP
  - Continuous Access P9000 XP
  - 组合 (Continuous Access P9000 XP + Business Copy P9000 XP)
  - MU 编号
- 复本管理选项

  - 在备份完成之后保留复本
  - 跟踪即时恢复的复本
- 在会话开始时
  - 如果尚未同步，则同步磁盘
  - 如果镜像磁盘尚未同步，则中止会话
- 在会话结束时
  - 为备份 (重新同步) 准备下一镜像磁盘
- 应用程序系统选项
  - 卸载应用程序系统上的文件系统
  - 使应用程序命令行停止/静默
  - 重新启动应用程序命令行
- 备份系统选项
  - 使用与应用程序系统上相同的装载点
  - 备份系统上安装路径的根目录
  - 将目录添加到装载路径
  - 在目标装载点自动卸除文件系统
  - 让备份系统处于启用状态
  - 以读取/写入模式启用备份系统

文件系统选项

这些选项适用于文件系统备份的每个对象。

基本选项为保护。

有多组**高级**文件系统选项：

- 文件系统选项
- 其他文件系统选项
- WinFS 文件系统选项

文件系统选项

- 编目保护
- Post-exec
- Pre-exec
- 公共
- 报告级别

其他文件系统选项

- 备份文件的大小
- 将 POSIX 硬链接作为文件进行备份

数据安全性

- 将完整 DR 映像复制到磁盘
  - 无
  - AES 256 位
  - 编码
- 显示统计信息
- 不保留访问时间属性
- 增强型增量备份
- 使用本机文件系统更改日志提供程序(如果有)
- 在备份期间锁定文件
- 日志记录

  Data Protector 日志记录级别定义了在备份期间写入内部数据库的关于备份文件和目录的详细信息量。有如下四个日志记录级别：
  - 全部记录
  - 记录文件
  - 日志目录
  - 不记录任何内容
- 软件压缩

WinFS 文件系统选项

- 异步读取(A)
- 对卷备份进行重复数据删除
- 备份目录的共享信息
- 检测 NTFS 硬链接
- 不使用归档属性
- **打开文件**
  - 重试次数
  - 超时
- 将打开的锁定文件报告为
- **MS Volume Shadow Copy 选项**
  - 使用卷影复制
  - 允许回退

磁盘映像选项

这些选项适用于选择进行备份的所有磁盘映像对象。

基本选项为保护。

可以设置以下**高级**磁盘映像选项：

- 编目保护
- **数据安全性**
  - 无
  - AES 256 位
  - 编码
- 显示统计信息
- Post-exec
- Pre-exec
- 公共
- 报告级别
- 软件压缩

设备选项

对特定备份规范中当前所选的备份设备可以设置这些选项。这些选项是在配置备份设备或更改其属性时所设置的一部分选项。所列选项对某个特定备份规范有效。这些选项优先于在“设备和介质”上下文中设置的选项（这些选项一般适用于各自的设备）。

设备属性 - 常规

- CRC 检查
- 并发
- 基于驱动器的加密
- 介质池
- prealloc 列表
- 重新扫描

计划选项

安排备份时，可以设置其他选项。对于每次计划备份，都可以指定备份类型（完整或增量；特定集成还有某些其他备份类型）、数据保护、优先级、网络负载、重复模式和估计持续时间。对于ZDB，可以选择 ZDB 到磁盘 + 磁带或 ZDB 到磁盘（如果启用了即时恢复）。

在计划程序中指定的数据保护优先于备份规范中任何其他地方的保护设置。

会话选项

- 备份类型
  - 完整
  - 增量
- 备份保护
- 网络负载
- 重复模式
- 估计持续时间

分割镜像/快照备份

- 分割镜像/快照备份

（此选项在 ZDB 提供，但仅限“ZDB 到磁盘 + 磁带”或“ ZDB 到磁盘”的情况下（启用了即时恢复））。

设置备份选项

创建新的备份规范时，可以设置备份选项。在这种情况下，遵循向导进入“选项”属性页。

还可以为已配置和保存的备份规范设置备份选项。

> **注意**可以在两个级别设置对象选项（文件系统和磁盘映像选项）。首先，可以为所有文件系统和为备份规范中的所有磁盘映像对象单独设置*默认对象选项*。然后，可以为*特定对象*设置这些选项。这些设置将优先于默认值。例如，要压缩除 CPU 较慢的某个客户机以外所有客户机中的数据，请在设置文件系统选项时启用**压缩**选项。然后，选择该慢速客户机，并对此客户机清除**压缩**选项。

执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**选项**选项卡。
4. 在“选项”页中，根据需要设置选项。单击某个**高级**按钮以设置高级选项（按照要设置的选项的类型）。

   除了备份规范选项外，还可以设置例如文件系统选项、磁盘映像选项等等，具体取决于配置其备份规范的数据类型。
5. 查找所需的选项，然后选择或取消选择该选项，或输入所需的信息。
6. 单击**确定**，然后单击**应用**以保存更改。

指定数据保护

运行交互式备份、启动保存的备份规范或排定备份时，可以指定数据保护。默认值为永久。

> **注意**由于操作系统限制，可以设置的最后保护日期为 2038 年 1 月 18 日。

指定备份规范级别的数据保护

创建新的备份规范时，或修改现有的备份规范时，可以指定数据保护。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**选项**选项卡。
4. 如果要备份文件系统，则在“文件系统选项”下指定保护选项。对于集成，单击“公共应用程序选项”下的**高级**，并在“选项”选项卡中指定**保护**选项。
5. 单击**确定**，然后单击**应用**以保存更改。

指定单独备份对象的数据保护

对文件系统和磁盘映像对象可以指定不同的保护期。

创建新的备份规范时，或修改现有的备份规范时，可以指定单独对象的数据保护。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**备份对象摘要**选项卡。
4. 右键单击对象，然后单击**属性**。
5. 单击“选项”选项卡并指定保护选项。
6. 单击**确定**，然后单击**应用**以保存更改。

指定计划备份的数据保护

可以为每个单独或定期计划的备份指定不同的保护期。计划向导中指定的数据保护优先于备份规范中的所有其他数据保护设置。

计划备份时，可以指定计划备份的数据保护。

使用 CLI 指定数据保护

使用 CLI 运行备份时，也可以指定数据保护。这将优先于备份规范中的所有数据保护设置。

1. 请输入以下命令：

   omnib -datalist Name -protect ProtectionPeriod

   其中， Name 是备份规范的名称。

   例如，要运行受到两周保护的备份，请输入：

   omnib -datalist MyBackup -protect weeks 2

   有关详细信息，请参阅 omnib 手册页或《Data Protector 命令行界面参考》。

更改特定对象的选项

可以将选项应用于特定对象，或手动更改默认选项。

可以在创建新备份规范的同时应用这些选项。在这种情况下，遵循向导进入“备份对象摘要”页。

还可以为已配置和保存的备份规范应用选项。

执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要为其应用特定对象的选项的备份规范，然后单击**备份对象摘要**选项卡。
4. 在“备份对象摘要”页中，可以更改对象属性、对象顺序或镜像选项。

   更改对象属性：

   1. 右键单击对象，然后单击**属性**。
   2. 在“对象属性”对话框中，更改特定对象的选项。根据所选的对象，显示以下某些选项卡：“常规”、“选项”、“其他”、“树/过滤器”、“WinFS 选项”、“选项”和“数据库”。单击相应的选项卡修改选项。
   3. 单击**确定 (OK)** 应用更改。

   要更改对象的顺序：

   1. 右键单击某个对象，然后单击**上移**或**下移**。重复该过程，直到获得所需的顺序为止。
   2. 单击“应用”。

   更改镜像选项：

   1. 选择某个对象，然后单击**更改镜像**。
   2. 要更改镜像的设备，请确保选择镜像，突出显示该镜像，并从**设备**下拉列表中选择一个设备。还可以取消选择所选备份对象的镜像。

更改备份设备选项

在创建新的备份规范的同时，可以设置备份设备选项和这些设备的顺序。在这种情况下，遵循向导进入“目标”属性页。

还可以为已配置和保存的备份规范设置备份设备选项。

执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要更改其设备选项的备份规范，然后单击**目标**选项卡。
4. 在“目标”属性页中，可以更改设备选项。
   - 要更改经过负载均衡的备份的设备，请取消选择设备，然后选择其他设备。
   - 要更改已经过负载均衡的备份的设备，请取消选择设备，然后选择其他设备。
   - 要更改未经过负载均衡的备份的设备，请选择要使用的所有设备。然后单击**备份对象摘要**选项卡，选择所需的对象，然后单击**更改设备**。
   - 要更改镜像对象的设备，请选择要用于特定镜像的所有设备。然后单击**备份对象摘要**选项卡，选择所需的对象，然后单击**更改镜像**。
   - 要更改设备的顺序（如果备份经过负载均衡），请右键单击任何所选设备，然后单击**将设备排序**。
   - 要设置其他设备属性，请右键单击任何所选设备，然后单击**属性**。
5. 指定所需的选项，然后单击**确定**。
6. 单击“应用”。

设置计划备份选项

安排备份时，可以设置其他选项。这些选项仅对所计划的备份有效，而对以交互方式启动的备份无效。在计划向导中指定的数据保护优先于备份规范中任何其他地方的保护设置。

为所计划的备份创建新备份规范时，可以设置计划备份选项。在备份向导中选择**保存并计划**选项，以计划备份。

在安排已配置和保存的备份规范中的备份时，也可以设置计划备份选项。有关如何在 Data Protector 中创建和编辑计划的详细信息，请参阅调度程序。

Exec 命令

pre-exec 和 post-exec 命令用于在备份或还原之前和/或之后执行额外的操作。此类操作包括检查要备份的文件数、停止某些事务处理或在备份之前关闭应用程序，随后将其重新启动。Data Protector 不提供 pre-exec 和 post-exec 命令。必须自行编写脚本以执行所需的操作。这些脚本在 Windows 系统中可编写为可执行文件或批处理文件，在 UNIX 系统中可编写为 shell 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

Client System 类型 (主机备份) 的备份对象有一种特殊行为。即使仅指定 pre-exec 和 post-exec 命令一次，对于每个文件系统（或逻辑驱动器）也会启动每种命令一次。

可以在如下两个级别上配置 pre-exec 和 post-exec 命令：

- 备份规范

  备份会话启动之前将执行 pre-exec 命令。备份会话停止后将执行 post-exec 命令。指定这些命令作为整个备份规的备份选项。默认情况下，在 Cell Manager 上执行备份会话的 pre-exec 和 post-exec 命令，但可以选择另一个系统。

- 备份对象

  备份对象之前启动备份对象的 pre-exec 命令。备份对象之后执行备份对象的 post-exec 命令。将这些命令指定为对象的备份选项。在正运行备份对象的磁带客户机的系统上执行对象的 pre-exec 和 post-exec 命令。

运行 pre-exec 和 post-exec 命令

完成以下步骤：

1. 整个备份规范的 pre-exec 命令启动并执行完毕。
2. 对于备份规范中的每个对象：
   1. pre-exec 命令启动并执行完毕。
   2. 备份对象。
   3. （备份规范中每个对象的）post-exec 命令启动并执行完毕。
3. 整个备份规范的 post-exec 命令启动并执行完毕。

用于备份规范的 Exec 命令

pre-exec 和 post-exec 命令 在 Windows 系统中可编写为可执行文件或批处理文件；在 UNIX 系统中可编写为 shell 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

pre-exec 和 post-exec 特征

- 命令的启动和位置以确保安全性
- 环境变量
- SMEXIT 值
- pre-exec 和 post-exec 命令的注意事项

命令的启动和位置以确保安全性

分别在备份会话前后启动备份会话的 pre-exec 和 post-exec 命令。默认情况下在 Cell Manager 上执行这些命令，但可以选择其他系统。

- Windows 系统

  在 Cell Manager 上执行时，pre-exec 和 post-exec 脚本均由Data Protector CRS 启动；而当远程执行时，在 Data Protector Inet 服务帐户 (默认情况下为本地系统帐户) 下执行。

  Cell Manager 及其他系统上的脚本必须位于 Data_Protector_ home\bin 目录中，用户必须仅指定文件名或相对路径名。

  对于 pre-exec 和 post-exec 命令，仅支持 .bat 、 .exe 和 .cmd 扩展名。要运行扩展名不受支持的（例如 .vbs ）脚本，请创建用于启动该脚本的批处理文件。然后配置 Data Protector，将批处理文件作为 pre-exec 或 post-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

  如果使用引号 ("") 指定路径名，请勿使用反斜杠和引号的组合 (\\")。如果需要在路径名末尾使用尾随的反斜杠，则要使用双反斜杠 (\\)。

> 注意禁止直接使用 perl.exe。

- UNIX 系统

  Pre-exec 和 post-exec 脚本由备份会话所有者启动，除非备份会话所有者具有 Backup as root 权限；那么，将以 root 启动这些命令。

  在 Cell Manager 或远程 UNIX 客户机上，备份规范的 exec 命令必须位于如下位置：

  HP-UX、Solaris 和 Linux 系统： /opt/omni/lbin

  其他 UNIX 系统： /usr/omni/bin

  对于位于 /opt/omni/lbin 或 /usr/omni/bin 目录中的命令，可仅指定文件名，否则要指定完整的路径名。

环境变量

以下环境变量由 Data Protector 设置，并且只能在 Cell Manager 上备份规范的 pre-exec 和 post-exec 脚本中使用，如果在任何其他系统上执行命令，则不能使用这些环境变量。

有关环境变量的详细信息，请参阅《Data Protector 帮助》。

- DATALIST
- MODE
- OWNER
- PREVIEW
- RESTARTED
- SESSIONID
- SESSIONKEY
- SMEXIT

SMEXIT 值

值	描述
0	成功备份了所有文件。
10	成功完成了所有代理，但并未备份所有文件。
11	一个或多个代理失败，或有数据库错误。
12	无任何代理完成了操作；Data Protector 中止了会话。
13	用户中止了会话。

pre-exec 和 post-exec 命令的注意事项

- 在 Windows 系统上，必须指定完整的文件名，包括扩展名 (例如 .exe 或 .bat)。
- 指定脚本名称时，如果因路径中有空格而需要使用单引号（UNIX 系统中）或双引号（Windows 系统中），则永远不要使用两者的组合。或者使用单引号，或者使用双引号。例如，"S'ilvousplat.bat" 错误，而允许使用 S'ilvousplat.bat。
- 成功完成后，pre-exec 或 post-exec 命令的退出值必须为零。
- 如果 pre-exec 命令失败 (返回的值小于 0)，则备份会话的状态会设置为 Failed，并且会中止会话。不再执行 post-exec 命令。
- 如果 post-exec 命令失败 (返回的值小于 0)，则备份会话的状态会设置为 Completed with errors。
- 如果 post-exec 命令返回的值小于 0 并且 omnib 命令返回 11，则备份状态会设置为 Completed with failures。
- 除非中止会话并且未执行或未设置 pre-exec 命令，否则始终执行 post-exec 命令。如果设置了 OB2FORCEPOSTEXEC omnirc 选项，则会始终执行 post-exec 命令。
- 默认情况下，在预览备份期间不执行 pre-exec 和 post-exec 命令。此行为由全局选项文件中的 ExecScriptOnPreview 选项定义。
- 处理 pre-exec 和 post-exec 命令的方式与处理命令提示符下输入的命令相同。但是，不允许使用特殊字符 ?、*、"、|、< 和 >。
- pre-exec 和 post-exec 命令的执行是使用管道机制实现的。pre-exec 或 post-exec 函数中启动的所有过程都必须结束，然后处理才能继续。
- 运行 pre-exec 或 post-exec 命令时，无法中止备份会话。
- pre-exec 和 post-exec 命令运行于后台模式。因此，不要使用任何需要用户交互的命令。
- 提供超时。默认情况下，pre-exec 和 post-exec 脚本必须至少每隔 15 分钟发送一些输出，否则将中止脚本。可通过修改 ScriptOutputTimeout 全局选项更改此时间间隔。
- pre-exec 和 post-exec 命令的任何输出都写入 IDB，并显示在 Data Protector GUI 中。
- 在某些情况下，由 pre-exec 或 post-exec 脚本在后台运行的进程可能会造成不便。要避免出现此类情况，可以按照以下方法之一使用分离功能:
  - **utilns/detach -com 脚本**: 当脚本退出时停止捕获输出，并且不等待已由脚本在后台启动的进程。
  - **detach 脚本**: 在后台启动此脚本，并且不等待输出或脚本退出。
- 可通过将 SmDisableScript 全局选项设置为 1，在 Cell Manager 上禁止执行会话 pre-exec 和 post-exec 命令。

- 可通过在 omnirc 文件中添加行 OB2REXECOFF=1，在所有客户机上禁止执行远程会话 pre-exec 和 post-exec 命令。
- 通过指定允许哪些 Cell Manager 访问客户机，可以保护客户机。只有受到允许的 Cell Manager 能够在客户机上执行 pre-exec 和 post-exec 命令。
- 在 UNIX 系统上，由命令写入 stdout 的文本将发送到会话管理器，并写入数据库。 stderr 将重定向到 /dev/null 。可将其重定向到 stdout ，以获取记录到数据库的错误消息。

指定备份规范的 pre-exec 和 post-exec 命令

要指定所保存的备份规范的 pre-exec 和 post-exec 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要为其指定 pre-exec 和 post-exec 命令的备份规范，然后单击**选项**选项卡。
4. 在“备份规范选项”下，单击**高级**。
5. 在“备份选项”对话框的“常规”选项卡中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
6. 单击**确定**，然后单击**应用**以保存更改。

用于特定备份对象的 Exec 命令

pre-exec 和 post-exec 命令在 Windows 系统中可编写为可执行文件或批处理文件；在 UNIX 系统中可编写为 shell 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

命令的启动和位置

分别在备份对象前后执行对象的 pre-exec 和 post-exec 命令。可以为备份规范中的所有对象或逐个为每个对象指定这些命令。备份集成（例如 Oracle）时，将数据库视为一个对象，因此在数据库备份前后执行这些命令。在运行磁盘代理的系统上执行这些命令。

Windows 系统：	以 Data Protector Inet Service 帐户（默认情况下为本地系统帐户）启动备份对象的 pre-exec 和 post-exec 脚本。 备份对象的 exec 脚本可位于运行 Disk Agent 的系统上的任何目录中。但是，对于客户机备份，它们必须位于 Data_Protector_home\bin 中。如果脚本位于 Data_Protector_home\bin 中，则仅指定文件名，否则必须指定完整路径名。 对于 pre-exec 和 post-exec 命令，仅支持 .bat 、 .exe 和 .cmd 扩展名。要运行扩展名不受支持的（例如 .vbs ）脚本，请创建用于启动该脚本的批处理文件。然后配置 Data Protector，将批处理文件作为 pre-exec 或 post-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。 如果使用引号 ("") 指定路径名，请勿使用反斜杠和引号的组合 (\\")。如果需要在路径名末尾使用尾随的反斜杠，则要使用双反斜杠 (\\)。
UNIX 系统：	Pre-exec 和 post-exec 脚本由备份会话所有者启动，除非备份会话所有者具有 Backup as root 权限；否则将以 root 身份启动这些命令。 备份对象的 exec 命令可位于运行磁盘代理的系统上的任何目录中。但是，对于客户机备份，这些命令必须位于默认的 Data Protector 管理命令目录中。如果这些命令位于默认的管理命令目录中，则仅需指定文件名，否则必须指定完整的路径名。

环境变量

对于 post-exec 命令，Data Protector 会设置 BDACC 环境变量。

pre-exec 和 post-exec 命令的注意事项

- 如果执行客户机系统（主机）备份，则在特定系统的第一次文件系统备份之前启动 pre-exec 脚本，同时在备份之后启动 post-exec 脚本。在这种情况下，无法导出 BDACC ，因为该变量与单个文件系统对象而非整个客户机系统 (主机) 相关。
- 在 Windows 系统上，必须指定完整的文件名，包括扩展名 (例如 .exe 或 .bat)。
- 指定脚本名称时，如果因路径中有空格而需要使用单引号（UNIX 系统中）或双引号（Windows 系统中），则永远不要使用两者的组合。或者使用单引号，或者使用双引号。例如，"S'ilvousplat.bat" 错误，而允许使用 S'ilvousplat.bat。
- 成功完成后，pre-exec 或 post-exec 命令的退出值必须为零。
- 如果 pre-exec 命令失败（返回非零值），则中止此对象的备份。对象的状态会设置为 Aborted ，并且磁盘代理停止处理，但会执行 post-exec 命令 (除非 post-exec 命令与 BDACC 环境变量相关)。不存在任何对象的备份。
- 如果 post-exec 命令失败 (返回非零值)，则对象的状态会设置为 Aborted 。存在对象的备份，并且可以还原数据。
- 如果客户机上没有可执行脚本或如果脚本的路径错误，则 Data Protector 显示脚本失败和会话中止的错误消息。
- 默认情况下，在预览备份期间不执行 pre-exec 和 post-exec 命令。该行为由 ExecScriptOnPreview 全局选项定义。

- 处理 pre-exec 和 post-exec 命令的方式与处理命令提示符下输入的命令相同。但是，不允许使用特殊字符 ?、*、"、|、< 和 >。
- 运行 pre-exec 或 post-exec 命令时，无法中止备份会话。
- pre-exec 和 post-exec 进程运行于后台模式。因此，不要在 pre-exec 和 post-exec 命令中使用需要用户交互的命令。
- 提供超时。默认情况下，pre-exec 和 post-exec 脚本必须至少每隔 15 分钟发送一些输出，否则将中止脚本。可通过修改 ScriptOutputTimeout 全局选项更改此时间间隔。
- pre-exec 和 post-exec 命令的任何输出都写入 IDB，并显示在 Data Protector 图形用户界面中。
- 在某些情况下，由 pre-exec 或 post-exec 脚本在后台运行的进程可能会造成不便。要避免出现此类情况，可以按照以下方法之一使用分离功能:
  - **utilns/detach -com 脚本**: 当脚本退出时停止捕获输出，并且不等待已由脚本在后台启动的进程。
  - **detach 脚本**: 在后台启动此脚本，并且不等待输出或脚本退出。
- 默认情况下，pre-exec 和 post-exec 命令应至少每隔 120 分钟向磁盘代理发送一次输出，否则将中止对象的备份。可通过修改 SmDaIdleTimeout 全局选项更改此时间间隔。
- 在 UNIX 系统上，由命令写入 stdout 的文本将发送到会话管理器，并写入数据库。 stderr 将重定向到 /dev/null 。可将其重定向到 stdout ，以获取记录到数据库的错误消息。

安全注意事项

pre-exec 和 post-exec 命令可能有危险，因为如果未经授权的人员使用这些命令，可能会产生大量攻击。如果不使用这些命令，建议将其禁用。此外，如果要使用 pre-exec 和 post-exec 脚本，请将其放在安全位置，以防未经授权的人员修改这些脚本。

将 StrictSecurityFlag 全局选项设置为 0x0100 后，仅限具有“作为 root 备份”或“作为 root 还原”权限的用户运行 pre-exec/post-exec 命令。

可通过在特定客户机上的 omnirc 文件中添加行 OB2OEXECOFF=1 ，对任何备份对象禁用 pre-exec 和 post-exec 脚本。要在任何客户机上禁止执行远程会话 pre-exec 和 post-exec 命令，请向特定客户机上的 omnirc 文件中添加 OB2REXECOFF=1 。

通过指定允许哪些 Cell Manager 访问客户机，可以保护客户机。只有受到允许的 Cell Manager 能够在客户机上执行 pre-exec 和 post-exec 命令。

指定所有对象的 pre-exec 和 post-exec 命令

要指定所保存的备份规范中所有对象的 pre-exec 和 post-exec 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要为其指定 pre-exec 和 post-exec 命令的备份规范，然后单击**选项**选项卡。
4. 在“文件系统选项”（磁盘映像备份的已保存备份规范中的“Disk Image 选项”）下，单击**高级**。
5. 在“文件系统选项”（磁盘映像备份的“Disk Image 选项”）对话框的“选项”选项卡中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
6. 单击**确定**，然后单击**应用**以保存更改。

指定单独对象的 pre-exec 和 post-exec 命令

要仅指定所保存的备份规范中单独对象的 pre-exec 和 post-exec 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 双击要为其指定 pre-exec 和 post-exec 命令的备份规范，然后单击**备份对象摘要**选项卡。
4. 右键单击对象，然后单击**属性**。
5. 在“对象属性”对话框中，单击**选项**选项卡。
6. 在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
7. 单击**确定**，然后单击**应用**以保存更改。

指定集成的 pre-exec 和 post-exec 命令

备份集成（例如 Oracle）时，将数据库视为一个对象，因此在数据库备份前后执行这些命令。这些命令在应用程序客户机上执行。

要指定所保存的备份规范中集合的 pre-exec 和 post-exec 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如 **Oracle Server**）。此时将显示所保存的全部备份规范。
3. 双击要为其指定 pre-exec 和 post-exec 命令的备份规范，然后单击**选项**选项卡。
4. 在“应用程序特有选项”下，单击**高级**。
5. 在“应用程序特有选项”对话框中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
6. 单击**确定**，然后单击**应用**以保存更改。

备份计划

可以配置无人看管备份，具体方法是排定备份会话使其在特定的时间执行。计划可按照每天、每周或每月的间隔进行设置。此外，您也可以指定计划选项，如网络负载和数据保护。

运行连续备份

一个备份完成之后可以启动另一个备份。例如，文件系统备份完成之后可以启动 Oracle 数据库的备份。

在第一个备份规范中使用 post-exec 命令启动连续备份。

完成以下步骤：

1. 计划第一个备份。
2. 单击**选项**选项卡，然后在**备份规范选项**下单击**高级**。
3. 在 Post-exec 文本框中，输入含有要在完成第一个备份后启动的备份规范名称的 omnib 命令 (例如 omnib -datalist name_of_the_backup_specification)，然后单击“确定”。

> **提示**还可以自行指定检查第一个备份的状态的脚本。

备份规范组

通过 Data Protector 可以将备份规范划分为不同的组。例如，如果管理大量备份规范，并且希望按常见特征将其分组，这一点会很有用。

将备份规范划分为有意义的组可便于查找和维护单独的备份规范。这样还可以将模板中的公共选项设置应用于整个组。例如，如果要将设备列表更改为组中的所有备份规范，则可以有选择地应用模板的设备设置。

提示可以将模板中的公共选项设置（例如用于设备的）应用于一组备份规范。选择组中的所有备份规范（单击组名，然后按 Ctrl+A），右键单击目标组，然后单击**应用模板**。

注意Data Protector GUI 所能显示的备份规范数有限。可显示的备份规范数量取决于备份规范的参数大小 (名称、组、所有权信息以及备份规范是否为负载均衡的信息)。此大小不应超过 80 KB。

大型企业的备份规范可能会以如下方式组织：

User_files	此组包含对 10 个部门中每个部门的所有用户每周执行一次完整备份的备份规范。
SERVERS_DR	此组包含供公司服务器为灾难恢复做准备的备份规范。每次安装新服务器时，都会创建新的备份规范，并将其添加到此组。
END_USER_ARCHIVE	此组用于保存按最终用户请求生成的备份规范。例如，要释放磁盘空间的最终用户必须首先将其硬盘存档。

查看备份规范组

Data Protector 帮助中的过程假定您使用默认的备份视图（按类型）。可以更改视图，以便查看按组排列的备份规范。执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，选择**分组依据**。

创建备份规范组

可以使用各种标准创建不同的备份规范组。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”下显示可用备份组的列表。
3. 右键单击**备份规范**项，然后单击**添加组**。此时将出现“添加新组”对话框。
4. 在“名称”文本框中，输入新组的名称，然后单击**确定**。

此时新备份规范组将显示在“备份规范”项下。现在可以将备份规范添加到相应的组中。

将备份规范保存到组中

可通过完成以下步骤将新的备份规范保存到特定组中:

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”下显示可用备份组的列表。

3. 展开**备份规范**，右键单击要向其添加备份规范的组，然后单击**添加备份**以打开备份向导。
4. 遵循向导创建新的备份规范。在向导的最后一页（“保存”、“启动”或“预览”页）中，单击**另存为**。此时将显示“将备份另存为”对话框。
5. 在“名称”文本框中，输入备份规范的名称。
6. 在“组”下拉列表中，选择要向其保存备份规范的组，然后单击**确定**以保存规范，然后退出向导。默认情况下，显示的备份组是被右键单击以启动向导的那个备份组。

此时将在所选组下显示保存的备份规范。

在各个组之间移动备份规范或模板

可以将备份规范或模板从一个备份组移至另一个备份组。执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”和“模板”下显示可用备份组的列表。
3. 展开**备份规范**或**模板**以及具有要移动的备份规范或模板的组。
4. 右键单击要移动的备份规范或模板，然后单击**更改组**。此时将显示“更改组”对话框。

   如果显示备份规范属性，则禁用**更改组**选项。
5. 在“名称”下拉列表中，选择要将备份规范或模板移至的组，然后单击**确定**。

此时备份规范或模板将显示在其新组下。

删除备份规范组

可以删除不再需要的备份规范组。完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。
3. 展开**备份规范**项和**模板**项。此时将显示可用备份组的列表。
4. 展开要删除的组。

> **重要说明**无法删除包含备份规范和模板的组。必须首先从组中删除或移动备份规范和模板。

5. 右键单击目标组，然后单击**删除组**。

   此时已删除目标备份规范组。

Windows 系统备份

备份过程与标准备份过程相同，但有一些方面是 Windows 所特有的。

要运行 VSS 文件系统备份，系统中必须至少有一个 NTFS 文件系统。

备份什么？

磁盘驱动器上的文件系统备份涉及读取目录结构，所选磁盘驱动器上的文件内容，以及有关文件和目录的 Windows 特定信息

- 压缩文件以压缩格式备份和还原
- 加密文件以加密格式备份和还原
- 使用复原文件系统 (ReFS) 格式化的卷上的数据
- 完整 Unicode 文件名
- FAT16、FAT32、VFAT 和 NTFS 属性

  备份文件后，即清除其存档属性。通过设置备份规范的高级文件系统备份选项中的不使用归档属性选项，可以更改此行为。
- NTFS 备用数据流
- NTFS 安全数据
- 目录共享信息

  如果通过网络共享目录，则默认情况下将备份共享信息。还原期间，默认情况下将还原共享信息，还原后将在网络上共享该目录。可通过清除备份目录的共享信息选项更改此行为。

不备份什么？

在备份规范中，可以指定备份要排除或跳过的文件的列表（专用排除列表）。除了专用排除列表以外，默认情况下 Data Protector 将排除以下内容：

- Windows 客户机或 Cell Manager 备份中的默认 Data Protector 日志文件目录。
- Windows 客户机或 Cell Manager 备份中的默认 Data Protector 临时文件目录。
- Windows Cell Manager 备份中的内部数据库目录。
- 注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup 中指定的文件。

例如，即使您在备份规范中选择了内部数据库目录，系统也会从 Cell Manager 备份中排除该目录。这是因为必须以一种特殊的方式备份 IDB 才能确保数据一致性。

所有 Data Protector 主机都将证书和私钥文件保留在以下位置：

- <programdata>/Omniback/Config/sscertificates（在 Windows 中）
- /etc/opt/omni/config/sscertificates/（在 Linux 中）

在文件系统备份期间，如果这些文件包含在上述位置中，则会备份除私钥以外的其他所有文件。

NTFS 3.1 文件系统功能

- NTFS 3.1 文件系统支持重分析点

  卷装入点、单实例存储 (SIS) 和目录联接都基于重解析点这个概念。这些重解析点被选择为任何其他文件系统对象。
- NTFS 3.1 文件系统支持符号链接。

  Data Protector 以处理 NTFS 重分析点的方式处理符号链接。
- NTFS 3.1 文件系统支持稀疏文件，这是减少磁盘空间分配量的一种高效方式。

  以稀疏方式备份这些文件可节省磁带空间。备份稀疏文件后，只能向 NTFS 3.1 文件系统以稀疏方式还原这些文件。
- 某些 NTFS 3.1 特有的功能由保留自身数据记录的系统服务控制。将这些数据结构作为 CONFIGURATION 的一部分进行备份。
- NTFS 3.1 文件系统支持与其他备用数据流一起由 Data Protector 备份的对象 ID。
- 加密的文件

  对于由 Microsoft 加密的 NTFS 3.1 文件均采用加密方式进行备份和还原，但只有在将这些文件解密后才能正确查看其内容。

重分析点

重解析点是附加了一种唯一标记（称为重分析点 ID）的普通文件系统对象。NTFS 3.1 目录或文件可以包含重分析点，此点通常通过定向到另一位置中的数据来模仿内容。

默认情况下，Data Protector 在遇到重分析点时，不遵循重分析点 ID。这也称为备份原始重分析点。这种情况影响配置备份的方式：

- 如果使用磁盘传递配置备份，则将对所有数据备份一次。
- 如果备份包含重分析点的文件系统或驱动器，则必须确保对重分析点所指的数据进行了备份。例如，不遵循 Windows 目录连接重分析点，因此必须单独备份联接。但 SIS 重分析点例外。

  单实例存储 (SIS) 服务定期检查磁盘上的文件。如果服务检测到多个相同的文件，则会将这些文件替换为重分析点，并将数据存储在常用的存储库中，从而减少磁盘空间的使用。

通过重分析点，可以按逻辑卷的形式装载磁盘驱动器。Data Protector 将装载的卷视为普通驱动器，因此这些卷可见，并作为可选择进行备份的对象。

稀疏文件

稀疏文件包含许多组零数据 - 例如，远远多于压缩文件。在备份时，Data Protector 自动跳过零的部分，以便仅为非零部分分配备份设备上的介质空间。

UNIX 和 Windows 稀疏文件不兼容。

备份系统磁盘时发出警告

系统磁盘上的某些文件始终繁忙，因此任何应用程序（包括磁盘代理）都无法将其打开。这些文件的内容只能作为 CONFIGURATION 的一部分进行备份。

文件系统备份访问这些文件时（如备份整个系统磁盘时），Data Protector 未能打开这些文件，并报告警告或错误。

虽然从文件系统备份的角度看此行为正确，但它会产生可管理性问题。由于始终报告大量警告，因此可能遗漏了另一个文件的失败。

从文件系统备份中排除通过 CONFIGURATION 备份进行备份的文件可避免出现警告。

> **注意**备份不活动的系统磁盘（例如在双引导情况下）时，以前列出的文件不是当前活动 CONFIGURATION 的一部分。可以在文件系统备份中备份这些文件，因此不应排除这些文件。

配置备份

对于 Windows 操作系统维护的特殊数据结构，不将其视为文件系统备份的一部分。通过 Data Protector，可以备份一种特殊的数据结构，称为 CONFIGURATION。

要执行配置备份，请在创建文件系统备份规范时，选择对象 CONFIGURATION 或只选择其某些部分。如果在备份向导中选择 CONFIGURATION，则始终备份事件日志、配置文件和用户磁盘配额。

CONFIGURATION 备份是使用 Microsoft 卷影复制服务执行的。

以下限制适用：

- 一次只能在系统中运行一个 CONFIGURATION 备份。
- 应成对备份 Active Directory 服务和 SysVol。

Windows 配置对象

- Active Directory 服务
- 证书服务器
- COM+ 类注册数据库 (ComPlusDatabase)
- DFS
- DHCP
- DNS 服务器
- EISA 实用程序分区
- 事件日志
- 文件复制服务
- Internet Information Server (IIS)
- 用户配置文件 (Documents and Settings)
- Windows 注册表 (Windows Registry)
- Removable Storage Management Database
- SystemRecoveryData
- SysVol
- 终端服务数据库
- 用户磁盘配额 (QuotaInformation)
- WINS 服务器 (WINS server)

CONFIGURATION 在各种 Windows 系统中有所不同。

对于某些对象，必须考虑一些特殊的要点。如下所列。

- Active Directory

  备份 Active Directory 服务时，也同时备份 File Replication Service 和分布式文件系统（Distributed File System，DFS）。有关复制文件和分发文件的所有配置信息都存储在 Active Directory 中。

- DFS

  Data Protector 将 Windows 分布式文件系统（Distributed File System，DFS） 备份为以下某项的一部分：

  - Windows 注册表（如果以独立模式配置 DFS）
  - Windows Active Directory（如果以域模式配置 DFS）

- DHCP 和 WINS

  Data Protector 备份 DHCP 和/或 WINS 数据库时，将停止相应的服务，然后在备份数据库之后重新启动该服务。建议在工作时间之外计划对运行 DHCP 和/或 WINS 服务的服务器进行 CONFIGURATION 备份。

  DHCP 和 WINS 服务还自行提供其数据库的内部备份副本。如果环境不能接受偶尔关闭这些服务，则可以从 Data Protector 备份中排除这些服务，并通过文件系统备份来备份数据库的内部备份副本。有关内部备份副本的位置以及如何确保足够频繁地制作这些副本的详细信息，请参见 Microsoft MSDN 文档。

- 配置文件

  如果选择整个系统进行备份，则将备份两次“配置文件”（一次作为文件系统备份的一部分，一次作为 CONFIGURATION 的一部分）。要避免出现这种情况，请从文件系统备份中排除配置文件数据。用户配置文件数据位于 c:\Documents and Settings 目录中:

  这些目录包含系统中配置的所有用户配置文件，并且由 Data Protector 进行备份。如果为多个用户配置系统，则每个定义的用户都有一个单独的用户配置文件。例如， All Users 和 Default User 配置文件包含所有已定义用户常用的配置文件组件和分配给新建用户的配置文件组件。

  Data Protector 从以下注册表项读取配置文件的位置：

  HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\

  CurrentVersion\Explorer\Shell Folders

  （有关常用配置文件组件的信息所在的位置）

  HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\

  CurrentVersion\Explorer\User Shell Folders

- 可移动存储管理器数据库

  要启用可移动存储管理器数据库配置对象的备份，请确保在将备份的系统中安装可移动存储管理器。

- 终端服务数据库

  要启用终端服务数据库配置对象的备份，请确保在将备份的系统中安装终端服务器授权服务。

Windows 服务

备份 Windows 服务意味着备份由相应服务使用的数据结构。有一个特定的数据库将导出（转储）到随后备份的文件中。如果在备份向导中选择 CONFIGURATION，则将始终备份 Windows 服务。

Windows 服务必须正常运行，以使 Data Protector 可以检测出该服务，并在备份向导中提供它作为一个可选项。如果在备份时服务未运行，则相应的备份对象将失败。

要备份某个服务，请在 CONFIGURATION 下选择相应的文件夹。例如，如果使用 Active Directory 发布证书吊销列表 (CRLs)，则将 Active Directory 服务连同证书服务器一起备份。

系统状态数据备份

Windows 系统状态由与 Windows 系统各个方面相关的若干元素组成。这些元素在其各自的 Windows 备份对象下形成各自的结构。

Windows 系统状态不是可选择的备份项。通过 Data Protector，可以备份单独的对象，如注册表或 COM+ 类注册数据库。建议备份整个 CONFIGURATION 树。要使用文件系统备份功能备份特定卷或整个客户机系统，您必须选择使用卷影复制选项。

系统状态包括以下内容：

- 启动文件： Ntldr.exe 、 Ntdetect.com 和 boot.ini
- Registry 和 COM+ Class Registration Database (ComPlusDatabase)
- System File Protection 服务 (保存在 System Volume Information 目录中)

如果安装和配置该服务，则 Windows Server 系统的系统状态数据还包括：

- ActiveDirectoryService
- CertificateServer
- Cluster Service information
- IIS Metadirectory
- RemoteStorageService
- RemovableStorageManagementDatabase
- SystemFileProtection
- SYSVOL directory
- TerminalServiceDatabase

系统状态数据还包括属于可安装的其他服务器角色或服务的数据。

远程存储服务

远程存储服务用于自动将不常访问的文件从本地移至远程存储。打开此类文件时，将自动检索远程文件。尽管 RSS 数据库是系统状态数据的一部分，但要手动备份这些数据库。

- 远程存储服务：
  - 远程存储引擎： %SystemRoot%\system32\RsEng.exe

    协调用于存储不常用数据的服务和管理工具
  - 远程存储文件： %SystemRoot%\system32\RsFsa.exe

    管理在远程存储文件上的操作
  - 远程存储通知： %SystemRoot%\system32\RsNotify.exe

    向客户机通知有关检索的数据
- 远程存储数据库：

  远程存储数据库位于以下目录中： %SystemRoot%\system32\RemoteStorage
  - RSS 引擎数据库： %SystemRoot%\system32\RemoteStorage\EngDb
  - RSS 引擎备份数据库： %SystemRoot%\system32\RemoteSorage\EngDb.bak
  - RSS 文件数据库： %SystemRoot%\system32\RemoteStorage\FsaDb
  - RSS 跟踪数据库： %SystemRoot%\system32\RemoteStorage\Trace

Removable Storage Management Database

可以备份可移动存储数据库，但此服务不用于 Data Protector 介质管理。由 Data Protector 配置设备之前，必须禁用与机械手介质更换器配合使用的本机机械手驱动程序。

系统文件保护

重新启动计算机之后，系统文件保护服务扫描并验证所有受保护系统文件的版本。如果系统文件保护服务发现受保护文件被覆盖，则该服务将检索文件的正确版本，然后替换错误的文件。通过 Data Protector，可以备份并还原受保护文件，以使其不被覆盖。在标准文件系统备份过程中可以使用移动繁忙文件选项备份受保护文件。

UNIX 系统备份

要在 UNIX 系统中执行备份，请使用标准备份过程。在备份使用 NFS 的磁盘时，对于 VxFS 快照备份，或对于 UNIX 磁盘映像备份，需要执行某些额外的步骤。

以下限制适用：

- 备份由 NFS 装载的文件系统时，并不保留所有文件属性。
- 可以备份的最大文件大小取决于操作系统和文件系统的限制。

备份什么？

- Data Protector 备份目录结构、常规文件和特殊文件。特殊文件分为字符设备文件、块设备文件、UNIX 域套接字、FIFO 文件、HP-UX 网络特殊文件和 XENIX 特殊命名文件。
- 不遵循符号链接，将其备份为符号链接。
- 不遵循装入点，将其备份为普通空目录。
- 如果有多个硬链接引用同一个文件，则只备份该文件一次。通过设置以文件形式备份 POSIX 硬链接选项可以更改此行为。通过设置**以文件形式备份 POSIX 硬链接**选项可以更改此行为。
- 基本 ACL（文件权限属性）和时间属性与所有受支持的 UNIX 平台上的文件一并进行备份。但是，在某些平台上对扩展 ACL 的支持有限。有关详细信息，请参阅*《Data Protector 平台和集成支持矩阵》*，网址为 https://docs.microfocus.com/?DP。读取文件之前保存上次访问每个文件的时间，然后在备份文件之后返回该原始值。通过设置**不保留访问时间属性**选项可以更改此行为。

应当从 UNIX 文件系统备份中排除什么？

- 内部数据库目录，它们需要通过特殊方式进行备份（在线）。
- 临时目录

NFS 备份

NFS（网络文件系统）是一种分布式文件系统协议，利用该协议，计算机可以通过网络访问文件，就像在其本地磁盘上一样。通过 NFS 可以备份从本地可访问的远程 UNIX 系统中的文件系统。

何时使用 NFS 备份？

- 当系统不是 Data Protector 单元的一部分或未安装磁盘代理时。
- 要备份 Data Protector 不支持的系统平台时。

当配置常规文件系统备份时，建议从备份中排除由 NFS 装载的文件系统。这样可以避免出现警告消息，而如果还要备份磁盘实际所在的系统，则可以避免对相同磁盘进行重复备份。

以下限制适用：

- 可以备份 HP-UX、Solaris 和 Linux 客户机上由 NFS 装载的卷。不能备份软链接、字符和设备文件。有关支持的平台的详细信息，请参阅最新支持矩阵，网址为 https://docs.microfocus.com/?DP。
- 不保留 ACL（访问控制列表）属性。NFS 不支持对远程文件采用 ACL。单独的手动条目可指定各种系统调用、库调用和命令的行为。通过网络传输具有可选条目的文件或操纵远程文件时，可以无提示地删除可选条目。

OpenVMS 文件系统备份

OpenVMS 文件系统的备份过程与标准文件系统备份过程相同，但有一些方面是 OpenVMS 所特有的。

要备份 OpenVMS 系统上的数据，请在 OpenVMS 系统上安装 OpenVMS 磁带客户机。

以下限制适用：

- 任何输入到 GUI 中或传递到 CLI 的文件规范都必须采用 UNIX 样式语法

  /disk/directory1/directory2/filename.ext.n

  字符串应当以斜线开头，后跟磁盘、目录和文件名，其间以斜线分隔。

  不要在磁盘名称后面加冒号。

  版本号前面应该用句点，而不是分号。

  OpenVMS 文件的文件规范不区分大小写，但位于 ODS-5 磁盘上的文件除外。例如，OpenVMS 文件规范

  1DGA100:[bUSERS.DOE]LOGIN.COM';1

  必须按以下形式指定：

  /1DGA100/USERS/DOE/LOGIN.COM.1
- 没有隐式版本号。必须始终指定版本号。仅备份选定的备份文件版本。如果要包括文件的所有版本，请在 GUI 窗口中选择所有版本，或者使用 CLI 在“仅有”(-only) 选项下包括文件规范，其中包括版本号通配符，如下所示:

  /DKA1/dir1/filename.txt.*
- 要成功备份带写保护的卷影磁盘，请在备份规范中启用**不保留访问时间属性 (Do not preserve access time attributes)** 选项。
- 如果备份期间启用了**不保留访问时间属性 (Do not preserve access time attributes)** 选项，则上次访问日期将更新为 ODS-5 磁盘上的当前日期和时间。在 ODS-2 磁盘上，此选项无效，因而所有日期保持不变。
- 在 OpenVMS 上不提供磁盘映像备份功能。没有与“BACKUP/PHYSICAL”等效的功能。
- OpenVMS 上不提供“将 POSIX 硬链接备份为文件”(-hlink)、“软件压缩” (-compress) 和“编码” (-encode) 选项。

  包含多个目录条目的文件仅使用主路径名备份一次。将次路径条目另存为软链接。还原期间，还会还原这些额外的路径条目。

  没有与 BACKUP/IMAGE 等效的功能。要制作 OpenVMS 可引导系统磁盘的还原副本，必须使用 OpenVMS WRITEBOOT 实用程序向还原磁盘上写入引导块。
- 无论启用还是禁用了“在备份期间锁定文件”(-lock) 选项，始终都会锁定要备份的文件。如果启用了 -lock 选项，则不会备份任何打开（用于写入）的文件。如果禁用了 -lock 选项，将备份任何打开的文件。
- pre-exec 和 post-exec 命令过程的默认设备和目录是 /omni$root/bin 。要在任何其他地方放置命令过程，文件规范所包含的设备和目录路径必须采用 UNIX 样式格式。例如：

  /SYS$MANAGER/DP_SAVE1.COM
- 为“跳过”(-skip) 或“仅有”(-only) 过滤器指定通配符时，使用 '*' 代表多个字符，使用 '?' 代表单个字符。
- Data Protector 文件库在 OpenVMS ODS-2 磁盘上不受支持。
- 在 OpenVMS 系统上，Data Protector 不支持卷和卷集上的磁盘配额。

  要对启用磁盘配额的卷上的数据执行备份，请配置 pre-exec 脚本，以便在开始备份之前在涉及的卷上禁用磁盘配额，并配置 post-exec 脚本，以便在完成备份之后启用磁盘配额。

备份什么？

目录结构和文件与以下文件系统信息一并进行备份：

- 文件和目录属性
- ACL（访问控制列表）

只能从装入的 FILES-11 ODS-2 或 ODS-5 卷备份文件。

Novell Open Enterprise Server 备份

Novell Open Enterprise Server (OES) 的备份过程与标准备份过程相同，但有一些方面是 Novell OES 所特有的。

以下限制适用：

- 不支持软件数据压缩。即使在选择了备份选项软件压缩时，也不会影响备份的数据。
- Internet 协议版本 6 (IPv6) 不支持 OES 群集配置。

先决条件

- 必须在 Novell OES 系统上安装 Data Protector 磁盘代理。
- 必须以双模式加载 Target Service Agent for File Systems (TSAFS)。
- 对于 NDS/eDirectory 备份，必须加载 Target Service Agent for Novell Directory Services (tsands)。
- 对于 GroupWise 备份，必须加载 GroupWise Target Service Agent for File Systems (TSAFSGW)。
- 必须选择用于登录 Novell OES 备份服务的用户帐户，并用 HPLOGIN 实用程序保存该用户帐户。可以使用任何用户帐户，但用于备份的文件和目录将仅限于用户帐户的那些文件和目录。
- 必须在 Novell OES 系统上安装 Storage Management Services (SMS)。
- 增量备份不支持 Target Service Agent for File Systems (TSAFS) 缓存。在 Novell OES 客户机上对 TSAFS 使用 --noCachingMode 选项可禁用缓存。有关详细信息，请参阅 Novell 文档 https://www.novell.com/documentation/open-enterprise-server-2018/bkup_sms_lx/data/hhc3nq5m.html。

备份和还原压缩文件

Novell OES 提供文件压缩功能。默认情况下，Data Protector 以其压缩格式备份压缩文件，随后以其压缩格式还原压缩文件。只能将此类文件还原到具有压缩卷的 Novell OES。

备份什么？

- 本机 Linux 卷
- Novell GroupWise 数据

备份每个文件之后，将清除文件的存档标志，并设置存档日期/时间。

配置 Novell OES

以下配置任务可用:

- 使用 HPLOGIN 实用程序保存用户名和密码
- 以双模式加载 Target Service Agent for File Systems
- 加载 GroupWise Target Service Agent for File Systems
- 加载 Target Service Agent for Novell Directory Services

使用 HPLOGIN 实用程序保存用户名和密码

HPLOGIN 实用程序位于目录 /opt/omni/lbin 中。运行此实用程序，将正确的用户凭据 (用户名和密码) 保存到文件 /root/OMNI$CFG.DAT 中。

执行以下步骤：

1. 以 root 用户身份运行 HPLOGIN 实用程序:

   ```
   /opt/omni/lbin/hplogin
   ```

2. 指定应用于备份的管理员凭据 (例如 admin.ACME)

以双模式加载 Target Service Agent for File Systems

执行以下步骤：

1. 在目标系统上配置 Target Service Agent for File Systems (TSAFS)。默认情况下，在 Linux 模式下加载 TSAFS。将其更改为双模式：
   1. 检查是否已加载 TSAFS：

      ```
      /opt/novell/sms/bin/smsconfig -t
      ```

   2. 如果已加载，则将其卸载：

      ```
      /opt/novell/sms/bin/smsconfig -u tsafs
      ```

   3. 以双模式加载 TSA：

      ```
      /opt/novell/sms/bin/smsconfig -l tsafs --tsaMode=Dual --noCachingMode
      ```

2. 要配置该代理的自动加载，请执行以下操作：
   1. 将以下行添加到配置文件 /etc/opt/novell/sms/smdrd.conf 中:

      ```
      autoload: tsafs --tsamode=dual --noCachingMode
      ```

3. Open Enterprise Server Linux 上 TSAFS 配置文件的完整路径名为 /etc/opt/novell/sms/tsafs.conf 。加载 TSAFS 后，它会读取该配置文件获取其默认配置。将 readbuffersize 调整为 262144 或更多，将 readthreadsperjob 调整为 8 或更多，以提高增量备份的性能。

加载 Target Service Agent for Novell Directory Services

可以手动加载 Target Service Agent for Novell Directory Services (tsands) 代理或将其配置为在 Novell OES 启动期间自动加载。

执行以下任务:

- 要手动加载该代理，请执行以下操作：
  1. 运行以下命令以检查该代理是否已加载：

     /opt/novell/sms/bin/smsconfig -t
  2. 如果该代理未加载，请加载它：

     /opt/novell/sms/bin/smsconfig -l tsands
- 要配置该代理的自动加载，请执行以下操作：
  1. 将以下行添加到配置文件 /etc/opt/novell/sms/smdrd.conf 中:

     autoload: tsands

加载 GroupWise Target Service Agent for File Systems

可以手动加载 GroupWise Target Service Agent for File Systems (TSAFSGW) 代理或将其配置为在 Novell OES 启动期间自动加载。

执行以下任务:

- 要手动加载该代理，请执行以下操作：
  1. 运行以下命令以检查该代理是否已加载：

     /opt/novell/sms/bin/smsconfig -t
  2. 如果该代理未加载，请通过提供合适参数来加载它：

     /opt/novell/sms/bin/smsconfig -l tsafsgw --home DomainDirectory --home PostOfficeDirectory
- 要配置该代理的自动加载，请执行以下操作：
  1. 将以下行添加到配置文件 /etc/opt/novell/sms/smdrd.conf 中 (将参数占位符替换为实际值):

     autoload: tsafsgw --home DomainDirectory --home PostOfficeDirectory

备份性能

配置备份时，应虑备份性能因素。由于可变因素和排列组合众多，因此无法给出满足所有用户要求并且经济上负担得起的明确建议。但是，尝试提高备份或还原的性能时，应考虑以下几点：

基础架构

基础结构对备份和还原的性能有着巨大影响。最重要的因素是要有多条并行性的数据路径和使用高速设备。

- 网络与本地备份和还原

  通过网络发送数据会引入额外的开销，因为网络也成为性能考虑因素的一部分。对于以下情况，Data Protector 处理数据流的方式有所不同：

  - 网络数据流：磁盘到内存到网络到内存到设备
  - 本地数据流：磁盘到内存到设备

  要最大程度地提高性能，建议对大容量数据流使用本地备份配置。

- 所使用的设备、计算机系统本身以及硬件的并行使用也对性能有明显的影响。

  要努力使备份或还原性能达到最大限度，可以：

  - 设置适当的并发以实现设备流式传送
  - 优化段和块大小
  - 调整磁盘代理缓冲区的数量
  - 使用软件或硬件压缩
  - 使用基于磁盘的备份设备 — 文件库
  - 计划完整备份和增量备份
  - 使用合成备份和磁盘分段等高级备份策略
  - 优化备份对象向介质的分布
  - 禁用文件系统扫描

对象镜像和备份性能

对象镜像对备份性能有影响。在 Cell Manager 和介质代理客户机上，写入镜像的影响与备份额外对象的影响相同。在这些系统中，备份性能的降低将取决于镜像数。在磁盘代理上，镜像对性能无影响，因为备份对象只读取一次。

备份性能还取决于设备块大小和设备连接等因素。如果备份和对象镜像所用设备的块大小不同，则将在会话期间将镜像数据重新打包，此过程会占用额外的时间和资源。如果通过网络传输数据，则将增加网络负载并消耗更多时间。

设备之外的高性能硬件

计算机系统自身读取磁盘和写入设备的速度对性能有着直接影响。备份期间，通过读取磁盘、处理软件压缩（解压缩）等操作加载系统。

除了 I/O 性能和网络类型之外，磁盘读取数据速率和可用 CPU 也是系统自身的重要性能标准。

硬件并行性

可以将并行使用多个数据路径作为提高性能的一种非常高效的方法。其中包括网络基础架构。并行性技术在以下情况中大有助益：

- 如果有若干系统在本地备份，即磁盘和相关设备连接到相同的系统。
- 如果通过网络备份若干系统。在这种情况下，网络流量的路由需要经过优化，以使数据路径不发生重叠现象，否则会降低性能。
- 如果有若干对象（磁盘）备份到一个或若干（磁带）设备。
- 如果可以使用特定系统之间的若干专用网络链路。例如，system_A 有 6 个要备份的对象（磁盘），而 system_B 有 3 个快速磁带设备。解决方案是在 system_A 与 system_B 之间放置 3 条专用于备份的网络链路。
- 如果使用了若干设备，并启用了负载均衡选项。

并发

为每个介质代理启动的磁盘代理数量称为磁盘代理（备份）并发，使用设备的高级选项或在配置备份时可以修改此项。备份规范中设置的并发优先于设备定义中设置的并发。

Data Protector 提供的默认磁盘代理数足以满足大多数情况。例如，在标准 DDS 设备上，两个磁盘代理可以发送设备流式传送所需的足够数据。对于带有多个驱动器、每个驱动器受一个介质代理控制的库设备，可以单独设置每个驱动器的并发数目。

对性能的影响

如果设置正确，则备份并发可提高备份性能。例如，如果您的库设备有四个驱动器，每个驱动器受一个介质代理控制，每个介质代理从两个磁盘代理并发地接收数据，来自八个磁盘的数据同时进行备份。

多个数据流

同时可以将磁盘的多个部分备份到多个设备。此方法可提高备份速度，对于将容量很大且速度很快的磁盘备份到相对较慢的设备时很有用。多个磁盘代理从磁盘并行读取数据，并将数据发送到多个介质代理。

请注意，如果通过多个磁盘代理备份一个装载点，数据将包含在多个对象中。要还原整个装载点，必须在一个备份规范中定义装载点的所有部分，然后还原整个会话。

设备流式传送

要最大限度地提高设备的性能，必须使其进行流式传送。如果设备可以向介质输送足够的数据，使数据保持不断前移，则设备就是在进行流式传送。否则，必须让磁带停止转动，设备等待更多数据，然后将磁带倒回一些，继续写入磁带等等诸如此类。也就是说，如果向磁带写入的数据速率小于或等于计算机系统可以向设备提供的数据速率，则设备就是在进行流式传送。设备流式传送还取决于其他因素，如网络负载和一次操作中写入备份设备的数据的块大小。在以网络为中心的备份基础架构中，设备流式传送值得关注。对于本地备份（其中磁盘和设备都连接到相同的系统），如果磁盘足够快，则并发为 1 即可满足需要。

配置设备流式传送

要使设备可以进行流式传送，必须向设备发送足够数量的数据。Data Protector 会为将数据写入设备的每个介质代理启动多个磁盘代理。

块大小

段并不作为完整单位，而是分为更小的子单位，称为块。设备硬件按设备类型特有的块大小处理其接收的数据。

Data Protector 对于不同的设备类型使用相应的默认设备块大小。块大小适用于 Data Protector 创建的所有设备，并适用于不同平台上运行的介质代理。

增加块大小可提高性能。配置新设备时或使用设备的高级选项更改设备属性时，可以调整发送到设备的块。还原时可适应块大小。

> ⚠ **警告**为受特定操作系统上所运行的 Data Protector Media Agent 控制的设备增加块大小之前，请确保所需块大小不会超过该操作系统支持的默认最大块大小。如果超过限制，则 Data Protector 无法从这类设备还原数据。有关是否可以调整最大支持块大小以及如何调整的信息，请参见操作系统文档。

应在格式化磁带之前更改块大小。介质头上写入了设备块大小，以使 Data Protector 了解要使用的大小。如果设备的块大小与介质的块大小不同，就会发生错误。

但是，在更改设备的块大小之前，需要检查所使用的主机适配器支持的块大小。老式 SCSI 卡（如 Adaptec 2940）的最小块大小通常为 56 KB。用于较新 SCSI 卡的最小块大小为 64 KB。

通过修改 Windows 介质代理客户机的注册表，可以增加其上的最大块大小。该过程取决于主机总线适配器类型：SCSI、光纤通道或 iSCSI。有关详细信息，请参见链接的示例主题。

更改特定主机总线适配器的块大小之前，请参见供应商文档，或与供应商技术支持人员联系。

段大小

介质可划分为数据段、目录段和头段。头信息存储在头段中，大小与块大小相同。数据存储在数据段的数据块中。每个数据段的信息存储在相应的编目段中。这些信息先存储在介质代理内存中，然后写入介质的编目段和 IDB。

段大小（以 MB 为单位度量）是数据段的最大大小。如果要备份大量小型文件，可以通过编目段的最大大小限制实际段大小。段大小可以由用户针对每个设备进行配置，并且在还原期间和导入介质期间会影响性能。配置新设备时或使用设备的高级选项更改设备属性时，可以调整段大小。

最佳段大小取决于设备中使用的介质类型和要备份的数据类型。每盘磁带的平均段数为 50。通过将磁带的本机容量除以 50，可以算出默认段大小。对于所有介质类型，最大编目大小都限制为一个固定数字 (12 MB)。

达到第一个限制后，Data Protector 即完成一个段。备份大量小文件时，将更快地达到介质目录限制，而这会使段大小更小。

磁盘代理缓冲区的数量

Data Protector介质代理和磁盘代理使用内存缓冲器保存等待传输的数据。该内存分为许多个缓冲区（每个磁盘代理对应一个缓冲区，具体取决于设备并发数）。每个缓冲区由 8 个磁盘代理缓冲器组成 (大小与配置的设备块大小相同)。

配置新设备时或使用设备的高级选项更改设备属性时可以更改此值，但很少有这种必要。更改此设置有两个根本原因：

- 内存不足：介质代理所需的共享内存可以按如下方法计算：

  DAConcurrency*NumberOfBuffers*BlockSize

  例如，将缓冲器的数量从 8 个改为 4 个即可减少 50% 的内存消耗，但也会产生性能问题。

- 流式传送

  如果可用网络带宽在备份期间变化很大，则介质代理要有足够的数据可供写入，设备才能保持流式传送模式，这一点很重要。在这种情况下，应增加缓冲器的数量。

软件压缩

从磁盘读取数据时，由客户机 CPU 执行软件压缩。这样可减少通过网络发送的数据，但需要客户机提供大量 CPU 资源。

默认情况下，软件压缩处于禁用状态。通常，只有在为了提高性能时才应使用硬件压缩。只应在通过慢速网络对许多系统进行备份时使用软件压缩，这种情况下在通过网络发送数据之前即可压缩这些数据。

如果使用了软件压缩，就会禁用硬件压缩，因为试图压缩数据两次实际上会使数据膨胀。

硬件压缩

大多数新型备份设备都提供了内置的硬件压缩功能，在设备配置过程中创建设备文件或 SCSI 地址时可启用该功能。

硬件压缩由一个设备完成，该设备从介质代理客户机收到原始数据，然后以压缩模式将这些数据写入磁带。硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数据较少。

请考虑以下有关硬件压缩的内容：

- 请小心使用硬件压缩，因为以压缩模式写入的介质不能使用处于非压缩模式的设备读取，反之亦然。
- 请勿同时使用软件和硬件压缩，因为双重压缩会降低性能，并且不会产生更好的压缩结果。
- Ultrium LTO 驱动器使用自动硬件压缩，无法禁用。建议在使用 Data Protector 配置 Ultrium LTO 驱动器时，禁用软件压缩。
- 用不支持硬件压缩的设备读取使用硬件压缩写入的介质时，Data Protector 无法识别介质和读取数据。而是将此类介质视为未知介质或新介质。

配置设备时，如果从下拉列表中选择 SCSI 地址，则 Data Protector 将自动确定设备能否使用硬件压缩。

在 UNIX 系统中，可通过选择硬件压缩设备文件启用硬件压缩。

在 Windows 系统中，如果因检测不成功需要手动输入 SCSI 地址，则向设备/驱动器 SCSI 地址的末尾添加 C ，例如：scsi:0:3:0C（或如果加载了磁带驱动程序，则为 tape2:0:1:0C ）。如果设备支持硬件压缩，则会使用硬件压缩，否则将忽略 C 选项。

要在 Windows 系统中禁用硬件压缩，请向设备/驱动器 SCSI 地址的末尾添加 N ，例如：scsi:0:3:0N 。

对于多路径设备，要单独为每个路径设置此选项。

磁盘映像备份和文件系统备份

在磁盘映像备份与文件系统备份之间进行选择时，应考虑其优点和缺点。在大多数情况下，建议采用文件系统备份。

	文件系统备份	磁盘映像备份
备份一致性	文件可以在备份过程中锁定，并以一致的状态进行备份。会保留文件和目录的结构。	文件在备份过程中不会锁定，并以时间点状态进行备份。无法浏览文件和目录的结构。
备份大小	备份数据占用的空间与文件和文件夹数据在备份时的累积大小相同。	备份数据在备份介质上占用的空间与原始备份卷的大小相同。
备份和还原速度	当备份磁盘未满且文件数较少时，备份和还原速度较快。	当备份磁盘已满且存在大量小文件时，备份和还原速度较快。
还原可用性	更容易在还原的文件中导航，因为保留了文件和目录的结构。	会还原整个磁盘或磁盘分区，无法浏览文件和目录的结构。

注意在 Windows 系统中，可以使用 VSS 写入程序执行磁盘映像和文件系统备份。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。这在备份系统卷时非常重要。

向介质分配对象

可以相应地配置备份，以使备份数据在几个不同配置中的介质上结束。例如，可以配置一个备份，其中一个对象到一个介质，或若干对象到若干介质，并且每个介质都包含每个对象中的数据。

某些条件下，某种分散方式在备份性能方面可能具有优势，但它可能不是最佳的还原配置。应相应地定义备份策略，以使您优化备份的设置（因为经常进行备份），并同时具有可接受的还原介质情况。

文件系统扫描

Data Protector 备份文件之前，将对选择进行备份的树执行一次扫描。这会影响性能。由于 Windows 系统中的快速文件系统扫描和 UNIX 系统中的文件系统扫描功能所产生的影响可忽略不计，因此建议不要仅为提高性能而更改默认设置。

根据要备份的系统，文件系统扫描有所不同：

系统	文件系统扫描功能	如何禁用该扫描功能？
Windows	快速文件系统扫描（始终选择）	可以通过将 OB2NOTREEWALK omnirc 选项设置为 1 禁用文件系统扫描。
	检测 NTFS 硬链接（默认：未选中）	选择检测 NTFS 硬链接选项会使性能显著降低。只有存在 NTFS 硬链接时才应选择它。
UNIX	检测硬链接并计算大小（默认：已选中）	选择将 POSIX 硬链接备份为文件选项时，会使文件系统扫描处于非活动状态。

其他性能提示

遵照表中列出的提示，可以提高备份或还原的性能。

什么可提高性能？	如何提高性能？
修补程序	确保已安装与网络性能有关的所有修补程序。
设备的位置	尽可能使用本地设备。
LAN 卡	可以在总线上将 FDDI 卡上移，以使其获得更高的优先级。使用 ftp 在介质代理与磁盘代理系统之间传输大型文件，以查看传输速度与 Data Protector 性能相比如何。 请注意，以半双工配置的网卡会降低性能。
高速设备	如果怀疑到磁带设备的持续数据流速度太慢，或设备未正确处理该数据流，可以在介质代理客户机上模拟高速设备。
设备配置	可以调整发送到设备的块以提高性能。
CRC 检查选项	可以禁用 CRC 检查选项。如果启用，则此选项会因 CRC 计算（由介质代理客户机执行）而影响性能。
日志记录和报告级别	如果更新 IDB 所用时间过长，可以通过将日志记录设置为无日志而将其禁用。 通过将报告级别设置为“严重”可以过滤消息。
Data Protector 应用程序客户机	如果应用程序客户机 (Oracle、SAP R/3) 的还原会话耗时过长，则可以减小 SmWaitforNewClient 值。将其值设置为小于默认值（5 分钟）的值。

管理介质

Data Protector 提供强大的介质管理功能，通过此功能可以更简单高效地管理大量介质。系统使用 IDB 存储有关备份、恢复和介质管理事件的信息。

Data Protector 介质管理的高级功能为：

- 保护免遭意外覆盖。
- 介质池使您可以考虑大型介质集，而不必担心每个单独的介质。
- 可以在不以物理方式访问介质的情况下将所有与介质相关的目录数据从一个 Data Protector Cell Manager 传输到另一个。
- 自由池功能使您可以避免备份因缺少（空闲）介质而失败。
- 跟踪所有介质、每个介质的状态，以及在多个 Data Protector 单元之间共享这些信息：数据保护到期时间、备份用介质的可用性以及备份到每个介质的内容的编目。
- 可以明确定义对特定备份要使用哪些介质和哪些设备。
- 自动识别 Data Protector 介质和其他常用磁带格式。
- 识别和支持大型库中的条码设备以及支持条码的 silo 设备。
- 可以在多个 Data Protector 单元之间共享集中式介质信息。
- 支持介质保管，也称为归档或场外存储。
- 在介质上交互或自动创建其他数据副本。
- 详细的筛选和分页设置。

自定义设备和介质视图

通过配置 MediaView 、 MagazineView 、 SCSIView 、 ExternalView 、 JukeboxView 、 ACSView 和 DASView 全局选项，可以自定义“设备和介质”上下文的默认视图。通过指定对应的令牌字符串，自定义将在库或介质管理上下文中显示的属性。

相关主题

- 介质池
- 介质生命周期

介质池

介质池表示用于备份一组同类介质。可以定期备份用一个介质池、存档备份用一个、每个部门用一个等等。每个介质池定义介质使用情况、分配策略和介质状态因素。

自由池

自由池是当池中所有介质都在使用时可用的同类介质的辅助源。配备自由池有助于避免备份因缺少空闲介质而失败。

受保护介质属于某个特定的池（例如属于 SAP 池），而空闲介质可以自动移至其他几个池所使用的自由池。这个公用空闲池用于向使用这个自由池的所有池分配空闲介质。可以对每个介质池决定是否要将其与某个自由池相联系。

默认介质池

默认介质池是 Data Protector 作为设备定义的一部分提供的池。如果在备份规范中没有指定任何介质池，则使用此池。

自由池特征

自由池是可以配置为允许跨介质池共享空闲介质的介质池，这些池可以减少因装载请求而导致的操作员干预。自由池的使用为可选。

自由池的属性

自由池：

- 如果将空闲池与介质池相联系，或如果空闲池不为空，则无法删除该空闲池
- 与常规池不同的是它无法用于分配，因为它不能容纳受保护的介质。因此，分配策略选项（严格/宽松、可追加/不可追加）不可用。
- 仅包含空闲的 Data Protector 介质（无未知或空白介质）。

何时使用自由池？

在以下两种场合下，介质在常规池和自由池之间移动：

- 如果常规池中没有空闲介质，Data Protector 将从自由池中分配介质。这样将使介质自动移至常规池。
- 介质上的所有数据都到期（并且介质位于常规池中）时，可将介质自动移至自由池。

介质质量计算

“链接”池之间以相同方式计算介质质量。仅对自由池可配置介质状态因素，并且所有使用自由池的池都将继承这些因素。不使用自由池的池有拥有其自己单独的计算基础。

自由池的局限性

- 无法将受保护的介质移至自由池。
- 无法在介质上使用某些操作（如导入、复制和循环回收），因为可以在受保护的介质上进行这些操作。
- 选择了箱盒支持选项的池无法使用自由池。
- 使用空闲池时，可能会遇到池中出现暂时不一致的情况（1 天）（例如常规池中有一个不受保护的介质等待解除对空闲池的分配）。
- 如果自由池中有包含不同数据格式类型的介质，则 Data Protector 自动重新格式化所分配的介质（如有必要）。例如，可以将 NDMP 介质重新格式化为正常介质。

创建自由池

要创建含有默认属性的自由池，请完成以下步骤:

1. 创建介质池时，选择“分配策略”选项卡。
2. 选择**使用自由池**选项，然后键入一个非现有的新名称。单击“下一步”。此时将自动创建一个含有此类型介质默认设置的自由池。

要创建自定义自由池，请按照下面的步骤操作。

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，右键单击**池**，然后单击**添加自由池**以打开向导。
3. 在“池名称”文本框中键入自由池的名称，在“说明”文本框中键入说明（可选），并在“介质类型”下拉列表中选择用于备份设备的介质类型。

单击“下一步”。
4. 更改“介质状态因素”对话框中的设置（可选）。
5. 单击**完成**以创建自由池，然后退出向导。

可以修改已配置的自由池。但是，无法修改其介质类型。

介质池属性

配置介质池时，指定介质池属性。某些属性可以接下来修改。

介质池属性 - 常规

- 描述
- 池名称
- 介质类型

介质池属性 - 分配

介质分配策略定义介质池中访问介质的顺序，以使介质均匀地磨损。包括：

- 严格
- 宽松
- 首先分配未格式化的介质
- 使用自由池
- 将自由介质移至自由池
- 箱盒支持

介质池属性 - 条件

介质状态因素

介质状态因素定义介质的状态，因此确定介质能够可靠地用于备份的时间长度。例如，备份到旧或磨损的介质更容易产生读/写错误。根据这些因素，Data Protector 将介质的状况从良好改为中等或差。对整个介质池而非每个介质设置状况因素。

重要说明要使 Data Protector 准确计算介质的状况，请在向介质池添加介质时使用新介质。

注意如果池使用自由池选项，则从空闲池继承介质状态因素。

可以选择的两个介质状态因素包括：

- 最大重写次数
- 有效期(月)

介质池属性 - 使用

介质使用策略控制如何将新备份添加到已使用的介质中。包括：

- 可追加
- 不可追加
- 仅对于增量可追加

介质池质量

池中质量最低的介质决定介质池的质量。例如，只要池中有一个介质为差，就会将整个介质池标为差。

介质的质量影响如何为备份选择介质，因为它影响能否写入介质和读取该介质所含数据。先选择状况良好的介质，然后再选择状况中等的介质。不选择状况差的介质进行备份。

介质状态取决于以下某个介质状态因素：

- 良好
- 中等
- 差

在介质池属性的“状况”属性页中，可以更改用于计算介质状况的介质状态因素。新的介质状态因素将用于计算介质池中所有介质的状况。

设备错误和介质质量

如果备份期间设备发生故障，则将此设备中用于备份的介质标为差。如果问题是因介质错误所致，这样可以防止未来再出错。

如果此错误是因不洁驱动器，请清洗驱动器，然后验证介质以重置其状况。

建议调查池中是否出现被标为差的介质。可以使用“验证”获取有关每个介质的状况的详细信息。建议不要只是循环回收介质。

创建介质池

Data Protector 提供默认介质池，但您可以根据自身需要创建自己的介质池。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，右键单击**池**，然后单击**添加介质池**以打开向导。
3. 在“池名称”文本框中键入介质池的名称，在“说明”文本框中键入说明（可选），并在“介质类型”下拉列表中选择将用于备份设备的介质类型。单击“下一步”。
4. 设置以下选项：
   - 更改“介质使用策略”和“介质分配策略”的默认值（可选）。
   - 要使用自由池，请首先选择**使用自由池**选项，然后从下拉列表中选择自由池。
   - 要禁用向自由池自动解除分配空闲介质，请选择**将空闲介质移动到自由池**选项。
   - 如果要配置支持箱盒的设备的介质池，则选择**箱盒支持**选项。此选项不能与介质池一起使用。

   单击“下一步”。
5. 更改“介质状态因素”对话框中的设置（可选）。
6. 单击**完成**以创建介质池，然后退出向导。

> **提示**可以修改已配置的介质池。但是，无法修改其介质类型。

修改介质池

可以修改介质池属性以更好地符合您的需要：可以更改介质池的名称、其说明、介质使用策略和介质分配策略或介质状态因素。无法更改介质类型。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，展开“介质”，然后单击“池”。此时将在结果区域中显示所配置介质池的列表。
3. 右键单击要修改的介质池的名称，然后单击**属性**。
4. 在“常规”属性页中，可以在“池名称”文本框中更改介质池的名称，或在“说明”文本框中更改说明。
5. 单击“分配”选项卡，以更改“介质使用策略”和“介质分配策略”的设置、(取消选择或) 选择自由池的使用、启用或禁用“将空闲介质移动到自由池”选项或者选择“箱盒支持”选项。
6. 单击**状况**选项卡，以更改“介质状态因素”对话框中的设置或将介质状况因素设置为默认。
7. 单击**应用**确认。

删除介质池

通过从 Data Protector 配置删除介质池，停止使用此介质池进行备份。无法删除用作备份设备的默认池的介质池。在这种情况下，更改所有设备的介质池或删除设备。

如果尝试删除非空介质池，则将提示您先导出或移动池中的所有介质。

重要说明如果删除备份规范中使用的介质池，则将从该规范中删除介质池。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，展开“介质”，然后单击“池”。此时将在结果区域中显示所配置介质池的列表。
3. 右键单击要删除的介质池，然后单击**删除**。确认操作。

   所配置介质池的列表中将不再显示已删除的介质池。

介质生命周期

介质生命周期以介质的使用开始，在达到最大使用标准时结束。它通常由以下部分组成：

准备备份用介质

这一阶段包括格式化/初始化介质和将其分配给介质池，具体方法是格式化 (未使用的介质和使用过的非 Data Protector 介质) 或导入 (使用过的 Data Protector 介质)。处理已使用过的介质时，请考虑使用回收/取消保护和导出功能。

使用备份用介质

这一阶段包括如何为备份选择介质、检查哪些介质状态因素（例如覆盖数）、如何将新备份追加到介质和数据保护何时到期。

将介质保管到安全位置

保管介质包括为安全存储准备介质和实际存储。要准备保管，需要设置相应的数据保护和编目保护策略，以创建保管位置的列表、以指定和修改介质位置、以弹出介质以及在某些情况下扫描设备。

Data Protector 支持各种级别的保管：

- 数据保护和编目保护策略。
- 轻松选择和弹出带库中的介质。
- 介质位置通知您存储介质的物理位置。
- 通过报告显示指定时间范围内用于备份的介质。
- 通过报告显示备份期间哪些备份规范使用了指定的介质。
- 通过报告显示存储在特定位置、其数据保护期在特定时间到期的介质。
- 显示还原所需介质的列表及其物理存储位置。
- 根据特定标准（如写入介质的时间或保护已到期的介质）才介质视图中筛选介质。

建议制作备份数据的副本用于保管，并在站点上保留原始介质以便可以进行还原。Data Protector 允许以交互方式创建或自动创建介质上数据的其他副本。

报废介质

介质到期（超过其最大使用标准）后，即将其标为差，并且不再被 Data Protector 使用。

介质类型

介质类型就是介质的物理种类，如 DDS 或 DLT。对于 Data Protector，在配置设备时选择相应的介质类型，而 Data Protector 将估算特定介质池的介质上的可用空间。

有关受支持的介质类型的详细信息，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。

介质质量

介质的质量影响如何为备份选择介质，因为它影响能否写入介质和读取该介质所含数据。先选择状况良好的介质，然后再选择状况中等的介质。不选择状况差的介质进行备份。

介质状态取决于以下某个介质状态因素：

- 良好
- 中等
- 差

可以查看介质的“信息”属性页以获取有关介质质量（状况）的信息。

在介质池属性的“选项”属性页中，可以更改用于计算介质状况的介质状态因素。新的介质状态因素将用于计算介质池中所有介质的状况。

介质质量有助于确定何时必须更换介质。

设备错误和介质质量

如果备份期间设备发生故障，则将此设备中用于备份的介质标为差。如果问题是因介质错误所致，这样可以防止未来再出错。

如果此错误是因不洁驱动器，请清洗驱动器，然后验证介质以重置其状况。

建议调查是否有介质被标为差。可以使用“验证”获取有关每个介质的状况的详细信息。建议不要只是循环回收介质。

选择介质

Data Protector 介质管理自动选择最适合备份的介质。介质选择的基本标准如下：

- 不选择状况差的介质进行备份。
- 只有在没有状况良好的介质可用时才使用状况中等的介质。
- 如果有，则首先使用状况良好的介质。
- 始终从指定的池选择介质。当池不包含不受保护的介质时，Data Protector 将访问自由池（如果已配置）。

此外，介质选择基于以下因素：

介质分配策略

可以使用介质分配策略影响如何为备份选择介质。可以指定宽松策略（任何合适的介质都可用于备份），或严格策略（特定介质必须以预定义顺序可用）。

预分配介质

可以指定介质池中的介质将用于备份的顺序。此顺序称为预分配列表。

介质状态

介质状态也会影响为备份选择的介质。例如，状况良好的介质在状况中等的介质之前用于备份。状况差的介质不用于备份。

只有在标为中等的介质上没有受保护的介质时才会使用这些介质。否则，将发出装载请求，索要空闲介质。

介质使用

介质使用策略控制如何将新备份添加到已使用的介质中，并影响为备份选择哪些介质。

限制

在 Travan 设备中使用的介质上不能追加备份。

可追加的介质必须处于良好状况，包含某些当前受保护的对象并且不得已满。如果有多个设备用于负载均衡，则可追加的概念按设备适用，即每个设备都使用可追加的介质作为会话中的第一个介质。在相同介质上追加数据的备份会话不一定与相同的备份规范有关。

> **注意**如果使用追加功能，并且备份需要多个介质，则只有所使用的第一个介质可以包含来自以前会话的备份数据。随后，Data Protector 将仅使用空的或不受保护的介质。

策略可以是：可追加、不可追加或只可追加增量。

可以在介质上为某个客户机创建还原链。这些介质将仅包含一个完整备份以及与同一客户机相关的增量备份：

- 对于每个具有**仅对于增量可追加**介质使用策略的客户机配置一个池。
- 将一个不同的池与备份规范中的每个客户机相关，或为每个客户机创建一个单独的备份规范。

请注意，偶尔将创建仅包含增量备份的介质。

介质选择因素

分配策略	首先分配未格式化的介质	Data Protector 选择顺序
宽松	关闭	1. 预分配列表（如果指定） 2. 可追加的（如使用策略中所设置） 3. 不受保护的 Data Protector 介质 4. 未格式化的介质 5. 中等介质
宽松	打开	1. 预分配列表（如果指定） 2. 可追加的（如使用策略中所设置） 3. 未格式化的介质 4. 不受保护的 Data Protector 介质 5. 中等介质
严格	不适用	1. 预分配列表（如果指定） 2. 可追加的（如使用策略中所设置） 3. 不受保护的 Data Protector 介质 4. 中等介质

使用不同的介质格式类型

Data Protector 可识别两种不同的格式类型和使用这些类型向介质写入数据：

- Data Protector (适用于 Data Protector 直接控制的备份设备)
- NDMP（适用于连接到 NDMP 服务器的备份设备）

两种格式类型使用两种不同的 Data Protector 介质代理组件（常规介质代理或 NDMP 介质代理）与备份设备进行通信。

以下限制适用：

- 由一种格式类型写入的介质在使用不同格式类型的备份设备中将被识别为空白或外部介质。
- 不能在相同介质上使用不同格式类型备份对象。
- 不能在同一系统上安装两个不同的 Data Protector 介质代理组件。
- 强烈建议对不同的介质格式类型使用不同的介质池。

WORM 介质

WORM（写入一次，读取多次）是一种数据存储技术，通过它可以将信息一次性写入介质，并防止驱动器擦除数据。WORM 介质有意设计为不可重写，因为它们旨在存储不希望意外擦除的数据。

使用 WORM 介质

Windows、HP-UX、Linux、Solaris 和 OpenVMS 操作系统支持 WORM 介质。

Windows 平台中安装的 Data Protector 不支持将 WORM 磁带检测为可重写。在其他平台中，Data Protector 不会将磁带识别为不可重写，并将它按照任何其他磁带的方式加以处理。尝试覆盖 WORM 介质上的数据时，将显示以下错误消息：

```
Cannot write to device ([19] The media is write protected.)
```

```
Tape Alert [ 9]: You are trying to write to a write-protected cartridge.
```

要防止出现这种情况，请执行以下操作：

- 将 WORM 介质的备份保护设置为“永久”。
- 将 WORM 介质和可重写的介质保存在不同的介质池中。

对于所支持的 WORM 介质支持进行所有 Data Protector 介质操作。有关受支持 WORM 磁带驱动器和介质的最新列表，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。

格式化介质

通过在 IDB 中保存有关介质的信息（介质 ID、说明和位置），并通过在介质（介质头）上写入这些信息，格式化（初始化）介质使其做好准备，供 Data Protector 使用。格式化介质时，还会指定其所属的介质池。

用填充块进行格式化

可以扩展介质头的大小，并用不可压缩的数据（填充块）将其填满。创建介质副本时这会很有用。填充块不复制到目标介质。这样可确保目标介质不会在源介质之前到达磁带末尾。

如果使用对象副本功能复制备份数据，则不需要填充磁带。

默认情况下禁用磁带填充。要启用它，请在备份设备所连接的系统上的 omnirc 文件中设置 OB2BLKPADDING_n 选项。

何时格式化介质

首先需要格式化介质，然后再用其进行备份。但是，当对于介质池使用宽松介质分配策略时，不需要用单独的一步格式化介质。如果将全局选项 InitOnLoosePolicy 设置为 1 (默认值为 0)，则 Data Protector 在选择新介质进行备份时即自动格式化这些介质。

首先必须格式化非 Data Protector 介质，然后再备份。

直到取消保护时才格式化具有受保护数据的 Data Protector 介质，此后可覆盖旧数据。

介质标签

格式化时，Data Protector 用唯一介质标签和介质 ID 标记每个介质。两者都存储在 IDB 中，并使 Data Protector 可以管理介质。介质标签是用户定义的说明和介质条形码的组合（如果为库选择了**在初始化时将条形码用作介质标签**选项）。条码显示为介质说明的前缀。例如，[CW8279]Default DLT_1 是一个介质标签，Default DLT_1 为说明，CW8279 为条码。（可选）在初始化介质期间，可以将条码作为介质标签写入磁带上的介质头。

格式化介质后，即无法更改介质自身上写入的介质标签和位置，除非再次将其格式化（这会导致覆盖数据）。修改介质属性仅更改 IDB 中的此信息。

尽管可以更改标签并排除条码数字，但建议不要这么做。在这种情况下，应手动跟踪分配给介质的实际条码和介质标签。

识别介质格式

如果介质已由某些其他应用程序使用，则 Data Protector 可识别介质上通用格式的数据。但是，建议不要依赖 Data Protector 来识别其他介质类型，因为能否识别取决于您所使用的平台。

要确保不覆盖任何 Data Protector 介质，必须选择严格分配策略。

Data Protector 按照所识别的格式做出不同的行动，如下表所示。

介质格式	备份行为	可能进行的操作
未知或新（空白）	宽松策略：用于备份 严格策略：不用于备份	格式化介质
写入时压缩的介质，当前以无压缩方式使用	宽松策略：用于备份 严格策略：不用于备份	格式化介质

写入时不压缩的介质，当前以压缩方式使用	宽松策略：用于备份 严格策略：不用于备份	格式化介质
外部 Data Protector（另一个单元中）	不用于备份	导入或强制格式化介质
tar、cpio、OmniBack I、ANSI label	不用于备份（无法保证）	强制格式化介质
Data Protector 不受保护的介质	用于备份	导出介质
Data Protector 受保护的介质	追加备份	回收（取消保护）介质

注意如果尝试用不支持硬件压缩的设备读取使用硬件压缩写入的介质，Data Protector 无法识别介质和读取数据。因此，将该介质视为未知或新。

格式化介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 Data Protector 介质，此后可覆盖旧数据。

注意直到向文件库设备进行首次备份后，才能将其格式化。这是因为此前设备不包含任何文件仓库，并且无法手动创建文件仓库。备份期间创建的文件仓库等同于介质。根据文件库设备的介质池介质分配策略，将自动删除新格式化的介质。

重要说明使用“强制操作”选项可用 Data Protector 可识别的其他格式 (tar、OmniBack I 等等) 将介质格式化，或重新格式化 Data Protector 介质。

直到取消保护后，才会格式化含有受保护数据的 Data Protector 介质。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，右键单击要向其添加介质的介质池，然后单击**格式化**以打开向导。
4. 选择目标介质所在的设备，然后单击**下一步**。
5. 指定新介质的**介质说明**和位置（可选），然后单击**下一步**。
6. 指定会话的其他选项：可以选择**在操作完成之后弹出介质**选项，或使用**强制操作**选项。还可以**指定介质大小**，或使**默认**选项保持选中状态。
7. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 Data Protector。

格式化箱盒中的所有介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 Data Protector 介质，此后可覆盖旧数据。

要在一步中格式化箱盒中的所有介质，请使用选择了**箱盒支持**选项的设备。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击所需的介质池。

4. 右键单击**箱盒**项，然后单击**格式化箱盒**以打开向导。
5. 选择库中要用其执行操作的驱动器，然后单击**下一步**。
6. 指定新介质的说明和位置（可选），然后单击**下一步**。
7. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选项保持选中状态。
8. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 Data Protector。

格式化箱盒中的单个介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 Data Protector 介质，此后可覆盖旧数据。

要格式化箱盒中的介质，请使用选择了**箱盒支持**选项的设备。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，右键单击要向其添加介质的介质池，然后单击**格式化**以打开向导。
4. 选择目标介质所在的设备以及要在其上执行操作的介质所在的插槽，然后单击**下一步**。
5. 指定新介质的说明和位置（可选），然后单击**下一步**。
6. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选项保持选中状态。
7. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 Data Protector。

格式化库设备中的介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 Data Protector 介质，此后可覆盖旧数据。

如果使用库设备，则可以使用 Ctrl 键选择多个插槽，并在一步中格式化多个介质。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，展开库设备，然后单击**插槽**。
3. 在结果区域中，右键单击要格式化的介质所在的插槽，然后单击**格式化**以打开向导。
4. 选择库中要用其执行操作的驱动器，然后单击**下一步**。
5. 选择要向其添加格式化的介质的介质池，然后单击**下一步**。
6. 指定新介质的**介质说明**和位置（可选），然后单击**下一步**。
7. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选项保持选中状态。
8. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 Data Protector。

导入介质

介质导入是在不丢失介质上数据的前提下将单元之外的 Data Protector 介质添加到介质池中的行为。此前必须已导出该介质，即该介质来自另一个 Data Protector 单元。

导入介质时，将有关介质上备份数据的信息读入 IDB 中，以使您以后可以浏览它进行还原。

- 在介质导入期间，不重新构造对象或介质大小等属性信息，因此所导入对象的大小显示为 0 kB。
- 根据所使用的备份设备和介质，导入可能会花费相当长的一段时间。
- 无法将介质导入自由池中。
- 如果尝试导入已删除的副本，并且原始介质不在 IDB 中，则首先需要使用强制操作选项导入原始介质，或使用作为原始副本导入选项导入副本。
- 在将数据保护已过期的 WORM 介质导入 Data Protector 单元时，请确保使用选项“保护”(默认情况下此值被设置为“永久”) 指定新的数据保护值。这允许将 Data Protector 附加到 WORM 介质。

何时导入介质？

通常在 Data Protector 单元之间移动介质时使用导入功能。在这种情况下，不更新有关介质上空间的信息。

应在一个备份会话中导入所使用的全部介质。如果在备份会话中仅添加部分介质，则无法还原跨越到其他介质的数据。

涉及文件库设备时，只能导入以前属于该文件库设备并且以前已导出的文件仓库。如果要从位于目标主机之外主机上的文件库导入介质，则只能将其导入介质库设备。

导入介质

要向介质池添加已由 Data Protector 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。 如果您希望覆盖最初适用于介质的保护值，请使用 OB2_IMPORT_OPTIONS omnirc 变量来应用自定义保护期。有关 omnirc 文件位置以及如何使用选项的信息，请参阅 Omnirc 选项。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，右键单击要向其导入介质的设备，然后单击**导入**以打开向导。
4. 选择要向其添加所导入介质的介质池，然后单击**下一步**。
5. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项（可选）。
6. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 Data Protector。

导入箱盒中的所有介质

要向介质池添加已由 Data Protector 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。要在一步中导入箱盒中的所有介质，请使用选择了**箱盒支持**选项的设备。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击箱盒中的介质所在的介质池。此时将显示“介质”和“箱盒”项。
4. 右键单击**箱盒**项，然后单击**导入箱盒**以打开向导。
5. 选择库中要用其执行操作的驱动器，然后单击**下一步**。
6. 指定新介质的说明（可选），或保留已设置的**自动生成**选项，然后单击**下一步**。
7. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项（可选）。
8. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 Data Protector。

导入箱盒中的单个介质

要向介质池添加介质，以使您以后可以浏览可供恢复的数据时，可导入已由 Data Protector 使用的介质。要导入箱盒中的介质，请使用选择了**箱盒支持**选项的设备。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击箱盒中的介质所在的介质池。此时将显示“介质”和“箱盒”项。
4. 右键单击**介质**项，然后单击**导入**以打开向导。
5. 选择目标介质所在的库的驱动器和插槽，然后单击**下一步**。
6. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项（可选）。
7. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 Data Protector。

导入库设备中的介质

要向介质池添加已由 Data Protector 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。如果使用库设备，则可以使用 Ctrl 键选择多个插槽，并在一步中格式化多个介质。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，展开库设备，然后单击**插槽**。
3. 在结果区域中，选择要导入的介质所在的插槽。
4. 右键单击所选插槽，然后单击**导入**以打开向导。
5. 选择交换器从中将加载要导入的介质的库的驱动器，然后单击**下一步**。
6. 选择要向其添加导入的介质的介质池，然后单击**下一步**。
7. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项（可选）。
8. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 Data Protector。

导出和导入含有加密备份的介质

要将加密备份中的数据恢复到不同 Data Protector 单元中的客户机，需要将介质和加密密钥导入到目标 Cell Manager，如以下各节所述。

- 没有 CMMDB 的 Cell Manager 环境或 MoM 环境
- 有 CMMDB 的 MoM 环境

> **注意**Data Protector 还通过命令行界面 (CLI) 提供加密密钥的高级手动管理（如使密钥过期、重新激活、导出、导入和删除密钥）。有关详细信息，请参阅 omnikeytool 手册页或《Data Protector 命令行界面参考》。

没有 CMMDB 的 Cell Manager 环境或 MoM 环境

在不使用本地 MMDB 的 Cell Manager 环境中或 MoM 环境中，执行以下步骤可导出和导入含有加密备份的介质：

1. 在原始 Cell Manager 上，从 IDB 导出介质。此操作还会将相关的加密密钥从密钥库导出到默认导出加密密钥目录下的 mediumID.csv 文件中。
2. 将 mediumID.csv 文件传输到目标 Cell Manager，并将其放置到默认导入加密密钥目录中。
3. 将导出的介质插入目标 Cell Manager 将使用的驱动器中。
4. 在目标 Cell Manager 上导入该介质。此操作还可从 mediumID.csv 文件中导入密钥。

> **注意**如果密钥文件不存在，则仍可导入介质，但目录导入将因缺少解密密钥而中止。

有 CMMDB 的 MoM 环境

在使用 CMMDB 的 MoM 环境中，MoM Manager 存储所有介质信息。但是，每个 Cell Manager 上的本地密钥库存储 CDB 和介质使用的加密密钥 ID。请注意，所有介质管理操作都需要在 MoM Cell Manager 上完成。

要在 CMMDB 位于 MoM Manager 上的情况下导出和导入含有加密备份的介质，请完成以下步骤:

1. 从 CMMDB 导出介质。密钥 ID 将导出到默认导出加密密钥目录下的 mediumID.csv 文件中。
2. 将 mediumID.csv 文件传输到目标 Cell Manager，并将其放置到默认导入加密密钥目录中。
3. 从 MoM Manager 中，从带库弹出介质。
4. 将介质从原始介质池移至目标介质池，后者与目标单元中的某个驱动器关联。此操作还可导入目录。
5. 将导出的介质插入目标 Cell Manager 将使用的驱动器中。
6. 在目标 Cell Manager 上导入该介质。此操作还可从 mediumID.csv 文件中导入密钥。

复制介质

Data Protector 介质复制功能使您能够在执行备份后复制介质。介质复制是创建包含备份的介质的精确副本的过程。可以将副本或原始介质移至一个安全位置用于归档或保管，并在站点上保留其他介质集用于恢复。

需要两个设备，一个用于源介质，一个用于目标介质。还可以在具有多个驱动器的库设备中复制介质。在这种情况下，使用一个驱动器用于源介质，另一个用于目标介质。

- 源介质和目标介质必须属于同一介质类型。
- 如果目标介质是具有数据保护的 Data Protector 介质，则首先必须回收介质，然后再将其格式化。

以下限制适用：

- 可以对介质（源介质）制作多个副本（目标介质），但不能对介质副本制作副本。
- 只能复制位于 Data Protector 中的介质（设备中的介质）。
- 由于介质复制旨在对通常移至不同位置的介质制作准确副本，因此文件库不支持此功能。要在文件库中制作数据的副本，请使用对象副本功能。
- 介质复制操作对自由池中的介质不可用。
- 受 NDMP 服务器控制的 NAS 设备的设备并发限制为 1。
- NDMP-Celerra 备份会话不支持介质复制。

何时复制介质

只要备份会话完成，即可复制介质。但是，需要考虑将用于复制介质的设备的可用性。建议等待所有使用特定设备的备份完成，然后再使用这些设备进行介质复制。

复制介质的结果

复制介质的结果是两个完全相同的介质集 — 原始介质集和副本。其中任何一个都可用于还原。

复制源介质之后，Data Protector 将其标记为不可追加，以防止追加新备份。（这一点导致原始备份与其副本不同。）随后将副本也标记为不可追加。

从副本还原

默认情况下，Data Protector 从原始介质集还原数据。但是，如果原始介质集不可用，但副本可用，则可使用副本进行还原。

如果还原期间设备中既没有原始介质集也没有副本，则 Data Protector 会发出一个装载请求，其中显示原始介质集和副本都是还原所需的介质。可以使用其中任意一个。

如果使用独立设备执行还原，则可以选择从副本而非从原始介质集还原。为此，请在将用于还原的设备中插入副本，或选择含有副本的设备。但是，如果使用库设备执行还原，并且原始介质集位于库中，则 Data Protector 将使用它进行还原。

> **注意**复制介质时，有可能目标介质在源介质之前达到磁带末尾。如果以流式传送模式写入源介质，并且在繁忙的系统上或通过负载繁重的网络制作副本（这两种情况会产生空白空间，磁带在此处停止并再次启动），则会发生这种情况。通过在格式化介质时启用磁带填充，可以阻止这种情况发生。

复制介质

可以复制介质用于归档或保管。需要单独启动每个介质的复制，因为在一个介质复制会话中只能复制一个介质。

在独立设备中复制介质

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击含有要复制的介质的设备，然后单击**复制**。
3. 选择目标介质所在的设备（库的驱动器和插槽），然后单击**下一步**。
4. 选择要向其添加介质副本的介质池，然后单击**下一步**。
5. 指定介质副本的说明和位置（可选），然后单击**下一步**。
6. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

> **提示**如果目标介质具有 Data Protector 可识别的其他格式 (tar 和 OmniBack I 等等) 或如果这些介质是不受保护的 Data Protector 介质，则使用“强制操作”选项。

7. 单击**完成**以开始复制，然后退出向导。

“会话信息”消息显示介质复制操作的状态。

在库设备中复制介质

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中的**介质**下，展开**池**，然后展开含有要复制的介质的介质池。右键单击介质，然后单击**复制**以打开向导。
3. 为要复制的介质选择驱动器，然后单击**下一步**。如果带库只有一个驱动器，则跳过此步骤。
4. 选择目标介质所在的设备（库的驱动器和插槽），然后单击**下一步**。
5. 选择要向其添加介质副本的介质池，然后单击**下一步**。
6. 指定介质副本的说明和位置（可选），然后单击**下一步**。
7. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

> **提示**如果目标介质具有 Data Protector 可识别的其他格式 (tar 和 OmniBack I 等等) 或如果这些介质是不受保护的 Data Protector 介质，则使用“强制操作”选项。

8. 单击**完成**以开始复制，然后退出向导。

“会话信息”消息显示介质复制操作的状态。

自动介质复制

自动介质复制是为包含备份的介质创建副本的自动化过程。与手动启动的介质复制相比，要外注意一些额外限制：

- 无法使用独立设备进行自动介质复制；而只能使用库设备。

  无法使用磁盘备份 (B2D) 设备进行自动介质复制。
- NDMP-Celerra 备份会话不支持自动介质复制。

自动介质复制

首先，创建自动介质复制规范。自动介质复制会话开始时，Data Protector 会根据自动介质复制规范中指定的参数生成介质列表，作为源介质。对于每个源介质，都会选择要将数据复制到的目标介质。目标介质从源介质所在的同一介质池、自由池或库内的空白介质中选择。

对于每个源介质，Data Protector 都会从您在自动介质复制规范中指定的设备中选择一对设备。自动介质复制功能提供其自己的负载均衡。Data Protector 通过利用尽可能多的设备和选择本地设备（如果其可用），尝试充分利用可用的设备。

会话开始的时候锁定设备。那时不可用的设备就不能用于会话中，因为会话开始后即无法锁定设备。请注意，对于每种介质类型必须至少有一对设备可用，整个会话才能成功完成。如果无法锁定会话必需的最少设备数，则会话将失败。

源介质定义目标介质的目标池。这意味着复制的介质将属于与原始介质相同的池。

副本的默认保护期与原始保护期相同。创建或修改自动介质复制规范时，可以设置不同的保护期。

自动介质复制功能不处理装载请求或清除请求。如果收到装载请求，则中止相关的介质对，但会话将继续。自动介质复制会话完成之后，可以手动复制未复制的介质。

如果发生介质错误，则该自动介质复制会话中将避免使用出错的设备。但是，如果没有其他设备可用，则将重新使用该介质。

自动介质复制的类型

自动介质复制分为两种类型：备份后介质复制和计划的介质复制。

- 备份后介质复制

  备份后介质复制发生在完成备份会话之后。它复制该特定会话中使用的介质。
- 计划的介质复制

  计划的介质复制发生在用户定义的某个时间。不同备份规范中使用的介质可以在单个会话中复制。创建自动介质复制规范来定义要复制的介质。

配置备份后介质复制

备份后介质复制是在备份会话结束之后为特定备份会话中所使用的介质创建副本的一个过程。

> **注意**如果中止备份会话，则即使只有一部分对象成功完成，也会启动备份后介质复制会话。

以下限制适用：

- 只能使用库设备。
- 源介质和目标介质必须属于同一类型。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**自动操作**，然后单击**添加备份后介质选项**以打开向导。
3. 在“备份规范”下拉列表中，选择要复制其介质的备份规范。在“介质操作类型”下拉列表中，选择**介质复制**，然后单击**下一步**。
4. 选择将使用的源设备和目标设备。对于每种介质类型，至少必须有一对设备（一个源设备和一个目标设备）。单击“下一步”。
5. 指定副本数、操作之后是否自动弹出介质以及目标介质的位置和保护。单击**完成**退出向导。

配置计划的介质复制

计划的介质复制是在计划时间为特定备份会话中使用的介质创建副本的一个过程。可以在一个会话中计划多个复制操作。如果有足够的设备可用，将同时复制这些介质。否则，将按顺序复制这些介质。

以下限制适用：

- 只能使用库设备。

- 源介质和目标介质必须属于同一类型。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**自动操作**，然后单击**添加计划的介质操作**以打开向导。
3. 在“介质操作名称”文本框中，键入操作的名称。在“介质操作类型”下拉列表中，选择**介质复制**，然后单击**下一步**。
4. 选择将使用的源设备和目标设备。对于每种介质类型，至少必须有一对设备（一个源设备和一个目标设备）。单击“下一步”。
5. 指定要从中搜索备份会话的时间范围。单击“下一步”。
6. 指定要复制的备份的备份规范。单击“下一步”。
7. 指定源介质的所需状况和保护。单击“下一步”。
8. 指定副本数、操作之后是否自动弹出介质以及目标介质的位置和保护。单击**完成**退出向导。或者，您可以使用计划程序计划介质复制。

扫描设备

扫描设备可更新有关设备中介质的 Data Protector 信息，或在手动更改介质位置之后更新该信息。

完成以下步骤：

1. 在上下文列表中，单击“设备和介质”。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，右键单击要扫描的设备，然后单击**扫描**。

此时“会话信息”消息将显示扫描操作的状态。

扫描库设备中的介质

扫描库的所选插槽中的介质可更新有关设备中介质的 Data Protector 信息。

根据所选插槽的数量，扫描可能需要花费一些时间。Data Protector 必须将每个插槽中的介质加载到驱动器中，然后读取介质头。

可以使用 Ctrl 键选择多个插槽，并在一步中扫描多个介质。但是，只能使用一个驱动器。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，双击库设备，然后双击**插槽**。
4. 在结果区域中，选择含有要扫描的介质的插槽。
5. 右键单击所选插槽，然后单击**扫描**以打开向导。
6. 选择交换器将从中加载要扫描的介质的带库的驱动器。
7. 单击**完成**以开始扫描，然后退出向导。

此时“会话信息”消息将显示扫描操作的状态。

> **提示**如果启用了条形码读取器支持选项，则可以使用**条形码扫描**选项快速扫描 SCSI 库。

扫描库设备中的驱动器

扫描库设备的驱动器可更新有关驱动器中介质的 Data Protector 信息。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，双击要扫描其驱动器的库设备，然后双击目标**驱动器**图标。
4. 右键单击要扫描的驱动器，然后单击**扫描**。

此时“会话信息”消息将显示扫描操作的状态。

激活条形码读取器支持

如果 SCSI 库设备使用含条形码的介质，则 Data Protector 可以使用条形码提供以下条形码支持：

- 识别前缀为 CLN 的磁带。
- 按介质的条码引用介质。Data Protector 显示介质条形码作为介质说明的前缀。
- 使用介质条码快速扫描库存储库的插槽中的介质。

提示如果在库属性中选择**在初始化时将条形码用作介质标签**选项，则默认情况下在初始化介质期间将启用**介质说明**选项中的**使用条形码**选项。如果未选择此选项，则默认选项为“自动生成”。Data Protector 自动格式化介质时将使用默认选项。

注意单元中的所有条码都必须唯一，而不考虑介质类型或有多个库这一事实。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，右键单击目标库设备，然后选择**属性**。此时将打开带库设备的“属性”页。
3. 单击**控制**选项卡，然后选择**条码读取器支持**选项。
4. 要在每次用此库初始化介质时将条形码写入到磁带上的介质头中，请选择**在初始化时将条形码用作介质标签**选项。
5. 单击**应用**确认。

扫描库设备的条形码

使用**条形码扫描**选项可快速扫描 SCSI 库。这比扫描无条码功能的存储库快得多。

要完成以下步骤，必须启用“条形码读取器支持”选项:

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，右键单击目标库设备，然后单击**条码扫描**。

此时“会话信息”消息将显示条码扫描操作的状态。

管理介质 - 其他功能

本主题提供有关管理以下介质功能的信息:

搜索和选择介质

可以搜索和选择介质池中或库设备中的介质。还可以使用“介质列表”报告列出介质。使用此功能可以定位和选择特定介质，而不浏览介质的整个列表。

介质选择对保管用途特别有用，如将上周写入的所有介质移至保管库。

在介质池中搜索和选择介质

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，右键单击介质池，然后单击**选择介质**。此时将显示“选择介质”对话框。
4. 根据介质说明、介质位置、会话、时间范围、保护搜索和选择介质，或使用“组合选择”选项。

在库设备中搜索和选择介质

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，双击库设备，右键单击**插槽**，然后单击**选择介质**。此时将显示“选择介质”对话框。
4. 根据介质说明、介质位置、会话、时间范围、保护搜索和选择介质，或使用“组合选择”选项。

使用介质列表报告搜索介质

完成以下步骤：

1. 在上下文列表中，单击**报告**，然后单击**任务**选项卡。
2. 在范围窗格中，展开**池和介质**，然后单击**介质列表**以打开向导。
3. 按照向导操作，指定搜索的标准。单击**完成**以显示搜索的结果。

预分配介质进行备份

可以指定介质池中的介质将用于备份的顺序。此顺序称为预分配列表。配置备份时，指定预分配列表。预分配列表的用途是控制哪些介质将用于备份会话。必须在每次备份之前将预分配列表与可用介质相匹配。

还可以在使用对象副本或对象合并功能时预分配介质。

根据介质池的分配策略，Data Protector 以两种不同方式行动：

- 如果将预分配列表与“严格”介质分配策略结合使用，则 Data Protector 预计将以该顺序提供备份设备中的介质。如果介质不可用，则 Data Protector 将发出装载请求。如果在 SCSI 交换器中加载预分配列表中提及的介质，则 Data Protector 将自动处理介质顺序。
- 如果将预分配列表与**宽松**介质分配策略结合使用，则首先使用预分配列表中的介质。如果介质不可用，则使用带库中的任何适用介质。

以下内容可能会提供其他信息：

- 还可以在使用对象副本或对象合并功能时预分配介质。
- 默认情况下，文件库介质池的介质使用策略为不可追加。由于此策略对文件库有益，因此建议不要更改它而使用文件库设备介质的预先分配列表。

要在所保存的备份规范中预先分配介质，请按照以下这些步骤进行操作：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如“文件系统”）。此时将显示所保存的全部备份规范。
3. 双击适当的备份规范，然后单击“目标”选项卡。
4. 在“目标”页中，右键单击选择用于备份的设备，然后单击**属性**。
5. 在“设备属性”对话框中，从“介质池”下拉列表中选择所需的介质池。
6. 在“prealloc 列表”下，单击**添加**。

   此时将显示所选介质池中介质的列表。
7. 选择某个介质，然后单击**添加**。
8. 对所需的所有介质重复步骤 6 和 7。完成后，单击**确定**，返回“目标”属性页。
9. 如果有多个设备用于备份，则重复步骤 4 到 8。
10. 单击**应用**保存更改。

回收介质

要取消对介质上所有已备份数据的数据保护，以使 Data Protector 可以在后续备份期间覆盖介质时，可循环回收（取消保护）介质。回收并不真正更改介质上的数据；它只是告知 Data Protector 此数据不再受保护。

回收可取消对介质上所有对象的保护。这还包括位于其他介质上的相同对象和会话中的数据。

回收操作对自由池中的介质不可用。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。此时将在结果区域中显示所配置介质池的列表。
3. 双击含有要循环回收的介质的介质池。
4. 右键单击目标介质名称，然后单击**回收**。还可以使用 Ctrl 或 Shift 键同时选择多个介质。

操作完成后，将介质的保护设置为“无”。

从介质导入编目

从介质导入目录可将文件名和文件版本等详细信息写入 IDB 中，从而使您能够浏览可供还原的文件和目录。

如果特定对象的编目保护已到期，并且不能再浏览其文件和目录，则还可以使用“导入编目”。如果 IDB 中已存在有关所指定介质的详细信息，则将不复制这些数据。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击要从中导入目录的介质所在的介质池。
4. 右键单击该介质，然后单击**导入编目**。
5. 如果有更多驱动器，则选择要向其导入介质的库驱动器，然后单击**下一步**。
6. 选择符合需要的**日志记录**选项。
7. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，可以浏览可供还原的文件和目录。

验证介质

验证介质可检查介质上的数据格式是否有效，并在 IDB 中更新有关介质的信息。只能验证驻留的 Data Protector 介质。根据所使用的备份设备和介质，验证可能会花费相当长的一段时间。

可以验证介质副本，然后再将其保管起来。如果备份期间报告了错误，也可以验证介质以检查备份是否可用。

验证介质时，Data Protector 执行以下操作：

- 检查具有有关介质信息（介质标识、说明和位置）的 Data Protector 头。
- 读取介质上的所有块，并验证块格式。
- 如果备份期间使用了 **CRC 检查**选项，则重新计算 CRC，并将它与介质上存储的对应值进行比较。在这种情况下，备份数据本身在每个块中一致。此检查级别的可靠性很高。

  如果未使用“CRC 检查”选项而通过了验证操作，则这意味着已读取了介质上的所有数据。介质未导致读错误，因此磁带的硬件状态至少可接受。可以将此检查级别视为部分判断标准。

在独立设备中验证介质

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击含有要验证的介质的设备，然后单击**验证**。
3. 在结果区域中，可以选择**在操作完成之后弹出介质**选项。单击**完成**验证介质。

   对于独立文件设备跳过此步骤。

此时“会话信息”消息将显示验证的状态。

在带库设备中验证介质

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中的**设备**下，展开库设备，然后展开**插槽**。右键单击含有要验证的介质的插槽，然后单击**验证**。
3. 在结果区域中，选择用于执行验证的库驱动器，然后单击**完成**。

此时“会话信息”消息将显示验证的状态。

移动介质

如果要重新组织备份并重新安排每个池的用途，则可以将介质从一个介质池移至相同类型的另一个介质池。要使用作为另一个介质池默认设备的设备中的介质时，此操作也很有用。

无法将介质移至空闲介质池。使用自由池时，在两个实例中移动介质（行为取决于所选的空闲池选项）：

- 选择（分配）用于备份的介质时，将这些介质从自由池移至常规池。
- 介质保护到期后，将介质从常规池移至自由池。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击要从中移动介质的介质池。此时将显示各自池中介质的列表。
4. 右键单击要移动的介质，然后单击**移动到池**以打开向导。还可以使用 Ctrl 或 Shift 键同时选择多个介质。
5. 选择要向其移动介质的介质池。
6. 单击**完成**以移动介质，然后退出向导。

提示要将介质移至另一个单元，请从一个单元导出介质，然后将其导入另一个单元。

导出介质

要将介质移至另一个 Data Protector 单元时，导出该介质。导出将从 IDB 中删除有关介质及其内容的信息。Data Protector 将不再认为此介质存在。介质上的数据保持不变。请注意，仅删除有关介质的信息。介质保留在原位，必须由操作员手动删除。

建议不要手动导出依赖日常维护来清理存储的备份到磁盘 (B2D) 设备上的介质，因为手动导出所有介质至关重要。允许通过日常维护来清理存储。

如果导出原始介质并仍有副本，则其中一个副本变为原本。

导出介质之前必须通过回收介质取消其保护。

应导出同一备份会话的所有介质。如果会话中的数据跨越多个介质，而您仅导出一个介质，则可能无法还原数据。Data Protector 仍知道介质上存在数据，但某些介质不再可用。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击含有要导出的介质的介质池，右键单击介质名称，然后单击**导出**。
4. 确认操作。

池中介质的列表中不再显示所导出的介质。

将编目介质数据复制到 MCF 文件

将与介质相关的编目数据复制到文件可将文件名和文件版本等详细信息写入介质容器格式 (MCF) 文件中，这些文件位于 Cell Manager 上的目录 Data_Protector_program_data\Config\Server\export\mcf （Windows 系统）或 /var/opt/omni/server/export/mcf （UNIX 系统）中。然后可以将这些文件导入另一个其中与介质相关的目录数据可供浏览的 Data Protector Cell Manager 中。

- 由于每个介质可能有大量目录数据，因此建议在一个单独的分区或装载点上存储文件。
- 通过将全局选项中的 EnableMCFCompression 设置为 1 ，可以减小文件的大小。默认情况下禁用压缩。

以下内容可能会提供其他信息：

- 不从原始 Cell Manager 删除与介质相关的目录数据。
- 此操作为每个介质创建一个 MCF 文件。

以下限制适用：

- 只能选择 Data Protector 介质。
- 由于 Data Protector 文件库的性质，无法从一个库导出介质再将其导入另一个库，因此应避免对此类介质执行“将编目复制到文件”和“从文件导入编目”。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后展开**池**。

3. 展开要复制其目录的介质所在的介质池。
4. 右键单击介质，然后单击**将目录复制到文件**。
5. 指定 MCF 文件的输出目录，此文件将包含与介质相关的目录数据。
6. 单击**完成**以开始复制，然后退出向导。

所导出的 MCF 文件可以传输到目标 Cell Manager。

> **提示**通过展开**设备**，右键单击所选设备的插槽，然后执行步骤 5 和 6，可以达到相同的结果。

从 MCF 文件导入编目介质数据

从原始 Cell Manager 中的介质容器格式 (MCF) 文件导入与介质相关的目录数据副本，使您可以浏览目标 Cell Manager 上的文件。

确保要导入的 MCF 文件已从原始 Cell Manager 转移而来，并在当前的 Cell Manager 上可访问。

以下限制适用：

- 从文件导入介质之后，需要有物理介质的操作（例如还原、介质复制）无法使用该介质。要使介质完全可供 Data Protector 操作使用，必须可通过物理方式访问该介质，并且通过使用 Data Protector 介质扫描可扫描到该介质，否则将发出装载请求。

以下内容可能会提供其他信息：

- 从 MCF 文件导入大量介质编目时，请确保导入的所有介质都是恢复链一部分。
- 可以在一个会话中从多种介质池导入不同类型的介质。
- Data Protector GUI 仅显示和允许选择扩展名为 mcf 的文件。目录树中隐藏其他文件。但是，可以通过命令行界面 (CLI) 选择这些文件。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，右键单击**池**，然后单击**从 MCF 文件导入编目**以打开向导。
3. 指定要导入的 MCF 文件。
4. 指定会话的其他选项：默认情况下，选择**如有可能，导入到原始池**选项。可以选择“新池的前缀”或**作为原始副本导入**选项。
5. 单击**完成**以开始导入，然后退出向导。

修改介质说明

介质说明有助于标识介质。说明写入介质上，并存储在 IDB 中。格式化新介质时可添加介质说明。如果在备份期间自动格式化介质，则可能要将自动创建的说明更改为更符合您需要的某些内容。

修改介质说明后，Data Protector 修改 IDB 中而非介质本身上的说明。如果导出介质然后再导入介质，则 IDB 中的说明将替换为介质中的说明。

还会更改介质标签的说明部分，但条码部分仍保持相同。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击含有要更改的介质说明的介质池。此时将显示介质池中介质的列表。
4. 右键单击含有要更改的说明的介质，然后单击**属性**以打开该介质的“常规”属性页。
5. 在“说明”文本框中，键入介质的新说明。
6. 单击**应用**确认。

修改介质位置

介质位于设备之外时，指定介质位置有助于查找介质。位置信息存储在 IDB 中。初始化介质时应输入位置，而将介质移至不同位置（保管），例如场外存储（“Shelf 4-Box 3”）时应修改位置。

位置从不写入介质头。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击含有要更改的介质位置的介质池。此时将显示介质池中介质的列表。
4. 右键单击含有要更改的指定位置的介质，然后单击**更改位置**以打开向导。
5. 指定介质的新位置。
6. 单击**完成**退出向导。

创建位置列表

可以创建常用预定义保管位置的列表。在不同介质管理任务（例如格式化介质时）中为特定介质选择位置时，即出现此预定义保管位置列表。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。

2. 在“编辑”菜单中，单击**位置**。
3. 输入所需的位置，然后单击**添加**按钮。重复此步骤，输入多个位置。
4. 单击**完成**。

设置介质位置优先级如果要还原、复制、合并或验证的对象版本存在于多个介质集上，则任何介质集都可用于操作。默认情况下，Data Protector 自动选择最合适的介质集。通过指定介质位置的优先级可以影响介质集的选择。

如果设置了介质位置优先级，则如果多个介质集同样符合介质集选择算法的条件，则 Data Protector 将使用优先级最高 (优先级 1 为最高，优先级 None 为最低) 的介质集。

可以在还原、对象副本、对象合并或对象验证会话级别取代介质位置优先级。

以下内容可能会提供其他信息：

- 默认情况下，仅当两个或更多介质集的评级相同时，才会考虑介质位置优先级。为使介质位置优先级优先于其他选择因素，请将全局选项 UserSpecifiedMediaPriorityHasHigherImportance 设置为 1。
- 为使介质位置优先级生效，必须指定每个介质的位置。可以对单独或多个介质进行此操作。
- 介质位置优先级不考虑使用介质复制功能获取的副本。仅当原始介质（用作源进行复制的介质）不存在或不能用时，才使用此类副本。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**位置**。
3. 在结果区域中，双击某个位置以显示其属性。
4. 在**位置优先级**下拉列表中，选择一个可用数字，其中 1 表示最高优先级。
5. 单击**应用**确认选择。

保管介质

建议制作备份数据的副本用于保管，并在站点上保留原始介质以便可以进行还原。Data Protector 允许以交互方式创建或自动创建介质上数据的其他副本。

配置备份规范时，需要具备所需的数据保护和编目保护策略集。需要在 Data Protector 中配置保管库。使用指示将从中保留介质的物理位置的名称。完成以下步骤:

1. 在 Data Protector Manager 中，更改要存储的介质的位置。
2. 从设备弹出介质，然后将介质存储在保管库中。

擦除介质

此功能仅对磁光盘可用。使用此功能在备份会话之前擦除磁光盘，并因此可加快备份速度。完成以下步骤：

1. 在上下文列表中，单击“设备和介质”。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，双击含有要擦除的介质的磁光设备。
4. 右键单击该介质，然后单击**擦除**以打开向导。
5. 选择**在操作完成之后弹出介质**选项（可选）。
6. 单击**完成**擦除介质，然后退出向导。

此时“会话信息”消息将显示擦除操作的状态。

检测写保护介质

通过将写入保护开关设置为打开，Data Protector 可以检测和处理通过机械方式保护的介质。

以下操作可以检测和处理写保护介质：

- 只读操作，如列表、扫描和验证。只读操作可检测写保护介质，并在没有任何警告的情况下进行操作。
- 写操作，如初始化、擦除和备份。写操作可检测写保护介质，并会中止会话，或跳过写保护介质。备份会话将写保护介质视为不可用介质，并按照介质分配策略行动。如果分配策略为严格，则发出装载请求。如果分配策略为宽松，则跳过该介质。

对写保护介质的检测和对该介质的写保护状态的所有更改都将被记录到 media.log 文件中。

> **注意**建议不要将写保护介质用于 Data Protector。

装载请求

装载请求是让您向设备中插入介质的一种屏幕提示。通过提供所需介质答复装载请求后，会话即可继续。

Data Protector 在以下情况下会发出装载请求：

- 指定的介质不可用。如果预分配列表用于备份，或恢复所需的介质缺少介质，则会发生此情况。
- 没有合适的介质可用。如果池内当前位于库中的介质不合适，如果独立设备中的介质不合适，或如果设备为空，则会发生此情况。
- 邮件插槽打开。在这种情况下，必须关闭邮件插槽。

Data Protector 将自动选择最适于备份的介质。必须了解为备份选择介质的方式。

库特有的介质管理

Data Protector 为复杂设备（如库）提供某些特定的介质管理任务，以简化对大量介质的管理。

某些任务（例如选择、复制、回收或移动介质以及修改介质位置）遵循标准过程。其他任务（如添加或删除插槽以及放入、弹出、验证、格式化、导入、扫描或擦除介质）可能取决于所使用的设备类型。

在支持条码的库中，Data Protector 可以根据条码生成介质说明，并在初始化期间将其写入磁带上的介质头。

库介质和其他应用程序

库中（尤其是在 ADIC/GRAU 和 StorageTek 等非常庞大的库中）的介质可以由许多应用程序使用，而不仅由 Data Protector 使用，因此必须了解哪些应用程序使用哪些介质以防覆盖介质。

理想情况下，专门将库与 Data Protector 配合使用，并允许 Data Protector 管理完整库。但是，如果有多个应用程序使用库，则应小心谨慎地向 Data Protector 和其他应用程序分配不重叠的介质子集。Data Protector 自身保持独立的介质分配策略。这表示如果已将某个特定的介质分配给 Data Protector (添加到 Data Protector 介质池)，则在其生存期内或直到从 Data Protector 介质池将其删除为止，该介质都受到 Data Protector 的控制。

重要说明对于每种类型的介质，都必须在 Data Protector 中配置一个库。虽然 ADIC/GRAU 或 StorageTek 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。因此，必须在系统中为每种介质类型都创建一个 Data Protector 库。

以下内容可能会有所帮助：

- 对于 ADIC/GRAU DAS 和 StorageTek 库，使用 Data Protector 命令处理介质。如果使用 ADIC/GRAU DAS 或 StorageTek ACS 命令手动处理介质，则 Data Protector 将无法跟踪介质上位置或信息的更改。
- 用 Data Protector 管理整个库。这样将进行集中式管理，其中可以跟踪库中的 Data Protector 和非 Data Protector 介质。
- 为每种介质类型至少创建一个介质池，例如一个池用于 4mm 介质类型，一个池用于 3480 介质类型。根据您所处的环境，可能要创建更多介质池，例如每个部门一个介质池。
- 确保 Data Protector 和其他应用程序不使用相同介质集。

用于库的查询操作

启动 Data Protector 查询操作后，将查询 DAS 或 ACS Library Server 上配置的所有介质，即使在 Data Protector 中将这些介质配置为属于 (同一个物理库的) 多个逻辑 ADIC/GRAU DAS 或 STK ACS 库时也是如此。此外，Data Protector 查询操作还查询在 DAS 或 ACS Library Server 上配置用于 Data Protector 以外应用程序的介质。因此，在 Data Protector 中启动查询操作之后，属于其他逻辑 ADIC/GRAU DAS 或 STK ACS 库的介质（启动查询操作的之外）将被移至启动该查询操作的逻辑 ADIC/GRAU DAS 或 STK ACS 库中。

因此，对于 ADIC/GRAU DAS 或 STK ACS 库，建议不要使用 Data Protector 查询操作。建议使用 Data Protector 添加 volser 操作手动添加 volser，而非使用 Data Protector 查询操作同步 IDB。

注意当不使用 Data Protector，而是使用 ADIC/GRAU DAS 实用程序配置逻辑库时，本节中的信息不适用于 ADIC/GRAU DAS 库的情况。如果使用 ADIC/GRAU DAS 实用程序配置多个逻辑库，则可以在此类库上安全地使用 Data Protector 查询操作。

查询 ADIC/GRAU DAS 和 StorageTek ACSLM 主机

要从服务器获取有关 ADIC/GRAU 或 StorageTek 库中存储库的信息，可以查询 DAS 或 ACSLM 主机（服务器）。查询用服务器的介质数据库的内容做出响应，然后将 IDB 中的信息与存储库中的实际信息进行同步。

如果已使用 GRAU DAS 或 StorageTek ACS 命令管理介质，则此操作非常有用，因为前者会导致与 IDB 的不一致 — Data Protector 不知道库存储库中介质的最新状态。

如果在存储库中对 ADIC/GRAU 库配置了多于 3970 个 volser，则无法成功完成 volser 扫描。解决此问题的方法是配置多个逻辑 ADIC/GRAU

库，以便将大型存储库中的插槽隔离为多个较小的存储库。

> **重要说明**对于 ADIC/GRAU DAS 和 STK ACS 库，当为同一个物理库配置了多个逻辑库时，建议不要查询 DAS 或 STK ACSLM Server。请手动添加 volser。但是，对于 ADIC/GRAU DAS 库，当不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上进行 Data Protector 查询操作。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在已配置设备的列表中，右键单击要查询的库，然后单击**查询**。

此操作将查询 DAS 或 ACSLM 主机中的信息。

添加插槽

Data Protector 全面支持处理库所用的介质池中的插槽和介质。添加插槽将为存储设备的介质配置一个位置。

在某些库中，配置库后将自动检测和添加插槽。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，右键单击库的名称，然后单击**属性**。
4. 单击“存储库”选项卡，指定要用于 Data Protector 的插槽，然后单击“添加”将插槽添加到列表中。使用短划线可一次输入多个插槽，例如 5-12。

   请确保使用带库所支持的格式。例如，向 SCSI 带库添加插槽时，请勿使用字母或以零开头。
5. 单击**应用**确认。

删除插槽

Data Protector 全面支持处理库所用的介质池中的插槽和介质。删除插槽将阻止Data Protector使用和访问存储库中的插槽。并将从 IDB 中删除有关插槽的信息。

仅支持对任何设备上的空插槽删除介质插槽。

此操作不会影响 GRAU DAS 库中的 volser，而只会从 IDB 中删除特定介质。因此，Data Protector 不知道存在这些介质，并且不使用这些介质。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，右键单击库的名称，然后单击**属性**。
4. 单击**存储库**选项卡，选择要删除的插槽，然后单击**删除**。
5. 单击**应用**确认。

此时插槽列表中不再显示该插槽。

放入介质

放入介质意味着将其以物理方式放入库存储库中，并自动将所添加的介质注册为库的成员。

可以选择要使用的插槽。放入介质不会影响其所属的介质池。

建议使用 Data Protector GUI 放入介质。如果使用设备的控制机构手动放入介质，则 IDB 中的信息将不再一致，并且必须扫描设备以更新此信息。

> **提示**可以在一个操作中将多个介质放入设备中。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中双击带库的名称。
4. 双击**插槽**，以便在结果区域中显示插槽的列表。
5. 右键单击要放入介质的插槽 (或多个插槽)，然后单击“放入”以启动会话。

此时将提示您根据需要将其他介质插入设备。

弹出介质

弹出介质意味着将其以物理方式从存储库插槽转移到带库设备中的插入/弹出区域（也称为邮件插槽）。

建议使用 Data Protector Manager 弹出介质。如果使用设备的控制机构手动弹出介质，则 IDB 中的信息将不再一致。要更新此信息，请扫描设备。

当介质因邮件插槽已满而无法弹出时，Data Protector 将重试该操作，直到邮件插槽变为空闲或直到预定义的时间限制到期为止。此重试期间，其他会话可访问机械手。

执行弹出期间，其他会话无法使用所指定的任何介质。

批量弹出介质

通过单一操作可从库中弹出多个介质。介质已满时，Data Protector 会指示您从邮件插槽取出介质，为选择要弹出的其他介质腾出空间。

预定义介质弹出

对于某些操作（如自动介质复制），可以在会话完成之后指定是否将自动弹出介质。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中双击带库的名称。
4. 双击**插槽**项，以便在结果区域中显示插槽的列表。
5. 右键单击要弹出的插槽 (或多个插槽)，然后单击“弹出”以打开向导。
6. 指定介质的新位置（可选）。
7. 单击**完成**弹出介质，然后退出向导。

此时“会话信息”消息将显示弹出操作的状态。

擦除库设备中的介质

擦除介质仅对磁光盘可用。只能在备份会话之前擦除磁光盘介质。这样可加快备份速度。

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，双击含有要擦除的介质的磁光设备。此时将显示“插槽”和“驱动器”项。
4. 双击**插槽**。
5. 右键单击含有擦除的介质的插槽，然后单击**擦除**以打开向导。
6. 在交换器将从中加载要擦除的介质的库中选择驱动器。
7. 单击**完成**擦除介质，然后退出向导。

此时“会话信息”消息将显示擦除操作的状态。

手动添加 volser

对于 ADIC/GRAU DAS 或 STK ACS 库，可以手动将 volser 添加到 Data Protector 中所配置的库，而非对库进行查询。对于 ADIC/GRAU DAS 或 STK ACS 库，当为同一个物理库配置了多个逻辑库后，建议采用此方法将 volser 添加到在 Data Protector 中所配置的库。但是，对于 ADIC/GRAU DAS 库，在不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上使用 Data Protector 查询操作代替手动添加 volser。

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，浏览要向其添加 volser 的库，然后将其展开。
3. 右键单击**插槽**，然后从弹出菜单中选择**添加 Volser**。
4. 在“前缀”文本框中，输入 volser 的前缀。通常由三个字母组成。

   在“从”文本框中，指定要添加到库的 volser 范围的起始数字。

   在“到”文本框中，指定要添加到库的 volser 范围的结束数字。
5. 单击“完成”，将 volser 添加到 IDB。

保护 Data Protector 环境

在 Data Protector 2019.08 及更高发布中，所有通信均通过传输层安全性 (TLS) 协议版本 1.2 进行。要在客户机和 Cell Manager 之间配置信任，必须在安装之前满足特定的先决条件。所有命令和脚本执行均通过 Cell Manager 路由。集中化命令执行可确保控制和数据都通过安全的 TLS 通道发送，从而保证数据完整性。此外，可以在 Data Protector 客户机主机之间执行命令，但不属于 Data Protector 单元的主机将无法进行通信，这样可显著降低安全漏洞的风险。

本主题包括以下信息:

- 安全注意事项: 本节提供有关可用于提高 Data Protector 安全性的高级设置，以及必须考虑的注意事项的信息。
- 安全建议和法律免责声明: 本节提供进一步增强 Data Protector 安全性所需遵循的准则。

安全注意事项

以下章节将介绍 Data Protector 的安全性元素。它们描述了可用于提高 Data Protector 安全性的高级设置，以及必须考虑的注意事项。

因为在整个环境中提高安全性需要进行其他设置，所以许多安全性功能无法在默认情况下启用。

以下章节描述的注意事项不仅在更改安全设置时适用，而且在配置新用户、添加客户机、配置应用程序代理或进行其他更改时也必须遵守。任何对安全设置的更改都可能对整个单元有效，应小心地计划这些更改。

安全性层

必须在不同的安全性关键层上计划、测试和实施安全性，以确保 Data Protector 的安全操作。这样的层是 Data Protector 客户机、Cell Manager 和用户。本节说明了如何在这些层上配置安全性。

客户机安全性

安装在单元的客户机上的 Data Protector 代理程序提供了许多强大的功能，例如访问系统上的所有数据。请注意，这些功能仅适用于在“单元授权机构” (Cell Manager 和安装服务器) 上运行的进程，并拒绝所有其他请求。

在保证客户机的安全性前，确定受信任主机列表是很重要的。此列表必须包括：

- Cell Manager
- 相关的安装服务器
- 对于某些客户机，还要包括将远程访问机械手的客户机列表。

> **重要说明**列表必须包含所有可能发出连接的主机名（或 IP 地址）。如果以上任意客户机是多宿主的（有多个网络适配器和/或多个 IP 地址）或是群集，则可能需要多个主机名。
> 如果单元中的 DNS 配置不统一，则可能需要考虑其他注意事项。

虽然并不总是需要保证单元中每个客户机的安全性，但是保证其他客户机将信任的计算机自身的安全性却很重要：

- Cell Manager / Manager-of-Managers
- 安装服务器
- 介质代理客户机

> **注意**不需要将用户界面客户机添加到受信任客户机的列表中。您可以使用 GUI 访问完整的 Data Protector 功能或仅访问特定环境，具体取决于用户权限。

Data Protector 用户

配置 Data Protector 用户时请考虑以下重要方面：

- 某些用户权限非常强大。例如，用户配置和客户机配置用户权限允许用户更改安全性设置。还原到其他客户机用户权限也非常强大，尤其当 (但不仅当) 与“作为 root 备份”或“作为 root 还原”用户权限结合时。
- 甚至不太强大的用户权限也有内在的风险与自身相关。可以配置 Data Protector 以限制某些用户权限，从而降低这些风险。
- Data Protector 仅带有几个预定义的用户组。建议在 Data Protector 环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。
- 除了按用户组成员资格分配用户权限以外，可能要进一步将某些用户组的操作设定为仅限于 Data Protector 单元的特定系统。可以通过配置 user_restrictions 文件来实施该策略。
- 用户配置与用户验证相关联。增强的验证如果没有详细的用户配置也没有价值，反之亦然 - 即使最详细的用户配置如果没有增强的验证也没有意义。
- 在 Data Protector 用户列表中没有“薄弱”的用户，这一点很重要。

注意用户规范的主机部分是最强的部分（尤其在有增强验证的情况下），而用户和组部分则无法可靠地进行验证。对于具有强大用户权限的任何用户，均应针对其将用于 Data Protector 管理的特定客户机进行配置。如果使用多个客户机，则为每个客户机添加一个条目。切勿将用户的“组/域”配置为“<任意>”，或将“客户机”配置为“<任意>”。另外，确保不允许不可信用户登录任何这些系统。

Cell Manager 安全性

Cell Manager 安全性很重要，因为 Cell Manager 可访问单元中的所有客户机和所有数据。

Cell Manager 的安全性可以通过严格的主机名检查功能来增强。但是，重要的是 Cell Manager 同时还要作为客户机受到保护，并且要仔细配置 Data Protector 用户。

虽然并不总是需要保证单元中每个客户机的安全性，但是保证其他客户机将信任的计算机自身的安全性却很重要：这些计算机在 Cell Manager、安装服务器和介质代理客户机之外。

请参阅安全建议和法律免责声明以保护 Cell Manager。

严格检查主机名

默认情况下，Cell Manager 使用相对简单的方法验证用户。它使用已启动用户界面或应用程序代理的客户机已知的主机名。此方法配置起来较简单，在将安全性视为“咨询”（例如，不期望恶意攻击）的环境中提供了合理的安全性级别。

而另一方面，严格主机名检查设置提供了增强的用户验证。这种验证使用由 Cell Manager 根据从连接中获得的 IP 地址进行反向 DNS 查询所解析的主机名。这施加了以下限制和注意事项：

限制

- 基于 IP 的用户验证的强度仅相当于网络中的防欺骗保护。安全性设计人员必须确定现有网络提供的防欺骗安全性级别是否足以满足特定的安全性要求。通过使用防火墙、路由器、VPN 等对网络分段可以增强防欺骗保护。
- 特定客户机内用户间的分离不如客户机间的分离强大。在高度安全的环境中，在同一客户机内一定不能将普通用户与强大用户混合在一起。
- 用户规范中使用的主机无法配置为使用 DHCP，除非将它们绑定到固定 IP 并在 DNS 中进行配置。

请意识到这些限制，以便正确地评估使用严格主机名检查可以达到的安全性级别。

主机名解析

在以下情况下，Data Protector 用于验证的主机名可能在默认用户验证与严格主机名检查间有所区别：

- 反向 DNS 查询返回不同的主机名。这可能是有意所为，或表明客户机或反向 DNS 表配置错误。
- 客户机是多宿主的（有多个网络适配器和/或多个 IP 地址）。该注意事项是否适用于特定的多宿主客户机，取决于它在网络中的角色及在 DNS 中对其进行配置的方式。
- 客户机是群集。

通过此设置启用的检查的性质可能要求重新配置 Data Protector 用户。您必须检查 Data Protector 用户的现有规范，以查看他们是否可能受到以上某种原因的影响。根据不同情况，可能需要更改现有规范，或添加新规范，以包含所有可能发出连接的 IP。

请注意，如果启用严格的主机名检查时必须修改用户规范，则当恢复到默认用户验证时也必须重新配置用户。因此，建议确定想要使用的用户验证并坚持使用下去。

可靠的反向 DNS 查询的先决条件是安全性的 DNS 服务器。您必须防止对所有未授权人员的物理访问和登录。

用 IP 而不是主机名配置用户，您可以避免一些 DNS 相关的验证问题，但是这种配置更难以维持。

要求

增强的验证不会自动对某些内部连接授予访问权限。因此，使用此验证后，必须为以下每种程序添加新用户：

- Windows 客户机中的任何应用程序代理 (OB2BAR)。针对 Windows 客户机，要求为安装了应用程序代理的每个客户机添加用户 SYSTEM、NT AUTHORITY、client。请注意，如果某客户机上的 Data Protector Inet 服务配置为使用特定帐户，则该帐户必须已配置。

启用功能

要启用严格主机名检查，请将 StrictSecurityFlags 全局选项设置为 **0x0001**。

“启动备份规范”用户权限

仅启动备份规范用户权限不能使用户使用 GUI 中的备份上下文。用户可从命令行使用 omnib 命令与 -datalist 选项启动备份规范。

> **注意**通过结合启动备份规范和启动备份用户权限，用户可在 GUI 中查看配置的备份规范并能够启动备份规范或交互式备份。

并不总是希望允许用户执行交互式备份。要仅允许还拥有保存备份规范权利的用户进行交互式备份，请将 StrictSecurityFlags 全局选项设置为 **0x0200**。

隐藏备份规范的内容

在高安全环境中，可能会将所保存备份规范的内容视为敏感甚至保密信息。可以将 Data Protector 配置为对所有用户隐藏备份规范的内容，具有保存备份规范用户权限的用户除外。为此，请将 StrictSecurityFlags 全局选项设置为 **0x0400**。

主机信任

主机信任功能仅需在有限数量的客户机内将数据从一个客户机恢复到其他客户机，从而减小了将“恢复到其他客户机”用户权限授予用户的需要。可以定义一组主机，彼此信任对方的数据。主机信任通常在以下情况下使用：

- 用于群集中的客户机（节点和虚拟服务器）。
- 如果客户机的主机名更改且旧备份对象的数据需要还原。
- 如果由于 DNS 问题导致客户机主机名与备份对象不匹配。
- 如果用户拥有多个客户机且需要将数据从一个客户机还原到另一个客户机。
- 将数据从一个主机迁移到另一个主机时。

配置主机信任

要配置主机信任，请在 Cell Manager 上创建文件 Data_Protector_program_data\Config\Server\cell\host_trusts（Windows 系统）或 /etc/opt/omni/server/cell/host_trusts（UNIX 系统）。彼此信任的主机组定义为包含在波形括号中的主机名列表。例如：

```
GROUP="cluster.domain.com" { cluster.domain.com node1.domain.com node2.domain.com } GROUP="Bajo" { computer.domain.com anothercomputer.domain.com }
```

监视安全事件

如果在使用 Data Protector 时遇到问题，可使用日志文件中的信息来确定问题。例如，记录的事件可帮助您确定配置错误的用户或客户机。

客户机安全性事件

客户机安全事件将记录在默认的 Data Protector 日志文件目录的单元中每个客户机上的 inet.log 文件中。

Cell Manager 安全事件

Cell Manager 安全事件将记录在默认的 Data Protector 服务器日志文件目录中的 security.log 文件中。

安全建议和法律免责声明:

> **重要说明**Micro Focus 鼓励客户实施磁盘加密 (Micro Focus 未提供此功能)。若未实施磁盘加密，您的系统可能面临更多的安全风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

> **重要说明**Micro Focus 鼓励客户针对各种网络级别和操作系统级别攻击部署安全控制，Micro Focus 未提供这些安全控制。若未实施这些控制，您的系统可能面临更多的安全风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

> **重要说明**Micro Focus 鼓励客户验证是否按照适用于客户的特定法律或监管标准处理任何 PII，Micro Focus 未提供这些标准。若未实施上述措施，您的系统可能面临更多的安全风险和/或隐私风险。您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

- Micro Focus 强烈建议将 Data Protector 管理员配置为 Cell Manager 计算机上的唯一用户。删除 Cell Manager 上的所有其他用户 (如果已配置)。
- 强烈建议您不要在安装了 Cell Manager 的计算机上安装任何其他应用程序或软件，平台供应商建议的安全补丁和更新除外。
- Micro Focus 鼓励您严格遵循 Data Protector Cell Manager 或客户机平台供应商提供的所有建议，包括但不限于安装重要的操作系统更新、安全补丁和帐户锁定设置。
- 要响应在 Data Protector 或 Data Protector 使用的第三方组件中发现的安全漏洞，请参阅 Micro Focus 支持门户上的最新安全公告。根据 Data Protector 产品和相关文档类型过滤您的搜索。
- Micro Focus 为每个新的 Data Protector 版本提供了增强的安全性，因此建议客户始终升级到最新版本，以从所有安全功能中获益。

- 对于基于磁盘的 Data Protector 目标设备，如文件库、介质库、StoreOnce 软件和智能缓存，建议使用平台提供的磁盘加密，例如 Windows 平台上的 bitlocker 加密。
- 用户不应访问任何可信客户机（Cell Manager、安装服务器、MA 和机械手客户机）。甚至允许匿名登录或 ftp 访问也可能为整体安全性带来严重的风险。
- 实际上必须严防未授权或不受信任的人员访问介质和磁带库（以及它们连接的客户机）。
- 备份、还原、对象或介质复制、对象合并或对象验证期间，通常会通过网络传输数据。如果使用网络分段无法完全分离不受信任的网络，请使用本地连接的设备、Data Protector 加密技术或自定义的编码库。请注意，更改编码库后应执行完整备份。
- 通过将 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode 参数的值设置为 1 来启用 **SafeDllSearchMode**。
- 如果您不使用任何此类脚本，请通过将全局选项 **SmDisableScript** 值设置为 **1** 来禁止在整个 Cell Manager 环境中执行 post-exec 和 pre-exec 脚本。但是，如果您在某些客户机上使用 post-exec 和 pre-exec 脚本，则可以通过将 omnirc 变量 **OB2REXECOFF** 值设置为 1 来禁止在其他客户机上执行这些脚本。有关详细信息，请参阅 CVE-2021-22517。

相关主题

- Data Protector 中的端口使用情况
- Data Protector 使用的 Windows 系统 API

防病毒排除项

本文档提供了结合使用防病毒解决方案和 Data Protector 的常规说明。这包括 Cell Manager 和 Data Protector 客户机。根据配置的不同，防病毒解决方案 (例如Windows Defender、Sophos、Trend Micro) 可能会在备份和还原期间导致性能下降，或导致应用程序中断。

建议排除项

为了解决与下面提到的 Data Protector 组件的性能或稳定性相关的问题，根据需要从实时 (访问时) 和计划扫描中排除目录或进程。并非所有组件在所有平台上都可用。排除目录或进程的步骤因使用的防病毒解决方案而异，不在本文档的讨论范围之内。

> **注意:**如果对防病毒解决方案实施更改 (例如添加排除项)，可能导致计算机系统针对恶意软件、恶意用户或病毒的安全性有所降低。公司有责任在实施前根据公司的安全策略协调这些更改，并在执行软件更新或其他更改时重新评估这些更改。

Windows 的防病毒排除项

如果在软件安装过程中更改了安装目录，则安装目录可能会有所不同。

组件	防病毒排除项 (建议)	使用情况
自动灾难恢复	C:\ProgramData\OmniBack\drim\tmp	用于恢复集创建的临时文件
	C:\Program Files\OmniBack\bin\drim\win-amd64\coolie.exe C:\Program Files\OmniBack\bin\drim\win-x86\coolie.exe	创建增强的自动灾难恢复 (EADR) 集的过程
Cell Manager	C:\ProgramData\OmniBack\server (对于独立系统) 共享磁盘上的文件夹 server (对于群集系统)	Cell Manager Internal Database (IDB) 和 Data Protector AppServer
	C:\ProgramData\OmniBack\tmp	Cell Manager 临时文件
	C:\Program Files\OmniBack\bin\postgres_bar.exe	Cell Manager 上的内部数据库备份和还原
	C:\Program Files\OmniBack\db\bin C:\ProgramData\Omniback\Server\DB80\pg	Data Protector PostgreSQL 安装
磁盘代理	C:\ProgramData\OmniBack\tmp\BBB	从基于块的备份恢复单个项期间使用的临时文件夹
	C:\Program Files\OmniBack\bin\vbda.exe C:\Program Files\OmniBack\bin\vrda.exe	标准卷备份和还原的进程
	C:\Program Files\OmniBack\bin\rbda.exe C:\Program Files\OmniBack\bin\rrda.exe	基于原始磁盘和块的备份和还原的过程
介质代理	C:\Program Files\OmniBack\bin\bma.exe C:\Program Files\OmniBack\bin\rma.exe	写入和读取备份设备的进程
报告服务器	C:\ProgramData\OmniBack\AppServer	Reporting Server AppServer
	C:\ProgramData\OmniBack\RS_idb	Reporting Server Database (RSDB)
	C:\ProgramData\OmniBack\tmp	报告服务器临时文件
StoreOnceSoftware	StoreOncelibrary 文件夹，位于 Store Root 中，属于 StoreOnceSoftware	StoreOnceSoftware deduplication device
	C:\Program Files\OmniBack\bin\StoreOnceSoftware.exe	运行 StoreOnceSoftware deduplication device
VMware GRE 装载代理	C:\ProgramData\OmniBack\tmp\VMwareGRE	用于 VMware VM 粒度恢复的临时文件夹 (缓存)
	Restore Paths 按照 VMware GRE 设置中的配置	用于 VMware VM 粒度恢复的临时文件夹 (非缓存)
	C:\Program Files\OmniBack\bin\FilterListener.exe C:\Program Files\OmniBack\bin\vmwaregre-agent.exe	VMware VM 粒度恢复的过程

Linux 和 Unix 的防病毒排除项

如果在软件安装过程中更改了安装目录，则安装目录可能会有所不同。

组件	防病毒排除项 (建议)	使用情况
自动灾难恢复	/opt/omni/bin/drim/tmp	用于恢复集创建的临时文件
	/opt/omni/bin/drim/linux-amd64/coolie /opt/omni/bin/drim/linux-x86/coolie	创建 EADR 恢复集的过程
Cell Manager	/var/opt/omni/server (对于独立系统) 共享磁盘上的文件夹 server (对于群集系统)	Cell Manager 内部数据库 (IDB) 和 AppServer
	/var/opt/omni/tmp	Cell Manager 临时文件
	/opt/omni/lbin/postgres_bar.exe	Cell Manager 上的内部数据库备份和还原
	/opt/omni/idb/bin /var/opt/omni/server/db80/pg	Data Protector PostgreSQL 安装
磁盘代理	/opt/omni/lbin/vbda /opt/omni/lbin/vrda	标准卷备份和还原的进程
	/opt/omni/lbin/rbda /opt/omni/lbin/rrda	基于原始磁盘和块的备份和还原的过程

组件	防病毒排除项 (建议)	使用情况
介质代理	/opt/omni/lbin/bma /opt/omni/lbin/rma	写入和读取备份设备的进程
报告服务器	/var/opt/omni/server/AppServer	Reporting Server AppServer
	/var/opt/omni/RS_idb	Reporting Server Database (RSDB)
	/var/opt/omni/tmp	报告服务器临时文件
StoreOnceSoftware	StoreOncelibrary 文件夹，位于 Store Root 中，属于 StoreOnceSoftware	StoreOnceSoftware deduplication device
	/opt/omni/lbin/StoreOnceSoftware	运行 StoreOnceSoftware deduplication device
VMware GRE 装载代理	/var/opt/omni/tmp/VMwareGRE	用于 VMware VM 粒度恢复的临时文件夹 (缓存)
	Restore Paths 按照 VMware GRE 设置中的配置	用于 VMware VM 粒度恢复的临时文件夹 (非缓存)
	/opt/omni/lbin/vmwaregre-agent.exe	VMware VM 粒度恢复的过程

已知问题

使用磁盘代理的文件系统的备份和还原性能不佳

用户报告表明在备份或还原期间吞吐量较低，这是由于配置实时扫描后防病毒解决方案执行附加文件系统读取或写入操作所致。如果在备份过程中执行额外的树遍历 (例如通过启用 File system statistics 或 NTFS hard link detection)，这将变得更加重要。

> 建议:在客户机上或针对上述磁盘代理进程禁用实时扫描 (读取或读写)。禁用其他树遍历以加快备份进程。

无法浏览 VMware GRE 请求

从 vCenter 浏览 VMware GRE 请求失败。扩展磁盘时报告错误。防病毒实时扫描会阻止访问由 FilterListenerService 映射到 Vmware GRE 装载代理上的本地文件系统的磁盘文件。

> 建议:在 VMware GRE 装载代理主机上禁用实时扫描。如果这样做不能解决问题，请完全删除防病毒解决方案，然后与软件供应商联系以找到永久解决方案。

无法浏览基于块的备份以进行单项恢复

浏览基于块的备份以还原单个项失败。扩展磁盘时报告错误。防病毒实时扫描会阻止访问由 FilterListenerService 映射到磁盘代理上的本地文件系统的磁盘文件。

> 建议:在磁盘代理主机上禁用实时扫描。如果这样做不能解决问题，请完全删除防病毒解决方案，然后与软件供应商联系以找到永久解决方案。

StoreOnceSoftware 服务失败

在备份期间，StoreOnceSoftware 服务失败，并报告设备脱机错误。 StoreOnceSoftware --list_stores 报告存储为“失败” 状态。重新启动服务是一项耗时的任务，或者一个或多个存储保持为“失败” 状态。这可能是由于实时扫描阻止了 StoreOnceSoftware 服务在内务管理期间及时访问文件，也可能是由于计划扫描阻止了及时访问此高度复杂的文件结构的其他部分。

> 建议:不要对 StoreOnceSoftware root 目录执行计划扫描或实时扫描。将 StoreOnceSoftware root 目录添加到防病毒解决方案的排除列表中。将任何文件移动到隔离位置，或在病毒扫描程序在 StoreOncelibrary 文件夹结构中识别出安全风险时删除文件，可能会损坏存储区，使其无法使用。

ISO 映像创建失败

请参阅灾难恢复故障诊断。

InstallShield 错误

请参阅安装故障诊断。

日志中报告了 PostgreSQL 错误

请参阅内部数据库故障诊断。

在 VMware 数据的粒度恢复期间尝试装载已还原的磁盘时出错

请参阅适用于 VMware 的 GRE 故障诊断。

用户安全性

Data Protector 用户是 Data Protector 的一个安全关键层。必须谨慎规划和测试用户的配置。

用户权限

某些用户权限很强大，因此象征着安全问题。例如，用户配置和客户机配置用户权限使用户可以更改安全设置。

还原到其他客户机用户权限也非常强大，尤其在与**作为 root 备份**或**作为 root 还原**用户权限结合时。

甚至不太强大的用户权限也有内在的风险与自身相关。可以配置 Data Protector 以限制某些用户权限，从而降低这些风险。

“启动备份规范”用户权限

用户可使用 omnib 与 -datalist 选项从命令行中启动备份规范的备份会话。

通过结合**启动备份规范**和**启动备份**用户权限，用户可在 GUI 中查看配置的备份规范并能够启动备份规范或交互式备份的备份会话。

并不总是希望允许用户执行交互式备份。要仅允许具有“保存备份规范”用户权限的用户进行交互式备份，请将 StrictSecurityFlags 全局选项设置为 0x0200 。

隐藏备份规范的内容

在高安全环境中，可能会将所保存备份规范的内容视为敏感甚至保密信息。

可以将 Data Protector 配置为对所有用户隐藏备份规范的内容，除具有“保存备份规范”用户权限的用户之外。为此，请将 StrictSecurityFlags 全局选项设置为 0x0400 。

主机信任

主机信任功能仅需在有限数量的客户机内将数据从一个客户机还原到另一个客户机，从而减少了将**还原到其他客户机**用户权限授予用户的需要。可以定义一组主机，彼此信任对方的数据。

主机信任通常在以下情况下使用：

- 用于群集中的客户机（节点和虚拟服务器）。
- 如果客户机的主机名更改且旧备份对象的数据需要还原。
- 如果由于 DNS 问题导致客户机主机名与备份对象不匹配。
- 如果用户拥有多个客户机且需要将数据从一个客户机还原到另一个客户机。

用户组

Data Protector 默认情况下只有少数几个预定义的用户组。建议在 Data Protector 环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。

用户限制

除定义特定用户组以外，还可以进一步限制用户操作，以仅对单元的特定系统执行操作。可通过在 Cell Manager 上配置 user_ restrictions 文件，强制执行此限制。这些限制仅适用于 Data Protector 用户组的成员，对管理员和操作员则不适用。

用户验证

用户配置与用户验证相关联。增强的验证如果没有详细的用户配置也没有价值，反之亦然 - 即使最详细的用户配置如果没有增强的验证也没有意义。

Data Protector 用户列表中不应存在“弱”用户规范，这一点很重要。请注意，用户规范的客户机部分是强部分（尤其在有增强的验证的情况下），而无法可靠地验证用户和组部分。

具有强大用户权限的用户应配置给特定的客户机，他们将用于 Data Protector 管理。如果使用了多个客户机，则应为每个客户机添加一个入口，而不是将这种用户指定为 user 、 group 、 <Any> 。不应允许不受信任的用户登录任何此类系统。

禁止在用户管理上下文的“名称”、“域或组”和“客户机系统”字段中选择“<任意>”。要启用此选项，请在位于以下位置的全局选项文件中将全局选项 EnableAnyOptionUserCtx 的值手动更改为 **1**:

- *Windows：* *<PROGRAMDATA>\Config\Server\Options*
- Linux： /etc/opt/omni/server/options

重要说明为用户管理上下文中的用户、组或客户机字段启用并使用“<任意>”选项，就会禁用或绕开安全功能，这会使系统面临更多的安全风险。使用此选项即表示您了解并同意承担所有相关风险，同样使 Micro Focus 免受损失。
如果为用户管理上下文中的用户、组或客户机选项启用并使用“<任意>”选项，Micro Focus 建议客户采取相应的保护措施来防范与用户权限相关联的风险，Micro Focus 并不提供这些保护措施。若未实施相应的保护措施，您的系统可能面临更多的安全风险。

您理解并同意承担所有相关的风险，并且不会归咎于 Micro Focus。在任何时候，客户都应自行负责评估其监管和业务要求。Micro Focus 不声明也不保证其产品符合客户开展其业务适用的任何特定法律或监管标准。

相关主题

相关任务

- 添加用户组
- 配置主机信任

保护客户机系统

可以保护单元中的选定客户机。

完成以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“客户机”，右键单击要保护的客户机，并单击“保护”。
3. 键入将允许访问选定客户机的系统名称，或使用“网络”(仅在 Windows GUI 上) 或“搜索”选项卡搜索系统。单击**添加 (Add)** 将每个系统添加到列表中。
4. 单击“完成”将选定系统添加到 allow_hosts 文件中。

客户机将验证每个请求的来源，并且仅允许从“在所选客户机上启用安全”窗口中选择的客户机收到的那些请求。这些客户机列在 allow_hosts 文件中。如果拒绝请求，则将事件记录到默认 Data Protector 日志文件目录中的 inet.log 文件。

如果不选择任何 Cell Manager 即单击“完成”，则您的 Cell Manager 自动可供访问，并将其 (主客户机名称) 添加到 allow_hosts 文件中。不能从列表中排除该 Cell Manager。

数据加密

通过 Data Protector 可以对备份数据进行加密，以使其与其他数据相比受到保护。提供以下两种数据加密技术：基于软件的和基于驱动器的加密。

Data Protector 软件加密简称 AES 256 位加密，以对于加密和解密使用相同密钥的高级加密标准 (AES) 加密算法为基础。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。

Data Protector 基于驱动器的加密使用驱动器的加密功能。具体实现和加密强度取决于驱动器的固件。Data Protector 仅启用该功能并管理加密密钥。

打开加密之后，不需要任何其他配置。但是，对于 AES 256 位加密，Data Protector 通过命令行界面 (CLI) 提供加密密钥的高级手动管理 (如使密钥过期、重新激活、导出、导入和删除密钥)。

使用 Data Protector GUI 或 CLI，可以确定对哪些备份对象加密或哪个备份介质含有加密对象，并可以获取这些对象的加密详细信息。

启用数据加密

以下限制适用：

- AES 256 位加密不对元数据（如文件名和文件大小）进行加密。
- 加密不适用于 ZDB 到磁盘备份和 ZDB 到磁盘 + 磁带备份的磁盘部分。
- 使用 AES 256 位加密备份的对象无法合并。
- 如果使用 AES 加密来执行到 StoreOnce Catalyst 设备的备份，则不支持还原操作。

创建新备份规范或修改已配置的备份规范时，可以启用基于软件的 AES 256 位加密。

必须有活动的加密密钥，然后才能执行加密的 IDB 备份，进而执行以下任务:

- 在文件系统备份规范中启用加密
- 在磁盘映像备份规范中启用加密
- 在内部数据库备份规范中启用加密
- 在应用程序集成备份规范中启用加密

在文件系统备份规范中启用加密

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”属性页中，单击“文件系统选项”的**高级**按钮。
5. 在“文件系统选项”窗口中，单击**其他**选项卡。在“数据安全性”下拉列表中，选择以下某项:
   - 无
     此数据安全选项不提供任何保护。默认情况下，数据安全设置为“无”。
   - 编码
     Data Protector 建议在备份期间使用 AES 256 位加密以确保数据安全性。选择安全性更低的“编码”选项后，Data Protector 将显示错误消息。
   - AES 256 位
     推荐选项。选择此选项可进行软件加密以保护数据。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。但是，如果出于数据安全考虑选择了 AES-256，则磁带客户机将切换到联邦信息处理标准 (FIPS) 模式来进行数据加密。
6. 单击**确定**，然后单击**应用**以保存更改。

> **提示**要仅加密所选的备份对象，请转到**备份对象摘要**选项卡，然后在对象的属性中选择 **AES 256 位**选项。

在磁盘映像备份规范中启用加密

完成以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“备份对象摘要”页中，单击**属性**按钮。
5. 在“对象属性”窗口中，单击**其他**选项卡。在“数据安全性”下拉列表中，选择以下某项:
   - 无
     此数据安全选项不提供任何保护。默认情况下，数据安全设置为“无”。
   - 编码
     Data Protector 建议在备份期间使用 AES 256 位加密以确保数据安全性。选择安全性更低的“编码”选项后，Data Protector 将显示错误消息。

- AES 256 位
  推荐选项。选择此选项可进行软件加密以保护数据。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。但是，如果出于数据安全考虑选择了 AES-256，则磁带客户机将切换到联邦信息处理标准 (FIPS) 模式来进行数据加密。

6. 单击**确定**，然后单击**应用**以保存更改。

在内部数据库备份规范中启用加密

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**内部数据库**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”页中的“常见应用程序选项”下，单击**高级**。
5. 在“公共应用程序选项”窗口中，单击**其他**选项卡。从“数据安全性”下拉列表中，选择以下某项:
   - 无
     此数据安全选项不提供任何保护。默认情况下，数据安全设置为“无”。
   - 编码
     Data Protector 建议在备份期间使用 AES 256 位加密以确保数据安全性。选择安全性更低的“编码”选项后，Data Protector 将显示错误消息。
   - AES 256 位
     推荐选项。选择此选项可进行软件加密以保护数据。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。但是，如果出于数据安全考虑选择了 AES-256，则磁带客户机将切换到联邦信息处理标准 (FIPS) 模式来进行数据加密。
6. 单击**确定**，然后单击**应用**以保存更改。

在应用程序集成备份规范中启用加密

有关支持 AES 256 位加密的应用程序集成的最新列表，请参阅最新支持矩阵。

不支持组合使用 Microsoft SQL Server 集成的“快速直接模式”和“AES 256 位”选项。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如 **MS SQL Server**）。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”属性页中，单击“公共应用程序选项”的**高级**按钮。
5. 在“公共应用程序选项”窗口中，单击**其他**选项卡。在“数据安全性”下拉列表中，选择以下某项:
   - 无
     此数据安全选项不提供任何保护。默认情况下，数据安全设置为“无”。
   - 编码
     Data Protector 建议在备份期间使用 AES 256 位加密以确保数据安全性。选择安全性更低的“编码”选项后，Data Protector 将显示错误消息。
   - AES 256 位
     推荐选项。选择此选项可进行软件加密以保护数据。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。但是，如果出于数据安全考虑选择了 AES-256，则磁带客户机将切换到联邦信息处理标准 (FIPS) 模式来进行数据加密。
6. 单击**确定**，然后单击**应用**以保存更改。

导出和导入含有加密备份的介质

要将加密备份中的数据还原到不同 Data Protector 单元中的客户机，需要将介质和加密密钥导入到目标 Cell Manager，如以下各节所述。

- 没有 CMMDB 的 Cell Manager 环境或 MoM 环境
- 有 CMMDB 的 MoM 环境

Data Protector 还通过命令行界面 (CLI) 提供加密密钥的高级手动管理 (如使密钥过期、重新激活、导出、导入和删除密钥)。有关详细信息，请参阅 omnikeytool 主题。

没有 CMMDB 的 Cell Manager 环境或 MoM 环境

在不使用本地 MMDB 的 Cell Manager 环境中或 MoM 环境中，执行以下步骤可导出和导入含有加密备份的介质：

1. 在原始 Cell Manager 上，从 IDB 导出介质。此操作还会将相关的加密密钥从密钥库导出到默认导出加密密钥目录下的 mediumID.csv 文件中。
2. 将 mediumID.csv 文件传输到目标 Cell Manager，并将其放置到默认导入加密密钥目录中。
3. 将导出的介质插入目标 Cell Manager 将使用的驱动器中。
4. 在目标 Cell Manager 上导入该介质。此操作还可从 mediumID.csv 文件中导入密钥。

> **注意**如果密钥文件不存在，则仍可导入介质，但目录导入将因缺少解密密钥而中止。

有 CMMDB 的 MoM 环境

在使用 CMMDB 的 MoM 环境中，所有介质信息都存储在 MoM Manager 上，但这些介质使用的加密密钥 ID 以及 CDB 存储在每个各自 Cell Manager 上的本地密钥库中。请注意，所有介质管理操作都需要在 MoM Cell Manager 上完成。

要在 CMMDB 位于 MoM Manager 上的情况下导出和导入含有加密备份的介质，请执行以下步骤：

1. 从 CMMDB 导出介质。密钥 ID 将导出到默认导出加密密钥目录下的 mediumID.csv 文件中。
2. 将 mediumID.csv 文件传输到目标 Cell Manager，并将其放置到默认导入加密密钥目录中。
3. 从 MoM Manager 中，从带库弹出介质。
4. 将介质从原始介质池移至目标介质池，后者与目标单元中的某个驱动器关联。此操作还可导入目录。
5. 将导出的介质插入目标 Cell Manager 将使用的驱动器中。
6. 在目标 Cell Manager 上导入该介质。此操作还可从 mediumID.csv 文件中导入密钥。

启用基于驱动器的加密

可以在以下过程中启用基于驱动器的加密：

- 配置驱动器或修改已配置的某个时。
- 配置备份、对象副本或对象合并规范或修改已配置的某个时。
- 配置自动介质操作或修改已配置的某个时。

有关支持基于驱动器加密的最新设备列表，请参阅 https://docs.microfocus.com/?DP 上的最新支持矩阵。

无法对 NDMP 服务器控制的设备或具有外部加密控制的库 (例如 SKM 控制下的 ESL 库) 中的驱动器使用基于驱动器的加密。

为优化性能，建议使用大小至少为 256 KB 的块。

> **注意**当备份到同时包含加密和未加密备份的介质时，可能会看到 Drive-based decryption enabled 消息。这意味着介质上的最后一个备份是加密备份，并且已自动将其解密，以便在添加新备份之前 Data Protector 可以检查该备份。

在驱动器配置中启用基于驱动器的加密

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，依次展开**设备**、所需的设备及其驱动器。
3. 右键单击所需的驱动器，然后单击**属性**。
4. 在“设置”属性页中，单击**高级**按钮。
5. 在“高级选项”窗口的**设置**选项卡中，选择**基于驱动器的加密**选项，然后单击**确定**。
6. 单击**应用**保存更改。

在备份规范中启用基于驱动器的加密

执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型（例如**文件系统**）。此时将显示所保存的全部备份规范。
3. 单击相应的备份规范。
4. 在“目标”页中，右键单击选择用于备份的设备，然后单击**属性**。
5. 在“设备属性”窗口中，选择**基于驱动器的加密**选项，然后单击**确定**。
6. 单击**应用**保存更改。

> **提示**要修改对象复制或对象合并规范，请在**对象操作**上下文中打开该规范，然后执行步骤 4 到 6。

为自动介质操作启用基于驱动器的加密

完成以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**自动操作**。此时将显示所有已配置的自动操作。
3. 单击要为其启用基于驱动器的加密的介质操作。
4. 在“选项”页中，选择**基于驱动器的加密**选项，然后单击**应用**。

注意基于驱动器的加密选项适用于自动介质操作中涉及的所有设备。

基于驱动器的加密和云设备加密的密钥管理

默认情况下，对于每个介质，都会为每个加密介质自动生成特定于该介质的密钥。如果要对使用基于驱动器的加密和云设备加密的所有加密介质使用相同的密钥，则可以设置以下两个全局变量:

- EnableCommonKeyEntity
- KeyEntity

有关这些变量的详细信息，请参考位于以下位置的 global 文件:

<PROGRAMDATA>\Config\Server\Options (Windows)

/etc/opt/omni/server/options (Linux)

注意: 为 KeyEntity 生成的密钥是唯一且随机的，因此请确保定期导出和备份密钥。

安全日志

如果在访问 Data Protector 功能或客户机时遇到问题，可以使用日志文件中的相关信息确定问题。例如，记录的事件可帮助您确定配置错误的用户或客户机。

客户机安全性事件

客户机安全事件将记录到单元中每个客户机的默认 Data Protector 日志文件目录中的 inet.log 文件。

检查客户机上 Data Protector 最近的活动很有用。

Cell Manager 安全事件

Cell Manager 安全事件将记录在 Data Protector 服务器日志文件目录中的 security.log 文件中。

出现第一个安全事件时即创建 security.log 文件。

用户验证和 LDAP

应在企业用户管理基础设施中结合将 Data Protector 作为企业系统进行身份验证和授权的功能。此连接允许向企业用户目录中配置的用户和组授予访问 Data Protector 用户界面的权限。

将在安全连接上执行用户身份验证，并将轻型目录访问协议 (LDAP) 用作基础技术。因此，用户可以使用其企业凭据访问 Data Protector 服务，而不需要维护单独的密码。此外，可以在企业目录中将管理员或操作员保留为组，从而符合已建立的授权和审批流程。

使用 Java 身份验证和授权服务 (JAAS) 登录模块在 Data Protector 嵌入式应用程序服务器 (AppServer) 的安全域中配置 LDAP 集成。可选的 LDAP 登录模块可提供 LDAP 身份验证和授权服务，可将这些服务通过必需的 Data Protector 登录模块映射到 Data Protector 权限。如果未配置 LDAP 集成，Data Protector 将按照以前版本中的流程运行。

Data Protector 使用登录模块堆栈中的登录模块对用户进行身份验证。当用户使用 Data Protector GUI 连接到 Cell Manager 时，用户身份验证将由以下登录模块执行:

1. LDAP 登录模块：对照现有 LDAP 服务器对用户凭据进行身份验证，例如用户名和密码。请参阅配置 LDAP 登录模块。
2. Data Protector 登录模块：对照 Data Protector 用户列表和 Web 访问密码对用户凭据进行身份验证。请参阅向 LDAP 用户授予权限。
3. 执行 LDAP 初始化和配置所需的所有步骤后，还可以检查配置。请参阅检查 LDAP 配置。
4. (可选) 将配置从不安全的 LDAP 修改为 LDAPS。请参阅安全地配置 LDAP。

> **注意**
>
> 当在 Data Protector 中将用户或客户机配置为允许其以典型方式访问 CLI 时，Data Protector GUI 不使用 LDAP 功能，且将不显示登录对话框。

配置 LDAP 登录模块

要配置 LDAP，需要满足以下先决条件:

- Cell Manager (AppServer) 必须能够与 LDAP 服务器通信 (通过端口 389/TCP (对于 LDAP) 或通过端口 636/TCP (对于 LDAPS))。
- 当配置 LDAPS 时，强烈建议首先配置并测试 LDAP。这可以作为 Data Protector GUI 配置过程的一部分来完成。
- LDAP 用户必须分配到 Data Protector 用户组 (直接分配或使用 LDAP 组) 并配置登录名 (userPrincipalName 属性，例如 user@testlab.net)。

> **注意**
>
> - 在 MoM 环境中配置 LDAP 登录模块时，请确保在每个 Cell Manager 上执行上述步骤。MoM 环境中的每个 Cell Manager 需具有相同的 LDAP 登录模块配置。
> - 从 Data Protector 10.04 (和更早版本) 升级到它时，可能需要重新创建 LDAP 配置。

要配置 LDAP 登录模块，请执行以下步骤:

1. 在上下文菜单中，单击“用户”，然后在“操作”菜单下选择“LDAP 配置”。

   将显示“LDAP 配置”窗口，其中包含现有 LDAP 配置信息。如果未配置 LDAP，则可以配置新的 LDAP 服务器。

2. 指定或编辑以下字段的值:

名称	描述	值
供应商	LDAP 服务器供应商	将 LDAP 服务器供应商指定为 ActiveDirectory。
名称	LDAP 配置名称	指定 LDAP 配置的名称。
LDAP 服务器	LDAP 服务器主机名或 IP 地址	指定 LDAP 服务器主机名或 IP 地址。
LDAP 端口	LDAP 服务器上的端口	指定 LDAP 服务器要使用的端口号。默认端口号为 389。在 GUI 中不配置 LDAPS。在最后一步完成所需的更改。
用户 DN	用户所在的 LDAP 树的完整 DN。此 DN 为 LDAP 用户的父项。	指定含有用户的 LDAP 树的 DN。例如：CN=Users,DC=mytestlab,DC=net 。
绑定 DN	用于与 LDAP 服务器初始绑定的用户	指定 LDAP 用户的 DN，以供 Keycloak 用于访问 LDAP 服务器。例如：CN=bindDN,CN=Users,DC=mytestlab,DC=net 。
绑定凭据	绑定 DN 用户的密码	指定绑定 LDAP 用户的密码。
测试连接	测试 LDAP 服务器连接	检查是否可以使用指定的服务器主机名/IP 地址和端口号连接到 LDAP 服务器。
测试身份验证	测试 LDAP 服务器身份验证	检查是否可以使用指定的“绑定 DN”和“绑定凭据”连接到 LDAP 服务器。**注意:** 如果已配置 LDAPS，则失败。如果需要，可以从 Keycloak 执行测试。

3. 单击“添加”以新建 LDAP 配置，或单击“修改”以确认对现有配置的更改。

删除 LDAP 配置

要删除现有 LDAP 配置，请执行以下步骤:

1. 在上下文菜单中，单击“用户”，然后在“操作”菜单下选择“LDAP 配置”。

   将显示“LDAP 配置”窗口，其中包含现有 LDAP 配置信息。

2. 单击“删除配置”以删除现有 LDAP 配置。在出现提示时确认。

向 LDAP 用户授予权限

只有获授 Data Protector 权限的 LDAP 用户才能连接到 Cell Manager。配置 LDAP 登录模块后，可以向 LDAP 用户/组授予所需的 Data Protector 权限。

要授予 Data Protector 权限，请执行以下步骤:

1. 启动 Data Protector GUI，然后向 LDAP 用户授予 Data Protector 权限。
2. 向 Data Protector 用户组添加 LDAP 用户。
3. 使用 LDAP 凭据登录。

向 Data Protector 用户组添加 LDAP 用户

要将 LDAP 用户添加至 Data Protector 用户组，请执行以下操作:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开“用户”，然后右键单击要添加 LDAP 用户的用户组。
3. 单击**添加/删除用户**打开向导。
4. 在“添加/删除用户”对话框的“手动”选项卡中，提供以下详细信息:
   - **类型**：选择 LDAP。
   - 当将“LDAP 用户”添加为“实体”时，以用户主体名称格式指定“名称”，例如 username@mytestlab.net 。
   - 当将“LDAP 组”添加为“实体”时，以判别名称格式指定“名称”，例如 CN=DPAdmin,OU=DPLocal,OU=Groups,DC=mytestlab,DC=net 。
   - **描述**: 此项可选。
5. 单击**完成**退出向导。

使用 LDAP 凭据登录

要使用 LDAP 凭据登录，请执行以下步骤：

1. 启动 Data Protector GUI 并连接至 Cell Manager。仅对于未配置进行基于典型 Data Protector 的身份验证的用户，才会显示登录对话框。
2. 在 LDAP 身份验证屏幕上提供 LDAP 凭据以访问 Data Protector。LDAP 用户可以属于任何可用的 Data Protector 用户组。

检查 LDAP 配置

以下过程讲解如何检查是否为特定 LDAP 用户或组正确设置了用户权限，方法是从 Web 浏览器中查询 Data Protector 登录提供程序服务 getDpAcl 。

要获取指定用户的 Data Protector 访问控制列表 (ACL)，请执行以下步骤：

1. 使用浏览器连接 Data Protector 登录提供程序 Web 服务。
2. 浏览器可能会提示您接受服务器证书。单击**接受**确认请求。
3. 将显示一个对话框，提示您提供登录凭据。提供之前使用 Data Protector 配置的有效 LDAP 用户名和密码。
4. 浏览器将返回以下访问控制列表 (ACL)： https://<server>:7116/dp-loginprovider/restws/dp-acl
5. 使用此 ACL 检查分配权限与为对应 Data Protector 用户组指定的 Data Protector 用户权限是否匹配。

安全地配置 LDAP

要安全地配置 LDAP，请按照下列步骤操作:

1. 从 LDAP 服务器导入 SSL 证书。
2. 将不安全的 LDAP 身份验证重新配置为 LDAPS。

注意**:** 使用 LDAP 组配置的用户不会在 Data Protector GUI 中列出。由于 LDAP 配置是直接通过 Keycloak 完成的，用户会在 Keycloak 数据库中自动同步，因此不会在“用户” 上下文中单独列出。

从 LDAP 服务器导入 SSL 证书

1. 使用 Cell Manager 上的 openssl s_client -connect <LDAP Server>:636 从 LDAP 服务器获取 SSL 证书。
2. 创建临时证书文件 C:\Temp\ldap_cert.pem 或 /tmp/ldap_cert.pem ，然后复制步骤 1 中 BEGIN CERTIFICATE 到 END CERTIFICATE 之间的行。
3. 从 Cell Manager 上的 javax.net.ssl.trustStore 获取信任库的位置，并从 standalone.xml 中的 javax.net.ssl.trustStorePassword 值获取密码。可以在 Windows 的 %DP_SDATA_DIR%Config\Server\AppServer\standalone.xml 和 Linux Cell Manager 的 /etc/opt/omni/server/AppServer/standalone.xml 中找到。
4. 使用步骤 3 中的值将您在步骤 1 中生成的 LDAP 服务器证书导入到 AppServer 信任库中。该命令位于 Windows 的 "%DP_HOME_DIR%jre\bin\keytool" -importcert -keystore "trustStoreLocation" -alias "ldap" -file C:\Temp\ldap_cert.pem -storepass trustStorePassword 和 Linux Cell Manager 的 /opt/omni/jre/bin/keytool -importcert -keystore trustStoreLocation -alias "ldap" -file /tmp/ldap_cert.pem -storepass trustStorePassword 中。
5. 使用 omnisv -restart 重新启动 Data Protector AppServer hpdp-as 或 Data Protector 服务。

将 LDAP 身份验证重新配置为 LDAPS

1. 如果 DpKeycloakUser 的密码未知，请运行以下命令重置该密码：omniusers -resetpass -name DpKeycloakUser -pass Password_123
2. 在浏览器 https://localhost:7116/auth/admin/DataProtector/console 中打开 Keycloak 管理控制台，然后修改 LDAP 的设置以使用 LDAPS。使用步骤 1 中的以下登录凭据连接 Keycloak 控制台。
3. 修改 LDAP 属性:
    1. 单击“用户联合”，在已配置的 **Ldap** 提供程序上选择“编辑”
    2. 将“连接 URL” 从 http 修改为 https，并将端口从 389 更改为 636，然后使用“测试连接”按钮验证证书是否已加载且服务器有所响应。
    3. “保存”设置。
4. 重新启动 Data Protector AppServer。

配置 TLS 版本和密码套件

此页面提供有关如何在 Data Protector 应用程序服务器中配置 TLS 版本和密码套件的信息。

要配置 TLS 版本和密码套件，请完成以下步骤:

1. 导航到 Cell Manager 服务器上的以下路径:
   - Windows： Program Files\OmniBack\AppServer\bin 。例如： C:\Program Files\OmniBack\AppServer\bin 。
   - Linux： opt/omni/AppServer/bin 。
2. 创建具有以下内容的批处理文件:
   /subsystem=undertow/server=default-server/https-listener=https:undefine-attribute(name=ssl-context)
   /subsystem=elytron/server-ssl-context=LocalhostSSLContext:remove
   /subsystem=elytron/server-ssl-context=LocalhostSSLContext:add(key-manager="LocalhostKeyManager", protocols=["<TLS version>"], cipher-suite-filter="<Cipher list>", use-cipher-suites-order="false")
   /subsystem=undertow/server=default-server/https-listener=https:write-attribute(name=ssl-context,value=LocalhostSSLContext)

   示例：

   /subsystem=undertow/server=default-server/https-listener=https:undefine-attribute(name=ssl-context)
   /subsystem=elytron/server-ssl-context=LocalhostSSLContext:remove
   /subsystem=elytron/server-ssl-context=LocalhostSSLContext:add(key-manager="LocalhostKeyManager", protocols=["TLSv1.2"], cipher-suite-filter="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256", use-cipher-suites-order="false")
   /subsystem=undertow/server=default-server/https-listener=https:write-attribute(name=ssl-context,value=LocalhostSSLContext)
3. 运行以下命令：
   - **Windows**：
     "C:\Program Files\OmniBack\AppServer\bin\jboss-cli.bat" -c --command="run-batch --file=<name of batch file with absolute path>"

     示例:
     "C:\Program Files\OmniBack\AppServer\bin\jboss-cli.bat" -c --command="run-batch --file=C:/ProgramData/OmniBack/ciphertext.txt"

     Linux：
     "opt/omni/AppServer/bin/jboss-cli.sh" -c --command="run-batch --file=<name of batch file with absolute path>"

     示例：
     "opt/omni/AppServer/bin/jboss-cli.sh" -c --command="run-batch --file=</etc/opt/omni/ciphertext.txt>"
4. 重新加载应用程序服务器。
   - Windows： jboss-cli.bat -c --command="/:reload"
   - Linux： jboss-cli.sh -c --command="/:reload"

设置代理通信

要设置代理通信，请编辑以下 omnirc 变量:

- OB2SSLCIPHERLIST : 此变量用于设置密码列表。默认密码列表 (OpenSSL 格式) 为 ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:AES256-GCM-SHA384 。
- OB2USEOLDTLSVERSION : 此变量用于设置 TLS 协议版本。TLS 协议版本值为 TLSv1、TLSv1.1、TLSv1.2。默认值为 TLSv1.2。

防火墙支持

可以在 Data Protector 进程跨越防火墙进行通信的环境中配置 Data Protector。从 Data Protector 9.09 和 2019.02 开始，防火墙中必须打开的端口数量减少。这一变化仅在升级单元后出现，在此之前，旧客户机仍然以旧模式运行，使用与之前 Data Protector 版本相同的开放端口。

除了包括 StoreOnce 和文件库设备目标的 NDMP 三向备份/还原，无需为 Data Protector 进程的侦听端口设置 OB2PORTRANGE 和 OB2PORTRANGESPEC 变量。仍然可为 Data Protector 设置这些变量，以用于主机中的进程间通信。以下示例解释了使用情况：

示例 1：

Data Protector 9.09 MA 和早期版本的 Data Protector 9.09 DA

MA 打开与所有地址绑定的端口。在 netstat 输出中，这显示为 MA 在侦听 0.0.0.0:1234。

- 这里，“1234”是一个例子，实际端口取决于使用 OB2PORTRANGE 变量和 Data Protector 配置设置的动态端口范围。
- “0.0.0.0”表示“所有地址”，对于 IPv6，相当于 [::]。这表示客户机可以通过任何路由连接。

来自相同主机的其他进程无法打开端口 1234。DA 直接连接至 MA 主机 1234。在防火墙中，您必须打开端口 1234。

示例 2：

Data Protector 9.09 MA 和 Data Protector 9.09 DA:

- 由于 MA 不知道连接的 DA 是 Data Protector 版本 9.09 还是更早版本，因此 MA 仍然会打开端口 0.0.0.0:1234。
- 与示例 1 相比，如果您确定将只连接 Data Protector 9.09 客户机时，则不需要在防火墙中打开端口 1234。这取决于您升级主机的顺序。

示例 3：

MA 主机上已启用 Data Protector 9.09 MA、Data Protector 9.09 DA 和 Data Protector 防火墙

- MA 打开仅与环回接口绑定的端口。在 netstat 输出中，这显示为 MA 在侦听端口 127.0.0.1:1234，或者对于 IPv6，显示为 [::1]:1234。
- 旧 DA 将无法连接，因为无论是 Windows 还是一些其他防火墙，均无法从远程主机访问端口 1234。

> **注意**防火墙不阻止进程打开端口，仅连接至来自远程主机的这些端口。

Data Protector 中的通信

Data Protector 进程使用 TCP/IP 连接进行通信。Data Protector 需要以下端口：

- 每个 Data Protector 系统上的 Inet 端口（默认为 5555/5565）。

  > **注意**Windows inet 为多线程。

- Cell Manager 系统上的 IDB 服务端口（默认为 7112）。
- Cell Manager 系统上的应用程序服务器端口（默认为 7116）。
- StoreOnceSoftware.exe 二进制文件的规则必须保留在入站防火墙例外中。由于 StoreOnceSoftware.exe 不支持 (基于第三方代码的) 单个端口传递，但的确会打开入站端口并接受这些端口上的通信。

在防火墙中，这些端口必须打开（可从远程主机访问）。

此外，Data Protector 会打开许多动态端口。在防火墙中，升级 Data Protector 单元之前，这些端口必须保持打开状态。将单元升级到 Data Protector 2019.02 或更高版本之后，这些端口在进程 (IPC) 中使用，从防火墙的角度而言，不需要将其打开。但是，使用 StoreOnce 或文件库目标执行三向备份/还原的 NDMP 介质代理需要打开许多动态端口。这些端口的数量等于同时处理以进行备份/还原的最大对象数。

若要配置动态端口的范围，需要进行以下更改：

- 限制在升级整个单元之前仍然需要在防火墙中打开的端口。
- 防止 Data Protector 打开第三方应用程序可能需要的端口。
- Data Protector 可与可能需要打开自有端口的非 Data Protector 软件通信。从文件库或 StoreOnce 目标进行 NDMP 三向还原需要 NDMP 数据服务器打开许多动态端口，端口数量等于在任何给定时间同时还原的最大对象数。

注意在安装期间，需要为 Inet 打开以下端口：

- 全新 Data Protector 安装 - 5565
- 升级 Data Protector 安装 - 5555

配置机制

可以使用两个 omnirc 选项配置端口分配行为:

- OB2PORTRANGE

  该选项设置所有 Data Protector 进程从中打开动态端口的端口范围。

- OB2PORTRANGESPEC

在 Data Protector 2019.02 和 9.09 之前，端口范围有两个用途:

- 安全性: 限制 Data Protector 打开的端口，因此端口用户需要在防火墙中打开。
- 与其他软件的冲突: 非 Data Protector 软件可能需要端口 1000-2000 用于特定用途，因此通过使用 OB2PORTRANGE 阻止 Data Protector 使用该范围。这对 OB2PORTRANGE 有效。

注意

- 默认情况下，动态端口由操作系统分配。
- 这些选项不影响 Inet 的固定端口 (5555/5565)、IDB 服务端口 (7112) 和应用程序服务器端口 (7116)。
- 端口范围选项限制 Data Protector 端口使用。它们不能阻止非 Data Protector 应用程序分配来自该范围的端口。

参与通信的代理升级后，防火墙中打开的端口数量会减少。在此之前，Data Protector 使用旧方法进行通信。旧版磁盘代理与新介质代理搭配使用，反之亦然。在升级所有单元主机之前，用户应该使端口保持打开状态。

在 inetd 支持 -p <proc_limit> 选项的平台上，如果可能，避免使用该选项，否则建议使用大于 2200 的 proc_limit 值。

启用实际防火墙之前，建议测试 Data Protector 与已启用 Data Protector 防火墙的环境。

要在整个单元中启用 Data Protector 防火墙，请运行以下命令：

```
omnicc -firewall –all –enable_dp
```

要在部分单元中启用 Data Protector 防火墙，请指定单个主机，而非 -all。

例如，要测试磁盘代理是否可以通过防火墙与介质代理通信，请运行以下命令以关闭防火墙：

omnicc -firewall –host MAhost DAhost –enable_dp

与 -enable_dp 选项一起，在 Windows 防火墙中使用 -enable_os 选项禁用 Data Protector 规则。

使用这些选项进行测试后，用户可以继续关闭第三方防火墙（例如，路由器）。

相关任务

- Data Protector 10.0 中的端口使用情况

重新生成证书

本节提供了重新生成以下证书的步骤:

- INET 证书 - Cell Manager 与客户机之间进行通信所需的证书。
- 应用程序服务器证书 - 应用程序服务器与 Data Protector GUI 之间进行通信所需的证书。

在以下情况下，可能需要重新生成证书:

- 证书已更新或删除
- 证书已过期
- 对 Data Protector 升级过程进行故障诊断
- 服务器名称已更改

重新生成 INET 证书

您可以在 Cell Manager 或客户机主机上重新生成 INET 证书。

在 Cell Manager 主机上重新生成 INET 证书

1. 运行以下命令：
   Windows：
   <DP_Home>\bin\omnicc -secure_comm -regenerate_cert
   Linux/Unix:
   /opt/omni/bin/omnicc -secure_comm -regenerate_cert
2. 使用以下任一选项将 Cell Manager 证书重新分发给所有客户机主机:
   - 登录连接到此 Cell Manager 的每个客户机主机，然后运行以下命令:
     omnicc -secure_comm -configure_peer <CM_HOSTNAME>
     其中， CM_HOSTNAME 是 Cell Manager 主机的主机名。
   - 在 Cell Manager 主机中运行以下命令:
     omnicc -secure_comm -reconfigure_peer_all [input_file_path]
     如果存在可选的 input_file_path 参数，则应指向具有单元中所有客户机凭据的文件。仅当安装服务器在 Cell Manager 以外的客户机上安装时，才可以使用此选项。

在客户机主机上重新生成 INET 证书

1. 在客户机主机上运行以下命令:
   Windows：
   <DP_Home>\bin\omnicc -secure_comm -regenerate_cert
   Linux/Unix:
   /opt/omni/bin/omnicc -secure_comm -regenerate_cert
2. 在 Cell Manager 主机上运行以下命令以重新配置新的客户机证书:
   Windows：
   <DP_Home>\bin\omnicc -secure_comm -reconfigure_peer [client_host_name]
   Linux/Unix:
   /opt/omni/bin/omnicc -secure_comm -reconfigure_peer [client_host_name]

重新生成应用程序服务器证书

您可以使用现有的或新的应用程序服务器 ID 来重新生成应用程序服务器证书。

使用现有的应用程序服务器用户 ID 和服务器 ID 重新生成证书:

1. 运行以下命令：
   - **Windows**：

     perl "<DP_Home>\bin\omnigencert.pl" -recreate
   - **UNIX/Linux**:

     perl "/opt/omni/sbin/omnigencert.pl" -recreate
2. 停止 Data Protector 服务。
3. 启动 Data Protector 服务。

使用新的应用程序服务器 ID 重新生成证书

1. 运行以下命令：
   - **Windows**：

     perl "<DP_Home>\bin\omnigencert.pl" -server_id hostname.domain.net
   - **UNIX/Linux**:

     perl "/opt/omni/sbin/omnigencert.pl" -server_id hostname.domain.net

   其中，
   - *hostname.domain.net* 是 Cell Manager 主机的 FQDN。该值必须与 server_id 参数中指定的值相同。

2. 停止 Data Protector 服务。
3. 启动 Data Protector 服务。

配置自定义证书

在安装过程中，通过指纹验证，基于 OpenSSL 的自签名证书用于安全通信，以建立信任。如果您需要使用自定义证书，可以在安装 Data Protector 后，将 Data Protector 安装过程中生成的 OpenSSL 证书替换为自定义证书。以下步骤用于生成自定义证书、重新生成证书和重新分发证书。

> 注意不支持通配符证书 (公用名称或 SAN 名称中包含星号 "*")。

INET 通信的自定义证书

在安装期间，Data Protector 会生成用于 INET 代理通信的自签名证书。

要使用由受信任的机构签名的自定义证书，请执行以下步骤：

> 注意 <DP_CONFIG_PATH> (以下步骤中所提) 在 Windows 中默认为 C:\ProgramData\OmniBack\Config ，在 UNIX 中默认为 /etc/opt/omni 。

对于独立 Cell Manager 和客户端安装

1. 在所有客户端和 Cell Manager 上生成证书签名请求 (CSR)。这会在目录中生成 **localhost_csr.csr** <DP_CONFIG_PATH>\client\sscertificates\.

   Windows：

   ```
   cd "C:\Program Files\OmniBack\bin"
   perl.exe omnigencertss.pl -get_ssl_csr –hostname <virtual hostname>
   ```

   UNIX：

   ```
   /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl -get_ssl_csr –hostname <virtual hostname>
   ```

2. 将生成的 **localhost_csr.csr** 文件提交给第三方受信机构，并获取相应的证书。将其复制到以下目录：

   <DP_CONFIG_PATH>\client\sscertificates\ (作为 **localhost_cert.pem**)

3. 将 CA 证书复制到以下位置:

   <DP_CONFIG_PATH>\client\sscertificates\cacert.pem

   如果证书链中存在中间 CA，则应将链中的所有 CA 证书合并到一个 cacert.pem 文件中。将 CA 证书合并到单个文件中时，请从签署最终实体证书的 CA 证书开始。每个相应的证书都必须直接认证前一个证书。根证书应当是最后一个。

4. 重新启动系统上的 Data Protector INET 服务。

默认情况下，证书指纹打印验证会根据已知的存储证书来验证证书。无论是自签名证书还是自定义证书，它都有效。

对于 Cell Manager 群集安装

> 注意如果目录 “sscertificates” 尚不存在，则必须在 <DP_CONFIG_PATH>\server\ 下创建该目录。
>
> 建议在安全的位置保留此自定义证书和 **localhost_key.enc** 文件的副本。

1. 在 Cell Manager 的节点之一中生成证书签名请求。这会在目录中生成 **localhost_csr.csr** <DP_CONFIG_PATH>\client\sscertificates\.

   Windows：

   ```
   cd "C:\Program Files\OmniBack\bin"
   perl.exe omnigencertss.pl -get_ssl_csr –hostname <virtual hostname>
   ```

   UNIX：

   ```
   /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl –hostname <virtual hostname> -get_ssl_csr
   ```

2. 将生成的 **localhost_csr.csr** 文件提交给第三方受信机构，并获取相应的证书。将其复制到以下目录：

   <DP_CONFIG_PATH>\client\sscertificates\ 在集群的所有节点上为 **localhost_cert.pem**。

   <DP_CONFIG_PATH>\server\sscertificates\ 在集群的活动节点上为 **localhost_cert.pem**。

3. 将 CA 证书复制到群集所有节点上的以下位置:

   <DP_CONFIG_PATH>\client\sscertificates\cacert.pem

   如果证书链中存在中间 CA，则应将链中的所有 CA 证书合并到一个 cacert.pem 文件中。将 CA 证书合并到单个文件中时，请从签署最终实体证书的 CA 证书开始。每个相应的证书都必须直接认证前一个证书。根证书应当是最后一个。

4. 重新启动系统上的 Data Protector INET 服务。

默认情况下，证书指纹打印验证会根据已知的存储证书来验证证书。无论是自签名证书还是自定义证书，它都有效。

对于自定义证书，可以通过将 omnirc 选项 OB2_ENABLE_INET_ASV 设置为 1 来强制执行以下验证。

- 所有 CA 证书都应包含基本约束扩展，并将 CA 标志设置为 **true**，将密钥用法字段设置为 **CERTSign**。
- 最终实体证书应包含密钥用法和密钥用法扩展。
- 服务器证书在扩展密钥用法字段中应包含服务器身份验证和客户机身份验证。
- 如果应执行 OCSP 吊销检查，请相应地启用 omnirc 变量 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 。

重新生成证书

请运行以下命令以在 Data Protector 中重新生成证书:

```
omnicc -secure_comm -regenerate_cert
```

在群集感知 Cell Manager 安装中重新生成证书

在活动节点上运行以下命令，以生成将 CN 作为 Cell Manager 虚拟主机名的证书:

使用 omnicc -secure_comm -regenerate_cert 命令重新生成证书后，在群集的所有节点上，将新生成的证书和密钥文件 (localhost_key.enc 和 localhost_cert.pem) 从 **<OMNI_DATA>/config/server/sscertificates** 目录安全地复制并替换到 **<OMNI_DATA>/config/client/sscertificates** 目录。

在活动节点上，将新生成的证书和密钥文件 (localhost_key.enc 和 localhost_cert.pem) 从 <OMNI_DATA>/config/client/sscertificates 目录复制到 <OMNI_DATA>/config/server/sscertificates directory 。

之后，将 cacerts 文件从活动节点的以下位置复制到辅助节点：

Windows :

```
C:\Program Files\OmniBack\jre\lib\security
```

UNIX :

```
/opt/omni/jre/lib/security
```

重新分发证书

证书的重新分发必须在使用自定义证书时或将要重新生成证书时完成。

重新分发 Cell Manager 证书

1. 通过运行以下命令，在所有安装服务器 (所有 Windows 和 Unix) 中重新配置 Cell Manager 证书:

   ```
   omnicc -secure_comm -reconfigure_peer <CM hostname>
   ```

2. 要重新分发和重新配置，必须在 CM 上运行以下命令：

   ```
   omnicc -secure_comm -reconfigure_peer_all <input_file_path>
   ```

   <input_file_path> 参数为可选。该文件应该具备属于该单元的所有客户机的凭据。

   文件的格式为：

   ```
   -host "linux_client_hostname" -user "<username>" -pass "password"
   ```

   ```
   -host "windows_client_hostname" -user "<Domain>\<username>" -pass "<password>"
   ```

   这里，每行对应一个客户机，如上所示，必须提及用户名和密码。

   如果未指定 <input_file_path> ，尝试重新分发和配置 Cell Manager 证书时， omnicc 会提示客户机凭据。

   > **注意**对于 Windows 客户机， Domain 名称必须带有前缀。

重新分发客户机证书

如果重新生成客户机证书，则必须重新分发至 Cell Manager。运行以下命令：

```
omnicc -secure_comm -reconfigure_peer <client_host_name>
```

> **注意**对于群集感知 Cell Manager 安装，在重新生成或续订证书后，必须将新证书和密钥文件复制到活动和被动节点的 /etc/opt/omni/client/sscertificates/ 或 <OMNI_DATA/config/client/sscertificates path 。对于 Windows 群集，需要重新启动服务。

用于报告的证书

“报告”上下文中的“通知”部分添加了 **WarnCertificateExpiry** 通知。

借此，用户可为即将过期的证书生成通知。

默认情况下，为即将在 7 天后过期的证书生成通知。通过更改全局变量 **WarnCertificateExpiryBefore** 的值，可生成更早的通知。

AppServer 的自定义证书

在安装期间，Data Protector 会为 AppServer 生成自签名证书。或者，您可以在 Data Protector 之外生成服务器密钥和 CSR，并将其导入到 Data Protector AppServer 中。

要将自定义 CA 签名的自定义证书导入 AppServer 信任库，请执行以下步骤:

1. 生成服务器证书签名请求 (CSR)。以下命令在目录 <DP_CONFIG_PATH>\server\certificates_thirdparty 中生成 CSR 文件和私钥文件。

   Windows：

   "%DP_HOME_DIR%bin\perl.exe" "%DP_HOME_DIR%bin\omnigencert.pl" -get_ssl_csr -server_id <CellManagerHost>

   UNIX：

   /opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -get_ssl_csr -server_id <CellManagerHost>

   建议将生成的私钥文件 (**serverkey.pem**) 的副本保留在安全的位置。

2. 将生成的 **server.csr** 文件提交给第三方受信机构，并获取相应的证书。将它以 **server.pem** 复制到临时文件夹中。

   建议将自定义证书的副本保留在安全的位置。

3. 将现有证书文件夹 (<DP_CONFIG_PATH>\server\certificates) 复制到 Cell Manager 中的临时文件夹。
4. 如果涉及中间证书颁发机构，请通过将 CA 证书合并到单个文件中来创建连接的 **pem** 文件。从签署最终实体证书的 CA 证书开始。每个相应的证书都必须直接认证前一个证书。根证书应采用以下格式的最后一个：

   ```
   -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE-----
   ```

5. 运行以下命令，将签名证书导入 AppServer 密钥库:

   Windows：

   "%DP_HOME_DIR%bin\perl.exe" "%DP_HOME_DIR%bin\omnigencert.pl" -import_ssl_certs -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

   UNIX：

   /opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -import_ssl_certs -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

6. 在以下位置将文件夹 **certificates_thirdparty** 重命名为 **certificates** (如果未自动执行):

   <DP_CONFIG_PATH>\server\

7. 通过运行 omnisv -restart 命令重新启动 Data Protector 服务。

要在 Data Protector 之外生成服务器密钥和 CSR，并将其导入到 AppServer 中，请运行以下命令:

Windows

"%DP_HOME_DIR%bin\perl.exe" "%DP_HOME_DIR%bin\omnigencert.pl" -import_ssl_key_certs -server_private_key <Full_path_to_server_private_key.pem> -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

Unix

/opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -import_ssl_key_certs -server_private_key <Full_path_to_server_private_key.pem> -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

对于自定义证书，可以通过将 omnirc 变量 OB2_ENABLE_APP_SERVER_ASV 设置为 1 来强制实施以下其他证书验证。

- 所有 CA 证书都应包含基本约束扩展，并将 CA 标志设置为 true，将密钥用法字段设置为 **CERTSign**。
- 最终实体证书应包含密钥用法和扩展密钥用法扩展。
- 服务器证书在扩展密钥用法字段中应包含服务器身份验证 。
- 此外，如果应该执行 OCSP 吊销检查，请相应地启用 omnirc 变量 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 。

omnirc 选项

以下 omnirc 选项可用于由外部 CA 签名的自定义证书的其他安全验证：

OB2_ENABLE_INET_ASV=0

默认值： 0

将此变量设置为非零值可为 INET 通信启用其他证书验证。

如果启用，除指纹验证外，还将执行以下验证：

- Data Protector 将验证 CA 证书是否包含将 CA 标志设置为 true 的基本约束扩展，以及密钥用法字段是否包含 **CERTSign**。
- Data Protector 将验证自定义证书是否包含扩展密钥用法扩展。
- 作为客户机的 Data Protector 将验证服务器证书的扩展密钥使用字段中是否存在“服务器身份验证”。
- 作为客户机的 Data Protector 将验证服务器证书是否包含基本约束扩展并将 CA 标志设置为 false。

仅当使用自定义证书并且包含中间 CA 证书和根 CA 证书列表的 CA 证书链文件以 **cacert.pem** 形式保存在所有 Data Protector 客户机和 Cell Manager的 **sscertificates** 目录中时，才应启用此功能。

在以下位置中找到 **sscertificates** 目录:

C:\Program Data\OmniBack\Config\client\ （在 Windows 系统中），/etc/opt/omni/client/ （在 UNIX 系统中）。

OB2_ENABLE_APP_SERVER_ASV=0

默认值： 0

将此变量设置为非零值可为应用程序服务器通信启用附加证书验证。

- Data Protector 将验证 CA 证书是否包含基本约束扩展，并将 CA 标志设置为 true，密钥用法字段包含 **CERTSign**。
- Data Protector 将验证自定义证书是否包含扩展密钥用法扩展。
- 作为客户机的 Data Protector 将验证服务器证书的扩展密钥使用字段中是否存在“服务器身份验证”。

仅当按说明使用自定义证书时，才应启用此功能。

OB2_ENABLE_INET_SERVERSIDE_ASV=0

默认值： 0

设置此变量可为通信的服务器端上的 INET 通信启用附加证书验证。

如果启用，除了服务器端的指纹验证外，还将执行以下验证。

- Data Protector 将在 CA 标志设置为 true 且密钥使用字段设置为 **CERTSign** 的情况下验证 CA 证书的基本约束扩展。
- Data Protector 将验证自定义证书是否包含扩展密钥用法扩展。
- 作为服务器的 Data Protector 将验证客户机证书的扩展密钥使用字段中是否存在“客户机身份验证”。
- 作为服务器的 Data Protector 将验证客户机证书是否包含基本约束扩展，并将 CA 标志设置为 false。

仅当启用 OB2_ENABLE_INET_ASV 时适用。

OB2_SKIP_CERT_FIELDS_ASV=0

默认值： 0

将此变量设置为非零值可跳过证书中的基本约束、密钥用法和扩展密钥用法字段验证。

将此变量设置为仅执行证书吊销检查（OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 设置为非零值时）。

OB2_CERT_CHAIN_MAX_DEPTH=9

默认值： 9

有效值：1 - 9

将此变量设置为应允许的证书链的最大深度。

OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV=0

默认值： 0

指定 OCSP 证书吊销检查级别。

0 -禁用 OCSP 吊销检查。

1 -为证书链启用了 OCSP 吊销检查。

2 -仅对最终实体证书启用了 OCSP 吊销检查。

仅在启用 OB2_ENABLE_INET_ASV 或 OB2_ENABLE_APP_SERVER_ASV 时适用。OCSP 验证仅支持 "http" URL。不支持 "https" URL。

OB2_CERT_VALID_IF_UNKNOWN_OCSP_RESPONSE_ASV=0

默认值: 0

设置此变量以接受其 OCSP 吊销状态为 V_OCSP_CERTSTATUS_UNKNOWN 的证书。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

OB2_CERT_VALID_IF_OCSP_FAILED_ASV=0

默认值: 0

设置此变量以接受无法验证其 OCSP 吊销状态的证书。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

OB2_OCSP_REQUEST_TIMEOUT=30 seconds

默认值：30 秒。

设置此变量可调整 OCSP 响应的等待时间。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

OB2_OCSP_CHECK_NONCE=1

默认值： 1

将此变量设置为 0 以禁用检查 OCSP 响应的随机数。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

OB2_OCSP_RESPONSE_LEEWAYTIME=300 seconds

默认值：300 秒

为了避免拒绝有效的响应，请允许时间自当前时间起的 OB2_OCSP_RESPONSE_LEEWAYTIME 之内。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

OB2_OCSP_RESPONSE_MAXAGE=300 seconds

默认值：300 秒

为避免接受非常旧的响应，此参数指定可以接受的最大响应期限。

仅在启用 OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV 时适用。

从 GUI 连接

如果使用已安装单元控制台组件的主机来连接多个 Cell Manager，安装 CC 组件的主机应受到其试图连接的 Cell Manager 的保护，并且所有 CM 都应使用 GUI 主机进行保护。

例如：

案例 1：

如果主机 X 用于连接 Cell Manager 主机 CM1、主机 CM2 和主机 CM3 (都为 10.00 或更高版本)，在主机 X 中运行以下命令:

```
Omnicc –secure_comm –configure_peer <hostCM1>
```

```
Omnicc –secure_comm –configure_peer <hostCM2>
```

```
Omnicc –secure_comm –configure_peer <hostCM3>
```

在上述提及的所有 Cell Manager 中运行以下命令:

```
Omnicc –secure_comm –configure_peer <hostX>
```

案例 2：

如果主机 X 为 2019.02 之前的版本，而主机 CM1、主机 CM2 和主机 CM3 为 10.00 或更高版本，请在所有三个 Cell Manager 中运行以下命令:

```
Omnicc –secure_comm –configure_for_gui <hostX>
```

案例 3：

如果 CM 的主机为 10.00 之前的版本，而主机 X 为 10.00 或更高版本，在主机 X 中执行以下命令：

```
Omnicc –secure_comm –configure_for_gui <hostCM1>
```

```
Omnicc –secure_comm –configure_for_gui <hostCM2>
```

```
Omnicc –secure_comm –configure_for_gui <hostCM3>
```

案例 4：

如果主机 CM1 为 10.00 之前的版本，主机 CM2 和 主机 CM3 和主机 X 为10.00 或更高版本。在主机 X 中运行以下命令：

```
Omnicc –secure_comm –configure_for_gui <hostCM1>
```

```
Omnicc –secure_comm –configure_peer <hostCM2>
```

```
Omnicc –secure_comm –configure_peer <hostCM3>
```

在主机 CM2 和主机 CM3 中运行以下命令

```
Omnicc –secure_comm –configure_peer <hostX>
```

使用 GUI 客户机连接到 Cell Manager

在建立安全通信信任关系后，连接到 Cell Manager。如果登录的用户不是 Data Protector 用户，请按照以下步骤添加用户。

1. 使用 GUI (“用户”上下文) 或 CLI (omniusers -add) 添加主机 X 详细信息 (用户名、域、客户机和密码)。
2. 要使用户连接到 Data Protector GUI，需要将密码与帐户关联。
3. 从 GUI 连接到 Cell Manager。

严格检查主机名

默认情况下，Cell Manager 使用相对简单的方法验证用户。它使用已启动用户界面或应用程序代理的客户机已知的主机名。此方法比较容易配置，并在将安全视为“建议”（即预计不会出现恶意攻击）的环境中可提供合理的安全级别。

而另一方面，严格主机名检查设置提供了增强的用户验证。这种验证使用由 Cell Manager 根据从连接中获得的 IP 地址进行反向 DNS 查询所解析的主机名。要启用严格主机名检查，请将 StrictSecurityFlags 全局选项设置为 0x0001 。

限制

- 基于 IP 的用户验证的强度仅相当于网络中的防欺骗保护。安全性设计人员必须确定现有网络提供的防欺骗安全性级别是否足以满足特定的安全性要求。通过用防火墙、路由器、VPN 等将网络分段可以实现防欺骗保护。
- 特定客户机内用户间的分离不如客户机间的分离强大。在高安全环境中，不应在相同客户机中混合存在常规用户和高权限用户。
- 规范中使用的主机无法配置为使用 DHCP，除非将它们绑定到固定 IP 并在 DNS 中进行配置。

请了解这些限制，以便正确地评估通过此设置所能达到的安全程度。

要求

增强的验证不会自动对某些内部连接授予访问权限。因此，使用此验证后，必须为以下程序添加新用户：

- Windows 客户机中的任何应用程序代理 (OB2BAR)。必须为每个装有应用程序代理的客户机添加用户 SYSTEM 、 NT AUTHORITY 和 client 。请注意，如果将某客户机上的 Inet 配置为使用特定帐户，则必须已配置该帐户。

主机名解析

在以下情况下，Data Protector 用于验证的主机名可能在默认用户验证与严格主机名检查间有所区别：

- 反向 DNS 查询返回不同的主机名。这可能是有意所为，或表明客户机或反向 DNS 表配置错误。
- 客户机是多宿主的（有多个网络适配器和/或多个 IP 地址）。此注意事项是否适用于特定的多宿主客户机，取决于该客户机在网络中的角色及在 DNS 中对其的配置方式。
- 客户机是群集。

通过此设置启用的检查的性质可能要求重新配置 Data Protector 用户。必须检查 Data Protector 用户的现有规范，以查看这些用户是否可能受到以上任何原因的影响。根据不同情况，可能需要更改现有规范，或添加新规范，以包含所有可能发出连接的 IP。

请注意，如果启用严格的主机名检查时必须修改用户规范，则当恢复到默认用户验证时也必须重新配置用户。因此，建议确定想要使用的用户验证并坚持使用下去。

可靠的反向 DNS 查询的先决条件是安全性的 DNS 服务器。您必须防止对所有未授权人员的物理访问和登录。

通过使用 IP 进行验证（而非使用主机名），可解决某些潜在的与 DNS 相关的验证问题，但维护起来比较困难。

相关主题

相关任务

- 添加用户

配置主机信任

可以定义一组主机，彼此信任对方的数据。

完成以下步骤：

1. 在 Windows Cell Manager 上，创建 Data_Protector_program_data\Config\Server\cell\host_trusts 文件。

   在 Linux Cell Manager 上，创建 /etc/opt/omni/server/cell/host_trusts 文件。

2. 在文件中，列出受信任主机。

   例如：

   ```
   GROUP="cluster.domain.com" { cluster.domain.com node1.domain.com node2.domain.com } GROUP="DFG" { computer.domain.com anothercomputer.domain.com }
   ```

3. 保存文件。

Data Protector 中的端口使用情况

下表提供了有关 Data Protector 外部的不同 Data Protector 组件和系统的网络通信要求 (使用的端口) 的信息。Data Protector 客户机 (包括 Cell Manager) 之间的大多数通信都使用 Data Protector INET 端口。

> 注意**:** 如果需要，可以使用 omnicc 命令更改客户机或整个单元的 Data Protector INET 端口。Cell Manager 和 Data Protector 单元的所有客户机必须使用相同的 INET 端口才能彼此通信。

默认情况下，对于 Data Protector 10.x 的新部署，Data Protector INET 端口为 5565；对于从 Data Protector 9.x 及更早版本升级的环境，Data Protector INET 端口为 5555。

主 Data Protector 实体	辅助 Data Protector 实体或外部实体	TCP 端口	附加信息
Cell Manager	装有 Data Protector 9.09 及更高版本的客户机	INET	客户机通信和数据传输，需要双向通信。
	装有 Data Protector 9.09 之前的版本的客户机	INET、动态端口	客户机通信和数据传输。可以使用 omnirc 选项配置动态端口 OB2PORTRANGE.
	OpenVMS 上的客户机	INET、动态端口	客户机通信和数据传输。可以使用 omnirc 选项配置动态端口 OB2PORTRANGE.
	Data Protector GUI	INET、7116	Windows 客户机上的图形用户界面，用于管理 Cell Manager。GUI 实例连接到 Cell Manager 上的端口 7116。
	报告服务器	7116、8443 (默认值)	将报告服务器连接到 Cell Manager。报告服务器连接到 Cell Manager 上的端口 7116，而 Cell Manager 连接到报告服务器上的端口 8443 (或另一个已配置的端口)。
	外部 Cell Manager	INET、7116	导入外部 Cell Manager 以进行自动替换同步 (ARS)。
	MoM Cell Manager	INET、7112、7116	Managers Manager 配置中的 Cell Manager 之间的连接。
	vCenter Server 上的 VMware GRE 插件	INET、7116	从 vCenter 进行的 VMware VM 粒度恢复。GRE 插件连接到 Cell Manager 上的端口 7116。
Windows 安装服务器	未安装 Data Protector 的新客户机	139、445	通过 SMB 的 Windows 客户机远程安装。
	现有客户机，Data Protector 10.20 (2018.11) 之前的版本	139、445	通过 SMB 的 Windows 客户机远程安装或升级。
	现有客户机，Data Protector 10.20 (2018.11) 版及更高版本	INET	通过 Data Protector INET 的 Windows 客户机远程安装或升级。
Linux 安装服务器	未安装 Data Protector 的新 Linux 客户机	22	通过 SSH 的 Linux 或 UNIX 客户机远程安装。
	现有客户机，Data Protector 10.20 (2018.11) 之前的版本	22	通过 SSH 的 Linux 或 UNIX 客户机远程安装或升级。
	现有客户机，Data Protector 10.20 (2018.11) 版及更高版本	INET	通过 Data Protector INET 的 Linux 或 UNIX 客户机远程安装或升级。
介质代理	数据域提升设备	111、2049、2051	Dell EMC 数据域中使用的数据域提升协议。
	StoreOnce Catalyst 设备	9387、9388	HPE StoreOnce 备份系统中使用的 StoreOnce Catalyst 协议。
	StoreOnceSoftware	9387、9388	Data Protector StoreOnceSoftware 中使用的 StoreOnce Catalyst 协议。
	CIFS 共享上的文件库	139、445	用于访问 CIFS/SMB 共享的 SMB 协议。
	云原生设备 (Azure、S3 或兼容)	443	与 Blob 存储的 HTTPS 连接。
	ACSLS	30031	SSI 代理与 ACSLS 控制之间的通信。可能需要其他配置才能限制与此端口的通信。
NDMP 介质代理	双向 NDMP 配置中的 NAS 系统	10000	管理 NAS 系统和 NDMP 操作。
	三向 NDMP 配置中的 NAS 系统	10000、动态端口	管理 NAS 系统和 NDMP 操作。动态端口是使用 NDMP StoreOnce 或文件库时同时处理的最大对象数。可以使用 omnirc 选项配置动态端口 OB2PORTRANGE.
磁盘代理	CIFS 共享的备份/还原	139、445	在 CIFS 共享中备份和还原数据时使用。
Hyper-V 备份主机 (VEPA)	Hyper-V 服务器	INET、135、5986	在 Hpyer-V 主机或群集上管理 VM 和 Hyper-V 快照。

主 Data Protector 实体	辅助 Data Protector 实体或外部实体	TCP 端口	附加信息
VMware 备份主机 (VEPA)	VMware ESXi 主机	443、902	在主机上管理 VM 和 VMware 快照，从磁盘获取更改后的块。
	VMware ESXi 主机	111、2049	从备份主机上的临时 NFS 共享进行 VM 的 PowerOn 和 LiveMigrate。
	VMware vCenter 服务器	443	在 vCenter 托管的主机或群集上管理 VM 和 VMware 快照。
VMware 装载代理	vCenter Server 上的 VMware GRE 插件	INET	从 VMware GRE 插件到装载代理的通信。
	Windows 目标 VM 上的文件恢复	139、445	将单个项目 (GRE) 直接还原到 Windows (SMB) 上运行的 VMware VM。
	Linux 目标 VM 上的文件恢复	111、2049	将单个项目 (GRE) 直接还原到 Linux (NFS) 上运行的 VMware VM。
	带智能缓存设备的系统	139、445	智能缓存设备上存储的 VM 的 PowerOn、LiveMigrate 和 VMware GRE。

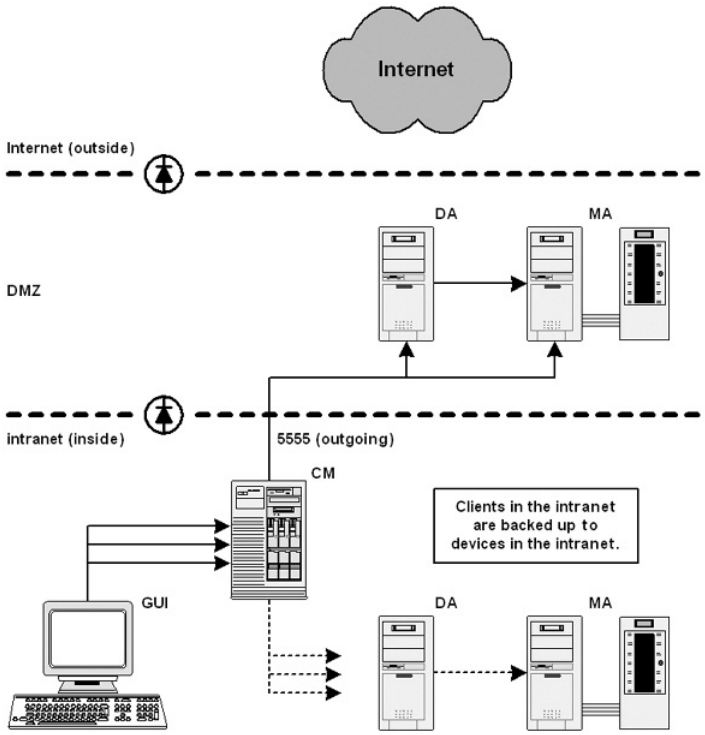
相关主题

- DMZ 中的磁盘代理、介质代理和应用程序代理
- DMZ 中的磁盘代理和应用程序代理
- 防火墙支持

DMZ 中的磁带客户机和介质代理

可以配置备份环境，以使 Cell Manager 和 GUI 在内部网中，并使某些磁盘代理、应用程序代理和介质代理在 DMZ 中。

配置图



打开的端口

Data Protector 打开以下端口进行配置：

1. 磁盘代理和介质代理需要在端口 5555/5565 上接受来自会话管理器的连接：
   - 允许 CM 系统连接到 DA 系统中的端口 5555/5565
   - 允许 CM 系统连接到 MA 系统中的端口 5555/5565
2. 启用**重新连接已断开的连接**时，MA 和 DA 连接到会话管理器：
   - 允许 MA 和 DA 系统连接到 CM 系统中的端口 5555/5565
3. 应用程序代理需要连接至会话管理器和 CRS：
   - 允许应用程序服务器系统连接到 CM 系统中的端口 5555/5565

- 第 2 点和第 3 点允许从 DMZ 连接到 内部网，这是一个潜在的安全风险。
- 在备份和生产网络的情况下，需要通过每个 IP 地址配置或导入主机两次。还必须为备份网络配置安全通信。

限制

- 此单元可以备份 DMZ 中的客户机以及 Intranet 中的客户机。但是，必须将每组客户机都备份到在位于防火墙同端的客户机上配置的设备。

  如果防火墙不限制从 Intranet 到 DMZ 的连接，则可以将 Intranet 中的客户机备份到在 DMZ 中客户机上配置的设备。但是，建议不要这样做，因为以此方式备份的数据更容易受到攻击。

- 如果 DMZ 中的设备具有在不同客户机上配置的机械手，则此客户机也必须在 DMZ 中。

DMZ 中的磁盘代理和应用程序代理

您可以按如下方式配置备份环境:

- Intranet 包含 Cell Manager (CM)、介质代理 (MA) 和 GUI。
- DMZ 网络包含磁盘和应用程序代理 (DA)。

> 注意**:** 您必须在 DMZ 中本地安装客户机，因为不支持跨防火墙远程安装客户机。

打开的端口

Data Protector 打开以下端口进行配置：

1. 磁盘代理需要在端口 5555/5565 上接受来自会话管理器的连接。因此，允许 CM 系统连接到 DA 系统中的端口 5555/5565
2. 磁盘代理需要连接到 MA 系统中的端口 5555/5565: 因此，允许 DA 系统连接到 MA 系统中的端口 5555/5565。

> 注意**:** 此规则允许从 DMZ 连接到 Intranet，这是一个潜在的安全风险。

3. 启用“重新连接已断开的连接” 选项时，DA 连接到会话管理器: 因此，允许 DA 系统连接到 CM 系统中的端口 5555/5565。
4. 应用程序代理需要连接至会话管理器和单元请求服务器 (CRS): 因此，允许应用程序代理系统连接到 CM 系统中的端口 5555/5565。

通用标准指南

本节提供 Micro Focus Data Protector 2021.02 发布的通用标准配置的必需信息。此发布的对应软件版本为 A.10.91，可以使用此版本在目标系统中识别该软件。

重要说明Data Protector 发布 2020.05、软件版本 A.10.70 已通过国家信息安全保证联盟 (NIAP) 通用标准评估和验证方案 (CCEVS) 认证。
https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11048
在当前发布中，Micro Focus 验证了相同的安全功能要求，并且本节中提供了当前发布的相关配置步骤。

重要说明必须按照本节所述安装并配置，Data Protector 部署才会满足通用标准要求。本节中提到的任何配置或限制将覆盖文档其他章节中的任何冲突建议。

目标系统

您必须在非群集环境中的 Windows Server 2016 操作系统上安装 Data Protector。可以在硬件平台上运行该操作系统或在 VMware ESXi 虚拟环境中进行部署。Data Protector 的评估测试是在 Intel Xeon Gold 6140 处理器上运行的 VMware ESXi 6.5 上部署的 Windows Server 2016 Standard 上完成的。

未评估和不包括的功能

评估配置不包括 Data Protector 的下列功能:

- 远程管理 — 在评估配置中，用户界面组件只能安装在 Cell Manager 角色中的 TOE 实例所在的平台上，因此为 Cell Manager 提供了本地管理。用户界面不得安装在网络中的其他平台（例如管理员工作站）上，并且不支持远程管理。
- 远程身份验证 — Data Protector 支持使用 LDAP 进行远程身份验证，但是此功能未经测试，也不是 Data Protector 使用 TLS 保护与外部 LDAP 服务器的通信的功能。
- REST API — Data Protector 提供 REST API 以访问管理功能，但是此接口不用于评估配置。

安装

必须按照安装一节所述的安装过程安装 Data Protector。

您还必须安装 Microsoft 发布的所有最新安全补丁，以解决发现的漏洞。

配置

本节所述的配置步骤必须在安装 Data Protector 后立即执行一次。这些步骤将确保 Data Protector 安装满足与凭据和私钥存储、x509 证书验证、加密算法使用等相关的要求。

1. 在所有客户机主机和 Cell Manager 主机上，激活安装 Data Protector 的驱动器上的 BitLocker 加密。
2. 在所有客户机主机和 Cell Manager 主机上，确保仅使用经 FIPS 批准的加密算法。为此，在 Data Protector 主目录中的 omnirc 文件中将 OB2_ENABLE_FIPS_MODE 变量设置为 1。有关详细信息，请参阅配置 omnirc 变量。
3. 在 Cell Manager 主机上，为 KMS 密钥库启用基于 Windows DP-API 的加密。为此，在 Data Protector 主目录中的 omnirc 文件中将 OB2_ENABLE_KMS_PLATFORM_ENCR 变量设置为 1。有关详细信息，请参阅配置 omnirc 变量。
4. 在所有客户机主机和 Cell Manager 主机上，安装自定义证书和安全私钥，以满足通过 INET 通信的证书和协议要求。有关详细信息，请参阅确保 Cell Manager 与客户机之间的 TLS 通信 (INET 通信) 的安全。
5. 在所有客户机主机和 Cell Manager 主机上，启用验证以满足所有证书验证要求。有关详细信息，请参阅为 INET 通信启用自定义证书验证。
6. 在 Cell Manager 和客户机之间的安全通信期间，为证书验证建立引用标识，如下所示:
    1. 在 Data Protector 环境中，在 Cell Manager 主机中为每个客户机主机运行一次以下命令，以在 Cell Manager 中存储客户机的引用标识:
       omnicc -secure_comm -configure_peer <client hostname>
       验证提供的主机名是否与命令参数中提供的主机名匹配，并接受证书。
    2. 在每个客户机上运行以下命令，以在每个客户机主机上存储 Cell Manager 的引用标识:
       omnicc -secure_comm -configure_peer <client hostname>
       验证提供的主机名是否与命令参数中提供的主机名匹配，并接受证书。完成此设置后，在每次连接请求期间都会自动向传入证书验证引用标识符。
7. 由于在网络上通过 https 协议提供 REST 接口的应用服务器被排除在评估之外，请按照以下步骤防止通过网络访问应用程序服务器:
    1. 要允许 Cell Manager 中的客户机应用程序访问环回接口上的应用程序服务器，请将 omnirc 变量 OB2_APPS_RESTRICT_TO_LOOPBACK 设置为 1。有关详细信息，请参阅配置 omnirc 变量。
    2. 要将应用程序服务器重新配置为仅侦听环回接口，请执行以下命令:
       C:> cd C:\Program Files\OmniBack\bin
       C:\Program Files\OmniBack\bin> perl.exe omniasutil.pl -remoteguiconnection disable
       其中， C:\Program Files\OmniBack 是安装期间可自定义的安装目录。

Micro Focus OpenSSL 模块用于已通过 NIST 认证的 INET 通信上的加密操作: https://csrc.nist.gov/projects/cryptographic-algorithm-

validation-program/details?validation=32281

无需与加密模块相关的手动配置即可满足通用标准要求。在 Data Protector 的通用标准评估期间，未评估或测试其他加密模块 (应用程序服务器中的 Bouncy Castle) 的使用。

自定义

配置步骤完成后，系统自动满足通用标准的所有其他要求。但是，本节提供了一些您必须遵守的其他配置原则，以避免偏离通用标准要求。

配置 TLS 版本

默认情况下，仅支持符合通用标准要求的 TLS 版本 v1.2。因此，管理员不得尝试手动更改或配置 TLS 版本。

配置密码套件

下表列出了默认情况下 Data Protector 支持的所有密码套件 (采用 IANA 格式和相应的 OpenSSL 格式)。

IANA 格式	**OpenSSL 格式**
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384

无需更改任何配置以满足通用标准要求。但是，如果需要更改该列表，则有可能是进一步限制使用的密码。

将变量 OB2SSLCIPHERLIST 设置为要支持的密码列表，采用 OpenSSL 格式，用冒号 (:) 分隔。

例如，要将支持的密码限制为 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256，则在 omnirc 文件中设置以下内容:

```
OB2SSLCIPHERLIST=DHE-RSA-AES128-SHA256
```

加密密钥生成

对于用于实体身份验证的 x.509 证书，Data Protector 使用密钥大小为 4096 位、符合 FIPS 186-4 标准的 RSA 方案生成非对称加密密钥。密钥生成方案和密钥大小都是不可配置的。
对于 TLS 密钥建立，支持符合 FIPS 186-4 标准的 ECC 和 FFC 方案。
方案选择基于连接期间协商的密码套件。
如果协商以 TLS_ECDHE 开头的密码套件，则选择 ECC 方案。密钥交换期间使用的 secp256r1、secp384r1 和 secp521r1 密钥大小是不可配置的。
如果协商以 TLS_DHE 开头的密码套件，则选择 FFC 方案。使用的 DHE 密钥大小为 2048，不可配置。

软件更新

后续 Data Protector 发行版提供了软件更新。您可以从 Data Protector 图形用户界面 (GUI) 检查当前软件版本，如下所示:

在 Cell Manager 主机上，运行 manager.exe 并单击“帮助 > 关于”。弹出窗口显示了产品版本。

在客户机主机上，可以通过运行以下命令确定版本:

```
omnicc –version
```

管理员必须通过定期访问以下链接检查最新发行版:

https://entitlement.microfocus.com/mysoftware/index

Data Protector 作为一组 Windows Installer 文件 (.MSI) 和安装程序分发，所有这些文件都由 Micro Focus 代码签名服务签名。只有在 Data Protector 验证了数字签名的更新后，更新才会成功。您可以使用 Microsoft 的 SignTool 验证安装程序和 MSI 文件的数字签名 (https://docs.microsoft.com/en-us/dotnet/framework/tools/signtool-exe)。可以使用以下命令验证:

```
signtool verify /pa <path_to_msi/setup_file>
```

安装程序根据安装过程中选择的组件自动触发所选单个 MSI 文件的安装。

通用标准配置

本节提供了执行满足通用标准要求所需的特定配置的详细步骤。建议仔细阅读通用标准指南一节，需要时仅使用该节内容作为参考。

配置 omnirc 变量

本节介绍设置 omirc 变量的步骤。在继续操作之前，建议参考 omnirc.tmpl 模板文件。此文件提供有关受支持变量、其使用目的和配置文件语法的信息。它在 <DP_CONFIG_PATH> 中提供。

注意: 除非在安装过程中更改了默认值，否则 DP_CONFIG_PATH 的默认值为 C:\ProgramData\OmniBack\Config 。

1. 在 <DP_CONFIG_PATH> 下使用名称 omnirc 创建文件 (如果它尚未存在)。
2. 编辑在步骤 1 中创建的文件，并在文件的开头或结尾插入新行以设置变量。例如，要将名为 OB2_ENABLE_KMS_PLATFORM_ENCR 的变量设为 1，必须插入一行并添加以下内容: OB2_ENABLE_KMS_PLATFORM_ENCR=1
3. 通过运行以下命令保存文件并重新启动 Data Protector 服务:
   omnisv –restart

当设置多个配置变量时，您可以设置所有必需的变量，然后重新启动服务。

确保 Cell Manager 与客户机之间的 TLS 通信 (INET 通信) 的安全

必须为 INET 通信安装可信 CA 签名的自定义证书，且必须将 RSA 私钥存储在 Windows 证书库中。这对于所有客户机主机和 Cell Manager 主机都是必需的。

1. 要获取用于 INET 通信的自定义证书并在文件系统中安装，请参阅“配置自定义证书”页中的“用于 INET 通信的自定义证书”。按照以下步骤将 RSA 私钥移动到 Windows 证书存储中。
2. 打开命令提示符，并通过运行以下命令切换到 sscertificates 文件夹：
   cd <DP_CONFIG_PATH>\Config\client\sscertificates
   注意: 除非在安装过程中更改了默认值，否则 DP_CONFIG_PATH 的默认值为 C:\ProgramData\OmniBack\Config 。
3. 通过执行以下命令，创建带有证书和私钥的 pkcs12 文件:

   ```
   cd <Install_Folder>\OmniBack\bin\
   perl.exe omnigencertss.pl -get_key_pkcs12 -pkcs_password <YourPassword>
   ```

   其中 <YourPassword> 是您选择的密码，将用于保护 pfx 文件。在下一步骤中必须使用此密码导入 pkcs12 文件。
4. 在 Windows 的本地计算机证书存储中创建文件夹 DPcerts ，并通过运行以下命令来导入密钥：
   certutil -p <YourPassword> -importPFX DPcerts localhost_pfx.pfx
   <YourPassword> 上面命令中的内容应该与您在步骤 2 中指定的相同。
5. 从 <DP_CONFIG_PATH>\config\client\sscertificates 文件夹中删除私钥文件 localhost_key.enc 和 localhost_pfx.pfx 文件。
   注意: 如果以后要使用此私钥重新生成证书签名请求 (CSR)，则必须将其存储在另一个安全位置，在重新生成 CSR 时复制到 sscertificates 文件夹中。
6. 将 omnirc 文件中的 OB2_INET_USE_WIN_CERT_STORE 变量设置为 **1**。
7. 重新启动 Data Protector 服务。

启用 INET 通信的自定义证书验证

此过程应用于所有客户机主机和 Cell Manager 主机。

设置以下 omnirc 变量，以启用通用标准所需的证书验证。

```
OB2_ENABLE_INET_ASV=1

OB2_ENABLE_INET_SERVERSIDE_ASV=1

OB2_ENABLE_OCSP_REVOCATION_CHECK_DEPTH_ASV=1
```

如果需要，使用以下附加变量优化 OCSP 验证行为:

如果应用程序必须接受 OCSP 状态未知的证书，则设置 OB2_CERT_VALID_IF_UNKNOWN_OCSP_RESPONSE_ASV=1 。默认情况下，OCSP 响应中的未知状态导致证书验证失败，因此不接受证书。

如果应用程序必须接受未验证 OCSP 状态的证书，则设置 OB2_CERT_VALID_IF_OCSP_FAILED_ASV=1 。默认情况下，除非状态经过验证且有效，否则不接受证书。

有关值和相应系统行为的详细信息，请参阅配置自定义证书。

设置群集

如何备份群集中的数据

通过 Data Protector 群集集成，可以从以下位置备份数据：

- 本地群集节点磁盘
- 共享群集节点磁盘/池

在 Data Protector GUI 中，本地磁盘列于其所连接的群集节点下方。群集共享磁盘 (在组或包中定义) 在虚拟服务器下列出。这样可防止创建用于备份共享磁盘的备份规范。如果特定群集节点上共享磁盘不可用，则此类备份会失败。

为了区分 MSCS 上的本地群集节点磁盘和共享群集节点磁盘，Data Protector 查询 MSCS 数据库以获取物理群集磁盘资源的列表。将专有群集磁盘资源（例如 NetRAID 4 磁盘类型）形式的所有群集磁盘都视为本地群集节点磁盘。

创建备份规范时，可以看到以下三个或更多个可以备份的系统：

- 活动节点（备份本地磁盘时选择）
- 非活动节点（备份本地磁盘时选择）
- 虚拟服务器（备份共享磁盘时选择）

备份本地磁盘

要备份群集本地磁盘，请确保在要备份的本地磁盘所在的每个群集节点上以本地方式安装了 Data Protector 磁盘代理组件（在 MSCS 上还要安装 MS 群集集成组件）。在 Veritas Cluster 上，将节点导入到 Data Protector 单元。配置备份规范时，指定物理节点名称，并定义要备份其哪些本地磁盘。

备份共享磁盘

要备份群集共享磁盘，请确保已在每个群集节点上安装 Data Protector 磁盘代理组件 (在 MSCS 上还要安装 MS 群集集成组件)，并确保已将虚拟服务器导入 Data Protector 单元。

在 Windows 系统上

配置备份规范时，会显示共享磁盘。需要选择虚拟服务器并定义要备份的共享磁盘。

在 HP-UX 系统中

配置备份规范时，会显示共享磁盘和装载点。需要选择虚拟服务器并定义要备份的共享磁盘。请注意，备份虚拟服务器时，对象所有权将获得运行群集包的固定主机的所有权。因此，当发生故障转移时，相同的对象备份将显示不同的所有权。要避免出现这种情况，请将备份规范中的所有权设置为虚拟服务器。

在 Veritas 群集系统中

从共享磁盘的任何群集节点中只能以本地磁盘的形式备份共享磁盘。为每个节点创建一个备份规范，其中指定相同的共享磁盘。要保护磁盘，请在每个备份规范中指定一个 post-exec 脚本，该脚本将检查是否有错误，并在第一个系统上的备份失败后在其他系统上启动备份。

在 IBM HACMP 群集中

创建备份规范时，指定虚拟服务器作为要从中进行备份的客户机，然后选择要备份的共享磁盘或数据库应用程序数据。

关于备份 Serviceguard 中的数据库应用程序

当备份在与 Cell Manager 同一群集中运行的数据库应用程序时，请注意，如果该应用程序在 Cell Manager 之外的节点上运行，则该应用程序的备份将失败。强烈建议在相同软件包中配置该应用程序和 Cell Manager。

相关任务

- 添加 Data Protector 组件
- 创建备份规范

Data Protector 和 Microsoft 群集服务器集成

作为其高可用性的一部分，Data Protector 可与 Microsoft 群集服务器 (MSCS) 相集成，从而使您可以备份完整群集（本地和共享磁盘）以及群集环境中运行的应用程序。

假定您熟悉 MSCS。如果不熟悉，请参见 MSCS 联机文档获得详细信息。

许可和 MSCS

购买 Data Protector Cell Manager 的许可证时，请注意，许可证将与虚拟服务器绑定，并且无论 MSCS 群集中的哪个系统运行 Data Protector Cell Manager，这个许可证都会起作用。

配置

有两种方式可以配置集成：

- Data Protector Cell Manager 可安装在 MSCS 上。这样可提高 Data Protector Cell Manager 的可用性，并在故障转移时允许在群集节点之间迁移 Data Protector 服务，从而自动重新启动失败的备份会话。
- Data Protector 群集感知客户机可以安装在 MSCS 中，因此支持文件系统备份和群集感知应用程序的备份。

  要备份群集感知应用程序，请在配置备份规范时使用其虚拟服务器名称。

> **注意**群集服务组件（例如数据库管理器）可保持中央群集数据库前后一致，该数据库存储有关节点、资源或组的状态更改的信息。群集数据库必须存储在群集的共享磁盘卷上。

如何管理群集感知备份

在 Data Protector 群集 Cell Manager 中，备份会话是群集感知会话。可以设置相应的选项，定义在发生 Data Protector 或其他群集感知应用程序的故障转移时的备份行为。

Data Protector 的故障转移

如果在备份期间发生群集感知 Data Protector 的故障转移，则所有运行和挂起的备份会话都将失败。在 Data Protector GUI 中和备份规范中，可以设置三个选项之一，来定义在 Data Protector 故障转移时自动重新启动备份会话。

Data Protector 之外应用程序的故障转移

由于群集感知 Data Protector 是群集环境中的存储应用程序，因此它需要了解群集中可能正在运行的其他应用程序。如果这些应用程序正在 Data Protector 以外的节点上运行，并且如果某些应用程序故障转移到正在运行 Data Protector 的节点，则这会导致此节点上的负载较高。因此，以前仅管理过备份操作的节点现在还必须处理关键的应用程序请求。通过 Data Protector，可定义这种情况下应发生什么，以便保护关键应用程序数据，并再次进行负载均衡。

可以：

- 中止所有正在运行的备份会话

  如果备份的重要性低于应用程序，则 Data Protector 可以自动中止所有正在运行的会话，以便在应用程序的故障转移之后均衡负载。

  要设置此选项，需要使用 omniclus 命令创建相应的脚本。
- 临时禁用备份活动

  如果备份的重要性低于应用程序，则 Data Protector 还可以自动将 Cell Manager 禁用一段时间，以便在应用程序的故障转移之后均衡负载。所有正在运行的会话继续运行，但直到再次启用 Cell Manager 时才能启动新的备份。

  要设置此选项，需要使用 omniclus 命令创建相应的脚本。
- 根据已用会话时间中止正在运行的会话

  要在应用程序的故障转移之后均衡负载，可以根据备份会话已运行的时间中止这些会话。如果某个正在运行的特定备份会话刚刚结束，则 Data Protector 可以继续该会话。如果备份会话刚刚启动，并且如果该会话不重要，则 Data Protector 可以中止该会话。

要设置这些选项之一，需要使用 omniclus 命令创建相应的脚本，并在 Data Protector GUI 中设置群集备份选项。

- 根据逻辑 ID 中止正在运行的会话

  如果某个正在运行的特定备份会话比应用程序更重要，则 Data Protector 可以继续此会话。要在故障转移之后均衡负载，可以通过使用一个重要会话的中止 ID，中止除了该会话以外的所有备份会话。

  要设置此选项，需要使用 omniclus 命令创建相应的脚本，并在 Data Protector GUI 中设置群集备份选项。

自动重新启动失败的会话

如果在备份活动期间发生 Cell Manager 的故障转移，则备份会话将失败。如果在备份规范中选择了对应选项，则可以自动重新启动失败的会话。

要在备份规范中选择相应选项，需要修改规范。

执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型。
3. 单击要修改的备份规范。
4. 在“选项”属性页中的“备份规范选项”下，单击**高级**。
5. 在“备份选项”窗口中，单击**群集**。
6. 选择一个自动会话重新启动选项：
   - 故障转移时不重新启动备份
   - 重新启动失败对象的备份
   - 重新启动所有对象的备份
7. 单击**确定**保存更改，然后退出向导。

> **注意**创建新的备份规范时也可以设置以上选项之一。

使用 omniclus 命令创建脚本

在 Data Protector 群集 Cell Manager 与其他应用程序共享该群集的系统中，对应用程序进行负载均衡很重要。

如果在故障转移时将某些其他应用程序移至 Data Protector 群集 Cell Manager 所运行的系统，则这样会导致此系统中的负载过高。

要在故障转移之后均衡负载，可以：

- 中止所有正在运行的会话
- 临时禁用备份活动
- 根据已用会话时间中止正在运行的会话
- 根据逻辑 ID 中止正在运行的会话

要定义任意这些选项，需要使用 omniclus 命令。此命令用作发生应用程序的故障转移时将运行的脚本的一部分。需要提前创建此脚本，并将其定义为应用程序组中的一种新资源类型。

执行以下步骤：

1. 在 Data_Protector_home\bin 目录中，使用以下命令行选项之一创建批处理文件:
   - 要中止所有正在运行的会话，请使用：

     omniclus -clus Data Protector virtual server -session * -abortsess

     * 通配符表示所有会话。可将其替换为特定备份规范的名称，以便仅中止该特定备份会话。
   - 要将 Cell Manager 禁用一段时间，请使用：

     omniclus -clus Data Protector virtual server -inhibit minutes
   - 要根据已用会话时间中止正在运行的会话，请使用：

omniclus -clus Data Protector virtual server -session * -abortsess

> **重要说明**要使用此命令，还需要在备份规范中指定群集备份选项**如果小于指定的时间，则中止**或**如果大于指定的时间，则中止**。

- 要根据逻辑 ID 中止正在运行的会话，请使用：

  omniclus -clus Data Protector virtual server -session backup_specification -abortsess -abortid logical_operator_ID

> **重要说明**要使用此命令，还需要在备份规范中指定群集备份选项**检查中止 ID**。必须在脚本中使用备份规范中指定的相同会话 ID。

2. 在 Windows 群集管理器中，将新资源添加到应用程序组。对于“资源类型”，选择**一般应用程序**。对于“可能的所有者”，选择将运行此脚本的节点。这是正在运行 Data Protector 的节点。在“常规应用程序参数”窗口中，输入批处理文件的路径名称 (例如 C:\program_files\omniback\bin\clus.bat) 和 omniclus 命令 Data_Protector_home\bin 的目录。

关于 Microsoft 群集服务器的灾难恢复

可以使用除了磁盘查递灾难恢复之外的任何灾难恢复方法恢复 Microsoft 群集服务器 (MSCS)。有关特定灾难恢复方法的所有详情、限制和要求也适用于 MSCS 的灾难恢复。选择适于群集的灾难恢复方法，并将其包括在灾难恢复计划中。请考虑每个灾难恢复方法的限制和要求，然后再做决定。从测试计划中执行测试。

必须符合灾难恢复的所有先决条件（例如一致和最新的备份、经过更新的 SRD 文件、更换了故障硬件等等）才能恢复 MSCS。

可能出现的场景

MSCS 的灾难恢复有两种可能出现的场景：

- 非活动节点上发生的灾难
- 群集中的所有节点都经历了灾难

相关任务

- 恢复 Microsoft 群集服务器
- 更新 SRD 文件 (Windows 客户机)
- 导出 Microsoft 群集客户机

Data Protector 和 MC/ServiceGuard 集成

作为其高可用性的一部分，Data Protector 可与用于 HP-UX 和 Linux 系统的 Serviceguard (SG) 相集成，从而能够备份完整群集 (本地和共享磁盘) 以及群集环境中运行的应用程序。

假定您熟悉 Serviceguard。如果不熟悉，请参阅《管理 Serviceguard》手册获取详细信息。

许可和 Serviceguard

购买 Data Protector Cell Manager 的许可证时，请注意，许可证将与虚拟服务器绑定，并且无论 SG 群集中的哪个物理节点运行 Data Protector 群集包，只要包正在其中一个节点上运行，该许可证就会起作用。

在 Serviceguard 上添加组件时，将组件添加到活动节点上。然后在其他节点上启动该包，并将组件添加到此节点上。

配置

有两种方式可以配置集成：

- Data Protector Cell Manager 可在 SG 中进行安装。这样在故障转移时 Data Protector 服务可从一个群集节点自动迁移到另一个，并因此自动重新启动失败的备份会话。

  处于非活动状态的群集节点同样可作为安装服务器使用。
- Data Protector 群集感知客户机可以安装在 SG 中，因此支持文件系统备份和群集感知应用程序的备份。

在 Serviceguard 中配置 Cell Manager

决定哪些系统将作为主 Cell Manager 和辅助 Cell Manager。

配置阶段

1. 配置主 Cell Manager
2. 配置辅助 Cell Manager
3. 配置 Cell Manager 包

需要满足以下先决条件:

- 应安装群集，并且群集正在运行。
- 选作主 Cell Manager 和辅助 Cell Manager 的系统必须装有 Serviceguard 以及建议的补丁，并且必须被配置为同一群集的成员。有关 Serviceguard 安装和配置的说明，请参阅《管理 Serviceguard》手册。
- 必须在主节点和每个辅助节点上安装 Data Protector Cell Manager 和建议的补丁以及适用于群集中所需集成的所有其他 Data Protector 软件组件。
- 在此群集环境中，Data Protector Cell Manager 应有自己的包。在 Serviceguard 中安装 Data Protector Cell Manager 之前，需要从网络管理员处获得以下信息:
  - 虚拟服务器名称（群集包中指定的主机名）
  - 包 IP 或虚拟 IP 地址

  此外，还将需要在共享磁盘上创建卷组。
- 确保群集节点和包 IP（虚拟 IP）位于相同的子网上。
- 如果环境中有 DNS，则确保将群集中的所有节点和包 IP 都注册到 DNS 服务器。

配置主 Cell Manager

执行以下步骤：

1. 在两个 Cell Manager 均可访问的共享磁盘上创建卷组。

   > **注意**如果要使用 ob2 磁盘作为群集锁磁盘，则应已为其创建卷组。

2. 为卷组创建逻辑卷。
3. 根据群集文档设置卷组属性。

4. 创建一个装载点目录（例如 /omni_shared ），然后将逻辑卷装载到此目录：
   1. mkdir /omni _ shared
   2. mount lv_path/omni_shared
5. 修改 /etc/opt/omni/server/sg/sg.conf 模板文件。

> **注意** SHARED_DISK_ROOT 选项应包含装载点目录的名称（例如 SHARED DISK ROOT=/omni_shared ）。
>
> CS_SERVICE_HOSTNAME 选项应包含虚拟 Cell Manager 的名称，因为网络已知该名称。群集中的每个包都需要有自己的虚拟 IP 地址及其网络名称（例如 CS_SERVICE HOSTNAME=ob2cl.company.com ）。

6. 配置主 Cell Manager。运行脚本时，确保当前位置不在 /etc/opt/omni/ 或 /var/opt/omni/ 目录或其子目录中。还要确保 /etc/opt/omni/ 或 /var/opt/omni/. 中没有装载子目录。运行:

   /opt/omni/sbin/install/omniforsg.ksh -primary

   注意，运行此脚本之后，已停止 Data Protector 服务，并且随后将重新启动该服务。
7. 卸载装载点目录：

   umount dirname
8. 取消激活所创建的卷组：

   vgchange -a n vg_name
9. 导出在主 Cell Manager 上创建的卷组。

配置辅助 Cell Manager

执行以下步骤：

1. 创建卷组以供导入，然后将其导入。
2. 设置卷组属性。
3. 创建装载点目录（与主 Cell Manager 上创建的相同），然后将逻辑卷装载到此目录。
4. 配置辅助 Cell Manager：

   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname

   其中， dirname 表示装载点或共享目录 (例如 /omni_shared)。
5. 卸载装载点目录：

   umount dirname
6. 取消激活所导入的卷组：

   vgchange -a n vg_name

配置 Cell Manager 包

需要满足以下先决条件:

- 在两个群集节点上都应安装并配置了 Data Protector Cell Manager。
- 配置 Data Protector 群集包之前，应创建并编辑一个群集配置文件。

> **注意**任何一个群集节点上都不再运行 Data Protector 后台程序。

在主 Cell Manager 节点上执行以下步骤：

1. 检查群集配置文件（例如 cluster.conf ）是否有错误：

   cmcheckconf -C /etc/cmcluster/cluster.conf

   如果有错误，则修复这些错误。

   如果没有错误，则启用该配置：

   cmapplyconf -C /etc/cmcluster/cluster.conf

2. 启动群集：

   cmruncl

3. 创建和修改 Data Protector 群集包文件。
4. 检查和传播 Data Protector 群集包文件。

创建卷组

在 Serviceguard 中配置主和辅助 Cell Manager 时，需要在两个 Cell Manager 均可访问的共享磁盘上创建卷组。

> **注意**共享卷组将包含 IDB 和配置文件，因此如果主系统失败，并且在辅助系统中重新启动 Data Protector Serviceguard Cell Manager，则 Cell Manager 将拥有所有相关数据。当考虑共享磁盘的大小时，请牢记这一点。

要创建卷组，请执行以下步骤:

1. 为新卷组创建一个目录：

   mkdir vg_name

   > **注意** vg_name 是 /dev 目录的子目录包含的卷组的路径名。

2. 列出系统中现有的所有卷组，以检查哪些次要编号正在使用中：

   ll /dev/*/group

3. 为卷组创建组文件：

   mknod vg_name/group c 64 0xNN0000

   > **注意** NN 是可用的次要编号。

4. 在 Data Protector Cell Manager 使用的磁盘上创建物理卷：

   pvcreate -f pv_path ...

   > **注意** pv_path 与 pvcreate 命令一起使用，指 /dev/rdsk 目录的子目录包含的物理卷的字符 (原始) 设备路径名 (例如物理卷 c0t1d0 的字符 pv_path 为 /dev/rdsk/c0t1d0)。

5. 创建新的卷组：

   vgcreate vg_namepv_path ...

   > **注意** pv_path 与 vgcreate 命令一起使用，指将分配到新卷组的物理卷的块设备路径名。它位于 /dev/dsk 目录的子目录中 (例如物理卷 c0t1d0 的块 pv_path 是 /dev/dsk/c0t1d0)。

为卷组创建逻辑卷

在 Serviceguard 中配置主 Cell Manager 时，在共享磁盘上创建卷组之后，为此组创建逻辑卷。

执行以下步骤：

1. 为卷组创建新的逻辑卷：

   lvcreate -L lv_size -n lv_namevg_name

> **注意** /etc/opt/omni 和 /var/opt/omni Data Protector 目录将位于该处。

lv_size 是表示分区大小的数字（以 MB 为单位）。

lv_name 是逻辑卷的名称。

2. 在逻辑卷上创建日记文件系统：

   newfs -F FStypelv_path

> **注意** FStype 指定要在其上进行操作的文件系统类型。

lv_path 是逻辑卷的字符（原始）特殊设备路径名称。

> **注意**如果要镜像新的逻辑卷，请参见 HP-UX LVM 文档以了解配置步骤。

设置卷组属性

在 Serviceguard 中配置主和辅助 Cell Manager 时，为卷组创建逻辑卷之后，需要设置卷组属性。

需要在群集中的 Cell Manager 上执行此操作。

- 在 HP-UX 中设置卷组属性
- 在 Linux 中设置卷组属性

在 HP-UX 中设置卷组属性

要设置组属性，请执行以下步骤:

1. 从常规模式取消激活卷组：

   vgchange -a n vg_name

2. 标记供群集使用的卷组：

   vgchange -c y vg_name

> **注意**如果这是群集锁磁盘，并且正在使用较新版本的 Serviceguard (例如，11.09)，则此操作将自动完成。

3. 以独占模式使用卷组：

   vgchange -a e vg_name

在 Linux 中设置卷组属性

要设置组属性，请执行以下步骤:

1. 从常规模式取消激活卷组：

   vgchange -a n vg_name

2. 标记供群集使用的卷组：

   vgchange -a y /dev/vg_ob2_sg

导出卷组

在 Serviceguard 中配置主 Cell Manager 之后，需要导出已在 system1 (主 Cell Manager) 上创建的卷组。然后，在配置辅助 Cell Manager 时，将在 system2（辅助 Cell Manager）上导入该卷组。

执行以下步骤：

1. 从 system1 导出 LVM 配置信息：

   vgexport -p -m mapfilevg_name

   mapfile 指定要将逻辑卷名称和编号写入到的文件的路径名。

2. 将映射文件传输到 system2：

   rcp mapfile second_system: mapfile

导入卷组

在 Serviceguard 中配置辅助 Cell Manager 时，首先需要导入已在主 Cell Manager 上创建的卷组。

执行以下步骤：

1. 为要导入的卷组创建目录：

   mkdir vg_name

2. 查找下一个可用的次要编号：

3. 为卷组创建组文件：

   mknod vg_name/group c 64 0xNN0000

4. 导入卷组：

   vgimport -m mapfile -v vg_namepv_path ...

   > **注意** mapfile 是要从中读取逻辑卷名称和编号的文件的名称。

   pv_path 是物理卷的块设备路径名称。

创建和修改 Data Protector 群集包文件

在 Serviceguard 中配置主和辅助 Cell Manager 之后，需要创建 Data Protector 群集包文件。

> **注意**包名称 ob2cl 仅用作示例。应输入由网络管理员或域管理员提供的名称。

执行以下步骤：

1. 在 /etc/cmcluster 目录中创建将容纳 Data Protector 包的目录:

   mkdir /etc/cmcluster/ob2cl

2. 更改为 /etc/cmcluster/ob2cl 目录：

   cd /etc/cmcluster/ob2cl

3. 在 Data Protector 包目录中创建包配置文件：

   cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf

4. 在 Data Protector 包目录中创建包控制文件：

   cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl

5. 修改 Data Protector 包配置文件 (例如， /etc/cmcluster/ob2cl/ob2cl.conf)
6. 修改 Data Protector 包控制文件 (例如， /etc/cmcluster/ob2cl/ob2cl.cntl)

检查和传播 Data Protector 群集包文件

在 Serviceguard 中配置主和辅助 Cell Manager 并创建 Data Protector 群集包文件之后，需要检查和传播这些文件。

> **注意**Data Protector 包名称 ob2cl 和群集配置文件名 cluster.conf 仅用作示例。应使用由网络管理员或域管理员提供的名称。

执行以下步骤：

1. 将包控制文件复制到群集中名为 system2 的其他节点:

   remsh system2 "mkdir /etc/cmcluster/ob2cl" rcp /etc/cmcluster/ob2cl/ob2cl.cntl system2: /etc/cmcluster/ob2cl/ob2cl.cntl

2. 在所有群集节点上将 Data Protector 共享磁盘作为（先前创建的）群集卷组：

   vgchange -c y vg_name

3. 检查 Data Protector 包：

   cmcheckconf -P /etc/cmcluster/ob2cl.conf

   如果检查成功，则添加 Data Protector 包：

   cmapplyconf -P /etc/cmcluster/ob2cl.conf

4. 启动包：

   cmrunpkg ob2cl

   此时应形成群集，并且 Data Protector Cell Manager 包应正常运行。

5. 手动导入虚拟服务器主机名：

   omnicc -import_host virtual_hostname -virtual

6. 如果在 Serviceguard 中还安装了 Data Protector 安装服务器 (默认)，则需要导入此安装服务器:

   omnicc -import_is virtual_hostname

7. 要在辅助节点上运行 Data Protector 命令，需要打开 Data Protector GUI，然后将辅助节点的 root 用户添加到 admin 用户组。

将客户机导入单元

导入表示在某个系统上安装 Data Protector 软件之后手动将系统添加到单元中。添加到 Data Protector 单元的系统将变为 Data Protector 客户机。系统成为单元的成员后，有关新客户机的信息即写入位于 Cell Manager上的 IDB 中。

> **注意**在单元中导入客户机对环境的安全性有很大影响。

无法导入属于另一个 Cell Manager 的客户机。也无法导入装有 Data Protector Cell Manager 软件的客户机。

导入客户机系统

执行以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 输入客户机的名称或浏览网络以选择要导入的客户机（仅在 Windows GUI 上）。

   如果导入配置有多个 LAN 卡的客户机，请选择**虚拟主机**选项。选择该选项后，必须导入同一系统的所有名称。

   如果导入 NDMP 客户机，请选择 **NDMP 服务器**选项并单击**下一步**。指定 NDMP 服务器的相关信息。

   如果要导入 HP OpenVMS 客户机，则在**名称**文本框中键入 OpenVMS 客户机的 TCP/IP 名称。

   如果要导入 Microsoft Exchange Server DAG 虚拟主机以进行 Data Protector Microsoft Exchange Server 2010 集成，请选择“虚拟主机”。

   如果要为 Data Protector 虚拟环境集成导入客户机，可以选择适用于独立 VMware ESX(i) Server 系统的 **VMware ESX(i)**、适用于 VMware vCenter Server 系统的 **VMware vCenter**，也可以选择适用于 Microsoft Hyper-V 系统的 **Hyper-V**。单击**下一步**并指定登录凭据。

4. 单击**完成 (Finish)** 以导入客户机。

所导入客户机的名称将显示在结果区域中。

导入群集感知客户机

在群集感知客户机上本地安装 Data Protector 软件后，将表示群集感知客户机的虚拟服务器导入 Data Protector 单元。

需要满足以下先决条件:

- 必须在所有群集节点上都安装 Data Protector。
- 所有群集包必须正在群集内运行。
- 在 Serviceguard 中，如果 Cell Manager 和应用程序位于同一群集中，请确保将 Cell Manager 包移至应用程序节点，然后再导入虚拟服务器。

Microsoft 群集服务器

执行以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在范围窗格中，右键单击 **MS 群集**，然后单击**导入群集**。
3. 输入代表要导入的群集客户机的虚拟服务器的名称，或浏览网络以选择虚拟服务器。
4. 单击**完成 (Finish)** 以导入群集客户机。

此时结果区域中将显示所导入 MS 群集客户机的名称。

> **提示**要导入特定的群集节点或虚拟服务器，请在“范围窗格 (Scoping Pane)”中右键单击其群集并单击**导入群集节点 (Import Cluster Node)** 或**导入群集虚拟服务器 (Import Cluster Virtual Server)**。

Serviceguard 和 Veritas

执行以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 键入虚拟服务器的主机名（如应用程序群集包中所指定），或浏览网络以选择要导入的虚拟服务器（仅限 Windows GUI 中）。

   选择**虚拟主机**选项指明这是一个群集虚拟服务器。
4. 单击**完成 (Finish)** 以导入虚拟服务器。

此时结果区域中将显示所导入群集客户机的名称。

共享设备和 Serviceguard

可以在 SAN 环境中实现 Data Protector 与 Serviceguard 的集成。由于群集基于在节点之间共享网络名称、磁盘和磁带等资源，因光纤通道和 SAN 也很适合作为实现存储设备共享的技术。**配置基础** 群集中的节点可以共享由 SAN 连接的设备，以便执行对群集中正在运行的应用程序的无 LAN 备份。由于群集感知应用程序运行在虚拟主机上，因此这些应用程序随时可以在群集中的任何节点上运行。要执行此类应用程序的无 LAN 本地备份，需要用虚拟主机名而非真实节点名称配置逻辑设备。

可以为单个物理设备配置所需数量的逻辑设备，但所有设备必须使用相同的锁名称。

要在多个系统之间共享设备，请为要在其本地使用该设备的每个系统配置一个逻辑设备。

以下是配置浮动和静态驱动器的示例。这些示例显示了由 /dev/rmt/0m 和 /dev/rmt/st3m 标识的设备。这两个设备文件所指的物理设备相同，因此锁名称 (Lib1_Drive_1) 相同。

配置浮动驱动器

必须根据虚拟主机配置应从这两个主机都可访问的驱动器（取决于包正在哪个主机上运行）。例如：

主机名	node_Appl
设备控制路径	/dev/rmt/st3m
锁名称	Libl_Drive_1

配置静态驱动器

还可以使用静态主机名和本地设备文件（可以使用本地 HP-UX 设备文件）以标准方式使用驱动器。应在节点上配置本地驱动器。例如：

主机名	Host_A
设备控制路径	/dev/rmt/0m
锁名称	Lib1_Drive_1

相关任务

- 在 Serviceguard 中配置 Cell Manager
- 将客户机导入单元

Data Protector 和 HACMP 群集集成

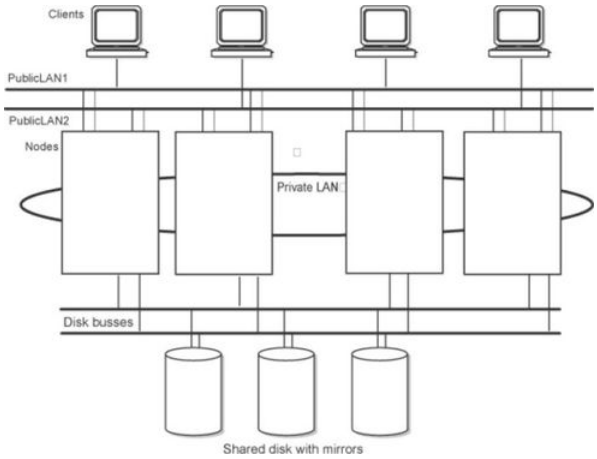
HACMP 软件是 IBM 关于建立基于 UNIX 的任务关键计算环境的解决方案，它基于高可用性 (HA) 和群集多处理 (CMP) 技术。它确保具备应用程序等关键资源可供处理。

创建 HACMP 群集的主要原因是为任务关键应用程序提供一个高度可用的环境。例如，HACMP 群集可以运行一个数据库服务器程序，为客户机应用程序提供服务。客户机向服务器程序发送查询，后者通过访问存储在共享外部磁盘上的数据库响应其请求。

要确保 HACMP 群集中这些应用程序的可用性，请由 HACMP 控制这些应用程序。HACMP 确保即使群集中有组件发生故障，应用程序对客户机进程也保持可用。如果有组件发生故障，则 HACMP 将应用程序（连同确保可访问应用程序的资源一起）移至群集中的另一个节点。

通过虚拟服务器名称（虚拟环境域名）访问整个群集，该名称代表网络上的整个 HACMP 群集。

典型的 HACMP 群集设置



如图所示，HACMP 群集由以下物理组件组成：

- 节点
- 共享外部磁盘接口
- 网络
- 网络接口
- 客户机

节点

节点组成了 HACMP 群集的核心。每个节点都由一个唯一名称标识，并包含一个用于运行 AIX 操作系统、HACMP 软件和应用程序软件的处理器。节点可能拥有一组资源磁盘、卷组、文件系统、网络、网络地址和应用程序。

共享外部磁盘接口

每个节点都可以访问一个或多个共享外部磁盘设备（以物理方式连接到多个节点的磁盘）。共享磁盘存储任务关键数据，通常进行镜像或配置 RAID 以形成数据冗余。注意，HACMP 群集中的节点使用内部磁盘存储操作系统和应用程序二进制文件，但不共享这些磁盘。

网络

HACMP 软件作为 AIX 操作系统的一个独立分层组件，旨在配合任何基于 TCP/IP 的网络一起工作。节点使用网络可：

- 允许客户机访问群集节点、
- 使群集节点可以交换波动信号消息、
- 序列化对数据的访问（在并发访问环境中）。

HACMP 软件定义两种类型的通信网络，具体取决于这些网络所使用的通信接口基于 TCP/IP 子系统（基于 TCP/IP）还是基于非 TCP/IP 子系统（基于设备）。

客户机

客户机是可以通过 LAN 访问群集中节点的处理机。每个客户机都运行一个“前端”，即客户机应用程序，

以查询群集节点上运行的服务器应用程序。

如何安装和配置 Data Protector IBM HACMP 群集集成

本主题介绍如何在适用于 AIX 的 IBM 高可用性群集多处理 (HACMP) 环境中安装和配置 Data Protector。

执行以下步骤：

1. 在所有群集节点上安装 Data Protector 磁盘代理组件。
2. 将群集节点和虚拟服务器（虚拟环境包 IP 地址）导入到 Data Protector 单元中。
3. 配置 Data Protector 设备和介质池。
4. 如果 HACMP 环境中安装了 Informix Server，并且要将其备份为群集感知应用程序，请在所有群集节点上安装 Data Protector Informix 集成组件，然后如“集成”所述配置 Data Protector Informix Server 集成。

示例：包配置文件的模板

以下是在 Serviceguard 环境中配置 Data Protector Cell Manager 包时需要修改的包配置文件的模板。

在此文件中，修改以下字段：

PACKAGE_NAME

NODE_NAME

RUN_SCRIPT （与 Data Protector 包控制文件相同）

RUN_SCRIPT_TIMEOUT

HALT_SCRIPT （与 Data Protector 包控制文件相同）

HALT_SCRIPT_TIMEOUT

SERVICE_NAME （对于服务名称，可以输入任何名称，但请注意，在以后的控制文件中将使用相同的名称。）

SERVICE_FAIL_FAST_ENABLED

SERVICE_HALT_TIMEOUT

SUBNET

****

****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******

****

******* Note: This file MUST be edited before it can be used. ********

* For complete details about package parameters and how to set them, *

* consult the Serviceguard or ServiceGuard OPS Edition manpages *

* or manuals. *

********** # Enter a name for this package. This name will be used to identify the

package when viewing or manipulating it. It must be different from

the other configured package names. PACKAGE_NAME ob2cl # Enter the failover policy for this package. This policy will be used

to select an adoptive node whenever the package needs to be started.

The default policy unless otherwise specified is CONFIGURED_NODE.

This policy will select nodes in priority order from the list of

NODE_NAME entries specified below.

#

```
# The alternative policy is MIN_PACKAGE_NODE. This policy will select

# the node, from the list of NODE_NAME entries below, which is

# running the least number of packages at the time this package needs

# to start.

FAILOVER_POLICY CONFIGURED_NODE

# Enter the failback policy for this package. This policy will be used

# to determine what action to take when a package is not running on

# its primary node and its primary node is capable of running the

# package. The default policy unless otherwise specified is MANUAL.

# The MANUAL policy means no attempt will be made to move the package

# back to its primary node when it is running on an adoptive node.

#

# The alternative policy is AUTOMATIC. This policy will attempt to

# move the package back to its primary node whenever the primary node

# is capable of running the package.

FAILBACK_POLICY MANUAL

# Enter the names of the nodes configured for this package. Repeat

# this line as necessary for additional adoptive nodes.

# Order IS relevant. Put the second Adoptive Node AFTER the first

# one.

# Example : NODE_NAME original_node

# NODE_NAME adoptive_node  NODE_NAME partizan

NODE_NAME lyon

# Enter the complete path for the run and halt scripts. In most cases

# the run script and halt script specified here will be the same script,

# the package control script generated by the cmmakepkg command. This

# control script handles the run(ning) and halt(ing) of the package.

# If the script has not completed by the specified timeout value,

# it will be terminated. The default for each script timeout is
```

```
# NO_TIMEOUT. Adjust the timeouts as necessary to permit full

# execution of each script.

# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of

# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl

RUN_SCRIPT_TIMEOUT NO_TIMEOUT

HALT_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl

HALT_SCRIPT_TIMEOUT NO_TIMEOUT

# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the

# SERVICE_HALT_TIMEOUT values for this package. Repeat these

# three lines as necessary for additional service names. All

# service names MUST correspond to the service names used by

# cmrunserv and cmhaltserv commands in the run and halt scripts.

#

# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or

# NO. If set to YES, in the event of a service failure, the

# cluster software will halt the node on which the service is

# running. If SERVICE_FAIL_FAST_ENABLED is not specified, the

# default will be NO.

#

# SERVICE_HALT_TIMEOUT is represented in the number of seconds.

# This timeout is used to determine the length of time (in

# seconds) the cluster software will wait for the service to

# halt before a SIGKILL signal is sent to force the termination

# of the service. In the event of a service halt, the cluster

# software will first send a SIGTERM signal to terminate the

# service. If the service does not halt, after waiting for the

# specified SERVICE_HALT_TIMEOUT, the cluster software will send

# out the SIGKILL signal to the service to force its termination.
```

```
# This timeout value should be large enough to allow all cleanup

# processes associated with the service to complete. If the

# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be

# assumed, meaning the cluster software will not wait at all

# before sending the SIGKILL signal to halt the service.

#

# Example: SERVICE_NAME DB_SERVICE

# SERVICE_FAIL_FAST_ENABLED NO

# SERVICE_HALT_TIMEOUT 300

#

# To configure a service, uncomment the following lines and

# fill in the values for all of the keywords.

#

#SERVICE_NAME service name

#SERVICE_FAIL_FAST_ENABLED YES/NO

#SERVICE_HALT_TIMEOUT number of seconds

SERVICE_NAME omni_sv

SERVICE_FAIL_FAST_ENABLED NO

SERVICE_HALT_TIMEOUT 300

# Enter the network subnet name that is to be monitored for this package.

# Repeat this line as necessary for additional subnet names. If any of

# the subnets defined goes down, the package will be switched to another

# node that is configured for this package and has all the defined subnets

# available.

SUBNET 10.17.0.0

# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,

# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify Package

# Resource Dependencies. To define a package Resource Dependency, a

# RESOURCE_NAME line with a fully qualified resource path name, and
```

```
# one or more RESOURCE_UP_VALUE lines are required. The
# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are optional.
#
# The RESOURCE_POLLING_INTERVAL indicates how often, in seconds, the
# resource is to be monitored. It will be defaulted to 60 seconds if
# RESOURCE_POLLING_INTERVAL is not specified.
#
# The RESOURCE_START option can be set to either AUTOMATIC or DEFERRED.
# The default setting for RESOURCE_START is AUTOMATIC. If AUTOMATIC
# is specified, ServiceGuard will start up resource monitoring for
# these AUTOMATIC resources automatically when the node starts up.
# If DEFERRED is selected, ServiceGuard will not attempt to start
# resource monitoring for these resources during node start up. User
# should specify all the DEFERRED resources in the package run script
# so that these DEFERRED resources will be started up from the package
# run script during package run time.
#
# RESOURCE_UP_VALUE requires an operator and a value. This defines
# the resource 'UP' condition. The operators are =, !=, >, <, >=,
# and <=, depending on the type of value. Values can be string or
# numeric. If the type is string, then only = and != are valid
# operators. If the string contains whitespace, it must be enclosed
# in quotes. String values are case-sensitive. For example,
# Resource is up when its value is
# --------------------------------
# RESOURCE_UP_VALUE = UP "UP"
# RESOURCE_UP_VALUE != DOWN Any value except "DOWN"
# RESOURCE_UP_VALUE = "On Course" "On Course"
#
```

```
# If the type is numeric, then it can specify a threshold, or a range to

# define a resource up condition. If it is a threshold, then any operator

# may be used. If a range is to be specified, then only > or >= may be used

# for the first operator, and only < or <= may be used for the second operator.

# For example,

# Resource is up when its value is

# --------------------------------

# RESOURCE_UP_VALUE = 5 (threshold)

# RESOURCE_UP_VALUE > 5.1 greater than 5.1 (threshold)

# RESOURCE_UP_VALUE > -5 and <10 between -5 and 10 (range)

#

# Note that "and" is required between the lower limit and upper limit

# when specifying a range. The upper limit must be greater than the lower

# limit. If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then

# they are inclusively OR'd together. Package Resource Dependencies may be

# defined by repeating the entire RESOURCE_NAME block.

#

# Example : RESOURCE_NAME /net/interfaces/lan/status/lan0

# RESOURCE_POLLING_INTERVAL 120

# RESOURCE_START AUTOMATIC

# RESOURCE_UP_VALUE = RUNNING

# RESOURCE_UP_VALUE = ONLINE

#

# Means that the value of resource /net/interfaces/lan/status/lan0

# will be checked every 120 seconds, and is considered to

# be 'up' when its value is "RUNNING" or "ONLINE".

#

# Uncomment the following lines to specify Package Resource Dependencies.

#
```

#RESOURCE_NAME Full_path_name

#RESOURCE_POLLING_INTERVAL numeric_seconds

#RESOURCE_START AUTOMATIC/DEFERRED

#RESOURCE_UP_VALUE op string_or_numeric [and op numeric]

The default for PKG_SWITCHING_ENABLED is YES. In the event of a

failure, this permits the cluster software to transfer the package

to an adoptive node. Adjust as necessary.

PKG_SWITCHING_ENABLED YES # The default for NET_SWITCHING_ENABLEDis YES. In the event of a

failure, this permits the cluster software to switch LANs locally

(transfer to a standby LAN card). Adjust as necessary.

NET_SWITCHING_ENABLED YES # The default for NODE_FAIL_FAST_ENABLED is NO. If set to YES,

in the event of a failure, the cluster software will halt the node

on which the package is running. Adjust as necessary.

NODE_FAIL_FAST_ENABLED

NO

示例：包控制文件的模板

以下是在 Serviceguard 环境中配置 Data Protector Cell Manager 包时需要修改的包控制文件的模板。

在此文件中，修改以下字段：

- VG [n]
- LV [n]
- FS [n]
- FS_MOUNT_OPT [n]
- IP
- SUBNET
- SERVICE_NAME （与配置文件中使用的相同）
- SERVICE_CMD（必须为: "/etc/opt/omni/server/sg/csfailover.ksh start"）
- SERVICE_RESTART

要确保在故障转移时重新启动 Cell Manager 包，请将 SERVICE_RESTART 参数设置为 -R (无数次重新启动服务；不建议这样做) 或设置为 -r number_of_restarts (按定义次数重新启动服务)。

```
**********************************************************************
# * *
# * HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template) *
# * *
# * Note: This file MUST be edited before it can be used. *
# * *
# **********************************************************************

# UNCOMMENT the variables as you set them.
# Set PATH to reference the appropriate directories.
PATH=/usr/bin:/usr/sbin:/etc:/bin
# VOLUME GROUP ACTIVATION:
```

```
# Specify the method of activation for volume groups.

# Leave the default ("VGCHANGE="vgchange -a e") if you want volume

# groups activated in exclusive mode. This assumes the volume groups have

# been initialized with 'vgchange -c y' at the time of creation.

#

# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment

# out the default, if your disks are mirrored on separate physical paths,

#

# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"), and comment

# out the default, if your disks are mirrored on separate physical paths,

# and you want the mirror resynchronization to occur in parallel with

# the package startup.

#

# Uncomment the third line (VGCHANGE="vgchange -a y") if you wish to

# use non-exclusive activation mode. Single node cluster configurations

# must use non-exclusive activation.

#

# VGCHANGE="vgchange -a e -q n"

# VGCHANGE="vgchange -a e -q n -s"

#VGCHANGE="vgchange -a y"

VGCHANGE="vgchange -a e Default

# VOLUME GROUPS

# Specify which volume groups are used by this package. Uncomment VG[0]=""

# and fill in the name of your first volume group. You must begin with

# VG[0], and increment the list in sequence.

#

# For example, if this package uses your volume groups vg01 and vg02, enter:

# VG[0]=vg01

# VG[1]=vg02
```

```
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vg_ob2cm
# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]="";FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
# LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a;FS_MOUNT_OPT[0]="-o rw"
# LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b;FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
# in reverse order during package shutdown. Ensure that volume groups
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
#LV[0]=""; FS[0]="";FS_MOUNT_OPT[0]=""
LV[0]=/dev/vg_ob2cm/lv_ob2cm
FS[0]=/omni_shared
```

```
FS_MOUNT_OPT[0]=""

# FILESYSTEM UNMOUNT COUNT

# Specify the number of unmount attempts for each filesystem during package

# shutdown. The default is set to 1.

FS_UMOUNT_COUNT=2

# IP ADDRESSES

# Specify the IP and Subnet address pairs which are used by this package.

# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first

# IP and subnet address. You must begin with IP[0] and SUBNET[0] and

# increment the list in sequence.

#

# For example, if this package uses an IP of 192.10.25.12 and a subnet of

# 192.10.25.0 enter:

# IP[0]=192.10.25.12

# SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)

#

# Hint: Run "netstat -i" to see the available subnets in the Network field.

#

# IP/Subnet address pairs for each IP address you want to add to a subnet

# interface card. Must be set in pairs, even for IP addresses on the same

# subnet.

#

IP[0]=10.17.3.230

SUBNET[0]=10.17.0.0

# SERVICE NAMES AND COMMANDS.

# Specify the service name, command, and restart parameters which are

# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",

# SERVICE_RESTART[0]="" and fill in the name of the first service, command,

# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
```

```
# and SERVICE_RESTART[0] and increment the list in sequence.

#

# For example:

# SERVICE_NAME[0]=pkg1a

# SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"

# SERVICE_RESTART[0]=""

# Will not restart the service.

#

# SERVICE_NAME[1]=pkg1b

# SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"

# SERVICE_RESTART[1]="-r 2"

# Will restart the service twice.

#

# SERVICE_NAME[2]=pkg1c

# SERVICE_CMD[2]="/usr/sbin/ping"

# SERVICE_RESTART[2]="-r 1"

# Will restart the service an infinite

# number of times.

#

# Note: No environmental variables will be passed to the command, this

# includes the PATH variable. Absolute path names are required for the

# service command definition. Default shell is /usr/bin/sh.

#

SERVICE_NAME[0]=omni_sv

SERVICE_CMD[0]="/etc/opt/omni/server/sg/csfailover.ksh start"

SERVICE_RESTART[0]="-r

2"
```

设置对象合并

使用 Data Protector 对象合并功能可以将备份对象的还原链合并为此对象的全新合并版本。使用此功能后，即不再需要运行完整备份。而是可以无限地运行增量备份，并根据需要合并还原链。

对象合并会话期间，Data Protector 从源介质读取备份数据，合并数据，然后合并后的版本写入目标介质。对象合并会话可以得到指定对象版本的合成完整备份。

对象合并的类型

可以用交互方式启动对象合并会话，也可以指定自动启动会话。Data Protector 可提供两种自动对象合并：备份后对象合并和计划的对象合并。

备份后对象合并

自动对象合并规范中指定的备份会话完成后进行的对象合并即为备份后对象合并。它合并根据在该特定备份会话中备份的自动对象合并规范所选的对象。

计划的对象合并

计划的对象合并发生在用户定义的某个时间。可以在一个预定对象合并会话中合并不同备份会话期间备份的对象。

如何合并对象

首先，创建对象合并规范。在规范中，选择要合并的对象版本、要使用的介质和设备以及会话选项。

设备的选择

需要分别使用单独的设备读取完整备份、读取增量备份以及写入合成完整备份。目标设备的块大小可以大于源设备。但是，为避免影响性能，建议这些设备的块大小相同，并且连接到相同系统。

会话中不能使用该会话开始时没有的设备。如果发生介质错误，则该会话中将避免使用出错的设备。

对象合并选项

可以在对象合并规范中启用源对象过滤并指定数据保护、编目保护和日志记录级别。其中大部分选项的等效选项也用于备份。

介质集的选择

如果将参与合并的对象版本有副本位于不同的介质集上，则这些介质集中的任何一个都可以用作源。默认情况下，Data Protector 自动选择最合适的介质集。通过指定介质位置的优先级可以影响介质集的选择。

介质选择的总体过程与还原相同。以交互方式合并对象时，可以手动选择要使用的介质集。配置自动对象合并时无法选择介质，因为通常稍后执行对象的备份。

合并对象的所有权

合并备份对象的所有者为原始备份对象的所有者，而非调用对象合并会话的 Data Protector 用户。

标准对象合并任务

下面是对象合并功能的先决条件和限制：

先决条件

- 在启用增强型增量备份选项的情况下执行将合并的所有备份。

- 将合并的所有增量备份都位于一个文件库或 B2D 设备中。
- 还原链完成，表示其包含的所有对象版本的状态为“已完成”或“已完成/错误”，并且持有这些对象版本的所有介质均可用。
- 配置了必要的备份设备，并已准备好介质。
- 需要在将参与对象合并会话的每个系统上安装介质代理。
- 需要有适当的用户权限用于启动对象合并会话。对于备份也适用相同的用户权限。
- 要执行虚拟完整备份，所有备份（完整、增量和虚拟完整）都必须位于使用分布式文件介质格式的一个文件库中。

限制

- 目标设备的块大小必须等于或大于源设备。
- 同一介质不能在同一对象合并会话中同时用作源介质和目标介质。
- 读取源介质时，该介质不可用于还原。
- 使用 AES 256 位加密备份的对象合并不能使用。

  除智能缓存外，所有 B2D 设备均支持对象合并。

> **注意**每当更改备份规范中软件压缩或编码选项的设置时，都必须执行一次完整备份，作为后续对象合并的基础。

以交互方式合并对象

根据需要，可以从“对象”或“会话”起点选择对象进行交互式合并。不能保存交互式对象合并规范，只能启动对象合并会话。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**交互**。
3. 单击**对象**或**会话**打开向导。
   - 单击**对象**以列出对象。
   - 单击**会话**以列出从中向介质写入对象的会话。
4. 选择希望合并的对象的时间点。无法选择完整备份，因为就此类备份本身而言无法合并。

   选择时间点将选择整个还原链。如果对于同一时间点存在若干还原链，则选择所有链，但实际仅使用一个链。以蓝色标记您的选择，以黑色标记组成还原链的其他增量，以灰色（阴影）标记相应的完整备份。蓝色复选标记指示将进行合并的时间点。

   可以为合并选择多个时间点，并且还原链可以重叠。如果选择的时间点已有黑色复选标记，则该复选标记将变为蓝色。

   要清除所选的还原链，请单击蓝色复选标记。此时将清除整个还原链，除非某些对象版本是另一个还原链的一部分，这种情况下这些对象版本仍保持选中状态，并有黑色复选标记。

   单击“下一步”。
5. 指定将读取增量备份和完整备份的设备。

   通过选择特定文件库或 B2D 设备（智能缓存除外）作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

   默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击“下一步”。
6. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。
7. 根据需要指定选项。单击“下一步”。
8. 此时将显示包含所选对象的介质的列表。

   可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。
9. 查看将参与操作的对象版本。如果使用备用还原链，可能发生实际并不使用列出的所有对象版本的情况。单击“下一步”。
10. 查看所选时间点的摘要。要更改特定时间点的选项，请在列表中选择该时间点，然后单击**属性**。
11. 单击**完成**退出向导。

配置备份后对象合并

自动对象合并规范中备份规范的名称所指定的备份会话完成后进行的对象合并即为备份后对象合并。它合并在该特定备份会话中备份的符合指定标准的对象。

如果备份会话失败，则备份后对象复制会话不会启动。如果备份会话已中止，但包含完成的对象，则默认情况下备份后对象复制会话将复制完成的对象。要禁用已中止会话的复制，请将全局选项 CopyStartPostBackupOnAbortedSession 设置为 0。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**自动**。
3. 右键单击**备份后**，然后单击**添加**以打开向导。
4. 选择包含要合并的对象的备份规范。单击“下一步”。
5. 指定用于对象合并操作的对象筛选器。单击“下一步”。
6. 指定将读取增量备份和完整备份的设备。

   通过选择特定文件库或 B2D 设备（智能缓存除外）作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

   默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击“下一步”。
7. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。
8. 根据需要指定选项。单击“下一步”。
9. 单击**另存为...**，输入规范名称，然后单击**确定**以保存备份后对象合并规范。

计划对象合并

计划的对象合并发生在用户定义的某个时间。它合并符合指定标准的对象。可以在一个预定对象合并会话中合并不同备份会话期间备份的对象。

当有许多可选择的还原链时，Data Protector 合并包含时间点最新的对象版本的那个还原链。例如，备份会话：Full、Incr1、Incr2、Incr2、Incr2 会生成三个还原链，但 Data Protector 仅合并由 Full、Incr1、和最后一个 Incr2 组成的链。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。
4. 选择包含要合并的对象的备份规范。单击“下一步”。
5. 为对象合并操作指定时间筛选器。将仅合并指定时间范围内备份的对象。单击“下一步”。
6. 指定用于对象合并操作的对象筛选器。单击“下一步”。
7. 指定将读取增量备份和完整备份的设备。

   通过选择特定文件库或 B2D 设备（智能缓存除外）作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

   默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击“下一步”。
8. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。
9. 根据需要指定选项。单击“下一步”。
10. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象合并规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

    有关如何在 Data Protector 中使用调度程序创建和编辑计划的详细信息，请参阅调度程序。

复制对象合并规范

可以复制已配置和保存的对象合并规范。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**、**自动**，然后展开**备份后**。此时将显示所保存的全部备份规范。
3. 在结果区域中，右键单击要复制的对象合并规范，然后单击**复制为**。此时将显示“复制为”对话框。
4. 在“名称”文本框中，键入所复制的对象合并规范的名称。
5. 单击**确定**。

所复制的对象合并规范显示在范围窗格的“对象操作”上下文中以及结果区域中的新名称下。

设置对象复制

关于复制备份数据

复制已备份数据有一些好处。可以复制数据以提高其安全性和可用性，或为了操作原因而这样做。

Data Protector 可提供以下方法来复制已备份数据：对象副本、对象镜像、介质复制和备份到磁盘 (B2D) 设备上的复制。

	对象复制	复制	对象镜像	介质复制
复制什么	一个或若干备份会话、对象复制会话或对象合并会话中对象版本的任意组合	来自备份会话、对象复制会话或对象合并会话的对象集	备份会话中的一组对象	整个介质
复制时间	完成备份后的任何时间	完成备份后的任何时间	备份期间	完成备份后的任何时间
源和目标介质的介质类型	可以不同	仅能将数据复制到相同类型的 B2D 设备	可以不同	必须相同
源和目标介质的大小	可以不同	目标设备必须具备足够的空间用于删除了重复数据后的数据	可以不同	必须相同
是否可追加目标介质	是	否	是	否
操作的结果	包含所选对象版本的介质	存储在目标 B2D 设备上的完全相同的副本	包含所选对象版本的介质	与源介质相同的介质

相关主题

- 关于对象副本
- 关于复制
- 关于对象镜像
- 关于介质复制

复制已备份数据

复制已备份数据有一些好处。可以复制数据以提高其安全性和可用性，或为了操作原因而这样做。

Data Protector 可提供以下方法来复制已备份数据：对象副本、对象镜像、介质复制和备份到磁盘 (B2D) 设备上的复制。

	对象复制	复制	对象镜像	介质复制
复制什么	一个或若干备份会话、对象复制会话或对象合并会话中对象版本的任意组合	来自备份会话、对象复制会话或对象合并会话的对象集	备份会话中的一组对象	整个介质
复制时间	完成备份后的任何时间	完成备份后的任何时间	备份期间	完成备份后的任何时间
源和目标介质的介质类型	可以不同	仅能将数据复制到相同类型的 B2D 设备	可以不同	必须相同
源和目标介质的大小	可以不同	目标设备必须具备足够的空间用于删除了重复数据后的数据	可以不同	必须相同
是否可追加目标介质	是	否	是	否
操作的结果	包含所选对象版本的介质	存储在目标 B2D 设备上的完全相同的副本	包含所选对象版本的介质	与源介质相同的介质

相关主题

- 对象复制
- 复制
- 对象镜像
- 介质复制

对象复制

Data Protector 对象复制功能使您能将所选对象版本复制到特定介质集。可以从一个或多个备份会话、对象复制会话或对象合并会话中选择对象版本。在对象复制会话中，Data Protector 会从源介质读取备份的数据，传输数据，并将其写入目标介质。

对象复制会话可以得到包含指定对象版本副本的介质集。

以下是对象副本功能的特征：

- 会话的启动

  可以用交互形式启动或自动启动对象副本会话。

- 介质的选择

  作为源介质，可以使用包含备份的原始介质集、包含对象副本的介质集或者作为介质副本的介质集。

  但是，启动对象复制会话之后即无法选择介质集。如有装载请求，需要提供由 Data Protector 请求的特定介质，或其完全相同的副本（使用介质复制功能创建）。

- 介质类型

  可以将对象复制到不同类型的介质。此外，目标设备的块大小可以等于或大于源设备的块大小。

- 介质策略

  可以向已包含备份或对象副本的介质追加数据。

- 保护策略

  可以对源对象和对象副本单独设置保护周期。

可以用交互形式启动对象复制会话，或指定自动启动会话。

自动对象复制

在自动对象副本规范中，可以指定一个或多个标准用于选择将复制的对象版本：

- 备份规范 - 仅复制使用特定备份规范备份的对象版本。
- 对象副本规范 - 仅复制使用特定对象副本规范复制的对象版本。
- 对象合并规范 - 仅复制使用特定对象合并规范合并的对象版本。
- 数据保护 - 仅复制受保护的对象版本。
- 现有副本数 - 仅复制不超过指定成功复制数的对象版本。
- 库 - 仅复制位于指定库中介质上的对象版本。
- 时间范围（仅在预定对象副本规范中）- 仅复制指定时间段内备份的对象版本。

Data Protector 可提供两种自动对象复制：备份后对象复制和计划的对象复制。

备份后对象复制

备份后对象复制以及（备份后对象复制的子集）复制后和合并后对象复制，发生在自动对象副本规范中指定的会话完成之后。它们复制根据该特定会话中写入的自动对象复制规范选择的对象。

计划的对象复制

计划的对象复制发生在用户定义的某个时间。在一个计划的对象副本会话中可以复制不同会话中的对象。

如何复制对象

首先，创建对象复制规范。在规范中，选择要复制的对象、要使用的介质和设备、会话选项，以及当同一对象位于多个介质集上时，影响 Data Protector 如何选择介质集的介质位置优先级。

设备的选择

您需要将要使用的设备与源介质和目标介质分开。目标设备的块大小可以大于源设备。但是，为避免影响性能，建议目标设备和源设备具有相同的

块大小，且连接到同一系统或 SAN 环境。

默认情况下对于对象复制要进行负载均衡。Data Protector 通过使用尽可能多的设备，最优地利用可用的设备。

如果不指定要用于对象副本规范中的源设备，则 Data Protector 将使用默认设备。默认情况下，将使用用于写入对象的设备作为源设备。如果需要，可以更改源设备。如果不按对象选择目标设备，则 Data Protector 将自动从您在对象复制规范中选择的那些设备中选择最合适的设备。

会话开始的时候锁定设备。那时不可用的设备就不能用于会话中，因为会话开始后即无法锁定设备。如果发生介质错误，则该复制会话中将避免使用出错的设备。

对象副本选项

可以在对象复制规范中启用源对象过滤并为对象副本指定数据保护、编目保护和日志记录级别。其中大部分选项的等效选项也用于备份。

根据策略，备份的对象及其副本可以指定相同或不同的选项值。例如，可以对一个备份对象指定**无日志**值以提高备份性能，然后在后续的对象复制会话中对相同的对象指定**全部记录**值。

要创建与所备份对象完全相同的副本，请为对象副本指定相同的日志记录级别。请考虑这一点：日志记录级别高于“无日志”的每次对象复制都对 IDB 大小有影响。

选择从中进行复制的介质集

如果要复制的对象版本存在于多个介质集（用 Data Protector 数据复制方法之一创建的）上，则任何介质集都可用作复制源。默认情况下，Data Protector 会自动选择要使用的介质集。通过指定介质位置的优先级可以影响介质集的选择。

介质选择的总体过程与还原相同。以交互方式复制对象时，可以在起始点为“对象”或“会话”时手动选择要从中进行复制的介质集。配置自动对象复制时无法选择介质，因为通常稍后执行对象的备份。

对象副本完成状态

复制对象

如果 IDB 中记录了状态为“已完成”或“已完成/错误”的对象所在的所有介质，则可以复制这些对象。如果复制操作成功，则所复制对象的状态与相应所备份对象的状态相同。

如果已中止对象复制会话，或如果该会话因其他原因失败，则此类会话生成的对象副本处于“失败”状态。无法再次复制状态为“失败”的对象复本；其数据和编目保护设置为“无”。

源对象

如果对象副本会话失败，则所复制的源对象保持不变。

如果对象复制会话完成但有错，则成功复制的源对象将其数据和编目保护设置为源对象选项中指定的值。

如果中止对象复制会话，则所有源对象的数据和编目保护均保持不变。在这种情况下，如果要更改任何所复制对象的保护，则必须在 IDB 中手动进行。

对象副本所有权

复制备份对象的所有者为原始备份对象的所有者，而非调用对象复制会话的 Data Protector 用户。

相关任务

- 标准对象复制任务
- 高级对象复制任务
- 设置介质位置优先级

标准对象复制任务

下方是对象复制功能的先决条件和限制：

先决条件

- 需要在将参与对象复制会话的每个系统上安装介质代理。
- 需要至少在 Data Protector 单元中配置两个备份设备。
- 需要为对象复制会话准备好介质。
- 需要有适当的用户权限用于执行对象复制会话。

以下限制适用：

- 无法将使用 ZDB 备份的对象复制到磁盘。
- 无法复制使用 NDMP 备份功能备份的对象。
- 无法在一个对象复制会话中创建一个对象版本的多个副本。
- 目标设备的块大小必须等于或大于源设备。
- 同一介质不能在同一对象复制会话中同时用作源介质和目标介质。
- 对象复制期间，用作源的介质不可用于还原。
- 无法取消 SAP MaxDB、DB2 UDB 或 SQL 集成对象的多路复用。
- 无法复制在向导最后一页中以交互方式运行的会话过程中备份、复制或合并的对象。
- 无法从同一个对象复制规范中同时启动两个或更多个对象复制会话。
- 不支持使用 Data Protector 9.x 及后续版本将对象从使用 Data Protector 8.x 执行的文件库 (FL) VMware 备份复制到智能缓存设备。

重要说明请考虑以下几点：

- Data Protector SAP MaxDB、DB2 UDB 和 Microsoft SQL Server 集成具有相互依赖的数据流。因此，对象复制操作必须在介质上保留对象的布局才能进行还原。要确保这一点，请选择这些集成中备份 ID 相同的所有对象进行复制。否则，无法从此副本进行还原。
- 复制 SAP MaxDB、DB2 UDB 或 Microsoft SQL Server 集成对象所需的最少设备数与用于备份的设备数相等。用于备份和复制这些对象的设备的并发必须相同。
- 如果从 ZDB 到磁盘 + 磁带会话复制对象时选择了成功复制之后更改数据和编目保护选项，则请注意，在指定时期之后可以覆盖源对象。覆盖介质之后，将不能再使用 GUI 从此备份进行即时恢复。
- 如果中止对象复制会话，则所有源对象的数据和编目保护都保持不变。在这种情况下，如果要更改任何所复制对象的保护，则必须在 IDB 中手动进行。

以交互方式复制对象

备份对象后，可以将其复制到新的介质集中。

根据需要，可以选择用于从“介质”、“对象”或“会话”起始点开始的交互式复制的对象。不能保存交互式对象副本规范，只能启动对象复制会话。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**介质**、**对象**或**会话**以打开向导。
   - 单击**介质**可列出介质池和介质。
   - 单击**对象**以列出备份数据的类型，如“文件系统”、“数据库”等等。
   - 单击**会话**以列出从中向介质写入对象的会话。
4. 选择要复制的对象。

   如果在之前的步骤中选择了会话，则可以右键单击集成对象并单击**选择备份集**，以选择具有相同备份 ID 的所有集成对象。

   注意从 Data Protector 2018.11 (10.20) 开始，对于 VMware 备份，虚拟机磁盘将视为并行运行的对象。虚拟机的磁盘对象会列在**介质**列表中，但它们处于禁用状态，表明虚拟机磁盘已备份到介质。将在虚拟机对象上执行复制或验证操作，并将其所有关联的磁盘对象视为内部对象。

   自 Data Protector 2018.11 (10.20) 起，对于 VMware 集成，只有在“介质”列表中选择虚拟机对象后，才会启用“下一步”选项。

   单击“下一步”。

5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。选择原始设备，然后单击**更改**。新设备的名称出现在“设备状态”下。新设备将仅用于此会话。

   有关设备的详细信息，请右键单击该设备，并单击**信息**。

   指定对象复制期间所选设备不可用（例如如果被禁用或已在使用中）时 Data Protector 应做些什么。选择自动设备选择或原始设备选择。

   单击“下一步”。

6. 选择用于对象复制操作的目标设备。

   可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

   单击“下一步”。

7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。

   或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。选择“使用复制”后，“复制到外部单元”即启用。

8. 此时将显示包含所选对象的介质的列表。

   如果起始点是“对象”或“会话”，则还会列出介质位置优先级。可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。

9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

   可以指定源对象选项、目标对象选项和目标设备。如果使用了“对象”或“会话”起始点，则当存在多个副本时，可以手动选择将使用对象版本的哪个副本。

10. 单击**完成**启动复制会话。

配置备份后对象复制

备份后对象复制在自动对象复制规范中的备份、对象复制或对象合并规范的名称所指定的备份会话、对象复制会话或对象合并会话完成之后发生。它复制该特定会话中符合指定标准的对象。

如果备份会话失败，则备份后对象复制会话不会启动。如果备份会话已中止，但包含完成的对象，则默认情况下备份后对象复制会话将复制完成的对象。要禁用已中止会话的复制，请将全局选项 CopyStartPostBackupOnAbortedSession 设置为 0。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**自动**。
3. 右键单击**备份后**，然后单击**添加**以打开向导。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。单击“下一步”。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击“下一步”。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击“下一步”。
7. 在所选备份规范中用于备份的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。

   或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。

10. 单击**另存为...**，输入规范名称，然后单击**确定**以保存备份后对象复制规范。

计划对象复制

计划的对象复制发生在用户定义的某个时间。可在一个排定对象复制会话中复制来自不同备份会话、对象复制会话或对象合并会话的对象。

> **提示**也可以使用基于 Web 的调度程序的高级设置来计划对象复制会话。要访问调度程序，请在上下文列表中单击**主页**，然后单击左侧窗格中的**调度程序**。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**自动**。

3. 右键单击**预定**，然后单击**添加**以打开向导。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。

   还可以按备份组查看备份规范。这样，如果向某个备份组添加备份规范或从该组删除备份规范，则对象复制功能自动确认更改，而您无须手动修改对象副本规范。

   请注意，如果从组视图更改为任何其他视图，则显示一条警告消息，提醒更改视图将删除当前所选的全部内容。如果继续，将清除以前所选的全部内容。

   单击“下一步”。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击“下一步”。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击“下一步”。
7. 在所选备份规范中用于备份的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。

   或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。
10. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象复制规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

重新启动失败的对象复制会话

由于网络连接问题或系统不可用，对象复制会话期间可能会发生某些对象失败的情况。解决了妨碍的问题后，可以重新启动出现问题的会话。此操作只会重新启动失败的对象。

您必须位于 Data Protector Admin 用户组中，或者拥有 Data Protector 监视用户权限。

以下限制适用：

- 无法重新启动以交互方式运行（意味着它们是基于未保存的对象副本规范）的失败会话。
- 无法同时重新启动多个会话。

> **重要说明**重新启动失败的对象复制会话之前，请勿更改对象复制规范。否则将无法重新启动所有对象。

执行以下步骤：

1. 如果您使用的是普通 Cell Manager，在上下文列表中单击**内部数据库**。

   如果您使用的是管理器的管理器，在“上下文列表”中选择**客户机**，然后展开**企业客户机**。选择会话出现问题的 Cell Manager。从“工具”菜单中，选择“数据库管理”以打开新的 Data Protector GUI 窗口，其中显示了“内部数据库”上下文。
2. 在范围窗格中，展开**内部数据库**，然后单击**会话**。

   此时将在结果区域中显示会话的列表。每个会话的状态显示在“状态”列中。
3. 右键单击失败、中止或完成但发生过失败或出现错误的会话，然后选择**重新启动失败的对象**以复制失败的对象。
4. 单击**是**确认。

复制对象复制规范

可以复制已配置和保存的对象复制规范。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**、**自动**和**备份后**。此时将显示所保存的全部对象复制规范。
3. 在结果区域中，右键单击要复制的对象复制规范，然后单击**复制为**。此时将显示“复制为”对话框。
4. 在“名称”文本框中，键入所复制的对象复制副本的名称。
5. 单击**确定**。

所复制的对象副本规范显示在范围窗格的“对象操作”上下文中以及结果区域中的新名称下。

配置对象复制到云

您可以配置将对象从云复制到本地备份设备，从而使该操作可以交互方式或按调度的间隔发生。云中的对象复制完成后，之后，您便可在本地备份设备和客户机之间执行恢复。

以下限制适用:

- 云 B2D 不支持介质复制。配置对象复制到云时，您仍可根据介质、会话或对象选择对象。

配置到云的交互式对象复制

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**介质**、**对象**或**会话**以打开向导。
   - 单击**介质**可列出介质池和介质。
   - 单击**对象**可列出备份数据的类型。
   - 单击**会话**以列出从中向介质写入对象的会话。
4. 选择要复制的对象。

   如果在之前的步骤中选择了会话，则可以右键单击集成对象并单击**选择备份集**，以选择具有相同备份 ID 的所有集成对象。

   单击“下一步”。
5. 选择云设备作为源设备。

   用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。选择原始设备，然后单击**更改**。新设备的名称出现在“设备状态”下。新设备将仅用于此会话。

   有关设备的详细信息，请右键单击该设备，并单击**信息**。

   指定对象复制期间所选设备不可用（例如如果被禁用或已在使用中）时 Data Protector 应做些什么。选择**自动设备选择**或**原始设备选择**。

   单击“下一步”。
6. 选择对象复制操作的本地目标设备。单击“下一步”。
7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。
8. 此时将显示包含所选对象的介质的列表。

   如果起始点是“对象”或“会话”，则还会列出介质位置优先级。可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。
9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

   可以指定源对象选项、目标对象选项和目标设备。如果使用了“对象”或“会话”起始点，则当存在多个副本时，可以手动选择将使用对象版本的哪个副本。
10. 单击**完成**启动复制会话。

配置从云的计划对象复制

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。单击“下一步”。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击“下一步”。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击“下一步”。
7. 选择云设备作为源设备。

   在所选备份规范中用于备份的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
8. 选择对象复制操作的本地目标设备。单击“下一步”。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。
10. 右键单击日期，然后单击**排定**以显示“排定复制”对话框。根据需要指定选项，然后单击**确定**。单击“下一步”。
11. 单击**另存为...**，输入规范名称，然后单击**确定**以保存调度的对象复制规范。

复制对象

通过 Data Protector 复制功能，可以在两个具有复制功能的备份到磁盘 (B2D) 设备之间复制对象，而无需通过介质代理传输数据。可以选择备份会话、对象复制会话或对象合并会话。在复制会话期间，Data Protector 会从正在复制的会话中读取对象，然后启动从源 B2D 设备到目标设备的复制。

复制会话的结果为来自指定会话的所有对象的副本。

以下内容定义复制功能：

- 会话的启动

  可以用交互形式启动或自动启动复制会话。

- 目标设备的选择

  可以筛选具有复制功能的设备并选择适当的设备。

- 保护策略

  可以对源对象和对象副本单独设置保护周期。

可以用交互方式启动复制会话，也可以指定自动启动会话。

自动复制

在自动复制规范中，可以指定一个或多个标准用于选择将复制的对象版本：

- 备份规范 - 仅复制使用特定备份规范备份的对象版本。
- 对象副本规范 - 仅复制使用特定对象副本规范复制的对象版本。
- 对象合并规范 - 仅复制使用特定对象合并规范合并的对象版本。
- 数据保护 - 仅复制受保护的对象版本。
- 现有副本数 - 仅复制不超过指定成功复制数的对象版本。
- 库 - 仅复制位于指定库中介质上的对象版本。
- 时间范围（仅在预定对象副本规范中）- 仅复制指定时间段内备份的对象版本。

Data Protector 可提供两种自动复制：备份后复制和排定复制。

备份后复制

备份后复制以及（备份后复制的子集）复制后和合并后复制，发生在自动对象副本规范中指定的会话完成之后。它们复制根据写入该特定会话的自动复制规范选择的对象。

安排的复制

安排的复制在用户定义的时间发生。可在单个计划的复制会话中复制来自不同会话的对象。

以下限制适用：

- 仅可为复制选择备份、对象副本、对象合并或对象复制会话。不支持选择单个对象。
- 不支持源或目标设备上不同的块大小。
- 配置交互会话时，一次仅可选择一个会话。

注意事项

- 由于复制基于会话，所以可能会覆盖单个对象的设置。例如，如果会话中已包含一个对象的多个副本，Data Protector 将忽略选项“仅包括副本数小于指定值的对象”，并复制会话中的所有对象，其中包括此对象，即使这样会导致对象的副本数超出此选项所允许的数量。
- 默认情况下，Data Protector 将选择原始对象版本（如果找到同一对象的多个副本）作为源设备。在某些情况下，原始版本可能会因为其属于不同的介质类型而无法复制。

  通过选择能够复制的库或特定库，选择正确的源设备。

- 配置 Data Protector 复制时必须始终从物理装置上的一个源存储复制到装置上的一个目标存储。Data Protector 不支持以下操作:
  - 从装置上的两个或多个源存储复制到装置上的一个目标存储。
  - 从装置上的两个或多个源存储复制到装置上的两个或多个目标存储。
  - 从装置上的一个源存储复制到装置上的两个或多个目标存储。

如何启用复制

可以*在创建对象副本规范时*启用从一个 B2D 设备到另一个 B2D 设备的复制：

1. 请确保源和目标设备能够复制。使用**能够复制**过滤器过滤设备，或明确选择特定的 B2D 设备。
2. 设置复制操作选项时，请选择**使用复制**。

自动复制同步

通过 Data Protector 复制功能，可以在两个具有复制功能的备份到磁盘 (B2D) 设备之间复制对象，而无需通过介质代理传输数据。自动复制同步功能是正常复制的扩展，借助它可以在由不同 Cell Manager 管理的两个重复数据删除设备之间复制备份元数据。通过此功能，可以在两个重复数据删除设备之间轻松交换备份数据及其他元数据。

确保源 Cell Manager 上的 Data Protector 用户（CRS 在其帐户下运行）有权访问目标 Cell Manager。

注意事项

对于集成备份，不要从部分失败的备份会话（即已完成但有错误的备份会话）执行自动复制同步过程。复制将会成功，但是从复制的会话恢复可能会失败。

以下限制适用：

- 考虑对正常复制功能应用的所有限制。
- 目标 Cell Manager 的版本应与源 Cell Manager 的版本相同或更高。
- 源 Cell Manager 和外部 Cell Manager（目标 Cell Manager）中为复制选择的设备必须指向相同的物理设备和数据存储。
- 一次可复制的最大介质数取决于目标设备上的可用空闲连接数。例如，如果目标设备具有 100 个空闲连接，建议同时复制不超过 100 个介质。此外，如果要使用目标设备执行其他操作，可同时复制的介质数必须少于可用的空闲连接数。

  对于 StoreOnce 和数据域提升设备，分别检查可用的数据连接和复制流。有关支持的流的详细信息，请参见各自的设备手册。
- 不支持使用旧版 GUI 的自动复制同步列表。您可能会看到以下错误消息：“分析复制规范文件时出错。文件可能已损坏或无效。”此消息表明旧版的 Data Protector GUI 不支持新列表。
- 自动复制同步过程不支持**仅包括复本数小于指定值的对象**选项。
- 复制后，不会同步对复制的对象版本所做的更改。例如，如果更改源 Cell Manager 上这些对象版本的保护，不会修改目标 Cell Manager 上的对象版本保护。
- 不能将自动复制同步与 CMMDB 一起使用。

自动复制同步包含两个步骤：

1. 导入外部 Cell Manager
2. 执行对象复制会话

导入外部 Cell Manager

触发自动复制同步的第一步是将外部 Cell Manager 导入源 Cell Manager。要导入外部 Cell Manager：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 键入客户机的名称或浏览网络以选择要导入的客户机（仅在 Windows GUI 上）。如果导入的是管理重复数据删除设备的 Cell Manager，请选择 **Data Protector 外部单元服务器**。

> **注意**: 如果执行的是自动复制同步过程，需要以上步骤。

4. 单击**完成 (Finish)** 以导入客户机。

所导入客户机的名称将显示在结果区域中。

注意: 只能在导入的 Cell Manager 上执行自动复制同步操作。您将无法使用该 Cell Manager 执行其他任何操作。

执行对象复制会话

将外部 Cell Manager 导入源 Cell Manager 后，可以执行对象复制会话，将备份数据和其他元数据复制到外部 Cell Manager 中。根据要求，您可以执行调度的、备份后或交互式对象复制。

要执行对象复制会话：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，导航至**复制 > 对象复制 > 自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。您也可以执行交互式或备份后对象复制会话。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。单击“下一步”。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击“下一步”。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击“下一步”。
7. 默认情况下，在选定备份规范中用于备份的设备在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击“下一步”。

   选中**显示能够复制**复选框，以仅选择具有备份到磁盘（重复数据删除）设备的设备。只有在备份到磁盘设备上才可以进行复制。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。

   选择**使用复制**以启用两个 B2D 设备之间的复制而不是复本的复制。

   选择**复制到外部单元**以启用将对象复制到之前导入的外部单元服务器（此 Cell Manager 包含第二个重复数据删除设备）。

   单击“下一步”。
10. 从下拉菜单中选择之前导入的外部单元服务器。这样将列出链接到备份到磁盘存储的设备。

    从目标 Cell Manager 创建且具有相同存储名称的所有设备都会显示在此处。因此，确保选择具有正确存储名称的设备来执行复制。

    选择所需的设备或网关，然后单击**下一步**。
11. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象复制规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

运行调度的对象复制会话以完成自动复制同步过程。

高级对象复制任务

为了以下多种用途，创建已备份数据的其他副本：

- 保管

  您可以制作已备份、已复制或已合并对象的副本，并将其保存在多个位置。
- 释放介质

  要只保存介质上受保护对象的版本，您可以复制此类对象版本，然后释放介质以便覆盖。
- 取消复用介质

  您可以复制对象以消除数据的交叉存取。
- 合并还原链

  您可以复制还原到一个介质集所需的所有对象版本。
- 迁移到其他介质类型

  您可以将备份复制到不同类型的介质。
- 支持高级备份概念

  您可以使用磁盘分段等备份概念。

释放介质

介质可以包含保护期各异的备份对象。可能会发生受保护对象仅占用少量介质空间的情况。但是，直到所有对象的保护都到期后，才能重用此类介质。

要使介质的使用合理化，可以使用对象复制功能释放仅包含某些受保护对象的介质。将受保护的对象复制到新的介质集中，并且可以重用该介质。也可以从失败的对象释放介质。在对象复制会话中不复制这些对象。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**介质**打开向导。
4. 在“对象”页中，选择选项仅启用受保护对象的选择。展开介质池，然后选择要释放的介质。单击“下一步”。
5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
6. 选择用于对象复制操作的目标设备。

   可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

   单击“下一步”。
7. 在“选项”页中的“源对象”选项下，选择成功复制之后更改数据和编目保护，以便在复制这些对象之后删除源对象的保护。选择在成功完成复制之后回收失败的源对象的数据和编目保护，以删除失败的源对象的保护（不会复制这些对象）。根据需要指定其他选项。单击“下一步”。
8. 此时将显示包含所选对象的介质的列表。单击“下一步”。
9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。可以指定源对象选项、目标对象选项和目标设备。
10. 单击**完成**启动复制会话。

取消介质的多路复用

多路复用的介质包含多个对象的交错数据。此类介质可能由于多个并行设备的备份会话而产生。复用介质会削弱备份的隐私安全，而且需要更多时间才能还原。

使用对象复制功能，可以取消介质的多路复用。来自多路复用介质的对象将复制到若干介质。

Data Protector 仅读取一次源介质。要能取消介质上所有对象的多路复用，操作所需的最小目标设备数与用于写入对象的设备并发相同。如果可用设备较少，则目标介质上仍对某些对象进行多路复用。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**会话**打开向导。
4. 展开所需的会话，然后选择要复制的对象。单击“下一步”。
5. 如果不希望取消多路复用操作占用为定期备份而配置的设备，并且如果要在取消多路复用操作期间仅使用一个设备读取数据，则执行此步骤。

   将源设备映射到单个设备。

   > **重要说明**如果使用一个独立文件设备作为源设备，则跳过此步骤。如果使用文件介质库设备或文件库设备作为源设备，请确保将源设备映射到相同文件介质库中或相同文件库中的设备。

   右键单击每个设备，然后单击**更改设备**。选择新设备，然后单击**确定**。
6. 单击“下一步”。
7. 选择用于对象复制操作的目标设备。所需的设备数取决于写入对象时使用的设备并发。

   右键单击每个所选的驱动器，然后单击**属性**。将**并发**选项设置为 1。单击**确定**。

   可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

   单击“下一步”。
8. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。
9. 此时将显示包含所选对象的介质的列表。

   可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。
10. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

    可以指定源对象选项、目标对象选项和目标设备。如果存在多个副本，则还可以手动选择将使用对象版本的哪个副本。
11. 单击**完成**启动复制会话。

合并还原链

使用对象复制功能，可以将对象版本的还原链复制到新的介质集。从这种介质集可以更快更方便地还原，因为不需要加载多个介质和寻找所需的对象版本。

对于集成对象无法选择还原链。

> **注意**Data Protector 还提供一个更强大的功能，称为对象合并。使用对象复制可以将还原链的所有备份复制为一个序列的同时，对象合并将备份合并为一个新的对象版本，合成完整备份。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**对象**打开向导。
4. 在“对象”页中，展开某种数据类型，然后展开客户机及其逻辑磁盘或装载点以显示对象版本。右键单击要复制的对象，然后单击**选择还原链**。单击“下一步”。
5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
6. 选择用于对象复制操作的目标设备。

   可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

   单击“下一步”。
7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。
8. 此时将显示包含所选对象的介质的列表。

   可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。
9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

   可以指定源对象选项、目标对象选项和目标设备。如果存在多个副本，则还可以手动选择将使用对象版本的哪个副本。
10. 单击**完成**启动复制会话。

迁移到其他介质类型

可以使用对象复制功能将备份数据迁移至块大小相同或更大的另一种介质类型。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**介质**打开向导。
4. 选择要复制的对象，然后单击**下一步**。
5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击“下一步”。
6. 选择用于对象复制操作的目标设备。

   可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

   单击“下一步”。
7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击“下一步”。
8. 此时将显示包含所选对象的介质的列表。单击“下一步”。
9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

   可以指定源对象选项、目标对象选项和目标设备。
10. 单击**完成**启动复制会话。

磁盘分段

磁盘分段的概念基于在若干阶段中备份数据。备份阶段由两部分组成：将数据备份到一种类型的介质，然后将数据复制到另一种类型的介质。通常可能以如下方式使用该功能

1. 数据备份到高性能和高可访问性、但容量有限的介质（例如系统磁盘）。此类备份通常在可能最需要快速还原的那段时间内保持可访问的状态。
2. 一段时间之后，使用对象复制功能将数据移至较低性能和较低可访问性、但容量很大的介质进行存储。

可以使用专为此用途配置的计划对象副本规范以此方式执行磁盘分段。

如下方法有可能作为一种替代方法：

1. 创建一个备份规范，将数据备份到高性能介质，该介质中将保护设置为需要还原功能的整个时期。
2. 创建自动备份后复制规范，将备份数据复制到较低性能的介质，并将原始备份的保留期重置为需要快速还原功能的关键时期。默认情况下，在原始备份规范中指定的保护期内保留辅助副本。

使用此方法后，关键时期内进行这两次复制都更加安全。

为什么要实施磁盘分段

使用磁盘分段概念会带来以下优点：

- 可提高备份和还原的性能。
- 可减少存储备份数据的成本。
- 可提高对于还原的数据可用性和可访问性。

磁盘分段和重复进行的小型备份

磁盘分段也消除了将大量小对象频繁备份到磁带的必要。由于要频繁装载和卸载介质，此类备份很不方便。使用磁盘分段可以降低备份时间和避免介质质量下降。

镜像对象

通过 Data Protector 的对象镜像功能，可以在备份会话期间将同一数据同时写入多个介质集。您可以将全部或部分备份对象镜像到一个或多个其他介质集。

使用对象镜像的成功执行备份会话的结果是得到一个包含已备份对象的介质集以及包含镜像对象的其他介质集。这些介质集上的镜像对象被视为对象副本。

对象镜像的优点

使用对象镜像功能可以达到以下目的：

- 由于存在多个副本，它可提高已备份数据的可用性。
- 它使得多地点保管介质变得更加容易，因为已备份数据可以镜像到远程站点。
- 由于相同数据写入到若干介质上，因此它提高了备份的容错能力。一个介质上的介质故障不会影响创建其他镜像。

限制

- 无法使用 ZDB 到磁盘或 NDMP 备份功能镜像对象备份。
- 无法在一个会话中将一个对象多次镜像到相同设备。
- 设备的块大小在镜像链中不得递减。这意味着：
- ** 用于写入镜像 1 的设备的块大小必须等于或大于用于备份的设备的块大小。
    - 用于写入镜像 2 的设备的块大小必须等于或大于用于写入镜像 1 的设备，以此类推。

如何使用对象镜像

配置备份规范时即可指定对象镜像。在备份规范中，选择要镜像的对象，然后指定镜像数。为了能够指定超过 5 个镜像，请增加 MaxNumberOfMirrors 全局选项的值。

分别为备份和每个镜像指定单独的设备。具有对象镜像的备份会话开始后，Data Protector 从备份规范中指定的那些设备中选择设备。为避免影响性能，建议设备采用相同的块大小，并且都连接到相同系统或 SAN 环境。镜像 SAP MaxDB、DB2 UDB 或 Microsoft SQL Server 集成对象所需的最少设备数与用于备份的设备数相等。

默认情况下对于对象镜像进行负载均衡。Data Protector 通过使用尽可能多的设备，最优地利用可用的设备。从命令行执行对象镜像操作时，负载均衡不可用。

复制介质

可以复制介质用于归档或保管。需要单独启动每个介质的复制，因为在一个介质复制会话中只能复制一个介质。

在独立设备中复制介质

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击含有要复制的介质的设备，然后单击**复制**。
3. 选择目标介质所在的设备（库的驱动器和插槽），然后单击**下一步**。
4. 选择要向其添加介质副本的介质池，然后单击**下一步**。
5. 指定介质副本的说明和位置（可选），然后单击**下一步**。
6. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

   提示如果目标介质具有 Data Protector 可识别的其他格式 (tar 和 OmniBack I 等等) 或如果这些介质是不受保护的 Data Protector 介质，则使用“强制操作”选项。

7. 单击**完成**以开始复制，然后退出向导。

“会话信息”消息显示介质复制操作的状态。

在库设备中复制介质

执行以下步骤：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中的**介质**下，展开**池**，然后展开含有要复制的介质的介质池。右键单击介质，然后单击**复制**以打开向导。
3. 为要复制的介质选择驱动器，然后单击**下一步**。如果带库只有一个驱动器，则跳过此步骤。
4. 选择目标介质所在的设备（库的驱动器和插槽），然后单击**下一步**。
5. 选择要向其添加介质副本的介质池，然后单击**下一步**。
6. 指定介质副本的说明和位置（可选），然后单击**下一步**。
7. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

   提示如果目标介质具有 Data Protector 可识别的其他格式 (tar 和 OmniBack I 等等) 或如果这些介质是不受保护的 Data Protector 介质，则使用“强制操作”选项。

8. 单击**完成**以开始复制，然后退出向导。

“会话信息”消息显示介质复制操作的状态。

设置对象验证

通过 Data Protector 对象验证功能，可以对备份对象进行验证。使用此功能，不必再单独以交互方式验证完整的备份介质。现在可以在计划的会话中或在操作后会话中以交互方式验证单个或多个介质上的单个或多个对象。

所验证的对象可以是原始备份对象、对象副本和合并对象。

数据验证

在对象验证会话期间，Data Protector 以验证介质时使用的类似方式验证各个备份对象的数据。

传递到主机

默认情况下，对其执行数据验证过程的目标主机是原始备份源主机。这样可验证 Data Protector 能否将备份数据从介质代理主机传递到该主机。此外，可以指定不同的目标主机，或可以在介质代理主机上执行验证，从而避免涉及任何网络。

对象验证会话的类型

可以用交互方式启动对象验证会话，也可以指定自动启动会话。Data Protector 可提供两种自动对象验证：备份后对象验证和计划的对象验证。

备份后对象验证

完成备份、对象复制或合并会话之后立即执行备份后对象验证，并验证这些会话期间创建的对象。在备份后对象验证规范中指定要验证的对象。这样将指定备份、对象复制和/或合并规范以定义所创建的对象，并提供用于筛选对象的标准。一个备份后对象验证规范中可以包括多个备份、对象复制和/或合并规范。

计划的对象验证

计划的对象验证在 Data Protector 计划程序中指定的时间执行，并验证指定时期内创建的备份、复制或合并对象版本。在计划的对象验证规范中指定要验证的对象和对象版本创建的有效期。这样将指定备份、对象复制和/或合并规范以定义所创建的对象，并提供用于筛选对象的标准。一个计划的对象验证规范中可以包括多个备份、对象复制和/或合并规范。

验证对象

首先，启动交互式会话，或创建对象验证规范。选择要验证的备份对象、源设备、介质和验证目标主机。

备份对象的选择

自动操作

对于自动对象验证规范，可以通过选择备份、对象复制或合并规范，然后按照保护、副本数、可用库或时间范围（仅计划）进行筛选，从而选择要验证的对象。在这种情况下，无法选择单独的对象版本进行验证：Data Protector 验证所有符合筛选器标准的对象版本。

交互式操作

对于交互式会话，可以从介质、会话或 IDB 中的对象选择向导列表中选择单独的对象。在这种情况下，可以选择所需对象版本的单独副本进行验证。

源设备的选择

默认情况下，Data Protector 执行自动设备选择。此外，可以强制选择原始设备，或选择新设备。

目标主机的选择

默认情况下，Data Protector 在源主机（即原始备份的源对象所在的主机）上执行验证过程，从而验证对象数据及其传递。还可以指定备用远程主机或介质代理主机，从而仅验证对象数据。请注意，所选目标主机必须装有 Data Protector 磁盘代理。

安排

使用 Data Protector 计划程序，以用于备份的相同方式对计划的验证操作执行计划。

有关如何在 Data Protector 中使用调度程序创建和编辑计划的详细信息，请参阅调度程序。

标准对象验证任务

下面是对象验证功能的先决条件和限制：

需要满足以下先决条件:

- 需要在将充当对象验证会话中的源主机的每个系统上安装介质代理。
- 需要在将充当对象验证会话中的目标主机的每个系统上安装磁盘代理。
- 对象验证处理中涉及的所有磁盘代理都必须为 A.06.11 或更高版本。
- 应配置必要的设备，并准备好介质。
- 您需要在源主机和目标主机上有适当的用户权限才能运行对象验证会话：这些是“启动还原”和“从其他用户还原”用户权限。
- 如果目标主机是 UNIX 主机，则必须有“作为 root 还原”权限。

以下限制适用：

- 读取源介质时，该介质不可用于还原。
- 应用程序集成对象的对象验证包括验证对象数据传递到目标主机以及这些数据从 Data Protector 格式的角度来看保持一致。未执行任何应用程序集成特有的检查。
- 对于使用 ZDB 到磁盘备份的对象或 ZDB 到磁盘 + 磁带的磁盘部分不能使用对象验证。
- 对象验证适用于以 Data Protector 磁带格式存储的备份，这样的备份可以使用标准 Data Protector 网络还原来还原。对象验证不适用于 ZDB 到磁盘或 ZDB 到磁盘 + 磁带中磁盘部分的备份，这样的备份使用即时还原进行还原。
- 不支持将对象验证与 Web 报告结合使用。

以交互方式验证对象

根据需要，可以选择用于从“介质”、“对象”或“会话”起始点开始的交互式验证的对象。不能保存交互式对象验证规范，只能启动对象验证会话。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。
3. 展开**交互**。
4. 单击**介质**、**对象**或**会话**以打开向导。
   - 单击**介质**可列出已将对象写入的可用介质。
   - 单击**对象**可列出已写入可用介质的对象。
   - 单击**会话**可列出从中已将对象写入可用介质的会话。
5. 选择要验证的对象。

   > **注意**从 Data Protector2018.11 (10.20) 开始，对于 VMware 备份，虚拟机磁盘将视为并行运行的对象。虚拟机的磁盘对象会列在**介质**列表中，但它们处于禁用状态，表明虚拟机磁盘已备份到介质。将在虚拟机对象上执行复制或验证操作，并将其所有关联的磁盘对象视为内部对象。
   >
   > 自 Data Protector2018.11 (10.20) 起，对于 VMware 集成，只有在“介质”列表中选择虚拟机对象后，“下一步”选项才会启用。

   单击“下一步”。
6. 选择将从中读取对象的源设备。默认情况下，选择自动选择设备。

   还可以强制选择原始设备，或者可通过单击**原始设备**再选择**更改设备**用其他驱动器代替。

   单击“下一步”。
7. 选择对象验证操作的目标主机。此主机必须装有所需版本级别的 Data Protector 磁带客户机。

默认情况下，选择原始备份源主机。还可以选择介质代理主机（其中装有所选的源设备）或从单元中选择装有所需版本级别的磁带客户机的任意主机。单击“下一步”。

8. 此时将显示包含所选对象的介质的列表。可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

   单击“下一步”。

9. 此时将显示选择进行验证的对象版本的摘要。

   - 要显示特定对象版本的详细信息，请在列表中选择该版本，然后单击**属性**。

     如果存在对象版本的多个副本，则默认情况下 Data Protector 选择一个最适合进行验证的副本。可以在属性中手动选择要验证哪个副本。

     单击**确定**。

   - 要从列表中删除对象版本，请在列表中选择该版本，然后单击**删除**。

10. 单击**完成**以关闭向导并启动验证。

配置备份后对象验证

备份后对象验证配置为在备份会话、对象复制会话或对象合并会话完成之后进行。

在自动对象验证规范中选择相关的备份、对象副本和/或合并规范的名称。运行使用这些所选规范中任意一种的会话时，在该会话完成之后，Data Protector 使用在对象验证规范中指定的标准，验证在会话期间产生的对象。

执行以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。
3. 展开**自动**，右键单击**备份后**，然后选择**添加**以打开向导。
4. 选择要紧跟在对象验证规范后的备份规范。单击“下一步”。
5. 选择要紧跟在对象验证规范后的对象副本规范。单击“下一步”。
6. 选择要紧跟在对象验证规范后的合并规范。单击“下一步”。
7. 如果需要，请指定用于对象验证操作的对象筛选器。将仅验证符合指定标准的对象。单击“下一步”。
8. 如果需要，请指定用于对象验证操作的带库筛选器。将仅验证指定库中介质上包含的对象。单击“下一步”。
9. 选择将从中读取对象的源设备。默认情况下，Data Protector 使用自动设备选择。

   此外，可以强制选择原始设备。这表示如果设备不可用，则 Data Protector 将等待到它可用为止。还可以通过右键单击**原始设备**并选择**更改设备**，用另一个驱动器代替原始设备，例如接下来由新设备替换原始设备。

   单击“下一步”。

10. 选择对象验证操作的目标主机。此主机必须装有 Data Protector 磁带客户机。

    可以选择：

    - 生成了原始备份对象的主机（默认选择）。这还将验证网络路径中的 Data Protector 组件。
    - 介质代理主机，即含有源设备的主机，但不涉及任何网络。
    - 备用远程主机，验证该主机的网络路径中的 Data Protector 组件。

    单击“下一步”。

11. 单击**另存为...**，输入规范名称，然后单击**确定**以保存验证规范。

配置计划对象验证

预定对象验证发生在用户定义的某个时间。可在一个排定对象验证会话中验证由不同备份会话、对象复制会话或对象合并会话生成的对象。

完成以下步骤：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。

3. 展开**自动**，右键单击**预定**，然后选择**添加**以打开向导。
4. 选择定义要为其安排验证的输出对象的备份规范。单击“下一步”。
5. 选择定义要为其安排验证的输出对象的对象副本规范。单击“下一步”。
6. 选择定义要为其安排验证的输出对象的合并规范。单击“下一步”。
7. 如果需要，请指定用于对象验证操作的对象筛选器。

   这使您可以根据保护、副本数或创建时间筛选可用对象。将验证符合筛选器标准的所有对象版本。

   单击“下一步”。
8. 如果需要，请指定用于对象验证操作的带库筛选器。将仅验证指定库中介质上包含的对象。单击“下一步”。
9. 选择将从中读取对象的源设备。默认情况下，Data Protector 使用自动设备选择。

   此外，可以强制选择原始设备。这表示如果设备不可用，则 Data Protector 将等待到它可用为止。还可以通过右键单击**原始设备**并选择**更改设备**，用另一个驱动器代替原始设备，例如接下来由新设备替换原始设备。

   单击“下一步”。
10. 选择对象验证操作的目标主机。此主机必须装有 Data Protector 磁带客户机。

    可以选择：

    - 生成了原始备份对象的主机（默认选择）。这还将验证网络路径中的 Data Protector 组件。
    - 介质代理主机，即含有源设备的主机，但不涉及任何网络。
    - 备用远程主机，验证该主机的网络路径中的 Data Protector 组件。

    单击“下一步”。
11. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存验证规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

自定义对象验证环境

通过修改在没有对象供验证会话进行验证时所生成的消息级别和会话状态，可以自定义对象验证环境。要实现此目的，请修改 SessionStatusWhenNoObjectToVerify 全局选项。

设置传统报告

要设置传统报告，请完成以下步骤:

1. 在上下文列表中选择“报告”。
2. 右键单击“报告”，然后单击“添加报告组”以打开向导。
3. 为报告组命名，然后按照屏幕上的说明操作。

有关使用传统报告的信息，请参阅传统报告。

设置报告服务器

必须在 Data Protector 中导入报告上下文并计划同步时间线。要设置报告服务器，请执行以下任务:

1. 导入报告服务器
2. 配置报告

导入报告服务器

必须导入报告服务器才能查看、生成和下载适用于备份环境的各种集成报告。要导入报告服务器，请执行以下步骤:

> **注意:**为确保报告服务器与 Cell Manager 之间的正确同步，建议您导入与 Cell Manager 版本相同的报告服务器。

1. 转到主页上下文，然后单击“报告”。
   随即右侧窗格中将显示包含“启动导入向导”的“导入报告服务器”。
2. 单击“启动导入向导”，然后输入报告服务器的主机名/IP 地址和端口号。
3. 输入向报告服务器分配的用户凭据，然后单击“下一步”。
4. 将显示证书详细信息。如果证书详细信息正确，则单击“下一步”。
   可选择同步 Data Protector 和报告服务器数据库，以在导入后立即启动或在稍后阶段启动。
   如果导入时未启用同步，则稍后可通过在“配置”页的“数据库”部分中选择“立即同步”进行触发。
5. 设置 ETL 的同步间隔。
   同步间隔应介于 30 分钟到 24 小时之间。经过每个同步间隔后，“报告”主页中将显示“同步状态”更新。
6. 单击“完成”完成报告服务器导入。

取消注册报告服务器

如果当前未使用报告软件或没有为当前 Cell Manager 生成报告，则可以断开与报告服务器的连接 (如果已通过“启动导入向导”导入它)。使用“报告”主页中的“取消注册报告服务器”按钮删除 Cell Manager 与报告服务器之间的连接。此举会从报告软件及关联中删除 Cell Manager 的所有引用。

启动和停止报告服务器

报告服务器包括 Data Protector 报告数据库服务器和 Data Protector 报告应用程序服务器。

报告数据库服务器

报告数据库服务器通过与 Cell Manager 数据库的同步操作来加载其数据库中所需的全部数据。它根据需要处理数据，并将处理后的数据返回给应用程序服务器。

要启动或停止报告数据库服务器，请执行以下操作:

- Windows 系统
  1. 转到“Windows”>“运行”。
  2. 输入 services.msc
  3. 转到 Data Protector 报告数据库服务器，然后单击“启动”或“停止”。
- Linux 系统
  - 在命令提示符处，输入以下命令: service rs_rest-db start/stop 。

报告应用程序服务器

报告应用程序服务器访问 Cell Manager 请求，并将其发送到数据库服务器以请求所需的数据。收到此数据后，它执行逻辑操作并将处理后的数据发送到 Cell Manager。

要启动或停止报告应用程序服务器，请执行以下操作:

- Windows 系统
  1. 转到“Windows”>“运行”。
  2. 输入 services.msc
  3. 转到 Data Protector 报告应用程序服务器，然后单击“启动”或“停止”。
- Linux 系统
  - 在命令提示符处，输入以下命令: service rs_rest-as start/stop 。

配置以下参数:

- 数据库
- 日志
- SMTP
- 端口
- 导出配置
- 导入配置
- RPO/RTO 配置

数据库

要配置数据库，请完成以下步骤:

1. 从左窗格中，选择 “配置”>“设置”。将显示配置列表。
2. 展开“数据库”部分。单击“数据库”旁边的向下箭头。
3. 完成以下步骤:
    1. 输入数据库必须同步的 Cell Manager 名称，然后单击“立即同步”。
    2. 输入必须保留 Cell Manager 数据的起始日期，然后单击“清除”。
    3. 输入数据库同步的保留策略和同步频率，然后单击“保存”。

日志

要配置日志，请完成以下步骤:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“日志”对应的向下箭头以展开该部分。
3. 完成以下步骤:
    1. 从“日志级别” 下拉列表中，选择以下某项: “调试”、“信息”、“警告”、“错误”。“总日志文件大小”字段显示日志文件的当前大小 (兆字节)。
    2. 在“最大文件大小” 字段中，指定日志文件的最大大小 (兆字节)。日志文件达到最大文件大小后，将对其进行存档并创建一个具有相同名称的新日志文件。
    3. 从“日志保留策略” 下拉列表中，选择日志的保留期限 (年)。这是保留日志存档的持续时间。
    4. 单击“保存” 。
    5. *可选*。单击“下载日志” 和“清除日志” 可分别下载和清除日志。

SMTP

可以将包含报告输出的电子邮件发送到指定的收件人。需要配置 SMTP 才能将报告作为电子邮件的附件进行发送。要配置 SMTP，请执行以下操作:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“SMTP”对应的向下箭头以展开该部分，然后指定以下内容。所有字段为必填字段。
    1. 用户名
    2. 密码
    3. 邮件服务器
    4. 端口
    5. 发件人电子邮件地址
3. 单击“保存”。

> 注意: 报告服务器不支持计划报告。因此，在配置 SMTP 后，您必须手动生成电子邮件并将其发送给配置的收件人。有关详细信息，请参阅发送报告部分。

端口

需要为报告服务器更新端口详细信息。 要配置端口，请执行以下操作:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“端口”对应的向下箭头以展开该部分。
3. 输入所需的详细信息，然后单击“保存”。

导出配置

可利用“导出配置”功能导出设置的配置详细信息以供其他报告服务器使用。 要配置导出部分，请执行以下操作:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“导出配置”对应的向下箭头以展开该部分。
3. 输入所需的详细信息，然后单击“导出”。

导入配置

可利用“导入配置”功能导入在其他报告服务器中设置的配置详细信息。要配置导入部分，请执行以下操作:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“导入配置”对应的向下箭头以展开该部分。
3. 输入所需的详细信息，然后单击“导入”。

RPO 和 RTO 配置

当用户生成 RPO 或 RTO 报告时，将显示已保存的 RPO 和 RTO 配置详细信息。要配置 RPO 和 RTO 设置，请执行以下操作:

1. 选择 “配置”>“设置”。将显示配置列表。
2. 单击“RPO/RTO 配置”对应的向下箭头，展开该部分。
3. 选择必须进行 RPO/RTO 配置的 Cell Manager。
4. 选择必须设置 RPO 和 RTO 的“客户机和应用程序类型”对。
5. 以分钟/小时数输入所需的 RPO 和 RTO，然后单击“保存”。

相关主题

有关集成报告的类型以及如何生成它们的详细信息，请参阅使用报告服务器。
有关报告服务器的故障诊断信息，请参阅对报告服务器进行故障诊断。

灾难恢复

本主题综述了灾难恢复过程、介绍了《灾难恢复指南》中使用的基本术语并概述了灾难恢复方法。

计算机灾难指的是任何使计算机系统无法引导的事件，无论是因为人为错误、硬件故障还是自然灾害。在这些情况中，计算机的引导分区或系统分区很有可能不可用，并且需要先恢复环境，然后才能开始正常的还原操作。灾难恢复包括对引导分区进行重新分区和/或重新格式化，并用定义环境的所有配置信息恢复操作系统。*必须* 完成此步骤，才能恢复其他用户数据。

“原始系统”指 Data Protector 在计算机灾难袭击系统之前备份的系统配置。

目标系统是指计算机灾难发生后的系统。目标系统通常处于不可引导状态，Data Protector 灾难恢复的目标是将该系统还原为原始系统配置。受影响系统与目标系统的区别在于目标系统已更换了所有故障硬件。

引导磁盘/分区/卷是指包含引导过程的初始步骤所需的文件的磁盘/分区/卷，而**系统磁盘/分区/卷**是指包含操作系统文件的磁盘/分区/卷。

> **注意**Microsoft 将引导分区定义为包含操作系统文件的分区，而将系统分区定义为包含引导过程的初始步骤所需的文件的分区。

“托管系统”是用于磁盘传递灾难恢复的工作 Data Protector 客户机，其中安装了磁盘代理。

“辅助磁盘”是可引导磁盘，其中安装了可联网的最小操作系统和 Data Protector 磁盘代理。它可以随身携带，用于在 UNIX 客户机磁盘传递灾难恢复的第一阶段引导目标系统。

灾难恢复操作系统 (DR OS) 是用于运行灾难恢复过程的操作系统环境。它为 Data Protector 提供了一个基本的运行时环境（磁盘、网络、磁带和文件系统访问）。必须首先安装并配置此操作系统，Data Protector 灾难恢复才能得以执行。

DR OS 可以是临时或活动的。**临时 DR OS** 专门用作还原其他某些操作系统与目标操作系统配置数据的主机环境。在目标系统还原为原始系统配置之后，它会被删除。“活动 DR OS”不仅托管 Data Protector 灾难恢复过程，还作为还原系统的一部分，因为它将自身的配置数据替换为原始配置数据。

“关键卷”指启动系统所需的卷和 Data Protector 卷。不考虑操作系统，这些卷包括：

- 引导卷
- 系统卷
- 包含 Data Protector 可执行文件的卷
- IDB 所在的卷（对于 Cell Manager）

> **注意**如果 IDB 位于多个卷上，则 IDB 所在的所有卷都会被视为关键卷。

除了上述的关键卷以外，CONFIGURATION 也是 Windows 和 Linux 系统的关键卷集的一部分。在 Windows 系统中，服务备份为 CONFIGURATION 备份的一部分。

在 Windows 系统中，CONFIGURATION 对象中包括的某些项可位于系统、引导、Data Protector 或 IDB 卷以外的卷上。在这种情况下，这些卷也是关键卷集的一部分：

- 用户配置文件卷
- Windows Server 系统上的证书服务器数据库卷
- Windows Server 的域控制器上的 Active Directory 服务卷
- Microsoft 群集服务器上的仲裁卷

在 Linux 系统上，CONFIGURATION 对象仅包含与自动灾难恢复方法相关的数据，例如卷、装载点、网络设置等类似项目。

可访问 Cell Manager 时执行**联机恢复**。在这种情况下，大多数 Data Protector 功能都可用（Cell Manager 可运行会话，还原会话会记录到 IDB 中，您可以使用 GUI 监控还原进度等等）。

在 Cell Manager 不可访问时，执行**脱机恢复**（例如，由于网络故障，Cell Manager 遭受灾难，联机恢复失败等等）。只有独立设备、SCSI

库、文件库和备份到磁盘 (B2D) 设备可用于脱机恢复。只能对 Cell Manager 执行脱机恢复。

如果在 SRD 文件中指定的所有介质代理系统均可访问，则会执行**远程恢复**。如果其中任意系统发生故障，则灾难恢复过程会故障切换到本地模式。这意味着会在目标系统上搜索本地连接的设备。如果只找到一个设备，则自动使用该设备。否则，Data Protector 会提示您选择设备，该设备将用于进行还原。注意，脱机 OBDR 始终在本地执行。

灾难是一种严重情况，但以下因素可能使情况更加恶化：

- 系统必须尽快、尽可能高效地恢复联机状态。
- 灾难恢复不是常见事件，并且管理员可能不熟悉所需的步骤。
- 执行恢复的现有人员可能只具有系统方面的基础知识。

灾难恢复不是经过定义、简单易用的解决方案。而是一个复杂的过程，涉及到执行的大量计划和准备工作。必须完整地定义一个分步过程，才能为从灾难情况中迅速恢复做好准备。

灾难恢复阶段

无论采用什么恢复方法，灾难恢复的过程都可分为四个连续的阶段：

1. 阶段 0

   阶段 0（准备）是成功实施灾难恢复的先决条件。必须在灾难发生前完成规划和准备。

2. 阶段 1

   在**阶段 1** 中，安装并配置 DR OS，此过程通常包括对引导分区进行重新分区和重新格式化，这是因为系统的引导或系统分区并非一直可用而环境需要在常规还原操作再次继续之前得到恢复。

3. 阶段 2

   在阶段 2 中，使用 Data Protector 定义环境所用的所有配置信息还原操作系统（还原成原样）。

4. 阶段 3

   只有在完成在此步骤后，才能还原应用程序和用户的数据（**阶段 3**）。

需要按照经完善定义的分步过程执行以确保快速且高效的还原。

手动灾难恢复方法

Windows 系统（辅助手动灾难恢复）中以及 UNIX 中支持手动灾难恢复。

这是基本灾难恢复方法，该方法涉及将目标系统恢复为原始系统配置。

首先，必须安装和配置 DR OS。然后使用 Data Protector 还原数据（包括操作系统文件），用还原后的操作系统文件替换操作系统文件。

对于手动恢复，重要的是要收集有关存储结构的信息（如分区信息、磁盘镜像和条带），这些信息不保留在平面文件中。

要成功执行手动灾难恢复，应定期运行完整客户机备份。在 Windows 系统中，此过程应包括 CONFIGURATION 备份和 SRD 文件生成。如果要执行 HP-UX 客户机的手动灾难恢复，则根据所选方法准备 Golden Image、可引导磁带或恢复归档（在 Ignite-UX 中使用 make_net_recovery 命令）。

遭受灾难之后，应手动安装操作系统，从而建立原始存储结构并（在 Windows 系统中）运行 drstart.exe 命令以启动关键卷的自动还原。

自动恢复的分区包括：

- 引导卷
- 系统卷
- 包含 Data Protector 的分区

使用标准 Data Protector 还原过程可恢复剩余的分区。

相关任务

- Windows 系统中的灾难恢复过程
- UNIX 系统中的灾难恢复过程

使用磁盘传递进行灾难恢复

磁盘传递灾难恢复 (DDDR) 方法在 UNIX 客户机上受支持。

此方法无需其他客户机，而需要装有最小化的操作系统、网络组件和 Data Protector 磁盘代理的可引导辅助磁盘（可以随身携带）。需要在灾难之前收集足够的信息才能正确地对磁盘进行格式化和分区。

此方法可以简单快速地恢复客户机。

提示此方法对热交换硬盘驱动器尤其有用，因为可以在电源仍接通且系统正在运行的同时断开硬盘驱动器与系统的连接，然后连接新驱动器。

相关任务

- UNIX 系统中的灾难恢复过程

增强型自动灾难恢复（EADR）

Data Protector 提供适用于 Windows 和 Linux Data Protector 客户机以及 Cell Manager 的增强型灾难恢复过程，尽可能减少用户干预。

备份时，EADR 过程将自动收集所有相关的环境数据。在配置备份期间，对于单元中的每个已备份客户机，临时安装和配置 DR OS 所需的数据打包到单个大型 **DR 映像（恢复集）**文件中，该文件存储在备份磁带（以及 Cell Manager（可选））上。

除了此映像文件外，Cell Manager 还将存储阶段 1 启动信息（存储在 P1S 文件中），该启动信息是对磁盘进行正确的格式化和分区所必需的。如果发生灾难，可以使用 EADR 向导从备份介质还原 DR OS 映像（如果在完整备份期间尚未在 Cell Manager 上保存该映像）。可以将其转换为**灾难恢复 CD ISO 映像**、将其保存在可引导 USB 驱动器上，或创建可引导网络映像。然后可以使用任何 CD 刻录工具将 CD ISO 映像刻录到 CD。

在从 CD 、USB 驱动器或网络启动目标系统时，Data Protector 将自动安装和配置 DR OS、对磁盘进行格式化和分区，最后用 Data Protector 将原始系统恢复到备份时的状态。

自动恢复的卷包括：

- 引导卷
- 系统卷
- 包含 Data Protector 安装和配置的卷

使用标准 Data Protector 还原过程可恢复剩余的卷。

为必须首先还原的任何关键系统提前准备灾难恢复映像，尤其是网络正常工作所需的系统（DNS 服务器、域控制器、网关等）、Cell Manager、介质代理和文件服务器等。

重要说明每次硬件、软件或配置更改之后都必须根据新的 DR 映像文件准备好一片新的灾难恢复映像。

相关任务

- Windows 系统中的灾难恢复过程
- UNIX 系统中的灾难恢复过程

一键式灾难恢复 (OBDR)

一键式灾难恢复用于恢复 Data Protector 客户机。

一键式灾难恢复 (OBDR) 是一种适用于 Linux Data Protector 客户机的 Data Protector 自动恢复方法，尽可能减少用户干预。

备份时，OBDR 将自动收集所有相关的环境数据。备份期间，临时安装和配置 DR OS 所需的数据打包在单个大型 OBDR 映像文件（恢复集）中，并存储在备份磁带上。灾难发生时，OBDR 设备（能够模拟 CD-ROM 的备份设备）用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。

然后，Data Protector 运行并配置灾难恢复操作系统 (DR OS)，对磁盘进行分区和格式化，最后使用 Data Protector 将原始操作系统还原为备份时的原样。

重要说明每次硬件、软件或配置更改之后都要执行新的备份。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

OBDR 过程根据所选的恢复范围恢复卷。

可按照 Data Protector 标准还原过程恢复所有剩余卷。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Windows 客户机使用一键式灾难恢复方法的常规步骤包括：

1. **阶段 1**

   从恢复磁带引导并选择恢复范围。

2. **阶段 2**

   根据您所选的恢复范围，系统将自动还原所选的卷。

   关键卷（引导分区和操作系统）始终会被还原。

3. **阶段 3**

   按照标准还原过程还原所有剩余分区。

重要说明建议限制对 OBDR 引导介质的访问。

以下各节将介绍有关在 Windows 系统上执行一键式灾难恢复的要求、限制、准备和恢复。

要求

- 在要允许使用此方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复组件。此外，必须在将准备 DR OS 映像的系统上安装自动灾难恢复组件。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 装有 Data Protector 的卷应至少有 800 MB 的可用空间。此空间是创建临时映像所必需的。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。

- 在 SAN 引导配置中，确保目标系统上的以下项目与原始系统上的一致。
  - 本地 HBA 的 BIOS 参数
  - SAN 磁盘 LUN 数目
- 在多路径 SAN 磁盘配置中，目标系统磁盘的 LUN 和 WWID 必须与原始系统上的一致。

以下限制适用：

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 不支持 USB 磁带存储设备。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION/SYSTEMRECOVERYDATA 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp。但是，如果您手动更新现有的备份规范，则系统将不会设置这一排除。要成功备份，请排除 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 文件夹。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：
  - fio-status – 列出所有 Fusion IO 磁盘的状态。
  - fio-format [path] – 执行 Fusion IO 磁盘的低级格式化。
  - fio-attach [path] – 将 Fusion IO 磁盘连接到系统。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为一键式灾难恢复做准备
2. 恢复操作系统
3. 还原用户数据。

如何为灾难恢复做准备

请仔细按照下方的说明为灾难恢复做准备，以确保快速高效地进行还原。准备过程与灾难恢复方法无关，其中包括开发详细的灾难恢复计划、执行一致和相关的备份以及更新 Windows 中的 SRD 文件。

本主题包含灾难恢复中适用于所有灾难恢复方法的的常规准备过程。对每个特定的灾难恢复方法都需要进行额外的准备。有关其他准备步骤，请参见对应主题。

请记住，使 Cell Manager 做好灾难恢复的准备至关重要，这一点需要多加注意。

重要说明请在灾难发生之前准备灾难恢复。

规划灾难恢复

制定一个详细的灾难恢复计划对灾难恢复的成功有着重要影响。要在具有多个不同的系统的大型环境中部署灾难恢复，请执行以下操作：

1. **计划**

   计划必须由 IT 管理部门进行准备，并且应包括以下步骤：

   - 将应首先恢复的最重要系统列一个清单。关键系统是网络正常运行所需的系统（DNS 服务器、域控制器、网关等等）、Cell Manager 和介质代理客户机。应在所有其他系统之前恢复这些系统。
   - 选择适用于系统的灾难恢复方法。根据这些方法，考虑每个系统需要哪些准备步骤。
   - 确定一种在恢复时获取必要信息（如存储 IDB 的介质、更新后 SRD 文件所在的位置以及 Cell Manager 备份介质的位置和标签）的方法。定义软件库的位置以便执行新的安装。
   - 创建详细的分步核对清单，指导您完成整个过程。
   - 创建并执行测试计划，以确认恢复将真正起作用。
   - *可选*: 如果计划使用虚拟名称 (具有第二个 NIC 并且希望在备份/恢复过程中使用第二个主机名的系统) 运行系统备份，请在将恢复的系统上设置 OB2_DR_CLIENT_NAME=<virtual-hostname> ，以便为该系统创建恢复映像。

2. **恢复准备**

   在运行备份之前执行以下准备步骤，以保证备份期间的环境一致性：

   所有系统：

   - 执行定期和一致的备份。
   - 需要了解卷组和分区的概念。在 UNIX 系统中，应了解有关存储环境结构的信息所在的位置。

   UNIX 系统：

   - 创建 pre-exec 脚本，用来收集存储结构和执行其他特定的客户机准备。
   - 创建工具，如具有最小操作系统、网络资源和已安装 Data Protector 磁盘代理的辅助磁盘。

   Windows 系统：

   - 确保具有有效的 CONFIGURATION 备份供您处理。
   - 更新 SRD 文件，并将其存储在安全位置。出于安全考虑，应限制对 SRD 文件的访问。

3. **执行恢复过程**

   按照已测试过的过程和清单恢复受影响系统。

警告不要更改为灾难恢复准备的系统上的默认 Inet 侦听端口。反之，如果此类系统受到灾难打击，灾难恢复进程可能会失败。

执行一致和相关备份

如果发生灾难，目标系统应恢复原始系统配置。此外，系统的操作和运行应该如同执行上一次有效备份之前那样。

这听起来很简单，但是某些环境会使情况变得很棘手。某些应用程序并非完全不活动，即使将其关闭也是如此。

> **注意**在 UNIX 系统中，系统引导完毕后，某些后台程序或进程就会因为各种原因而处于活动状态（运行级别 2）。此类进程甚至可能会将数据读入内存，并在其运行时将“dirty flag”写入某些文件。在标准操作阶段（标准运行级别 4）执行的备份对此类应用程序产生的重新启动不太可能没有错误。为了按照示例操作，如果在这样的伪恢复之后启动许可证服务器，它将发现从文件读取的数据不一致，并且将拒绝像预期那样运行服务。
>
> 在 Windows 系统中，当系统正常运行时无法替换许多系统文件，因为系统将其锁定。例如，无法还原当前正在使用的用户配置文件。必须更改登录帐户，或者必须停止相关服务。

根据备份运行时系统中活动的内容，可能会违反应用程序的数据一致性，从而导致恢复后重新启动和执行出现问题。

创建一致和相关备份

- 理想情况下，要在相关分区设置为脱机时执行备份，但通常无法满足这种条件。
- 备份期间检查系统中的活动。仅与操作系统相关的进程和联机备份的数据库服务可以在备份执行期间保持活动状态。
- 确保将系统活动降到最低限度。例如，仅核心操作系统、基本网络和备份应处于活动状态。不应运行任何底层应用程序服务。使用适当的 pre-exec 脚本可实现这一点。

灾难恢复使用 btrfs 子卷和通过文件系统 root 备份的卷中的数据（跨文件系统边界），以创建灾难恢复 ISO 映像并执行恢复和还原。这表示所有系统、配置文件和相关用户数据必须包括在 / (root) 文件系统对象的备份中。所有单独备份的数据 (使用 OB2_SHOW_BTRFS_MOUNTS 的数据) 只能用于常规磁盘代理文件系统还原操作，不适用于恢复过程。这仅适用于 Linux 操作系统。

> **注意**Data Protector 包括手动创建的 btrfs 快照中的数据。

一致和相关的备份中应包括的内容取决于您计划使用的灾难恢复方法和系统特有的情况（例如 Microsoft 群集服务器的灾难恢复）。请参见有关准备特定灾难恢复方法的主题。

加密备份

如果备份经过加密，则必须确保安全地存储加密密钥，并在启动灾难恢复时这些密钥可用。如果无法访问适当的加密密钥，灾难恢复过程就会中止。各种灾难恢复方法都有额外的要求。

Data Protector 10.04 在加密模型中引入了一些变化。加密密钥集中存储在 Cell Manager 上；因此灾难恢复客户机必须连接到 Cell Manager 才能获得加密密钥。可能会有以下两种灾难恢复的场景：

- 恢复从中可与 Cell Manager 建立连接的客户机。对于此类场景不需要进行与加密相关的其他准备，因为 Data Protector 会自动获取加密密钥。
- Cell Manager 的灾难恢复或独立客户机恢复，其中无法与 Cell Manager 建立连接。

  提示输入时，必须提供可移动介质（例如磁盘）上的加密密钥。

  这些密钥不是灾难恢复 OS 映像的一部分，会导出到密钥文件 (DR-ClientName-keys.csv)。必须将密钥手动存储到单独的可移动介质，如磁盘或 USB 闪存驱动器。确保始终具有每个备份的密钥的相应副本，以便为灾难恢复做好准备。如果加密密钥不可用，则无法执行灾难恢复。

在 Windows 上更新和编辑系统恢复数据

系统恢复数据 (SRD) 是一个使用 Unicode (UTF-16) 格式的文本文件，其中包含配置目标系统所需的信息。在 Windows 客户机上执行 CONFIGURATION 备份时将生成 SRD 文件，随后该文件将被存储在 Cell Manager 上的以下目录中：

Windows 系统： Data_Protector_program_data\Config\Server\DR\SRD

UNIX 系统： /etc/opt/omni/server/dr/srd 。

重要说明如果 IDB 不可用，则有关对象和介质的信息将仅存储在 SRD 文件中。

Cell Manager 上的 SRD 文件名与生成该文件的计算机的主机名相同 (例如 computer.company.com) 。

CONFIGURATION 备份之后，SRD 文件仅包含安装 DR OS 所需的系统信息。要执行灾难恢复，必须向 SRD 添加有关备份对象和相应介质的其他信息。只能在 Windows 或 Linux 客户机上更新 SRD。经过更新的 SRD 文件的名称为 recovery.srd 。

可以使用以下三种不同的方法更新 SRD 文件：

- 更新 SRD 文件向导（仅在 Windows 系统中提供）
- omnisrdupdate 作为独立设备实用程序的命令
- omnisrdupdate 作为备份会话 post-exec 脚本的命令

重要说明当您为 Cell Manager 更新 SRD 文件时，请指定一个比文件系统备份会话更新的 IDB 备份会话，以便可以在恢复后浏览文件系统备份会话和数据。

Windows 系统中的灾难恢复过程

Data Protector 在 Windows 系统上支持三种灾难恢复方法。无论选择哪种方法，准备阶段都是灾难恢复成功的先决条件。每种灾难恢复方法都有一些限制，在实现之前应考虑这些限制。

重要说明**:** 对于 Data Protector 版本低于 2019.05 的 Windows 系统的灾难恢复，您必须使用与灾难恢复主机相同的 Data Protector 版本的介质创建主机。由于 2019.05 中的 Visual Studio 版本升级，您不得使用 Data Protector 2019.05 或更高版本的介质创建主机。

增强型自动灾难恢复

增强型自动灾难恢复 (EADR) 用于恢复普通 Data Protector Cell Manager 和客户机，以及属于 Microsoft 群集服务器 (MSCS) 一部分的 Data Protector Cell Manager 和客户机。

要求

Windows Server 2016 :

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 新磁盘的大小必须等于或大于受影响的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 用于灾难恢复的所有必要数据的备份可能需要大量可用空间。通常 500 MB 便足够，最高可能需要 1 GB，具体取决于操作系统。
- 在 DR OS 映像创建期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 在引导 DR OS 映像时，网络必须可用。
- 在群集环境中，如果每个群集节点上的总线地址枚举相同，则可以成功备份群集节点。这表示需要：
  - 群集节点主板硬件相同
  - 两个节点上的 OS 版本（Service Pack 和更新）相同
  - 总线控制器的数量和类型相同
  - 必须在相同的 PCI 主板插槽中插入总线控制器。
- 在备份时应当激活操作系统。否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Server 2008 和更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包 (ADK):

  Windows Server 2008 :

  适用于 Windows Server 2008 的自动安装工具包 (AIK)

  Windows Server 2008 R2 :

  - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充 (可选)

  Windows Server 2012 :

  - Windows Server 2012 的评估和部署工具包 (ADK)
  - Windows Server 2016 的评估和部署工具包 (ADK)
- 对于从可引导 USB 设备进行的灾难恢复，请确保：
  - USB 存储设备的大小应至少为 1 GB
  - 目标系统支持从 USB 设备引导。较旧的系统可能需要更新 BIOS，否则可能完全无法从 USB 存储设备启动。
- 要为 Windows Server 2008 和更高版本的 Windows 系统创建可引导网络映像，必须满足以下条件:
  - 在目标系统上，已启用网络适配器以通过 PXE 协议进行通信。此系统的 BIOS 应与 PXE 协议兼容。
  - 已经在 Windows Server 2008 和更高版本的 Windows 系统上安装并配置 Windows 部署服务 (WDS) 服务器。WDS 服务器必须为 Active Directory 域的成员或 Active Directory 域的域控制器。
  - 具有活动范围的 DNS 服务器和 DHCP 服务器正在网络中运行。
- 要备份位于 Windows Server 2008 和更高版本上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。

有关进行灾难恢复所需的系统的详细信息，请参阅“支持矩阵”页中提供的“Data Protector 灾难恢复支持矩阵”。

限制

以下限制适用：

- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 可以在 Windows Server 2008 R2 系统 (在支持的所有平台上) 以及 Windows Server 2012 上创建可引导 USB 驱动器。
- 不支持恢复 SAN 引导配置。
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 不支持 Windows Server 2012 存储空间。

磁盘和分区配置

- 不支持动态磁盘（包括从 Windows NT 升级而来的镜像集）。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为增强的自动灾难恢复做准备。
2. 准备灾难恢复 CD。
3. 恢复 Cell Manager 和客户机系统。
4. 还原用户数据。

一键式灾难恢复

一键式灾难恢复 (OBDR) 用于恢复普通 Data Protector 客户机和属于 Microsoft 群集服务器 (MSCS) 一部分的 Data Protector 客户机。

要求

- 在要允许使用此方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复和用户界面组件。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 新磁盘的大小必须等于或大于受影响的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 在 OBDR 备份期间，Data Protector 所在的分区应至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 在引导 DR OS 映像时网络必须可用。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。
- 要创建 Windows Server 2008 及更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包:

  Windows Server 2008：

  适用于 Windows Server 2008 的自动安装工具包 (AIK)

  Windows Server 2008 R2：

  - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充 (可选)

  Windows Server 2012：

  - Windows Server 2012 的评估和部署工具包 (ADK)

  Windows Server 2016：

  - Windows Server 2016 的评估和部署工具包 (ADK)

- 要备份位于 Windows Server 2008 系统上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。

有关进行灾难恢复所需的系统的详细信息，请参阅“支持矩阵”页中提供的“Data Protector 灾难恢复支持矩阵”。

限制

以下限制适用：

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- 不支持恢复 SAN 引导配置。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 不支持 Windows Server 2012 存储空间。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。

磁盘和分区配置

- 不支持动态磁盘（包括从 Windows NT 升级而来的镜像集）。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。
- 在 NTFS 卷上安装了 Data Protector 的系统支持 OBDR。

完成以下步骤：

1. 为一键式灾难恢复做准备。
2. 恢复操作系统。请参阅“使用一键式灾难恢复恢复 Windows 系统”
3. 还原用户数据。

EISA 实用程序分区

EISA 实用程序分区 (EUP) 是由各种网络服务器出于管理目的所使用的一种分区。向 EUP 分配的系统标识号为 18 (0x12)，只有经过特殊设计的 BIOS 才能识别，对用户不可见。

EUP 格式化为一个标准的 DOS 分区，小于 32 MB（系统标识 4），以某个版本的 DOS 作为其驱动操作系统。由不同 DOS 版本充当 EUP 操作的驱动引擎使 BIOS 在引导时很容易将控制权转交给 EUP，但还原软件时这一点也可能会导致问题。不同版本的 DOS (例如 IBM 和 Microsoft) 的启动顺序实现不同，并且预期某些文件位于文件系统目录结构和群集排序中的某些位置。

辅助手动灾难恢复

在恢复时，Windows 需要安装灾难恢复操作系统 (DR OS)。恢复原始操作系统的过程通过 omnidr 命令自动执行。

决定进行灾难恢复之前，Windows 系统将进一步尝试恢复系统。通过以“安全”模式或从恢复软磁盘引导系统并尝试解决问题，可以实现这一点。

概述

确保已执行准备一章中提及的所有常规准备步骤。Windows 系统的常规辅助手动灾难恢复过程如下：

1. **阶段 1**
   a. 更换故障硬件。
   b. 重新安装操作系统（创建并格式化必需的卷）。
   c. 重新安装 Service Pack。
   d. 手动对磁盘进行重新分区，然后使用原始驱动器号分配重新建立存储结构。

> **提示**您可以将手动灾难恢复的阶段 1 与自动部署工具结合使用。

2. **阶段 2**
   a. 执行将安装 DR OS 并将启动关键卷还原的 Data Protector drstart 命令。
   b. drstart 命令完成后，必须重新启动系统。
   c. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤。有关详细信息，请参阅“高级任务”。
3. **阶段 3**
   a. 使用 Data Protector 标准还原过程还原用户和应用程序数据。

要求

- 这些分区的大小必须等于或大于故障磁盘上分区的大小。这样存储在崩溃磁盘上的信息可还原到一个新磁盘。此外，新卷的文件系统类型（FAT、NTFS）和压缩属性必须匹配。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 所有硬件都必须相同。
- 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复：

  omnicc –secure_comm –configure_for_dr <hostname_of_client_being_recovered>
- 联机恢复客户机之后，在 Cell Manager 上运行以下命令:

  omnicc –secure_comm –configure_peer <client_host_name> -overwrite

完成以下步骤：

1. 为辅助手动灾难恢复做准备
2. 安装和配置操作系统
3. 还原原始操作系统
4. (可选) 还原供应商特有分区
5. 还原用户数据

为辅助手动灾难恢复做准备 (Windows 系统)

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。提前准备，以便快速高效地执行灾难恢复。应特别注意 Cell Manager 的灾难恢复准备。

重要说明请在灾难发生之前准备灾难恢复。

常规准备

完成本节中列出的步骤前，还请参见规划灾难恢复以了解适用于所有灾难恢复方法的常规准备过程。要快速高效地从灾难中恢复，请考虑以下步骤并相应地准备环境：

需要 Windows 可引导安装 CD-ROM 以使系统可以从 CD-ROM 启动。如果没有可引导 CD-ROM 驱动器，则还可以使用 Windows 磁盘。

请确保具有适用于要恢复的系统的驱动程序。可能需要在 Windows 安装过程中安装某些驱动程序，如 HBA 和 SCSI 驱动程序。

要恢复受影响的系统，在灾难之前需要有关系统的以下信息：

- 如果在灾难之前未使用 DHCP，则需要 TCP/IP 属性（IP 地址、默认网关、子网掩码、DNS 顺序 (IPv4)、子网前缀长度以及首选和备用 DNS 服务器 (IPv6)）
- 客户机属性（主机名、域）

确保以下情况属实：

- 应具有有效的完整客户机备份映像 (包括有效的 CONFIGURATION 备份数据)。请参阅《Data Protector 帮助》索引: “备份, Windows 特有”和“备份, 配置”。
- 应具有要用于恢复的 SRD 文件，并用有关备份会话中对象的信息更新该文件。
- 为了恢复 Cell Manager，您应当具备有效的“内部数据库”备份映像，它是在客户机备份映像之后创建的。有关如何配置和执行 IDB 备份的详细信息，请参阅《Data Protector 帮助》索引: “IDB, 配置”。
- 在使用 Microsoft 群集服务器的情况下，一致的备份还包括（在相同的备份会话中）
  - 所有节点
  - 管理虚拟服务器（由管理员定义）
  - 如果将 Data Protector 配置为群集感知应用程序，则还包括 Cell Manager 虚拟服务器和 IDB。
- 具有引导分区的磁盘需要一定的可用磁盘空间以安装 Data Protector 灾难恢复 (15 MB) 和 DR OS。此外，还需要还原原始系统所需的空闲磁盘空间。

将 drsetup 映像（“drsetup 软盘”）复制到 U 盘驱动器或软盘上。软盘数目取决于平台以及 Windows 操作系统的版本。这些映像位于：

- 32 位 Windows 系统：

  Windows Server 2008 及更高版本: Data_Protector_program_data\Depot\DRSetupX86

  Data Protector 安装介质： \i386\tools\DRSetupX86

- AMD64/Intel EM64T 平台上的 64 位 Windows 系统：

  Windows Server 2008 及更高版本: Data_Protector_program_data\Depot\DRSetupX64

  Data Protector 安装介质： \i386\tools\DRSetupX64

发生灾难时，将受影响系统的已更新 SRD 文件保存到第一张软磁盘（磁盘 1）上。每个站点的所有 Windows 系统仅需要一组软磁盘，但始终必须将受影响客户机的已更新 SRD 文件复制到第一张软磁盘上。如果找到多个 SRD 文件，Data Protector 将要求您选择适当的版本。

还可以从 Data Protector 安装介质的 \i386\tools\DRSetup\disk1 位置或从网络直接运行 drstart 命令.

要按照灾难之前的样子重新创建各个磁盘分区，请记录每个分区的以下信息（恢复过程中将需要这些信息）：

- 分区的长度和顺序
- 分配给分区的驱动器号
- 分区的文件系统类型

此信息存储在 SRD 文件中。SRD 文件的 diskinfo 部分中的 -type 选项显示特定卷的卷文件系统类型：

如何从 SRD 文件中确定文件系统类型

类型编号	文件系统
1	Fat12
4 和 6	Fat32
5 和 15	扩展分区
7	NTFS
11 和 12	Fat32
18	EISA
66	LDM 分区

（可选）为供应商特有分区的恢复做准备。

下一页上的表是灾难恢复准备工作的示例。请注意表中的数据属于特定系统且无法用于任何其他系统。

使用 CLI 更新恢复软盘

Data Protector 不提供用于自动创建恢复映像 (软盘) 的命令。但是，您可以通过执行 omnisrdupdate 命令手动更新恢复集中第一个软盘的内容。将恢复集中的第一个软盘插入软盘驱动器并将位置指定为 a:\ ，例如:

Data Protector 客户机系统：

```
omnisrdupdate -session 10/04/2011-1 -host clientsys.company.com -location a:\ -asr
```

Data Protector Cell Manager：

```
omnisrdupdate -session 10/04/2011-1 10/04/2011-2 -host cmsys.company.com -location a:\ -asr
```

要手动创建恢复软盘，您还需要将 DRDiskNumber.cab 文件从 Data_Protector_program_data\Depot\DRSetup\DiskDiskNumber 文件夹复制到相应的恢复软盘。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备：

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：

  omnicc –secure_comm –configure_for_dr <cell_manager_hostname>
- 恢复完成之后，在介质主机上运行以下命令：

  omnicc –secure_comm –configure_peer <cell_manager_hostname>
- 定期备份 IDB。
- 在安全位置（而非在 Cell Manager 上）存储 Cell Manager 的 SRD 文件。

以下限制适用:

- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。

更新 SRD 文件 (Windows 客户机)

CONFIGURATION 备份之后，SRD 文件仅包含安装 DR OS 所需的系统信息。该文件位于 Cell Manager 上：

Windows 系统： Data_Protector_program_data\Config\Server\DR\SRD

UNIX 系统： /etc/opt/omni/server/dr/srd

要执行灾难恢复，必须向 SRD 添加有关备份对象和相应介质的其他信息。只能在 Windows 客户机上更新 SRD。Cell Manager 上的 SRD 文件

名与生成该文件的计算机的主机名相同 - 例如 computer.company.com 。经过更新的 SRD 文件的名称为 recovery.srd 。

SRD 文件中存储的有关备份设备或介质的信息可能在执行灾难恢复时过期。在这种情况下，执行灾难恢复之前，要编辑 SRD 文件以将错误信息替换为相关信息。

重要说明在安全位置（而非在 Cell Manager 上）存储 Cell Manager 的 SRD 文件。建议限制对 SRD 文件的访问。

可通过两种基本方法更新 SRD 文件: 使用 Data Protector 灾难恢复向导和使用 omnisrdupdate 命令。

- 在 Windows 系统上使用 Data Protector 灾难恢复向导更新 SRD 文件
- 使用 omnisrdupdate 命令更新 SRD 文件

在 Windows 系统上使用 Data Protector 灾难恢复向导更新 SRD 文件

完成以下步骤：

1. 在 Data Protector 上下文列表中，单击“还原”。
2. 在范围窗格中，单击**任务**，然后单击**灾难恢复**以打开灾难恢复向导。
3. 在“主机”下拉列表中，选择要为其更新 SRD 文件的系统。
4. 在“灾难恢复方法”列表中，选择 **SRD 文件更新**。单击“下一步”。

   首先在 Cell Manager 中搜索 SRD 文件。如果未找到，则 Data Protector 从上一个备份中还原该文件。
5. 选择还原逻辑卷和系统配置所需的对象和版本。为每个对象单击**下一步**。
6. 指定 SRD 文件的目标。单击**完成**。

使用 omnisrdupdate 命令更新 SRD 文件

可以将 omnisrdupdate 用作独立命令。

要更新 SRD 文件，请修改现有的备份规范，或用指定的 post-exec 脚本创建新的备份规范。

完成以下步骤：

1. 在 Data Protector 上下文列表中，单击“备份”。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”属性页中的“备份规范选项”下，单击**高级**。
5. 在“备份选项”窗口的 Post-exec 文本框中键入 omnisrdupdate 。
6. 在“客户机上”下拉列表中，选择将从中执行此 post-exec 脚本的客户机，然后单击**确定**。
7. 单击**应用**保存更改，然后退出向导。

使用 post-exec 脚本更新 SRD 文件

另一种更新 SRD 的方法是将 omnisrdupdate 命令用作备份 post-exec 脚本。为此，请修改现有的备份规范或创建新的备份规范。执行以下步骤修改备份规范，以便在备份会话停止时，SRD 文件使用有关已备份对象的信息进行了更新：

1. 在备份上下文中，展开**备份规范**项，然后展开**文件系统**。
2. 选择要修改的备份规范（它必须包含所有在 SRD 文件中标记为关键的备份对象，否则更新将失败。建议执行磁盘发现的客户机备份并在“结果区域”中单击“选项”。
3. 单击“备份规范选项”下的**高级**按钮。
4. 在 post-exec 文本框中键入 omnisrdupdate 。
5. 在“客户机上”下拉列表中，选择将从中执行此 post-exec 脚本的客户机，然后单击**确定**确认。它应该是源页上标记为要备份的客户机。

将 omnisrdupdate 命令作为 post-exec 实用程序执行时，会话 ID 将被自动获取，无需指定。

可以通过与独立实用程序相同的方式 (-location Path, -host ClientName) 指定其他所有选项。

重要说明由于 IDB 是在单独的会话中备份的，因此无法在 post-exec 脚本中使用 omnisrdupdate 更新 Cell Manager 的 SRD。

手动安装和配置 Windows 系统

灾难发生之后，应首先安装和配置操作系统。安装操作系统之后，可以进行系统数据恢复。

完成以下步骤：

阶段 1

1. 如果需要，请从 CD-ROM 安装 Windows 系统，然后安装其他驱动程序。必须将 Windows 操作系统安装在灾难之前所安装的相同分区上。请勿在安装系统期间安装 Internet Information Server (IIS)。

   重要说明如果已使用无人看管安装程序安装了 Windows 操作系统，则现在请使用相同的脚本重新安装 Windows，以确保将 %SystemRoot% 和 %SystemDrive%\Documents and Settings 文件夹安装到相同位置。

2. 显示“Windows Partition Setup”屏幕时，请执行以下操作：
   - 如果灾难之前系统上存在 EISA 实用程序分区 (EUP)，则使用 SRD 文件中存储的 EUP 信息创建（如果因灾难而不存在）和格式化“虚拟”FAT 分区。EUP 稍后将恢复到由“虚拟”分区占用的空间。“虚拟”分区之后立即创建和格式化临时引导分区。
   - 如果灾难之前系统上不存在 EUP，则创建（如果因灾难而不存在引导分区）和格式化引导分区（如果灾难之前磁盘上存在该分区）。

     Windows 安装程序提示输入 Windows 安装目录时，在引导分区上指定一个与原始 Windows 安装所在目录相同的新目录。

     注意安装期间，不要将系统添加到其以前所在的 Windows 域，而是要添加到工作组。如果要还原主域控制器 (PDC)，则确保目标还原系统不位于受影响 PDC 曾控制的域中。

3. 安装 TCP/IP 协议。如果灾难发生之前未使用 DHCP，请通过提供以下信息将 TCP/IP 协议配置为灾难前的状态：受影响客户机的主机名、其 IP 地址、默认网关、子网掩码和 DNS 服务器。可以从 SRD 文件获取此信息。确保标有**此计算机的主 DNS 后缀**的字段中包含您的域名。

   注意默认情况下，在 Windows 安装期间 Windows 将安装动态主机配置协议 (DHCP)。

   在 Windows Administrators 组中创建新的临时灾难恢复帐户 (例如 DRAdmin)，然后将其添加到 Cell Manager 上的 Data Protector Admin 组。

   灾难之前系统中不得存在该用户帐户。此过程中稍后将删除该临时 Windows 用户帐户。
4. 使用新创建的帐户注销和登录系统。
5. 创建和格式化所有未格式化的分区（如果使用“虚拟”EISA 实用程序分区，则包括该分区），如同灾难之前磁盘上存在这些分区那样。使用供应商特有的过程创建实用程序分区。必须将“虚拟”EISA 实用程序分区格式化为 FAT 文件系统。按灾难之前的方式向这些分区分配驱动器号。

阶段 2

1. 如果 SRD 文件中的信息并非最新（例如因为灾难之后更改了备份设备），并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
2. 从 Data_Protector_home\Depot\drsetup\disk1 (Cell Manager) 或 \i386\tools\drsetup\disk1 (Data Protector 安装介质) 目录中运行 drstart。

   如果已准备 drsetup 软盘，则也可以从第一个软盘上运行 drstart。
3. drstart 首先扫描当前工作目录、软盘驱动器和 CD-ROM 驱动器，以确定灾难恢复设置文件 (dr1.cab 和 omnicab.ini) 的位置。如果找到了所需的文件，则 drstart 实用程序将在 %SystemRoot%\system32\OB2DR 目录中安装灾难恢复文件。如果未找到这些文件，则应浏览查找它们或在 DR Installation Source 文本框中输入其路径。
4. 如果发现 SRD 文件 (recovery.srd) 与 dr1.cab 和 omnicab.ini 在同一目录中，drstart 会将 recovery.srd 复制到 %SystemRoot%\system32\OB2DR\bin 目录，并且 omnidr 实用程序将自动启动。否则，您可以在 SRD Path 文本框中输入 SRD 文件 (recovery.srd) 的位置或浏览查找该文件。单击“下一步”。

   如果在软盘上找到了多个 SRD 文件，Data Protector 将要求您选择一个适当的 SRD 文件版本。

   omnidr 成功完成之后，正常引导系统需要的所有关键对象都会还原。
5. 从 Cell Manager 上的 Data Protector Admin 组删除临时 Data Protector 用户帐户 (在阶段 1 期间添加)，除非灾难恢复之前 Cell Manager 上就存在该帐户。
6. 重新启动系统，登录并验证还原的应用程序正在运行。

阶段 3

7. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤（如恢复 MSCS 或 IIS、编辑 kb.cfg 和 SRD 文件）。有关详细信息，请参阅“高级恢复任务”一节。
8. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

第一次登录之后将删除临时 DR OS，但以下情况除外：

- 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
- 您手动执行带有 omnidr 或 -no_reset 选项的 -debug 命令。
- 灾难恢复失败。

还原 Data Protector Cell Manager 详情

执行 Windows 系统的常规手动灾难恢复过程之后，使用 Data Protector 执行额外步骤以还原 Cell Manager。

要使 IDB 恢复保持一致，请还原有关灾难恢复期间未还原的备份对象的信息。为此，请通过导入含有用于灾难恢复的 Cell Manager 完整客户机备份的介质来更新 IDB。

手动还原系统数据 (Windows 系统)

安装和配置操作系统 (阶段 1) 之后，可以恢复客户机或 Cell Manager。Cell Manager 和 Internet Information Server (IIS) 的灾难恢复还要求执行其他步骤。

还原 Windows 系统

完成以下步骤：

阶段 2

1. 如果 SRD 文件中的信息并非最新（例如因为灾难之后更改了备份设备），并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
2. 从 Data_Protector_home\Depot\drsetup\disk1 (Cell Manager) 或 \i386\tools\drsetup\disk1 (Data Protector 安装介质) 目录中运行 drstart。

   如果已准备 drsetup 软盘，则也可以从第一个软盘上运行 drstart。
3. drstart 首先扫描当前工作目录、软盘驱动器和 CD-ROM 驱动器，以确定灾难恢复设置文件 (dr1.cab 和 omnicab.ini) 的位置。如果找到了所需的文件，则 drstart 实用程序将在 %SystemRoot%\system32\OB2DR 目录中安装灾难恢复文件。如果未找到这些文件，则应浏览查找它们或在 DR Installation Source 文本框中输入其路径。
4. 如果发现 SRD 文件 (recovery.srd) 与 dr1.cab 和 omnicab.ini 在同一目录中，drstart 会将 recovery.srd 复制到 %SystemRoot%\system32\OB2DR\bin 目录，并且 omnidr 实用程序将自动启动。否则，您可以在 SRD Path 文本框中输入 SRD 文件 (recovery.srd) 的位置或浏览查找该文件。单击“下一步”。

如果在软盘上找到了多个 SRD 文件，Data Protector 将要求您选择一个适当的 SRD 文件版本。

omnidr 成功完成之后，正常引导系统需要的所有关键对象都会还原。

5. 从 Cell Manager 上的 Data Protector Admin 组删除临时 Data Protector 用户帐户 (在阶段 1 期间添加)，除非灾难恢复之前 Cell Manager 上就存在该帐户。
6. 重新启动系统，登录并验证还原的应用程序正在运行。

阶段 3

7. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤（如恢复 MSCS 或 IIS、编辑 kb.cfg 和 SRD 文件）。
8. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

第一次登录之后将删除临时 DR OS，但以下情况除外：

- 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
- 您手动执行带有 omnidr 或 -no_reset 选项的 -debug 命令。
- 灾难恢复失败。

还原 Data Protector Cell Manager 详情

执行 Windows 系统的常规手动灾难恢复过程之后，使用 Data Protector 执行额外步骤以还原 Cell Manager。

要使 IDB 恢复保持一致，请还原有关灾难恢复期间未还原的备份对象的信息。为此，请通过导入含有用于灾难恢复的 Cell Manager 完整客户机备份的介质来更新 IDB。

还原供应商特有的分区 (Windows 系统)

如果需要，可以用恢复供应商特有的分区 (VSP) 结束常规手动灾难恢复过程。

免责声明

恢复 VSP 可能是一个复杂过程，需要 Windows 操作系统的高级技术和知识。此处提供的信息仅为方便您使用。使用这些信息应由*您自担风险*。如果还原 VSP 之后更改了分区顺序，则将需要修改 boot.ini 文件。 boot.ini 文件有误将导致系统不可引导。

还原 Eisa 实用程序分区

完成以下步骤：

1. 如果未保留 Eisa 实用程序分区 (EUP)，则必须手动创建该分区。注意，EUP 应位于系统 BIOS 所识别的第一个磁盘上。由于 Disk Manager 无法创建 EUP，因此创建一个普通的 FAT16 分区，并向其分配一个驱动器号。
2. 使用 Data Protector 还原其内容。对于 Eisa 实用程序分区配置对象，选择**恢复为**选项。所分配的驱动器号必须是创建 EUP 期间分配的驱动器号，并且要还原到的目录必须为根目录 (\)。
3. 重新安排根目录条目（如有必要）。
   1. 运行 omnipm ，选择 EUP，然后单击“根...”。此时将显示 EUP 的根目录。
   2. 将根目录的条目重新排序到其原始位置。使用拖放或右键单击条目以显示选项菜单。

   将 FAT16 分区更改为真正的 EUP。
   1. 选择 EUP，然后单击**取消映射**。此时即删除驱动器号。
   2. 单击**类型**。此时将显示一个对话框窗口。选择 **Eisa 实用程序分区**。

相关任务

- 标准备份过程
- 合并 Microsoft 群集服务器的 P1S 文件

增强型自动灾难恢复 (EADR)

增强型自动灾难恢复 (EADR) 用于恢复 Data Protector Cell Manager 和客户机。

Data Protector 为 Linux Data Protector Cell Manager 和客户机提供增强型灾难恢复过程。

备份时，EADR 将自动收集所有相关的环境数据。在整个客户机系统的完整备份期间，对于单元中的每个已备份客户机，临时安装和配置 DR OS 所需的数据打包在单个大型恢复集文件中并存储在备份磁带上（以及可选存储在 Cell Manager 上）。

除此映像文件以外，对磁盘进行正确分区和格式化所需的阶段 1 启动文件（P1S 文件）存储在备份介质和 Cell Manager 上。灾难发生时，增强型自动灾难恢复向导用于从备份介质还原恢复集（如果其在完整备份期间未保存在 Cell Manager 上）并将其转换为灾难恢复 CD ISO 映像。可以使用任何 CD 刻录工具将 CD ISO 映像录制到 CD 上并用于引导目标系统。

启动 DR OS 映像后，Data Protector 将自动对磁盘进行格式化和分区，最后用 Data Protector 将原始系统恢复到备份时的状态。

重要说明

- Micro Focus 建议限制对备份介质、恢复集文件、SRD 文件和灾难恢复 CD 的访问。
- 使用 omnikeytool -export *keyFileName* [-password] 命令加密并导出的备份不支持灾难恢复。使用 omnikeytool -export *keyFileName* 命令导出密钥，而无需 -password 选项。有关更多信息，请参见 omnikeytool 命令页面。
- 跨多个介质的备份不支持 AES 加密的灾难恢复备份和还原。这适用于所有设备类型。
- 即使目标系统中可用的 NIC 少于源系统中的可用 NIC，使用 NIC 聚合的 EADR 恢复也是成功的。以下是此类 NIC 负载均衡的列表:
  - 激活备份
  - XOR (异或)
  - 广播
  - 动态链路聚合
  - 传输负载均衡 (TLB)
- 默认情况下，通过 EADR 磁盘分区大小调整支持，可以将源系统中磁盘的原始分区调整为新替换的磁盘大小。仅在以下情况下受支持:
  - 该磁盘是非 LVM 磁盘
  - 该磁盘具有单一分区，该分区具有以下属性:
    - 分区类型为非 LVM
    - 分区样式为 MBR 或 GPT
    - 分区具有 ext4/xfs 文件系统
  - 新替换的磁盘大小大于源系统中的原始磁盘
    无论该分区主机上的数据如何 (/boot, /home, /var, /tmp or user data)，都会调整磁盘分区的大小。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Linux 客户机使用增强型自动灾难恢复方法的常规步骤包括：

1. **阶段 1**
   a. 更换故障硬件。
   b. 从灾难恢复 CD 或 USB 闪存驱动器引导目标系统并选择恢复的范围。这是完全无人看管的恢复。
2. **阶段 2**
   a. 根据您所选的恢复范围，系统将自动还原所选的卷。关键卷（引导卷、根卷以及包含 Data Protector 安装和配置的卷）始终会被还原。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

重要说明提前为任何必须首先还原的关键卷（尤其是 DNS 服务器、Cell Manager、介质代理客户机、文件服务器等等）准备好 DR OS 映像。

提前为 Cell Manager 恢复准备好包含加密密钥的可移动介质。

以下各节将介绍与 Linux 客户机的 EADR 相关的要求、限制、准备步骤和恢复过程。

要求

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 备份时引导分区上还需要另外 200 MB 的可用磁盘空间。如果没有这些磁盘空间，则灾难恢复将失败。
- 在 EADR 准备期间，安装 Data Protector 所在的卷必须至少具有 800 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 系统的 BIOS 必须支持可引导 CD 扩展（如 El-Torito 标准所定义），并且必须支持通过 INT13h 功能 XXh 使用 LBA 寻址对硬盘驱动器进

行读/写访问。可以在系统的用户手册中或通过在引导之前检查系统设置而检查 BIOS 选项。

- 在 UEFI+Secureboot ON 模式下用于保护系统二进制文件的加密密钥在 RHEL 版本 8.0 到 8.5 之间是不同的。确保介质创建主机操作系统版本与 DA 客户机备份系统相同，以便创建 ISO 映像并在 UEFI+secureboot ON 模式下成功启动。
- 必须在系统上安装模块 dmsquash-live ，才能成功进行 EADR 备份。此模块是 dracut-live 包的一部分，默认情况下此包不会作为操作系统版本 8.x 安装的一部分进行安装。确保从操作系统 ISO 映像或 DVD 安装此包。
- 确保在 Cell Manager 的管理员组中添加以下用户以成功进行联机 EADR 恢复:

在 Windows 客户机中：
Type = Windows, name = Administrator, domain/group = <domain/group of DR client>, client = <DR client>
Type = Windows, name = SYSTEM, domain/group = NT AUTHORITY, client = <DR client>

在 Linux 客户机中:
Type = UNIX, name = root, Unix group = root, client = <DR client>

以下限制适用：

- 增强型自动灾难恢复 (EADR) 和一键式灾难恢复 (OBDR) 仅在 Linux 系统上可用。
- 必须在 Linux 系统上创建 Linux 系统的 DR ISO 映像。不可以在其他系统（Windows 系统、HP-UX 系统、Solaris 系统）上创建 DR ISO 映像。该限制不适用于更新 SRD 文件或其他任务。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData ，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。
- 不支持自定义内核安装或配置，仅支持随分发提供的原始内核。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 。但是，如果您手动更新现有的备份规范，则系统将不会设置这一排除。要成功备份，请排除 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 文件夹。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：
  - fio-status – 列出所有 Fusion IO 磁盘的状态。
  - fio-format [path] – 执行 Fusion IO 磁盘的低级格式化。
  - fio-attach [path] – 将 Fusion IO 磁盘连接到系统。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs（多种 btrfs raid 配置），因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 /etc/fstab 文件。需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。这同样适用于 GRUB 配置，因此请避免 UUID。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

> **注意**
>
> Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。父对象与其快照之间的整体写时复制 (COW) 关系会丢失。因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 /etc/fstab 文件中的 subvolid（请参阅《btrfs 文档》）装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 subvolid 不需要与备份期间的相同。尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

> **注意**
>
> 使用 fstab 中的 subvol 选项而不是 subvolid。

- 不支持使用基于以太网的光纤通道 (FCoE) LUN 和基于以太网的光纤通道 (FCoE) SAN 引导对系统执行 EADR。
- 连接有外部 USB 驱动器的系统支持备份和恢复。但 USB 驱动器上的数据无法备份或恢复。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为增强的自动灾难恢复做准备
2. 准备灾难恢复 CD
3. 恢复 Cell Manager 和客户机系统
4. 还原用户数据。

为增强的自动灾难恢复做的准备（Windows 和 Linux）

要做好准备而使灾难恢复成功，请遵照与所有灾难恢复方法的常规准备过程相关的说明，然后再执行本主题中列出的步骤。必须提前准备，以便快速高效地执行灾难恢复。应特别注意 Cell Manager 的灾难恢复准备。

> **重要说明**请在灾难发生之前准备灾难恢复。

在选择此灾难恢复方法前，请考虑以下要求和限制：

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 在 Windows Server 2008 及更高版本中，至少有一个卷必须为 NTFS 卷。
- 用于灾难恢复的所有必要数据的备份可能需要大量可用空间。通常 500 MB 便足够，最高可能需要 1 GB，具体取决于操作系统。
- 如果可引导 USB 设备连接到 Windows 客户机，则 CONFIGURATION 对象的备份可能会失败。定义 omnirc 选项 OB2_USE_SYSTEM_BOOT_VOL=1 以将系统卷设置为引导卷。
- 在 DR OS 映像创建期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 确保已启用自动装载功能。自动装载功能可确保所有卷（没有装载点）都处于联机状态。如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- 在群集环境中，如果每个群集节点上的总线地址枚举相同，则可以成功备份群集节点。这表示需要：
  - 群集节点主板硬件相同
  - 两个节点上的 OS 版本（Service Pack 和更新）相同
  - 总线控制器的数量和类型相同
  - 必须在相同的 PCI 主板插槽中插入总线控制器。
- 在备份时应当激活操作系统。否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Server 2008 和更高发布的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包 (ADK): Data Protector 将检查 WAIK/ADK 版本，如果没有适当的版本可用，将中止映像创建。
  - **Windows 7、Windows Server 2008 和 2008 R2**
    - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充
  - **Windows 8 和 8.1、Windows Server 2012 和 2012 R2**
    - Windows 8.1 更新的评估和部署工具包 (ADK)，版本 1.1
  - **Windows 10、Windows Server 2016**
    - Windows 10 的评估和部署工具包 (ADK)，版本 1703
  - **Windows 10、Windows Server 2019**
    - Windows 10 的评估和部署工具包 (ADK)，版本 1809
    - Windows PE ADK 加载项，版本 1809

- 对于从可引导 USB 设备进行的灾难恢复，请确保：
  - USB 存储设备的大小应至少为 1 GB
  - 目标系统支持从 USB 设备引导。较旧的系统可能需要更新 BIOS，否则可能完全无法从 USB 存储设备启动。
- 要为 Windows Server 2008 和更高版本的 Windows 系统创建可引导网络映像，必须满足以下条件:
  - 在目标系统上，已启用网络适配器以通过 PXE 协议进行通信。此系统的 BIOS 应与 PXE 协议兼容。
  - 已经在 Windows Server 2008 和更高版本的 Windows 系统上安装并配置 Windows 部署服务 (WDS) 服务器。WDS 服务器必须为 Active Directory 域的成员或 Active Directory 域的域控制器。
  - 具有活动范围的 DNS 服务器和 DHCP 服务器正在网络中运行。
- 要备份位于 Windows Server 2008 和更高版本上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。
- 在为 Linux 客户机创建恢复 ISO 映像的过程中，恢复介质创建主机必须安装 **squashfs 工具**和 **mkisofs**，才能成功创建恢复 ISO 映像。

以下限制适用：

- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 您可以在所有受支持的 Windows 平台上创建可引导 USB 驱动器
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 不支持 Windows Server 2012 存储空间。
- 请勿选择属于检查点重新启动备份会话的备份对象版本。
- 选择对象复制作为恢复源时，需遵守以下规则：
  - 只能选择完整备份对象的副本用于恢复。
  - 仅在从卷的列表中创建卷恢复集时才能选择对象副本。不支持会话。
  - 不支持介质副本。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs（多种 btrfs raid 配置），因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 /etc/fstab 文件。需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。这同样适用于 GRUB 配置，因此避免用于 root 设备的 UUID，并按名称更换设备。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

  > **注意**
  >
  > Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。父对象与其快照之间的整体写时复制 (COW) 关系会丢失。因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 /etc/fstab 文件中的 subvolid（请参阅《btrfs 文档》）装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 subvolid 不需要与备份期间的相同。尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

  > **注意**

使用 fstab 中的 subvol 选项而不是 subvolid。

磁盘和分区配置

- 不支持动态磁盘（包括从 Windows NT 升级而来的镜像集）。
- 驻留在 Windows 群集中的共享动态磁盘不支持 EADR。
- 如果系统保留卷驻留在动态磁盘上，在 Data Protector GUI 中，卷不由黄色图标指示，而是指示为绿色图标。
- 通过动态磁盘执行灾难恢复时，在启动 EADR 之前需要清除所有磁盘。
- EADR 会话之后，将重新创建所有卷，但只有恢复范围内的卷能够还原。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。
- 恢复使用 Intelligent Provisioning 工具 (1.4 和 1.5 版本) 部署的操作系统可能会由于错误的 MBR 分区信息而失败。注意: 这可能属于产品声明。
- 稀疏文件被还原为其完整大小。这可能会导致目标卷空间用尽。
- 不支持物理磁盘不完全属于存储池的存储空间配置。

常规准备

1. 执行完整的客户机系统备份。建议备份整个客户机，如若不然，您至少需要选择以下关键卷和对象：

   - 引导和系统卷
   - Data Protector 安装卷
   - CONFIGURATION 对象所在的卷
   - Active Directory 数据库卷（如果使用 Active Directory 控制器）
   - 仲裁卷（如果使用 Microsoft 群集服务器）

   在客户机完整备份期间，恢复集和 P1S 文件存储在备份介质上和（恢复集可选）Cell Manager 上。

   注意事项：

   ***Windows Server 2008 及更高版本*:**

   - 请确保同时备份存在的系统卷。
   - 可以通过使用 VSS 写入程序的磁盘映像备份来备份逻辑卷。VSS 磁盘映像备份可确保卷在备份过程中保持未锁定状态，并可由其他应用程序访问。必须使用常规文件系统备份来备份 IDB 和 CONFIGURATION 对象以及未装载的卷或作为 NTFS 文件夹装载的卷。

   ***Windows Server 2012 及更高版本*:**

   - 使用磁盘映像备份在以下情况下备份卷:
     - 重复卷

       在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。磁盘映像还原会保持卷的大小。
     - 使用复原文件系统 (ReFS) 的卷

   ***Microsoft 群集服务器*:**

   - 一致的备份包括 (在相同的备份会话中):
     - 所有节点
     - 管理虚拟服务器（由管理员定义）
     - 如果将 Data Protector 配置为群集感知应用程序，则包括 Cell Manager 虚拟服务器和 IDB。

     以上各项应包含在相同的备份会话中。
   - *群集共享卷：*执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。

     必须卸载虚拟硬盘 (VHD) 以确保一致性。
   - 执行备份之后，在 MSCS 中合并所有节点的 P1S 文件，以使每个节点的 P1S 文件都包含关于共享群集卷配置的信息。

     如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。如果要恢复 Cell Manager 或如果无法与 Cell Manager 建立连接，则需要该密钥。

   ***Windows Server 2008 和更高版本的 Windows Server 上的 Active Directory*:**

   - 如果您的 Windows Server 是 Active Directory 大小超过 512 MB 的域控制器，则需要修改客户机备份的备份规范: 在源页中，展开 CONFIGURATION 对象，并清除 ActiveDirectoryService 和 SYSVOL 项的复选框。

     > **注意**
     >
     > Active Directory 和 SYSVOL 将仍作为系统卷（C:\）备份的一部分进行备份。默认情况下，它们分别位于 C:\Windows\NTDS 和 C:\Windows\SYSVOL。

2. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复:

   ```
   omnicc –secure_comm –configure_for_dr <hostname_of_client_being_recovered> -overwrite
   ```

3. 联机恢复客户机之后，在 Cell Manager 上运行以下命令:

   omnicc –secure_comm –configure_peer <client_host_name>

4. 灾难发生之后，使用 EADR 向导将 DR 映像转换为灾难恢复 CD ISO 映像。

   ***Windows Server 2008 及更高版本*:** 或者使用 DR OS 映像代替灾难恢复 CD，创建可启动网络映像或可启动 USB 驱动器。

5. 使用支持 ISO9660 格式的任何 CD 录制工具在 CD 上录制灾难恢复 CD ISO 映像。此灾难恢复 CD 随后可用于引导目标系统并自动还原关键卷。

6. 执行灾难恢复测试计划。

7. 在 Windows 系统上，如果在启动后某些服务或驱动程序无法运行，则可能需要手动编辑 kb.cfg 文件。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备。

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：

  omnicc –secure_comm –configure_for_dr <cell_manager_hostname>

- 恢复完成之后，在介质主机上运行以下命令：

  omnicc –secure_comm –configure_peer <cell_manager_hostname>

- 定期备份 IDB。IDB 会话不应早于文件系统会话。
- 在安全位置（而非在 Cell Manager 上）存储 Cell Manager 的 SRD 文件。
- 提前为 Cell Manager 准备灾难恢复操作系统映像。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv（Windows 系统）或 /var/opt/omni/server/export/keys/DR-ClientName-keys.csv（UNIX 系统），其中 ClientName 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

将恢复集保存到 Cell Manager

在进行完整客户机备份期间，恢复集打包在单个大型文件中，并存储在备份介质上和（可选）Cell Manager 上。如果计划在 Cell Manager 上录制灾难恢复 CD，则将恢复集文件保存到 Cell Manager 会很有用，这是因为从硬盘获取恢复集比从备份介质还原要快得多。

如果在备份期间将恢复集保存到 Cell Manager，则系统会将其保存到默认的 Data Protector P1S 文件位置。

要更改默认位置，请指定一个新的全局选项 EADRImagePath = valid_path（例如 EADRImagePath = /home/images 或 EADRImagePath = C:\temp）。

请参阅《Data Protector 帮助》索引: “全局选项, 修改”。

> **提示**如果在目标目录中没有足够的可用磁盘空间，则可以创建装载点（Windows 系统）或另一个卷的链接（UNIX 系统）。

将备份规范中所有客户机的恢复集文件保存到 Cell Manager

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。
4. 在"结果区域"中，单击**选项**。
5. 在**文件系统选项**下，单击**高级**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Server 2008 及更高版本:** 在 **WinFS 选项**页中，选择**检测 NTFS 硬链接**，选中**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

   “WinFS 选项”选项卡

将备份规范中特定客户机的恢复集文件保存到 Cell Manager

要仅为备份规范中的特定客户机复制恢复集文件，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。
4. 在"结果区域"中，单击**备份对象摘要**。
5. 选择要将其恢复集文件存储在 Cell Manager 上的客户机，并单击**属性**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Server 2008 及更高版本:** 在 **WinFS 选项**页中，选中**检测 NTFS 硬链接**和**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

准备 DR OS 映像

灾难发生之前，应准备一个要录制在灾难恢复 CD 上或保存到可引导 USB 驱动器的 DR OS 映像，它随后可用于增强的自动灾难恢复。或者，也可以准备可引导的网络映像。

请注意，必须在将准备 DR OS 映像的系统上安装 Data Protector 自动灾难恢复组件。

每次硬件、软件或配置更改之后都必须根据新的恢复集准备好一个新的灾难恢复 OS 映像。

为必须首先恢复的任何关键系统提前准备 DR OS 映像，尤其是网络正常工作所需的系统（DNS 服务器、域控制器、网关等）、Cell Manager、介质代理客户机和文件服务器等。

建议对含有 OS 映像的备份介质和灾难恢复 CD 或 USB 驱动器的访问权限进行限制。

完成以下步骤：

1. 在 Data Protector 上下文列表中，单击“还原”。
2. 在“范围窗格”中，单击**任务**，然后单击**灾难恢复**以启动灾难恢复向导。
3. 在结果区域中，从**要恢复的主机**下拉列表中选择要为其准备 DR OS 映像的客户机，然后单击**验证**以验证该客户机。

   > **注意**
   >
   > 经过验证的客户机将添加到**要恢复的主机**下拉列表中。

4. 在**恢复介质创建主机**下拉列表中，选择要在其上准备 DR OS 映像的客户机。默认设置下，该客户机与为其准备 DR OS 映像的客户机一样。您在其上准备 DR OS 映像的客户机必须安装有相同 OS 类型（Windows、Linux），并且必须已安装“磁带客户机”。
5. 使**增强的自动灾难恢复**保持选中状态，并选择要从备份会话还是从卷列表构建卷恢复集。默认情况下，选择**备份会话**。

   单击“下一步”。
6. 具体取决于所选的恢复集构建方法：

   - 如果选择了备份会话，则应选择主机备份会话；如果是 Cell Manager，则选择 IDB 会话。
   - 如果选择了“卷”列表，则应为每个关键对象选择相应的对象版本。

   单击“下一步”。
7. 选择恢复集文件的位置。默认情况下，**从备份还原恢复集文件**处于选中状态。

   如果在备份期间已在 Cell Manager 上保存了恢复集文件，则应选择**指向恢复集文件的路径**并指定其位置。单击“下一步”。
8. 选择映像格式。可用的选项如下：

   - **创建可引导的 ISO 映像**: DR ISO 映像 (默认情况下为 recovery.iso)
   - **创建可引导 USB 驱动器**：可引导 USB 驱动器上的 DR OS 映像
   - **创建可引导的网络映像**: 可用于网络引导的 DR OS 映像 (默认情况下为 recovery.wim)
9. 如果创建的是可引导 ISO 映像或可引导网络映像，请选择要将创建的映像放置到的目标目录。

   如果要创建可引导的 USB 驱动器，请选择要在其中放置所创建的映像的目标 USB 驱动器或磁盘编号。

   > **重要说明**
   >
   > 在创建可引导的 USB 驱动器时，该驱动器上存储的所有数据将丢失。

10. 也可选择设置密码来防止对 DR OS 映像进行未授权的使用。锁图标指示是否设置了密码。

    单击**密码**打开“密码保护映像”对话框并输入密码。要删除密码，清除字段内容即可。
11. **Windows Server 2008 及更高版本**:

    查看并修改（如果需要）插入 DR OS 映像中的驱动程序的列表。

可以使用此选项将缺少的驱动程序添加到 DR OS 中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

> **重要说明**
>
> 在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要插入 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

12. 单击**完成**以退出向导并创建 DR OS 映像。
13. 如果要创建可引导的 CD 或 DVD，可使用支持 ISO9660 格式的刻录工具，将 ISO 映像刻录在 CD 或 DVD 上。

使用 EADR 恢复 Linux 系统

只有在完成所有准备步骤后，才能成功执行 Linux 系统的增强型自动灾难恢复。如果要恢复 Cell Manager，将先从内部数据库的备份映像将该内部数据库还原，然后从卷和 CONFIGURATION 对象的备份映像将卷和 CONFIGURATION 对象还原。

以下先决条件适用:

- 需要用新硬盘更换受影响的磁盘。
- 您应当具有要恢复的整个系统的有效完整文件系统备份（客户机备份）。
- 为了对 Cell Manager 进行灾难恢复，您应当具备有效的“内部数据库”备份映像，它应当比文件系统备份映像新。
- 需要灾难恢复 CD。

完成以下步骤：

阶段 1

阶段 3

1. 除非要执行脱机灾难恢复操作，否则向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector admin 帐户:

   > **注意**
   >
   > 灾难恢复过程只能由 root 用户执行。

   - 类型： root
   - 组\域: root
   - 客户机：正在恢复的系统的临时主机名

     在恢复阶段 1 期间向系统分配临时主机名。您可以在恢复阶段 2 之前切换到另一个 shell 检索该主机名，然后运行 hostname 命令。

   添加用户帐户
2. 从原始系统的灾难恢复 CD 引导客户机系统。
3. 显示以下消息时按 **Enter**：按 Enter，以便从恢复 CD 引导。
4. 首先将 DR OS 加载到内存中，然后显示范围菜单。选择恢复范围。有四种不同的恢复范围和两个其他选项：
   - Reboot：不执行灾难恢复，但重新启动计算机。
   - Default Recovery：恢复 /boot 和 / (根) 卷，以及 Data Protector 安装及配置文件所在的所有卷 (/opt 、 /etc 和 /var)。所有其他磁盘均未进行分区和格式化，可在阶段 3 中使用。
   - Minimal Recovery：仅恢复 /boot 和 / (根) 卷。
   - Full Recovery：恢复所有卷，而非仅恢复关键卷。
   - Show Recovery Scope [Yes]：加载“恢复范围”屏幕。
   - Run shell：运行 Linux shell。可以将其用于高级配置或恢复任务。
5. **阶段 2**
6. 此时将显示灾难恢复向导。要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。要继续执行灾难恢复，选择**继续进行还原**。

   > **注意**请确保 Cell Manager 和介质 (备份) 主机可访问。否则，可能需要修改 NIC 和 MAC 地址。

7. 如果灾难恢复备份经过加密，并且您要恢复 Cell Manager 或无法访问 Cell Manager 的客户机，则将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库（DR-ClientName-keys.csv）（例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器），并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。

8. 如果 SRD 文件中的信息并非最新（例如，因为灾难之后更改了备份设备），并且要执行脱机恢复，则应在继续此过程之前编辑 SRD 文件。
9. 在联机恢复期间更改备份设备需要使用 omnidbutil -changebdev 命令。识别用于还原的备份会话和当前使用的备份设备。可使用 GUI 或 omnidb -session <SessionID> -detail 完成此操作。然后使用 omnidbutil -changebdev FromDev ToDev -session SessionID 替换旧设备。在 EADR 期间将自动使用新设备。
10. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。

    请注意，Data Protector 将首先尝试执行联机还原。如果联机还原因任何原因而失败（如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager），则 Data Protector 将尝试执行远程脱机恢复。甚至如果远程脱机还原失败（例如，因为介质代理主机仅接受来自 Cell Manager 的请求），则 Data Protector 也将执行本地脱机还原。

11. 删除步骤 1 中从 Cell Manager 上 Data Protector admin 用户组创建的客户机的本地 Data Protector 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。
12. 如果要恢复 Cell Manager，则要使 IDB 一致。
13. 使用标准还原过程还原用户和应用程序数据。
14. 如果要执行群集中所有节点的灾难恢复，则需要其他步骤。

恢复后

灾难恢复完成后，使用以下命令重新生成证书：

- 在客户机上： omnicc -secure_comm -regenerate_cert [Hostname]
- 在 Cell Manager 上： omnicc -secure_comm -configure_peer {Hostname1 HostName2 ...]} [-accept_host]

相关任务

- 创建备份规范
- 备份磁盘映像
- 将完整 DR 映像保存到 Cell Manager
- 合并 MS 群集的 P1S 文件

为增强的自动灾难恢复做的准备（Windows 和 Linux）

要做好准备而使灾难恢复成功，请遵照与所有灾难恢复方法的常规准备过程相关的说明，然后再执行本主题中列出的步骤。必须提前准备，以便快速高效地执行灾难恢复。应特别注意 Cell Manager 的灾难恢复准备。

重要说明请在灾难发生之前准备灾难恢复。

先决条件

在选择此灾难恢复方法前，请考虑以下要求和限制：

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 在 Windows Server 2008 及更高版本中，至少有一个卷必须为 NTFS 卷。
- 用于灾难恢复的所有必要数据的备份可能需要大量可用空间。通常 500 MB 便足够，最高可能需要 1 GB，具体取决于操作系统。
- 在 DR OS 映像创建期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 确保已启用自动装载功能。自动装载功能可确保所有卷（没有装载点）都处于联机状态。如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- 在群集环境中，如果每个群集节点上的总线地址枚举相同，则可以成功备份群集节点。这表示需要：
  - 群集节点主板硬件相同
  - 两个节点上的 OS 版本（Service Pack 和更新）相同
  - 总线控制器的数量和类型相同
  - 必须在相同的 PCI 主板插槽中插入总线控制器。
- 在备份时应当激活操作系统。否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Server 2008 和更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包 (ADK):

  Windows Server 2008：

  适用于 Windows Server 2008 的自动安装工具包 (AIK)

  Windows Server 2008 R2：
  - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充

  Windows Server 2012：
  - 适用于 Windows Server 2012 的评估和部署工具包 (ADK 1.0)

  Data Protector 将检查 WAIK/ADK 版本，如果没有适当的版本可用，将中止映像创建。

  Windows Server 2012 R2：
  - 适用于 Windows Server 2012 R2 的评估和部署工具包 (ADK 1.1)
- 对于从可引导 USB 设备进行的灾难恢复，请确保：
  - USB 存储设备的大小应至少为 1 GB
  - 目标系统支持从 USB 设备引导。较旧的系统可能需要更新 BIOS，否则可能完全无法从 USB 存储设备启动。
- 要为 Windows Server 2008 和更高版本的 Windows 系统创建可引导网络映像，必须满足以下条件:
  - 在目标系统上，已启用网络适配器以通过 PXE 协议进行通信。此系统的 BIOS 应与 PXE 协议兼容。
  - 已经在 Windows Server 2008 和更高版本的 Windows 系统上安装并配置 Windows 部署服务 (WDS) 服务器。WDS 服务器必须为 Active Directory 域的成员或 Active Directory 域的域控制器。
  - 具有活动范围的 DNS 服务器和 DHCP 服务器正在网络中运行。

- 要备份位于 Windows Server 2008 和更高版本上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。
- 在为 RedHat 7 客户机创建恢复 ISO 映像的过程中，恢复介质创建主机必须安装 **squashfs 工具**，才能成功创建恢复 ISO 映像。
- 应具有管理特权，才能运行增强的自动灾难恢复 CLI 实用程序。

限制

- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 可以在 Windows Server 2008、Windows Server 2008 R2 系统 (在所有受支持平台上)、Windows Server 2012 和更高版本上创建可引导 USB 驱动器。
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 请勿选择属于检查点重新启动备份会话的备份对象版本。
- 选择对象复制作为恢复源时，需遵守以下规则：
  - 只能选择完整备份对象的副本用于恢复。
  - 仅在从卷的列表中创建卷恢复集时才能选择对象副本。不支持会话。
  - 不支持介质副本。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。

  注意仅在 Windows Server 2008 及更高版本上实施新的恢复会话监视器。

- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs（多种 btrfs raid 配置），因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 /etc/fstab 文件。需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。这同样适用于 GRUB 配置，因此避免用于 root 设备的 UUID，并按名称更换设备。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

  > **注意**Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。父对象与其快照之间的整体写时复制 (COW) 关系会丢失。因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 /etc/fstab 文件中的 subvolid（请参阅《btrfs 文档》）装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 subvolid 不需要与备份期间的相同。尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

  > **注意**使用 fstab 中的 subvol 选项而不是 subvolid。

磁盘和分区配置

- 驻留在 Windows 群集中的共享动态磁盘不支持 EADR。
- 如果系统保留卷驻留在动态磁盘上，在 Data Protector GUI 中，卷不由黄色图标指示，而是指示为绿色图标。
- 通过动态磁盘执行灾难恢复时，在启动 EADR 之前需要清除所有磁盘。
- EADR 会话之后，将重新创建所有卷，但只有恢复范围内的卷能够还原。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。
- 恢复使用 Intelligent Provisioning 工具 (1.4 和 1.5 版本) 部署的操作系统可能会由于错误的 MBR 分区信息而失败。
- 稀疏文件被还原为其完整大小。这可能会导致目标卷空间用尽。
- 不支持物理磁盘不完全属于存储池的存储空间配置。

常规准备

1. 执行完整的客户机系统备份。建议备份整个客户机，如若不然，您至少需要选择以下关键卷和对象：
   - 引导和系统卷
   - Data Protector 安装卷
   - CONFIGURATION 对象所在的卷
   - Active Directory 数据库卷（如果使用 Active Directory 控制器）
   - 仲裁卷（如果使用 Microsoft 群集服务器）

   对于 Data Protector Cell Manager 系统，请参阅 Cell Manager 的额外准备。

   请参阅《Data Protector 帮助》索引: “备份, Windows 特有”和“备份, 配置”

   在客户机完整备份期间，恢复集和 P1S 文件存储在备份介质上和（恢复集可选）Cell Manager 上。

   注意事项：

   Windows Server 2008 及更高版本:

   - 请确保同时备份存在的系统卷。
   - 可以通过使用 VSS 写入程序的磁盘映像备份来备份逻辑卷。VSS 磁盘映像备份可确保卷在备份过程中保持未锁定状态，并可由其他应用程序访问。必须使用常规文件系统备份来备份 IDB 和 CONFIGURATION 对象以及未装载的卷或作为 NTFS 文件夹装载的卷。

   ***Windows Server 2012 (R2)*:**

   - 使用磁盘映像备份在以下情况下备份卷:
     - 重复卷

       在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。磁盘映像还原会保持卷的大小。
     - 使用复原文件系统 (ReFS) 的卷

   ***Microsoft 群集服务器*:**

   - 一致的备份包括 (在相同的备份会话中):
     - 所有节点
     - 管理虚拟服务器（由管理员定义）
     - 如果将 Data Protector 配置为群集感知应用程序，则包括 Cell Manager 虚拟服务器和 IDB。

     以上各项应包含在相同的备份会话中。
   - *群集共享卷：*执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。

     必须卸载虚拟硬盘 (VHD) 以确保一致性。
   - 执行备份之后，在 MSCS 中合并所有节点的 P1S 文件，以使每个节点的 P1S 文件都包含关于共享群集卷配置的信息。

     如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。如果要恢复 Cell Manager 或如果无法与 Cell Manager 建立连接，则需要该密钥。

   Windows Server 2008 和更高版本的 Windows Server 上的 Active Directory:

   - 如果您的 Windows Server 是 Active Directory 大小超过 512 MB 的域控制器，则需要修改客户机备份的备份规范: 在源页中，展开 CONFIGURATION 对象，并清除 ActiveDirectoryService 和 SYSVOL 项的复选框。

> **注意**Active Directory 和 SYSVOL 将仍作为系统卷（C:/）备份的一部分进行备份。默认情况下，它们分别位于 C:/Windows/NTDS 和 C:/Windows/SYSVOL 中。

2. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复:

   omnicc –secure_comm –configure_for_dr<hostname_of_client_being_recovered> -overwrite

3. 执行客户机联机恢复之后，在 Cell Manager 上运行以下命令:

   omnicc –secure_comm –configure_peer <client_host_name>

4. 灾难发生之后，使用 EADR 向导将 DR 映像转换为灾难恢复 CD ISO 映像。

   ***Windows Server 2008 及更高版本*:** 或者使用 DR OS 映像代替灾难恢复 CD，创建可启动网络映像或可启动 USB 驱动器。

5. 使用支持 ISO9660 格式的任何 CD 录制工具在 CD 上录制灾难恢复 CD ISO 映像。此灾难恢复 CD 随后可用于引导目标系统并自动还原关键卷。

6. 执行灾难恢复测试计划。

7. 在 Windows 系统上，如果在启动后某些服务或驱动程序无法运行，则可能需要手动编辑 kb.cfg 文件。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备。

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：

  omnicc –secure_comm –configure_for_dr <cell_manager_hostname>

- 恢复完成之后，在介质主机上运行以下命令：

  omnicc –secure_comm –configure_peer <cell_manager_hostname>

- 定期备份 IDB。IDB 会话不应早于文件系统会话。
- 在安全位置（而非在 Cell Manager 上）存储 Cell Manager 的 SRD 文件。
- 提前为 Cell Manager 准备灾难恢复操作系统映像。

相关任务

- 创建备份规范
- 备份磁盘映像
- 准备 DR CD ISO 映像
- 将完整 DR 映像保存到 Cell Manager

将恢复集保存到 Cell Manager

在进行完整客户机备份期间，恢复集打包在单个大型文件中，并存储在备份介质上和（可选）Cell Manager 上。如果计划在 Cell Manager 上录制灾难恢复 CD，则将恢复集文件保存到 Cell Manager 会很有用，这是因为从硬盘获取恢复集比从备份介质还原要快得多。

如果在备份期间将恢复集保存到 Cell Manager，则系统会将其保存到默认 Data Protector `P1S` 文件位置。

要更改默认位置，请指定一个新的全局选项 `EADRImagePath = valid_path`（例如 `EADRImagePath = /home/images` 或 `EADRImagePath = C:\temp`）。有关全局选项的信息，请参阅全局选项。

> **提示**如果在目标目录中没有足够的可用磁盘空间，则可以创建装载点（Windows 系统）或另一个卷的链接（UNIX 系统）。

将备份规范中所有客户机的恢复集文件保存到 Cell Manager

要保存备份规范中所有客户机的恢复集文件，请执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。有关详细信息，请参阅 Data Protector 帮助索引: “创建，备份规范”。
4. 在"结果区域"中，单击**选项**。
5. 在**文件系统选项**下，单击**高级**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. 在 **WinFS 选项**页中，选择**检测 NTFS 硬链接**，选中**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

将备份规范中特定客户机的恢复集文件保存到 Cell Manager

要保存备份规范中特定客户机的恢复集文件，请执行以下步骤:

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。
4. 在"结果区域"中，单击**备份对象摘要**。
5. 选择要将其恢复集文件存储在 Cell Manager 上的客户机，并单击**属性**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. 在 **WinFS 选项**页中，选中**检测 NTFS 硬链接**和**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。在创建灾难恢复映像期间，密钥将自动导出至 Cell Manager 的文件 Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv（Windows 系统）或 /var/opt/omni/server/export/keys/DR-ClientName-keys.csv（UNIX 系统），其中，ClientName 是正在创建映像的客户机名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

准备 DR OS 映像

灾难发生之前，应准备一个要录制在灾难恢复 CD 上或保存到可引导 USB 驱动器的 DR OS 映像，它随后可用于增强的自动灾难恢复。或者，也可以准备可引导的网络映像。

请注意，必须在将准备 DR OS 映像的系统上安装 Data Protector 自动灾难恢复组件。

每次硬件、软件或配置更改之后都必须根据新的恢复集准备好一个新的灾难恢复 OS 映像。

为必须首先恢复的任何关键系统提前准备 DR OS 映像，尤其是网络正常工作所需的系统（DNS 服务器、域控制器、网关等）、Cell Manager、介质代理客户机和文件服务器等。

建议对含有 OS 映像的备份介质和灾难恢复 CD 或 USB 驱动器的访问权限进行限制。

步骤

1. 在 Data Protector 上下文列表中，单击“还原”。
2. 在“范围窗格”中，单击**任务**，然后单击**灾难恢复**以启动灾难恢复向导。
3. 在结果区域中，从**要恢复的主机**下拉列表中选择要为其准备 DR OS 映像的客户机，然后单击**验证**以验证该客户机。

   > 经过验证的客户机将添加到**要恢复的主机**下拉列表中。

4. 在**恢复介质创建主机**下拉列表中，选择要在其上准备 DR OS 映像的客户机。默认设置下，该客户机与为其准备 DR OS 映像的客户机一样。您在其上准备 DR OS 映像的客户机必须安装有相同 OS 类型（Windows、Linux），并且必须已安装“磁带客户机”。
5. 使**增强的自动灾难恢复**保持选中状态，并选择要从备份会话还是从卷列表构建卷恢复集。默认情况下，选择**备份会话**。

   单击“下一步”。
6. 具体取决于所选的恢复集构建方法：
   - 如果选择了备份会话，则应选择主机备份会话；如果是 Cell Manager，则选择 IDB 会话。
   - 如果选择了“卷”列表，则应为每个关键对象选择相应的对象版本。

   单击“下一步”。
7. 选择恢复集文件的位置。默认情况下，**从备份还原恢复集文件**处于选中状态。

   如果在备份期间已在 Cell Manager 上保存了恢复集文件，则应选择**指向恢复集文件的路径**并指定其位置。单击“下一步”。
8. 选择映像格式。可用的选项如下：
   - **创建可引导的 ISO 映像**: DR ISO 映像 (默认情况下为 recovery.iso)
   - **创建可引导 USB 驱动器**：可引导 USB 驱动器上的 DR OS 映像
   - **创建可引导的网络映像**: 可用于网络引导的 DR OS 映像 (默认情况下为 recovery.wim)
9. 如果创建的是可引导 ISO 映像或可引导网络映像，请选择要将创建的映像放置到的目标目录。

   如果要创建可引导的 USB 驱动器，请选择要在其中放置所创建的映像的目标 USB 驱动器或磁盘编号。

   > 在创建可引导的 USB 驱动器时，该驱动器上存储的所有数据将丢失。

10. 也可选择设置密码来防止对 DR OS 映像进行未授权的使用。锁图标指示是否设置了密码。

    单击**密码**打开“密码保护映像”对话框并输入密码。要删除密码，清除字段内容即可。
11. 查看并修改（如果需要）插入 DR OS 映像中的驱动程序的列表。

    可以使用此选项将缺少的驱动程序添加到 DR OS 中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

    > 在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要插入 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

12. 单击**完成**以退出向导并创建 DR OS 映像。
13. 如果要创建可引导的 CD 或 DVD，可使用支持 ISO9660 格式的刻录工具，将 ISO 映像刻录在 CD 或 DVD 上。

备份磁盘映像

可以使用**手动添加**功能以磁盘映像对象的形式备份 Windows 系统和 UNIX 系统磁盘。

> **注意**在 Windows Server 2008 和 Windows Server 2012 系统中，当为 EADR 或 OBDR 做准备时，可以使用 VSS 磁盘映像备份功能将卷备份为磁盘映像。因为未装载的卷、装载到 NTFS 文件夹的卷以及 CONFIGURATION 对象无法以磁盘映像形式进行备份，所以应使用文件系统备份功能来备份这类对象。

先决条件

- **UNIX 系统**：在磁盘映像备份之前卸除磁盘，稍后使用 pre-exec 和 post-exec 命令将其装回（例如，pre-exec：umount /dev/rdsk/disk1 ，post-exec: mount /dev/rdsk/disk1 /mount_dir）。

限制

- **Windows 系统**：如果因 Data Protector 无法锁定驱动器而打开了目标系统上的文件，则磁盘映像备份失败。

完成以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击**文件系统**，然后单击**添加备份**。
4. 在**创建新备份**对话框中，选择一个可用的模板，然后单击**确定**打开向导。
5. 通过单击**下一步**跳过向导中的所有属性页。在“目标”属性页中只需要选择将用于备份的设备。

   > **提示**如果备份经过负载均衡，则可通过右键单击选定设备，然后单击“对设备进行排序”，设置 Data Protector 使用设备时采用的顺序。

6. 在“备份对象摘要”页中，单击**手动添加**。
7. 在“选择备份对象”页中，单击**磁盘映像对象**选项，然后单击**下一步**。
8. 在“常规选择”页中，选择要用磁盘映像进行备份的客户机。
9. 在“常规对象选项”属性页中，可以指定如何处理报告、数据保护和编目保护。还可以指定 pre-exec 和 post-exec 脚本。单击“下一步”。
10. 在“高级对象选项”属性页中，可以指定磁盘映像对象的高级备份选项。单击“下一步”。
11. 在“磁盘映像对象选项”属性页中，指定磁盘映像中要备份的部分。使用以下格式：

    UNIX 系统：

    - 要指定磁盘映像的某个部分，请使用以下格式： /dev/rdsk/Filename ，例如： /dev/rdsk/c2t0d0
    - 要指定原始逻辑卷的某个部分，请使用以下格式： /dev/vgNumber/rlvolNumber ，例如： /dev/vg01/rlvol1

    > **重要说明**如果要执行即时恢复，请指定要备份的卷组中的所有原始逻辑卷。否则，将无法使用 Data Protector GUI 进行即时恢复，或者 (如果使用 Data Protector CLI 执行即时恢复) 数据可能会损坏。

    Windows 系统：

可以用两种方式指定磁盘映像的某个部分：第一种方式选择特定卷，第二种方式选择整个磁盘。在 ZDB 的情况下，请使用第二种方式：

- \\.\DriveLetter: ，例如： \\.\E:

> **注意**当为卷名称指定了驱动器号时，卷在备份过程中不会锁定。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

- \\.\PHYSICALDRIVE# ，其中， # 是要备份的磁盘的当前编号。例如： \\.\PHYSICALDRIVE3

12. 单击**完成**。
13. 在“备份对象摘要”页中，检查备份规范的摘要。单击“下一步”。
14. 在备份向导的结尾处，可以保存、开始或预览所配置的备份。此时会发生以下情况：
    - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
    - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

使用增强的自动灾难恢复恢复 Windows 系统

只有完成了所有准备步骤后，才能成功执行 Windows 系统的增强型自动灾难恢复。如果要恢复 Cell Manager，将先从内部数据库的备份映像将该内部数据库还原，然后从卷和 CONFIGURATION 对象的备份映像将卷和 CONFIGURATION 对象还原。

步骤

阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector 帐户:
   - 类型： Windows
   - 名称: SYSTEM
   - 组/域： NT AUTHORITY
   - 客户机：正在恢复的系统的临时主机名

     Windows 预安装环境 (WinPE) 向系统分配了临时主机名。通过在 WinPE 的命令提示符窗口中运行 hostname 命令，可以检索该主机名。
2. 从原始系统的灾难恢复 CD、可引导 USB 驱动器或可引导网络映像引导客户机系统。如果要从灾难恢复 CD 启动目标系统，请确保没有外部 USB 磁盘（包括 USB 密钥）连接到系统，然后再开始恢复过程。

   注意如果在恢复期间屏幕缩短，可用以下凭据登录：

   用户： DRM$ADMIN

   密码： Dr8$ad81n$pa55wD
3. 选择恢复范围和恢复选项。下面的步骤将随操作系统的不同而不同：
   1. 灾难恢复 GUI（安装程序向导）出现，并显示原始系统信息。单击“下一步”。

      提示当显示进度条时，系统会提供一些键盘选项。可以通过将鼠标悬停在进度条上来检查可用的选项及其说明信息。
   2. 在“恢复范围”页面上，选择恢复的范围：
      - Default Recovery : 恢复关键卷（系统磁盘、引导磁盘和 Data Protector 安装卷）。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
      - Minimal Recovery : 仅恢复系统磁盘和引导磁盘。
      - Full Recovery : 恢复“还原集”中的所有卷，而不是仅恢复关键卷。
      - Full with Shared Volumes: 对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 EADR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 Default Recovery 。
   3. （可选）要修改恢复设置，请单击**设置**以打开“恢复设置”页面。

      系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：
      - Use original network settings: 如果需要还原原始网络配置（例如，由于缺少 DHCP 服务器），可选择此选项。默认设置下未选中该选项，并且 DR OS 恢复环境会使用 DHCP 网络配置。
      - Restore BCD : 如果选择此选项，则 Data Protector 在灾难恢复会话期间还会提前还原引导配置数据 (BCD) 存储，然后在 Data Protector 还原会话中还原该存储。默认情况下选择此选项。
      - Restore DAT : 如果选中，Data Protector 灾难恢复模块还将还原 Microsoft VSS 写入程序的数据。默认设置下 ，DR 模块会跳过 VSS 写入程序数据的还原。如果在非 VSS 备份期间， Data Protector 无法备份关键写入程序，您可使用该选项。要在 DR 模块还原之前还原数据，可选择 Pre 。要还原 Data Protector 之后的数据，请选择“之后” 。
      - Initialize Disks Manually: 使用此选项可以手动映射原始系统磁盘和当前系统磁盘，并对它们进行初始化以使其与原始配置匹配。默认情况下，不选择此选项。

        如果选择了此选项，在恢复过程启动时将显示新的磁盘映射和初始化页面。灾难恢复模块将提供初始磁盘映射并显示初始映射尝试的结果。使用提供的选项更改磁盘映射。映射完成后，卷得到初始化并且系统将重新启动。
      - Restore Storage Spaces : 默认情况下，将还原存储空间。在恢复时，如果存储配置允许，您可以取消选项该选项并将虚拟磁盘直

接还原为物理磁盘。请注意，如果要将存储空间还原为不同的硬件或 USB 磁盘，则需要手动对磁盘进行初始化。

- Enable Dissimilar Hardware Restore：如果启用，Data Protector将在恢复过程中扫描系统中缺少的驱动程序。可通过从下拉列表中选择下列方法之一来启用该选项：
  - Unattend 默认此模式使用预定义的配置文件自动将操作系统配置到不同的硬件平台中。对于不同的硬件，这是主要的恢复模式。请在第一个实例中使用。
  - Generic：如果无人参与模式失败（可能是因为所还原的操作系统的配置不正确），可选择此项。它将调整所还原的操作系统注册表及其驱动程序和服务，以适应不同的硬件。
- Remove Devices：在启用了 Dissimilar Hardware 选项时可用。如果选中，Data Protector将从还原的操作系统的注册表中删除原始设备。
- Connect iSCSI Devices：如果原始计算机正在使用 iSCSI，则将启用并选定此选项。通过选择该选项，Data Protector 可在备份时自动还原基本 iSCSI 配置。如果未选中，将跳过 iSCSI 配置。

  您也可使用本机 Microsoft iSCSI 配置向导来管理更为复杂的 iSCSI 配置。如果 DR GUI 检测到某些 iSCSI 功能（例如安全选项）需要手动配置，则会提供选项来运行 Microsoft iSCSI 配置向导。
- Map Cluster Disks Manually： 如果选择此选项，您可以手动映射群集卷。如果不选择此选项，将自动映射卷。在执行自动映射后，建议检查所有卷是否已正确映射。
- Remove Boot Descriptor：在 Intel Itanium 系统中可用。删除由灾难恢复过程留下的所有引导描述符。
- Manual disk selection：在 Intel Itanium 系统中可用。如果磁盘设置显著变化，则灾难恢复模块可能找不到引导磁盘。使用此选项可选择正确的引导磁盘。

要将选项重置为默认设置，请单击**重置默认设置**。

单击**保存 >** 以保存更改。

4. 单击**完成**启动恢复。恢复过程开始，并且您可以监视进度。

   如果已使用 BitLocker 驱动器加密对卷进行了加密，则系统将提示您解锁已加密的驱动器。

> **提示**在灾难恢复 GUI 中，可以单击**任务**执行以下操作：
>
> - 运行命令提示符、任务管理器或磁盘管理器
> - 访问 Map Network Drives 和 Load Drivers 工具
> - 查看特定于灾难恢复过程的日志文件
> - 启用或禁用 DRM 配置文件，以及在文本编辑器中查看和编辑该文件
> - 编辑 WinPE 恢复环境的 hosts 文件
> - 访问“帮助”和查看 GUI 图标图例

阶段 2

3. 选择了恢复的范围之后，Data Protector 开始设置 DR OS。您可以监视进度。

   提示 To start recovery of the machine Hostname press F12 时等待 10 秒，以便从硬盘而非从 CD 引导。

   此时将显示灾难恢复向导。要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。

   可用的选项如下：

   - Debugs...：启用调试。
   - Omit deleted files：将不还原在连续增量备份期间删除的文件。这可能会减慢恢复速度。
   - Install only：此选项仅向目标系统安装临时操作系统，并因此结束灾难恢复的阶段 1。将不自动启动灾难恢复阶段 2。例如，如果要编辑 SRD 文件，可以使用此选项。

   此外，可以使用相应的按钮启动注册表编辑器、命令行或任务管理器。

   单击**完成**继续进行灾难恢复。

4. 如果 DR OS 映像受密码保护，请提供密码并继续恢复。
5. 如果灾难恢复备份经过加密，并且您要恢复 Cell Manager 或无法访问 Cell Manager 的客户机，则将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库（DR-ClientName-keys.csv）（例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器），并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。
6. 如果 SRD 文件中的信息并非最新（例如因为灾难之后更改了备份设备），并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
7. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。第一次登录之后将删除临时 DR OS，但以下情况除外：

- Minimal Recovery 处于选定状态。
- 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
- 您手动执行带有 omnidr 或 -no_reset 选项的 -debug 命令。
- 灾难恢复失败。

在 Windows Server 2008 及更高版本中，永不保留临时 DR OS。

注意，Data Protector 将首先尝试执行联机恢复。如果联机恢复因任何原因而失败（例如，Cell Manager 或网络服务不可用，防火墙正在阻止访问 Cell Manager）Data Protector 将尝试执行远程脱机恢复。甚至如果远程脱机还原失败（例如，因为介质代理主机仅接受来自 Cell Manager 的请求），则 Data Protector 也将执行本地脱机还原。

8. 删除步骤 1 中从 Cell Manager 上 Data Protector Admin 用户组创建的客户机的本地 Administrator 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。
9. 如果要恢复 Cell Manager，则要使 IDB 一致。

阶段 3

10. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

> **注意**Data Protector 在恢复之后不会还原卷压缩标志。备份时压缩的所有文件将还原为压缩形式，但如果还希望以压缩形式创建任何新文件，则必须手动设置卷压缩。

11. 如果要执行 Microsoft 群集服务器中所有节点的灾难恢复，则需要其他步骤。

EADR 的恢复后步骤

成功完成灾难恢复后，请执行以下任务：

Cell Manager 脱机恢复

完成灾难恢复（Cell Manager 的脱机恢复）后，请执行以下步骤：

1. 在 Cell Manager 上，运行以下命令:
    1. omnicc -secure_comm -regenerate_cert
    2. 使用 sc stop omniinet 和 sc start omniinet (在 Windows CM 上) 或 systemctl xinetd restart (在 Linux CM 上) 重新启动 Data Protector INET 服务
2. 在所有 Data Protector 客户机上，运行以下命令：omnicc -secure_comm -configure_peer <cellManagerHostName>

客户机联机恢复

完成灾难恢复（客户机联机恢复）后，请执行以下步骤：

1. 在恢复的客户机上，运行以下命令：
    1. omnicc -secure_comm -regenerate_cert
    2. 使用 sc stop omniinet 和 sc start omniinet (在 Windows 上) 或 systemctl xinetd restart (在 Linux 上) 重新启动 Data Protector INET 服务
    3. omnicc -secure_comm -configure_peer <CellManagerHostName>
2. 在 Cell Manager 上，运行以下命令： omnicc -secure_comm -configure_peer <ClientRecoveryHostName> -overwrite

客户机脱机恢复

完成灾难恢复（客户机脱机恢复）后，请执行以下步骤：

1. 在恢复的客户机上，运行以下命令：
    1. omnicc -secure_comm -regenerate_cert
    2. 使用 sc stop omniinet 和 sc start omniinet (在 Windows 上) 或 systemctl xinetd restart (在 Linux 上) 重新启动 Data Protector INET 服务
    3. omnicc -secure_comm -configure_peer <CellManagerHostName>
2. 在 Cell Manager 上，运行以下命令:
    1. omnisv status 以检查 Data Protector 的状态。如果 Cell Manager 服务未联机，请运行 omnisv restart 命令。
    2. omnicc -secure_comm -configure_peer <ClientRecoveryHostName> -overwrite
3. 在为客户机脱机 EADR 配置的介质代理上，运行以下命令：omnicc -secure_comm -remove_peer <ClientRecoveryHostName>

解决安全通信协议错误

当您在恢复后尝试与 Data Protector 客户机通信时，在命令中或启动的会话中可能显示以下错误:

```
尝试建立连接时，发生安全通信协议协商错误。 检查证书及其配置的有效性。
```

要解决此问题，请在客户机上重新启动 Data Protector 服务，然后重试运行该命令。

一键式灾难恢复

一键式灾难恢复 (OBDR) 是适用于 Windows Data Protector 客户机的 Data Protector 自动恢复方法，尽可能减少用户干预。备份时，OBDR 将自动收集所有相关的环境数据。备份期间，临时安装和配置 DR OS 所需的数据打包在单个大型 OBDR 映像文件中，并存储在备份磁带上。灾难发生时，OBDR 设备（能够模拟 CD-ROM 的备份设备）用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。

启动 DR OS 映像后，Data Protector 将自动对磁盘进行格式化和分区，最后使用 Data Protector 将原始操作系统还原为备份时的状态。

重要说明每次硬件、软件或配置更改之后都要执行新的备份。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

恢复的卷包括：

- 引导分区
- 系统分区
- 存储 Data Protector 安装数据的分区

使用标准 Data Protector 恢复过程可恢复任何剩余的分区。

概述

确保已执行“准备”一节中提及的所有常规准备步骤。对 Windows 客户机使用一键式灾难恢复方法的常规步骤包括：

1. **阶段 1**

   从恢复磁带引导并选择恢复范围。

2. **阶段 2**

   根据您所选的恢复范围，系统将自动还原所选的卷。

   关键卷（引导分区和操作系统）始终会被还原。

3. **阶段 3**

   使用标准 Data Protector 还原过程还原所有剩余分区。

重要说明建议限制对 OBDR 引导介质的访问。

以下各节将介绍有关在 Windows 系统上执行一键式灾难恢复的要求、限制、准备和恢复。另请参见“高级恢复任务”一节。

要求

- 必须在要使用此方法进行恢复的系统上安装 Data Protector 自动灾难恢复。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 新磁盘的大小必须等于或大于受影响的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 在 OBDR 备份期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 在引导 DR OS 映像时网络必须可用。

- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。
- 要创建 Windows Server 2008 及更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包:

  Windows Server 2008：

  适用于 Windows Server 2008 的自动安装工具包 (AIK)

  Windows Server 2008 R2：

  - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充

  Windows Server 2012：

  - 适用于 Windows Server 2012 的评估和部署工具包 (ADK 1.0)

  Windows Server 2012 R2：

  - 适用于 Windows Server 2012 R2 的评估和部署工具包 (ADK 1.1)
- 要备份位于 Windows Server 2008 系统上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。

以下限制适用：

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 不支持 Windows Server 2012 存储空间。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。

  注意仅在 Windows Server 2008 及更高版本上实施新的恢复会话监视器。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。

磁盘和分区配置

- 不支持动态磁盘（包括从 Windows NT 升级而来的镜像集）。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。
- 在 NTFS 卷上安装了 Data Protector 的系统支持 OBDR。

完成以下步骤：

1. 为一键式灾难恢复做准备
2. 恢复操作系统
3. 还原用户数据

为一键式灾难恢复做的准备（Windows 和 Unix）

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。提前准备，以便快速高效地执行灾难恢复。

重要说明请在灾难发生之前准备灾难恢复。

准备步骤

完成灾难恢复的常规准备之后，执行以下特定步骤以准备 OBDR。

1. 按照**不可追加**介质使用策略和**宽松**介质分配策略 (因为备份介质在 OBDR 备份期间进行格式化) 为 DDS 或 LTO 介质创建介质池。此外，将此介质池指定为 OBDR 设备的默认介质池。只有此类池中的介质可用于 OBDR。
2. 在要允许使用 OBDR 进行恢复的系统上本地执行 OBDR 备份。

   注意事项

   ***Windows Server 2008 及更高版本*:** 请确保备份所存在的系统卷（例如引导卷）。

   ***Windows Server 2012 (R2)*:** 使用磁盘映像备份在以下情况下备份卷:

   - 重复卷

     在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。磁盘映像还原会保持卷的大小。
   - 使用复原文件系统 (ReFS) 的卷

   ***Microsoft 群集服务器*:** 一致的备份包括 (在相同的备份会话中):

   - 所有节点
   - 管理虚拟服务器（由管理员定义）
   - 如果将 Data Protector 配置为群集感知应用程序，则为客户机系统的虚拟服务器。

   要使用 OBDR 方法在 MSCS 上自动还原所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点，以使共享磁盘卷在 OBDR 备份期间不会由另一个节点锁定。也就是说无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

   ***群集共享卷*:** 执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。必须在单独的设备上执行备份，因为只有在不可追加介质上才可以执行 OBDR 备份。

   必须卸载虚拟硬盘 (VHD) 以确保一致性。

   如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。如果无法建立和 Cell Manager 之间的连接，您将需要密钥。
3. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复：

   ```
   omnicc –secure_comm –configure_for_dr <hostname_of_client_being_recovered>
   ```
4. 联机恢复客户机之后，在 Cell Manager 上运行以下命令:

   ```
   omnicc –secure_comm –configure_peer <client_host_name> -overwrite
   ```
5. 执行灾难恢复测试计划。
6. 在 Windows 系统上，如果在系统启动后某些服务或驱动程序无法运行，则可能必须手动编辑 kb.cfg 文件。

编辑 kb.cfg 文件

kb.cfg 文件位于 Data_Protector_home\bin\drim\config 目录中，用于存储 %SystemRoot% 目录中的驱动程序文件位置的相关信息。此文件的用途是提供一种灵活的方法，使 Data Protector 可以在 DR OS 中包括驱动程序（和其他需要的文件），以使系统采用与引导相关的特定硬件或应用程序配置。默认 kb.cfg 文件已包含行业标准硬件配置所需的所有文件。

例如，某些驱动程序的功能分散到多个单独的文件中，驱动程序需要所有这些文件才能正常工作。有时，如果未在 kb.cfg 文件中逐个列出所有驱动程序文件，则 Data Protector 无法识别这些驱动程序文件。在这种情况下，DR OS 中将不包括这些驱动程序文件。使用 kb.cfg 文件的默认版本创建和执行测试计划。如果 DR OS 无法正常不引导或无法访问网络，则可能需要修改此文件。

如果要备份这些驱动程序，则以适当的格式将相关文件的信息添加至 kb.cfg 文件，如 kb.cfg 文件开头的说明所述。编辑文件的最简单方式是复制和粘贴现有行，并将其替换为相关信息。

请注意，路径分隔符为 "/" (正斜杠)。忽略空格，但引号中的路径名除外，因此相关条目可分散在多行中。还可以添加开头为 "#" (磅) 符号的注释行。

编辑完 kb.cfg 文件之后，将其保存到原始位置。然后，执行另一个客户机完整备份，将添加的文件包含在恢复集中。

注意由于系统硬件和应用程序的配置任务繁重，因此无法为所有可能的配置提供“即用型”解决方案。因此可以修改此文件以包括驱动程序或其他文件，风险自担。

对此文件的任何修改都由您自己承担风险，这些修改本身不受 支持。

警告建议创建并执行测试计划，以确保编辑 kb.cfg 文件之后灾难恢复可正常运行。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv（Windows 系统）或 /var/opt/omni/server/export/keys/DR-ClientName-keys.csv（UNIX 系统），其中 ClientName 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

创建一键式灾难恢复的备份规范

必须创建一键式灾难恢复 (OBDR) 备份规范，才能准备好 OBDR 引导磁带。

以下先决条件适用:

- 添加 OBDR 设备前，为 DDS 或 LTO 介质创建一个采用不可追加介质使用策略和宽松介质分配策略的介质池。必须选择所创建的该介质池作为 OBDR 设备的默认介质池。
- 此设备必须在本地连接到要允许使用 OBDR 进行恢复的系统。
- 在要允许使用 OBDR 方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复和用户界面组件。
- 必须在要允许使用 OBDR 进行恢复的系统上本地创建备份规范。

提示为了能够使用 OBDR 方法自动还原 MS 群集中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。实际上无法收集足够的信息为由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。

此备份规范属一键式灾难恢复方法所独有。默认情况下，会将必需卷备份为文件系统。但是，在 Windows Server 2008 及更高版本中，可选择通过 VSS 写入程序将逻辑卷备份为磁盘映像。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。要将逻辑卷备份为磁盘映像，必须修改为 OBDR 创建的备份规范。

创建 OBDR 的备份规范

1. 在 Data Protector 上下文列表中，单击“备份”。
2. 在范围窗格中，单击**任务**，然后单击**一键式灾难恢复向导**。
3. 在“结果区域”中，从下拉列表中选择要为其执行 OBDR 备份（在客户机上本地）的客户机，然后单击**下一步**。

4. 此时已选择需要备份的关键卷。单击“下一步”。

> **重要说明**
>
> 重要卷由系统自动选择，并无法取消选择。选择要保留的任何其他分区，因为在恢复过程中 Data Protector 将从系统中删除所有分区。

5. 选择要用于备份的本地设备或驱动器。只能选择一个设备或驱动器。单击“下一步”。
6. **Windows Server 2008 或更高版本:**

   查看并修改（如果需要）插入 DR OS 映像中的驱动程序的列表。

   可以使用此选项将缺少的驱动程序添加到 DR ISO 映像中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

   （可选）选择备份选项。

> **重要说明**
>
> 在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要添加 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

   Linux：选择备份选项。有关可用选项的更多详细信息，请参阅**索引：“备份选项”**。

   单击“下一步”。
7. （可选）安排备份。单击“下一步”。
8. 在“备份摘要”页中，查看备份规范设置，然后单击**下一步**。

   无法更改以前选择的备份设备或备份规范相互之间的先后顺序。仅可删除 OBDR 非必需备份对象，并且只能查看常规对象属性。也可以更改备份对象说明。
9. 将经过修改的备份规范保存为 OBDR 备份规范，以使其成为原始的一键式灾难恢复格式。(可选) 可使用“保存并计划”选项计划备份。
10. 1. 单击“启动备份”以交互方式运行备份。此时将显示“启动备份”对话框。单击“确定”开始备份。

       如果备份为加密备份，则 omnisrdupdate 实用程序将自动导出加密 ID，此操作作为 post-exec 命令执行。

系统的可引导映像文件（包含安装和配置临时 DR OS 所需的所有信息）将写在磁带的开头，以使其可引导。

> **重要说明**每次硬件、软件或配置更改之后执行新的备份并准备好可引导的备份介质。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

修改 OBDR 备份规范以使用磁盘映像备份

1. 在范围窗格中，单击已创建的 OBDR 备份规范。当系统询问您是否要将其视为 OBDR 备份规范或视为普通的备份规范，单击**否**。

> **注意**
>
> 当将一个 OBDR 备份规范保存为普通备份规范之后，该备份规范仍然可以用于 OBDR。

2. 在“备份对象摘要”页面中，选择要将其备份为磁盘映像的逻辑卷，然后单击**删除**。

> **注意**
>
> 只能备份逻辑卷。应使用文件系统备份来对配置对象、未装载或装载为 NTFS 文件夹的卷执行备份。

3. 单击“手动添加”以打开向导。
4. 在“选择备份对象”页中，单击**磁盘映像对象**选项，然后单击**下一步**。
5. 在“常规选择”页中，选择要用磁盘映像进行备份的客户机，并提供相应的描述信息。单击“下一步”。

> **注意**
>
> 对于每个磁盘映像对象，描述信息必须是唯一的。使用一个描述性名称，例如 [Disk Image C] for C: volume。

6. 在“常规对象选项”属性页中，将数据保护设置为**无**。单击“下一步”。

> 当将数据保护功能设置为**无**时，磁带内容可由更新的 OBDR 备份覆盖。

7. 在“高级对象选项”属性页中，可以指定磁盘映像对象的高级备份选项。单击“下一步”。
8. 在“磁盘映像对象选项”属性页中，指定磁盘映像中要备份的部分。使用以下格式：

   \\.\DriveLetter: ，例如： \\.\E:

> **重要说明**
>
> 当卷的名称被指定为驱动器号时，不会在备份过程中锁定该卷。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

9. 单击**完成**退出向导。
10. 在“备份对象摘要”页中，检查备份规范的摘要。指定为磁盘映像的逻辑卷应属于“磁盘映像”类型。单击“应用”。

使用一键式灾难恢复恢复 Windows 系统

只有完成了所有准备步骤后，才能成功执行 Windows 系统的一键式灾难恢复 (OBDR)。

以下先决条件适用:

- 需要用新硬盘更换受影响的磁盘。
- 应有一个可引导 OBDR 备份介质，其中含有要恢复的客户机的所有关键对象。必须在客户机上本地执行 OBDR 备份。
- 需要一个在本地连接到目标系统的 OBDR 设备。

要使用一键式灾难恢复恢复 Windows 系统，请完成以下步骤:

阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的帐户:

   Windows Server 2008 及更高版本:

   - 类型： Windows
   - 名称: SYSTEM
   - 组/域： NT AUTHORITY
   - 客户机：正在恢复的系统的临时主机名

     Windows 预安装环境 (WinPE) 向系统分配了临时主机名。通过在 WinPE 的命令提示符窗口中运行 hostname 命令，可以检索该主机名。

   添加用户帐户

   [[File:../Graphics/EADRandOBDR_Admin_Account.png|File:../Graphics/EADRandOBDR_Admin_Account.png]]
2. 将包含映像文件和备份数据的磁带插入 OBDR 设备中。
3. 关闭目标系统，并关闭磁带设备的电源。在启动恢复过程之前，确保没有外置 USB 磁盘（包括 USB 闪存）连接到系统。
4. 打开目标系统的电源，并在其初始化时，按磁带设备上的**弹出**按钮，并打开该设备的电源。有关详细信息，请参见设备文档。
5. 选择恢复范围和恢复选项。下面的步骤将随操作系统的不同而不同：

   Windows Server 2008 及更高版本:

   1. 灾难恢复 GUI（安装程序向导）出现，并显示原始系统信息。单击“下一步”。

      > **提示**
      >
      > 当显示进度条时，系统会提供一些键盘选项。可以通过将鼠标悬停在进度条上来检查可用的选项及其说明信息。

   2. 在“恢复范围”页面上，选择恢复的范围：

      - Default Recovery : 恢复关键卷（系统磁盘、引导磁盘和 Data Protector 安装卷）。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
      - Minimal Recovery : 仅恢复系统磁盘和引导磁盘。
      - Full Recovery : 恢复“还原集”中的所有卷，而不是仅恢复关键卷。
      - Full with Shared Volumes: 对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 EADR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 Default Recovery 。
   3. （可选）要修改恢复设置，请单击**设置**以打开“恢复设置”页面。

      系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：

      - Use original network settings: 如果需要还原原始网络配置（例如，由于缺少 DHCP 服务器），可选择此选项。默认设置下未选中该选项，并且 DR OS 恢复环境会使用 DHCP 网络配置。
      - Restore BCD : 如果选择此选项，则 Data Protector 在灾难还原会话期间还会提前还原引导配置数据 (BCD) 存储，然后在 Data Protector 还原会话中再还原该存储。默认情况下选择此选项。
      - Restore DAT : 如果选中，Data Protector 灾难恢复模块还将还原 Microsoft VSS 写入程序的数据。默认设置下 ，DR 模块会跳过 VSS 写入程序数据的还原。如果在非 VSS 备份期间， Data Protector 无法备份关键写入程序，您可使用该选项。要在 DR 模块还原之前还原数据，可选择 Pre 。要还原 Data Protector 之后的数据，请选择“之后”。
      - Initialize Disks Manually: 使用此选项可以手动映射原始系统磁盘和当前系统磁盘，并对它们进行初始化以使其与原始配置匹配。默认情况下，不选择此选项。

        如果选择了此选项，在恢复过程启动时将显示新的磁盘映射和初始化页面。灾难恢复模块将提供初始磁盘映射并显示初始映射尝试的结果。使用提供的选项更改磁盘映射。映射完成后，卷得到初始化并且系统将重新启动。
      - Restore Storage Spaces: 默认情况下，将还原存储空间。在恢复时，如果存储配置允许，您可以取消选项该选项并将虚拟磁盘直接还原为物理磁盘。请注意，如果要将存储空间还原为不同的硬件或 USB 磁盘，则需要手动对磁盘进行初始化。

- Enable Dissimilar Hardware Restore：如果启用，Data Protector 将在恢复期间扫描系统，以查看是否缺少驱动程序。可通过从下拉列表中选择下列方法之一来启用该选项：
  - Unattend 默认此模式使用预定义的配置文件自动将操作系统配置到不同的硬件平台中。对于不同的硬件，这是主要的恢复模式。请在第一个实例中使用。
  - Generic：如果无人参与模式失败（可能是因为所还原的操作系统的配置不正确），可选择此项。它将调整所还原的操作系统注册表及其驱动程序和服务，以适应不同的硬件。
- Remove Devices：在启用了 Dissimilar Hardware 选项时可用。如果选中，Data Protector将从还原的操作系统的注册表中删除原始设备。
- Connect iSCSI Devices：如果原始计算机正在使用 iSCSI，则将启用并选定此选项。通过选择该选项，Data Protector 可在备份时自动还原基本 iSCSI 配置。如果未选中，将跳过 iSCSI 配置。

  您也可使用本机 Microsoft iSCSI 配置向导来管理更为复杂的 iSCSI 配置。如果 DR GUI 检测到某些 iSCSI 功能（例如安全选项）需要手动配置，则会提供选项来运行 Microsoft iSCSI 配置向导。
- Map Cluster Disks Manually：在 Windows Server 2008 及更高版本上可用。如果选择此选项，您可以手动映射群集卷。如果不选择此选项，将自动映射卷。在执行自动映射后，建议检查所有卷是否已正确映射。

要将选项重置为默认设置，请单击**重置默认设置**。

单击**保存 >** 以保存更改。

4. 恢复过程开始，并且您可以监视进度。

   如果已使用 BitLocker 驱动器加密对卷进行了加密，则系统将提示您解锁已加密的驱动器。

> **提示**
>
> 在灾难恢复 GUI 中，可以单击**任务**执行以下操作：
>
> - 运行命令提示符、任务管理器或磁盘管理器
> - 访问 Map Network Drives 和 Load Drivers 工具
> - 查看特定于灾难恢复过程的日志文件
> - 启用或禁用 DRM 配置文件，以及在文本编辑器中查看和编辑该文件
> - 编辑 WinPE 恢复环境的 hosts 文件
> - 访问“帮助”和查看 GUI 图标图例

阶段 2

6. 选择了恢复的范围之后，Data Protector 开始直接将 DR OS 安装到硬盘。可以监视进度，而在安装 DR OS 后将重新启动系统。如果 DR OS 无法正常引导或无法访问网络，则可能需要编辑 kb.cfg 文件。在 Windows Server 2008 及更高版本中，不安装 DR OS，并且不执行系统重新启动。
7. 如果灾难恢复备份已加密，并且要恢复其 Cell Manager 无法访问的客户机，将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库（DR-ClientName-keys.csv）（例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器），并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。
8. 如果 SRD 文件中的信息并非最新（例如因为灾难之后更改了备份设备），并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
9. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。第一次登录之后将删除临时 DR OS，但以下情况除外：
   - Minimal Recovery 处于选定状态。
   - 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
   - 您手动执行带有 omnidr 或 -no_reset 选项的 -debug 命令。
   - 灾难恢复失败。

注意，Data Protector 将首先尝试执行联机还原。如果联机还原因任何原因而失败（如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager），则 Data Protector 将尝试执行远程脱机恢复。如果远程脱机还原失败（如因为介质代理主机仅接受来自 Cell Manager 的请求），则 Data Protector 将执行本地脱机还原。

10. 从 Cell Manager 上的 Data Protector admin 用户组删除在步骤 1 中创建的客户机本地 Administrator 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。

阶段 3

12. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

> **注意**
>
> Data Protector 在恢复之后不会还原卷压缩标志。备份时压缩的所有文件将还原为压缩形式，但如果还希望压缩任何新文件，则必须手动设置卷压缩。

13. 如果要执行 Microsoft 群集服务器中所有节点的灾难恢复，则需要其他步骤。

编辑 SRD 文件

在已更新 SRD 文件（recovery.srd）中存储的备份设备或介质相关信息可能在执行灾难恢复时过期。如果要执行联机恢复，那么这不会产生问题，因为必要的信息存储在 Cell Manager 上的 IDB 中。但是，如果要执行脱机恢复，则无法访问 IDB 中存储的信息。

例如，灾难不仅打击 Cell Manager，而且还会打击与之相连的备份设备。如果灾难之后将该备份设备更换为不同的备份设备，则 SRD 文件中存储的信息将不正确，从而恢复将失败。在这种情况下，编辑已更新 SRD 文件，然后执行灾难恢复的阶段 2，以更新错误信息，从而使得恢复成功。

要编辑 SRD 文件，请在文本编辑器中将其打开（有关 SRD 文件的位置，请参见下方特定方法的详情），然后更新已更改的信息。可以使用 devbra -dev 命令显示设备配置信息。

例如，如果目标系统的客户机名称已更改，则替换 -host 选项的值。还可以编辑有关以下内容的信息：

- Cell Manager 客户机名称（-cm），
- 介质代理客户机（-mahost），
- 设备名称（-dev），
- 设备类型（-type），
- 地址（-devaddr），
- 策略（-devpolicy），
- 机械手 SCSI 地址（-devioctl）
- 库插槽（-physloc）等。

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

对于某些灾难恢复方法和操作系统而言，灾难恢复中对经编辑的 SRD 文件的使用方式将有所不同。下方介绍了特定灾难恢复方法的具体信息。

出于安全原因，应限制对 SRD 文件的访问。

EADR/OBDR

如果 SRD 文件中的信息过时，则在继续定期 EADR/OBDR 过程之前，执行以下其他步骤。

完成以下步骤：

Windows 系统

1. 显示“灾难恢复向导”时，在倒计时期间按任意键停止向导，选择“仅安装”选项，然后单击“完成”。此选项仅向目标系统安装临时操作系统，并因此结束灾难恢复的阶段 1。如果选择**仅安装**选项，则将不自动启动灾难恢复阶段 2。
2. 选择**忽略已删除的文件**选项。该选项可在还原时间删除连续增量备份期间删除的文件。如果指定，在进行增量备份时，omnidr 二进制文件会将同一选项转发给 Data Protector 还原工具（omnir 和 omniofflr）。该选项对还原完整备份对象版本无效。但是，选择该选项可以大大延长还原的时间。
3. 运行 **Windows 任务管理器**（按 **Ctrl+Alt+Del**，然后选择**任务管理器**）。
4. 在 Windows 任务管理器中，单击**文件**，然后单击**新建任务(运行...)**。
5. 从“运行”对话框中运行以下命令： notepad C:\DRSYS\System32\OB2DR\bin\recovery.srd 然后按 **Enter**。此时将在记事本中打开 SRD 文件。
6. 编辑 SRD 文件。
7. 编辑 SRD 文件并将其保存到原始位置之后，从下列位置中运行以下命令 C:\DRSYS\System32\OB2DR\bin omnidr -drimini C:\$DRIM$.OB2\OBRecovery.ini
8. 在定期 EADR/OBDR 恢复过程中继续下一个步骤。

Linux 系统

1. 显示“灾难恢复向导”时，按 **q** 键在倒数期间停止向导，然后选择**仅安装**选项。此选项仅会在目标系统中安装最低版本的 Data Protector。如果选择“仅安装”选项，则将不自动启动灾难恢复阶段 2。
2. 切换到另一个 shell。编辑 SRD 文件 /opt/omni/bin/recovery.srd 。
3. 在编辑并保存 SRD 文件后，执行： omnidr -srd recovery.srd -drimini /opt/omni/bin/drim/drecovery.ini
4. 在恢复过程完成后，返回之前的 shell 并执行普通 EADR/OBDR 恢复过程中的下一步。

Windows BitLocker 驱动器加密

在 Windows Server 2008 及更高版本上执行灾难恢复期间，可以解锁使用 BitLocker Drive Encryption 加密的卷。

如果不解除对特定卷的锁定或如果该卷损坏，则无法解除锁定，并且因此必须格式化，灾难恢复之后对该卷不再加密。在这种环境下，需要再次对该卷进行加密。

请注意，还原系统卷时始终保持不加密状态。

完成以下步骤：

1. 当灾难恢复模块检测到加密卷时，系统会提示您解锁它。

   单击**是**启动 Unlocker 向导。请注意，如果单击**否**，加密的卷将保持锁定状态。
2. 在“选择锁定卷”页中，将列出检测到的加密卷。选择要解锁的卷，然后单击**下一步**。
3. 在“解锁卷”页（每个选定卷一页）中，系统会要求您指定解锁方法。可用的解锁方法如下：
   - 密码 (在 Windows Server 2008 及更高版本上可用)

     在加密卷时所使用的字符串。
   - 通行密码

     在加密卷时使用的长于通常密码的字符串。
   - 恢复密钥

     在每个加密卷上创建的特殊隐藏密钥。恢复密钥具有 BEK 扩展名，并保存在恢复密钥文本文件中。您可以单击**浏览**以找到恢复密钥文件。

   在文本框中键入所请求的信息，然后单击**下一步**。
4. 检查卷是否已成功解锁，然后单击**完成**。

> **注意**
>
> 如果解锁过程失败，可以查看错误信息，然后重试或跳过解锁过程。

恢复过程

如果在 Data Protector 灾难恢复 GUI 的“恢复选项”页上启用了对不同硬件的还原功能，系统将在恢复过程中扫描缺少的驱动程序。如果缺少任何关键的驱动程序（如存储、磁带、网络驱动程序或磁盘控制器），系统会提示您加载所缺少的驱动程序。

完成以下步骤：

1. 在灾难恢复过程中，当系统提示您加载缺少的驱动程序时，单击**是**启动“不同硬件”向导。如果单击**否**，驱动程序注入过程将被跳过。
2. 在“选择设备”页中，选择要加载驱动程序的设备。单击“下一步”。
3. 在“驱动程序搜索位置”页上，指定要在所运行的系统上用于保存驱动程序的位置。浏览到设备驱动程序，或在“驱动程序路径”文本框中键入位置，然后单击**添加路径**将指定的路径添加到列表。可以使用**搜索树深度**选项将搜索调整为您的特定系统范围。

   > **注意**
   >
   > 可以从搜索列表中删除指定的位置，方法是右键单击该位置，然后选择**删除**。

   将在指定的位置搜索缺少的驱动程序。单击“下一步”。
4. 在指定位置搜索缺少的驱动程序后，可能得到以下结果：
   - 找到设备驱动程序: 在“驱动程序路径”文本框中指定对应驱动程序信息文件（*.inf）的完整路径。验证该驱动程序是否正确，然后单击**下一步**加载它。
   - 找不到设备驱动程序：“驱动程序路径”文本框为空。执行以下某个操作：

     如果要搜索其他驱动程序，请单击**浏览**。在“浏览文件”对话框中，选择设备驱动程序的路径，然后单击**下一步**。

     如果不需要将驱动程序加载到该设备，可以将“驱动程序路径”文本框留空，并单击**下一步**进入下一个页面，或者单击**跳过**退出向导。

     > **注意**
     >
     > 如果指定了与设备不对应的驱动程序，此驱动程序将显示为无效，并且无法加载。如果驱动程序不正确，可以更改它或跳过加载过程。
5. 在“驱动程序安装进度”页中，可以查看是否已成功加载设备驱动程序。如果报告了任何错误，可以单击**重试**以重新尝试加载驱动程序。单击**完成**。

还原和准备 OS

还原 OS 的过程与标准的 EADR（从步骤 5 开始）和 OBDR（从步骤 6 开始）过程相同。之后，恢复过程将准备已还原的 OS 并使其适应不同的硬件来为应用程序和文件还原准备 OS。这包括插入引导关键型驱动程序、更新已还原的 OS 的注册表和映射网络。

由于所有引导关键型驱动程序都应存在（在阶段 0 期间加载到正在运行的 DR OS 映像中或在 OS 还原期间手动添加），因此插入操作将自动发生。但是可能需要您的干预才能纠正网络映射。

网络适配器映射

在还原不同的硬件之后，灾难恢复模块将检查所恢复的系统上的网络适配器是否与原始系统上的网络适配器不同。灾难恢复模块无法始终将原始系统的网络配置映射到其自身上的目标系统的网络配置。例如，当目标系统有一张网卡而原始系统有两张或更多网卡，或者向目标系统添加其他网络适配器时会发生这种情况。当检测到此类差异或无法自动确定正确的网络映射时，您可以选择将原始网络适配器映射到在目标系统上发现的网络适配器。

> **注意**网络映射仅在有可用的网络适配器的情况下发生。无法映射没有驱动程序的网络适配器。因此，您应在还原过程开始之前加载网卡驱动程序。

完成以下步骤：

1. 在“网络适配器映射”页中，在原始网络适配器下拉列表中选择原始系统的网络适配器。在当前网络适配器下拉列表中，选择目标系统上的一个可用网络适配器。单击**添加映射**。您创建的映射即被添加到列表中。

   > **注意**
   >
   > 可以从列表中删除映射，方法是右键单击映射然后选择**删除**。

2. 在映射所有需要的网络适配器之后，单击**完成**。

OS 成功还原后

不同的硬件还原将重置 OS 激活。OS 成功还原后，您应：

- 重新激活 OS。
- 检查并重新安装（如果需要）缺少的系统驱动程序。

还原用户和应用程序数据

此阶段与用于 EADR 的过程相同。

> **注意**OS 启动后，第三方应用程序服务和驱动程序可能无法加载。可能需要重新安装、重新配置这些应用程序或者在不需要这些应用程序时将其从当前系统中删除。

将物理系统恢复为虚拟机 (P2V)

Data Protector 支持恢复到为原始操作系统提供支持的虚拟环境，例如 VMware vSphere、Microsoft Hyper-V 或 Citrix XenServer。

目标虚拟机必须满足以下要求：

- 来宾操作系统必须与原始操作系统的类型相同（Windows 或 Linux）。
- 虚拟机的磁盘数量必须大于或等于原始系统的磁盘数量。
- 磁盘的大小必须大于或等于其原始对应版本的大小。
- 磁盘顺序必须与原始系统中的磁盘顺序相同。
- 分配给虚拟机的内存量可能会对恢复过程产生影响，因此建议至少为虚拟机分配 1 GB 的内存。
- 虚拟视频卡内存大小必须满足原始系统的基于原始系统的显示分辨率的要求。如果可能，请使用自动设置。
- 添加与原始计算机上数量相同的网络适配器。适配器必须连接到原始适配器所连接到的网络。

步骤

使用 DR OS 映像引导虚拟机并按照标准灾难恢复过程恢复到不同的硬件。

将虚拟机恢复为物理系统 (V2P)

使用标准灾难恢复过程恢复到不同的硬件，执行虚拟机到物理系统的灾难恢复。

Microsoft 群集服务器的灾难恢复

可以使用除了磁盘查递灾难恢复之外的任何灾难恢复方法恢复 Microsoft 群集服务器 (MSCS)。有关特定灾难恢复方法的所有详情、限制和要求也适用于 MSCS 的灾难恢复。选择适于群集的灾难恢复方法，并将其包括在灾难恢复计划中。请考虑每个灾难恢复方法的限制和要求，然后再做决定。从测试计划中执行测试。

必须符合灾难恢复的所有先决条件（例如一致和最新的备份、经过更新的 SRD 文件、更换了故障硬件等等）才能恢复 MSCS。

可能出现的场景

MSCS 的灾难恢复有两种可能出现的场景：

- 非活动节点上发生的灾难
- 群集中的所有节点都经历了灾难

为 Microsoft 群集服务器灾难恢复所做准备的详情

必须符合灾难恢复的所有先决条件（如一致和最新的备份映像、经过更新的 SRD 文件、更换了故障硬件等等）才能恢复 Microsoft 群集服务器 (MSCS)。有关特定灾难恢复方法的所有详情、限制和要求还适用于 MSCS 的灾难恢复。

MSCS 的一致备份映像包括：

- 所有节点
- 虚拟服务器
- 如果将 Data Protector 配置为群集感知应用程序，则 Cell Manager 应包括在备份规范中

EADR 详情

实际上无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。需要此信息才能还原所有共享群集卷。要在群集中所有节点的 P1S 文件中都包括有关共享群集卷的信息，请执行以下操作之一：

- 执行客户机完整备份之后，合并群集中所有节点的 P1S 文件中有关共享群集卷的信息，以使每个节点的 P1S 文件都包含有关共享群集卷配置的信息。
- 将所有共享群集卷临时移至将备份的节点上。此方式可收集有关所有共享群集卷的所有必要信息，但只有该节点可以作为主节点。

OBDR 详情

要更快还原，请使用 omnisrdupdate 命令作为 post-exec 命令，在 OBDR 备份之后更新 SRD 文件。执行 OBDR 时在软盘驱动器中插入具有经过更新的 SRD 文件的磁盘，以向 Data Protector 告知备份对象在磁带上的位置。还原 MSCS 数据库将更快，因为 Data Protector 不会在磁带中搜索 MSCS 数据库的位置。

为了能够自动还原 MSCS 中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

恢复 Microsoft 群集服务器

Microsoft 群集服务器 (MSCS) 的灾难恢复有两种可能的场景：

- 至少有一个节点正常运行
- 群集中的所有节点都经历了灾难

至少有一个节点正常运行

这是 MSCS 灾难恢复的基本场景。除了灾难恢复的其他先决条件以外，还必须满足以下先决条件。

- 至少有一个群集节点正常运行（活动节点）。

- 此节点上正在运行群集服务。
- 所有物理磁盘资源都必须联机（即，由群集拥有）。
- 具有所有正常的群集功能（群集管理组联机）。
- Cell Manager 处于联机状态。

在这种情况下，群集节点的灾难恢复与 Data Protector 客户机的灾难恢复步骤相同。应遵照将用于还原受影响的非活动节点的特定灾难恢复方法的说明。

仅还原本地磁盘，因为灾难之后将所有共享磁盘都移至正常运行的节点并锁定。

恢复辅助节点之后，该节点将在引导后加入群集。

恢复所有节点并且这些节点加入群集之后，可以还原 MSCS 数据库以确保其一致性。MSCS 数据库是 Windows 系统中 CONFIGURATION 对象的一部分。

群集中的所有节点都经历了灾难

在这种情况下，MSCS 中的所有节点都不可用，并且未运行群集服务。

除了灾难恢复的其他先决条件以外，还必须满足以下先决条件。

- 主节点必须对仲裁磁盘具有写访问权限（不得锁定仲裁磁盘）。
- 恢复 Cell Manager 时，主节点必须对所有 IDB 卷都具有访问权限。

在这种情况下，必须首先还原含有仲裁磁盘的主节点。如果已在群集中安装了 Cell Manager，则还必须还原 IDB。（可选）可以还原 MSCS 数据库。还原主节点之后，可以还原所有剩余的节点。

完成以下步骤：

执行主节点（包括仲裁磁盘）的灾难恢复。

增强型自动灾难恢复 (EADR)、一键式灾难恢复 (OBDR)：

当系统要求您选择恢复的范围时，请选择**完整(含共享卷)** 以还原仲裁磁盘。

重新启动系统。

还原 MSCS 数据库，此数据库是 Windows 系统中 CONFIGURATION 对象的一部分。MSCS 服务必须正在运行才能还原 MSCS 数据库，因此无法在灾难恢复的阶段 2 期间自动还原该数据库。但是，可以在阶段 2 结束时使用标准还原过程手动还原群集数据库。

除一键式灾难恢复 (OBDR) 之外的方法:

如果要恢复 Cell Manager，则要使 IDB 一致。

还原仲裁和 IDB 卷。如果所有其他卷未损坏，则这些卷将保留原样并由所恢复的主节点占用。如果这些卷已损坏，则必须执行以下步骤：

1. 禁用群集服务和群集磁盘驱动程序（MSDN Q176970 中所述的步骤）。
2. 重新启动系统。
3. 重建以前的存储结构。
4. 启用群集磁盘驱动程序和群集服务。
5. 重新启动系统，并还原用户和应用程序数据。

还原剩余的节点。

合并 Microsoft 群集服务器的 P1S 文件

执行备份之后，增强型自动灾难恢复 (EADR) 还需要另一个步骤才能还原活动节点。必须合并 Microsoft 群集服务器 (MSCS) 中所有节点的 P1S 文件中有关共享群集卷的信息，以使每个节点的 P1S 文件都包含有关共享群集卷配置的信息。需要这些信息才能还原所有共享群集卷。通过将所有共享群集卷临时移至将备份的节点，可以避免在备份之后合并 P1S 文件。在这种情况下，可以收集有关所有共享群集卷的所有必要信息。这意味着只有该节点可以作为主节点。

Windows

要合并所有节点的 P1S 文件，请从 Data_Protector_home\bin\drim\bin 目录中执行 merge.exe 命令:

```
merge p1sA_path ... p1sX_path
```

其中 p1sA 是第一个节点的 P1S 文件的完整路径， p1sX 是 MSCS 中上一个节点的 P1S 文件的完整路径。

经过更新的 P1S 文件的文件名结尾追加了 .merged（例如， computer.company.com.merged)。将合并的 P1S 文件重命名为其原始名称 (删除 .merged 扩展名)。

例如，要合并具有 2 个节点的 MSCS 中的 P1S 文件，请键入：

```
merge Data_Protector_program_data \Config\server\dr\p1s\node1.company.com Data_Protector_program_data\Config\server\dr\p1s\node2.company.com 。
```

合并后的文件将为 node1.company.com.merged 和 node2.company.com.merged 。

Linux

merge.exe 命令仅适用于装有 Data Protector 自动灾难恢复组件的 Windows 系统。在 Linux Cell Manager 上，执行以下步骤。

1. 将 P1S 文件复制到装有自动灾难恢复组件的 Windows 客户机上。
2. 合并这些文件。
3. 将合并后的 P1S 文件重命名为其原始名称。
4. 将合并后的 P1S 文件复制回 Linux Cell Manager。

在 Windows 系统中还原原始硬盘签名

Microsoft 群集服务器 (MSCS) 服务使用写入每个硬盘的 MBR 中的硬盘签名识别物理磁盘。如果已更换共享群集磁盘，则这意味着在灾难恢复的阶段 1 期间更改了磁盘签名。因此，群集服务无法将更换的磁盘识别为有效的群集资源，并且依赖于这些资源的群集组将失败。这一点仅适用于活动节点的还原（即，如果群集中的所有节点都遇到灾难），因为只要有至少一个节点正常运行，并占有资源的所有权，共享群集资源即可使用。此问题不适用于 EADR 和 OBDR 关键磁盘，因为将自动恢复所有 EADR 和 OBDR 关键磁盘的原始磁盘签名。如果更换了任何其他磁盘，则还必须还原其硬盘签名。

最关键的共享磁盘是群集仲裁资源。如果已将其更换，则必须还原原始磁盘签名，否则将无法启动群集服务。阶段 2 期间，MSCS 数据库将还原到系统卷上的 \TEMP\ClusterDatabase 目录中。重新引导系统之后，群集服务将不运行，因为在阶段 1 中更改了硬盘签名而无法识别仲裁资源。

在 Windows 中还原原始硬盘签名

在 Windows 系统中，可以通过运行 clubar 实用程序 (位于 Data_Protector_home\bin\utilns 中) 来解决此问题。该实用程序将还原原来的硬盘签名。 clubar 成功完成之后，将自动启动群集服务。

例如，要从 C:\temp\ClusterDatabase 还原 MSCS 数据库，请在命令提示符下键入:

```
clubar r C:\temp\ClusterDatabase force q: .
```

有关 clubar 的用法和语法的详细信息，请参阅 Data_Protector_home\bin\utilns 中的 clubar.txt 文件。

如果 Cell Manager 上的 Data Protector 共享磁盘与仲裁磁盘不同，则还必须还原该共享磁盘。要还原 Data Protector 共享磁盘和任何其他应用程序磁盘的签名，应使用 Windows 资源工具包中包括的 dumpcfg 实用程序。有关使用 dumpcfg 的详细信息，请运行 dumpcfg /? ，或参阅 Windows 资源工具包文档。有关 Windows 系统中硬盘签名问题的详细信息，请参见 MSDN 文章 Q280425。

获取原始硬盘签名

可以从 SRD 文件获取原始硬盘签名。签名是 SRD 文件中跟随在 -volume 关键字之后的数字。

仲裁磁盘的签名仅存储在活动节点的 SRD 文件中（备份时），因为它使仲裁磁盘处于锁定状态，并因此阻止其他节点访问仲裁磁盘。因此建议始终备份整个群集，因为需要群集中所有节点的 SRD 文件，只有所有 SRD 文件集中在一起所包括的信息才足以在阶段 1 中配置共享磁盘卷的磁盘。请注意，将 SRD 文件中存储的硬盘签名表示为十进制数，而 dumpcfg 需要十六进制值。

还原 Internet Information Server 详情

灾难恢复不支持 Internet Information Server (IIS)。要恢复 IIS，必须满足以下要求:

要求

- 不要在全新安装系统期间安装 IIS。

执行以下步骤：

1. 如果正在运行 IIS 管理服务，则停止或卸载该服务。
2. 运行 drstart 命令。

IIS 数据库以纯文本文件 (文件名为 DisasterRecovery) 形式还原到默认 IIS 位置 (%SystemRoot%\system32\inetsrv)。

成功引导之后，使用标准 Data Protector 还原过程或“IIS 备份/还原”管理单元还原 IIS 数据库。注意，这可能需要使用相当长的时间。

UNIX 系统中的灾难恢复过程

重要说明**:** 对于 Data Protector 版本低于 11.0 的 Linux 系统的灾难恢复，您必须使用与灾难恢复主机相同的 Data Protector 版本的介质创建主机。由于 11.0 中的 GCC 版本升级，您不得使用 Data Protector 11.0 或更高版本的介质创建主机。

以下限制适用：

- 群集环境恢复可能与标准过程有所不同。根据群集环境的配置，可能需要对环境执行额外的步骤和修改。
- 不支持 RAID。
- 增强型自动灾难恢复 (EADR) 和一键式灾难恢复 (OBDR) 仅在 Linux 系统上可用。

手动灾难恢复 (MDR)

手动灾难恢复是一种基础的恢复方法。此方法涉及以初始安装的相同方式重新安装系统从而恢复系统。Data Protector 用于还原所有文件，其中包括操作系统。

HP-UX 客户机的 MDR 基于 Ignite-UX 产品；这个应用程序主要是为 HP-UX 系统的安装和配置任务而开发的，它（除了是一个强大的系统管理界面）提供系统准备和从灾难恢复系统的功能。Ignite-UX 侧重于目标客户机的灾难恢复的同时，必须使用 Data Protector 还原用户和应用程序数据，以便完成灾难恢复的阶段 3。

Ignite-UX 提供 2 种不同的方法用于针对灾难准备系统和从灾难恢复系统：

- 使用自定义安装介质 (Golden Image)
- 使用系统恢复工具（make_tape_recovery、make_net_recovery）

使用自定义安装介质最适于 IT 环境中具有大量基本相同的硬件配置和 OS 版本，使用系统恢复工具则支持创建恢复存档（针对各个系统对这些存档进行了自定义）。

使用这两种方法都可以创建 DDS 磁带或 CD 等可引导安装介质。使用这些介质，系统管理员能够直接从故障客户机的系统控制台中执行本地灾难恢复。

此外，这两种方法还都可以通过向故障客户机分配合适的 Golden Image 或以前创建的“恢复存档”，用于运行基于网络的客户机恢复。在这种情况下，客户机直接从 Ignite 服务器引导，并且从所分配的仓库（必须位于网络上的 NFS 共享中）中运行安装。

完成以下步骤：

1. 为手动灾难恢复所做的准备
2. 手动安装和配置 HP-UX 系统
3. 还原系统数据

磁盘传递灾难恢复 (DDDR)

磁盘传递灾难恢复有两种可能的方法。可以使用正常运行的 Data Protector 客户机系统，并在连接到此客户机时创建新磁盘。此外，可以使用辅助磁盘，而不使用其他正常运行的客户机。需要在灾难之前收集足够的数据才能正确地对磁盘进行格式化和分区。

应在与目标系统相同硬件级别的系统上准备辅助磁盘。

完成以下步骤：

1. 为手动灾难恢复所做的准备
2. 手动安装和配置 HP-UX 系统
3. 还原系统数据

增强型自动灾难恢复 (EADR)

增强型自动灾难恢复 (EADR) 用于恢复 Data Protector Cell Manager 和客户机。

要求

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 备份时引导分区上还需要另外 200 MB 的可用磁盘空间。如果没有这些磁盘空间，则灾难恢复将失败。
- 在 EADR 准备期间，安装 Data Protector 所在的卷必须至少具有 800 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 系统的 BIOS 必须支持可引导 CD 扩展（如 El-Torito 标准所定义），并且必须支持通过 INT13h 功能 XXh 使用 LBA 寻址对硬盘驱动器进行读/写访问。可以在系统的用户手册中或通过在引导之前检查系统设置而检查 BIOS 选项。

以下限制适用：

- 必须在 Linux 系统上创建 Linux 系统的 DR ISO 映像。不可以在其他系统（Windows 系统、HP-UX 系统、Solaris 系统）上创建 DR ISO

映像。该限制不适用于更新 SRD 文件或其他任务。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。
- 不支持自定义内核安装或配置，仅支持随分发提供的原始内核。
- 在备份期间必须禁用 SELINUX 保护。如果启用了 SELINUX，客户机将无法恢复。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为增强的自动灾难恢复做准备
2. 准备灾难恢复 CD
3. 恢复 Cell Manager 和客户机系统
4. 还原用户数据

一键式灾难恢复 (OBDR)

一键式灾难恢复用于恢复 Data Protector 客户机。

要求

- 在要允许使用此方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复组件。此外，必须在将准备 DR OS 映像的系统上安装自动灾难恢复组件。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 装有 Data Protector 的卷应至少有 800 MB 的可用空间。此空间是创建临时映像所必需的。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。
- 在 SAN 引导配置中，确保目标系统上的以下项目与原始系统上的一致。
  - 本地 HBA 的 BIOS 参数
  - SAN 磁盘 LUN 数目
- 在多路径 SAN 磁盘配置中，目标系统磁盘的 LUN 和 WWID 必须与原始系统上的一致。

以下限制适用

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 不支持 USB 磁带存储设备。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为一键式灾难恢复做准备
2. 恢复操作系统
3. 还原用户数据。

手动灾难恢复

手动灾难恢复是一种基础的恢复方法。此方法涉及以初始安装的相同方式重新安装系统从而恢复系统。Data Protector 用于还原所有文件，其中包括操作系统。

HP-UX 客户机的 MDR 基于 Ignite-UX 产品；这个应用程序主要是为 HP-UX 系统的安装和配置任务而开发的，它（除了是一个强大的系统管理界面）提供系统准备和从灾难恢复系统的功能。

Ignite-UX 侧重于目标客户机的灾难恢复的同时，必须使用 Data Protector 还原用户和应用程序数据，以便完成灾难恢复的阶段 3。

> **注意**本节未涵盖 Ignite-UX 的完整功能。

概述

Ignite-UX 提供 2 种不同的方法用于针对灾难准备系统和从灾难恢复系统：

- 使用自定义安装介质 (Golden Image)
- 使用系统恢复工具（make_tape_recovery、make_net_recovery）

使用自定义安装介质最适于 IT 环境中具有大量基本相同的硬件配置和 OS 版本，使用系统恢复工具则支持创建恢复存档（针对各个系统对这些存档进行了自定义）。

使用这两种方法都可以创建 DDS 磁带或 CD 等可引导安装介质。使用这些介质，系统管理员能够直接从故障客户机的系统控制台中执行本地灾难恢复。

此外，这两种方法还都可以通过向故障客户机分配合适的 Golden Image 或以前创建的“恢复存档”，用于运行基于网络的客户机恢复。在这种情况下，客户机直接从 Ignite 服务器引导，并且从所分配的仓库（必须位于网络上的 NFS 共享中）中运行安装。

在受支持的位置使用 Ignite-UX GUI。

以下限制适用：

- 群集环境恢复可能与标准过程有所不同。根据群集环境的配置，可能需要对环境执行额外的步骤和修改。
- 不支持 RAID。

要恢复 Cell Manager，请完成以下步骤:

1. 为灾难恢复做准备
2. 安装和配置操作系统
3. 还原系统数据

要恢复客户机，请完成以下步骤:

1. 为手动灾难恢复所做的准备
2. 手动安装和配置 HP-UX 系统

为手动灾难恢复所做的准备

要做好准备而使灾难恢复成功，应遵照与常规准备过程相关的说明以及特定方法要求。必须提前准备，以便快速高效地执行灾难恢复。

为 Cell Manager 的手动灾难恢复所做的准备包括：

- 收集备份规范的信息
- 准备备份规范（使用 pre-exec 脚本）
- 执行备份
- 定期执行内部数据库备份会话

在 Cell Manager 上执行灾难恢复之前，必须进行所有这些准备步骤。

一次性准备

应在灾难恢复计划中记录这些文件的位置，以便在发生灾难时可以找到这些信息。此外，应考虑版本管理（每个备份有一组“辅助信息”）。

如果要备份的系统有在底层活动的应用程序进程，则应建立 minimal activity（经过修改的 init 1 run-level）状态，以便准备 Cell Manager 进行一致的备份。

HP-UX 系统

- 从 /sbin/rc1.d to /sbin/rc0.d 移动某些终止链接，并补充对引导部分的更改。终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统上配置了 rpcd（在 /etc/rc.config.d/dce 文件中配置 RPCD=1 选项）。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1（FS_mounted, hostname_set, date_set, syncer_running）
- 运行的进程： network、 inetd、 rpcd、 swagentd

备份系统

准备好备份规范之后，应执行备份过程。定期重复此过程，或至少在每次系统配置有更大更改之后，尤其是在物理或逻辑卷结构方面发生任何更改之后重复此过程。请特别注意 IDB 和文件系统备份：

- 定期备份 IDB（最好在单独的备份规范中，并计划在 Cell Manager 自身的备份之后）。
- 在连接到 Cell Manager 系统的某个特定设备上运行 IDB 和文件系统备份，以使您了解设备中的介质包含 IDB 的最新备份版本。

手动安装和配置 HP-UX 系统

灾难发生之后，应首先安装和配置操作系统（阶段 1）。然后可以恢复 Cell Manager。

完成以下步骤：

阶段 1

1. 替换受影响的磁盘。
2. 从操作系统安装介质引导系统。
3. 重新安装操作系统。安装期间，使用在准备阶段收集的数据（使用 pre-exec 脚本）重新创建和配置物理和逻辑存储/卷结构、文件系统、装载点、网络设置等等。

手动还原系统数据

安装和配置操作系统（阶段 1）之后，可以使用 Data Protector 恢复 Cell Manager。

以下先决条件适用:

- 您需要一个介质，其中包含 Cell Manager 系统根卷的最新备份映像，以及 IDB 的更新的最新备份映像。
- 需要连接到 Cell Manager 系统的设备。

完成以下步骤：

阶段 2

1. 在 Cell Manager 上重新安装 Data Protector 软件。
2. 从 IDB 和 /etc/opt/omni 目录各自的最新备份映像将它们还原至临时目录。这样可简化从备份介质中还原所有其他文件。删除 /etc/opt/omni/ 目录，并将其替换为临时目录中的 /etc/opt/omni 目录。这样将重新创建以前的配置。
3. 使用 omnisv -start 命令启动 Data Protector 进程。

阶段 3

4. 启动 Data Protector GUI，并从备份映像还原所需文件。
5. 重新启动系统。

现在应成功恢复了 Cell Manager。

为手动灾难恢复做的准备（HP-UX 客户机）

Ignite-UX 提供 2 种不同的方法用于针对灾难准备系统和从灾难恢复系统：

使用自定义安装介质 (Golden Image)

使用系统恢复工具（make_tape_recovery、make_net_recovery）

使用自定义安装介质 (Golden Image)

大型 IT 环境通常由大量基于相同硬件和软件的系统组成。如果使用已安装系统的完整快照安装其他系统，则可以显著缩短新系统用于安装 OS、应用程序和所需修补程序的时间。Ignite-UX 含有一项功能，通过该功能可以修改网络或文件系统设置等参数，以及将 Data Protector 等软件添加到映像 (用 Ignite-UX 命令 make_config)，然后再将此类 Golden Image 分配给另一个系统。因此，此功能可用于从灾难恢复系统。

使用自定义安装介质的常规步骤包括：

1. **阶段 0**
   1. 创建客户机系统的 Golden Image。
2. **阶段 1** 和 **2**
   1. 用替换磁盘替换故障磁盘。
   2. 从 Ignite-UX 服务器引导 HP-UX 客户机然后配置网络。
   3. 从 Ignite-UX 服务器安装 Golden Image。
3. **阶段 3**
   1. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

创建 Golden Image

将 /opt/ignite/data/scripts/make_sys_image 文件从 Ignite-UX 服务器复制到客户机系统上的一个临时目录中。

在客户机节点上运行以下命令，以便在另一个系统上创建客户机的压缩映像： make_sys_image -d directory of the archive -n name of the archive.gz -s IP address of the target system

此命令将在系统中用 -d 和 -s 选项定义的指定目录中创建以 gzip 格式压缩的文件仓库。确保 HP-UX 客户机已授予了对目标系统的无密码访问权限 (.rhosts 文件的一个条目中有目标系统上的客户机系统的名称)，否则命令将失败。

向目标系统上的 /etc/exports 目录添加目标目录，然后在目标服务器上导出该目录 (exportfs -av)。

在配置 Ignite-UX 服务器时，请将存档模板文件 core.cfg 复制到 archive_name.cfg：cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/OS_Release/archive_name.cfg.

示例： cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg

在复制的配置文件中检查和更改以下参数：

- 在 sw_source 节中：

  load_order = 0

  source_format = archive

  source_type="NET"

  # change_media=FALSE

  post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"

  post_config_script = "/opt/ignite/data/scripts/os_arch_post_c"

  nfs_source = "IP Target System:Full Path

- 在匹配的 OS archive 节中：

  archive_path = "archive_name.gz

通过对映像文件运行命令 archive_impact 确定 "impacts" 条目，并且复制配置文件的相同 "OS archive" 部分中的输出：/opt/ignite/lbin/archive_impact -t -g archive_name.gz .

示例： /opt/ignite/lbin/archive_impact -t -g /image/archive_HPUX11_31_DP70_CL.gz

impacts = "/" 506Kb

impacts = "/.root" 32Kb

impacts = "/dev" 12Kb

impacts = "/etc" 26275Kb

impacts = "/opt" 827022Kb

impacts = "/sbin" 35124Kb

impacts = "/stand" 1116Kb

impacts = "/tcadm" 1Kb

impacts = "/usr" 729579Kb

impacts = "/var" 254639Kb

要使 Ignite-UX 了解新创建的仓库，请将具有以下布局的 cfg 条目添加到 /var/opt/ignite/INDEX 文件中:

cfg "This_configuration_name" {

description "Description of this configuration”

"/opt/ignite/data/OS/config"

"/var/opt/ignite/data/OS/ archive_name.cfg"

}

示例：

cfg "HPUX11_31_DP70_Client" {

description "HPUX 11.i OS incl Patches and DP70 Client"

"/opt/ignite/data/Rel_B.11.31/config"

"/var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg"

}

确保保留一个或多个 IP 地址，用于引导 /etc/opt/ignite/instl_boottab 文件中配置的客户机。IP 地址的数字等于同时引导的客户机的数量。

上述过程完成之后，将拥有 HP-UX 客户机的 Golden Image（含有特定的硬件和软件配置），它可用于恢复相似布局的任何客户机。

需要重复这些步骤，为所有硬件和软件配置不同的系统创建 Golden Image。

通过 Ignite-UX，可以根据所创建的 Golden Image 创建可引导磁带或 CD。

使用系统恢复工具 (make_tape_recovery、make_net_recovery)

使用与 Ignite-UX 捆绑的系统恢复工具，可从磁盘故障中快速轻松地恢复。系统恢复工具的恢复存档仅包括必要的 HP-UX 目录。但是，还可以在存档中加入其他文件和目录 (例如其他卷组或 Data Protector 文件和目录) 以加快恢复过程。

make_tape_recovery 可创建针对系统自定义的可引导恢复（安装）磁带，并支持无人看管的灾难恢复，具体方法是将备份设备直接连接到目标系

统，并从可引导恢复磁带启动目标系统。在创建存档和恢复客户机期间，备份设备必须从本地连接到客户机。

make_net_recovery 可通过网络在 Ignite-UX 服务器或其他任何指定的系统上创建恢复归档。从由 Ignite-UX make_boot_tape 命令创建的可引导磁带启动或系统直接从 Ignite-UX 服务器引导之后，可以跨越子网恢复目标系统。直接从 Ignite-UX 服务器启动的过程可以借助 Ignite-UX bootsys 命令自动化，也可以在引导控制台上以交互方式指定启动过程。

使用系统恢复工具的常规步骤包括：

1. **阶段 0**
   a. 在 Ignite-UX 服务器上使用 Ignite-UX GUI 创建 HP-UX 客户机的恢复存档。
2. **阶段 1** 和 **2**
   a. 用替换磁盘替换故障磁盘。
   b. 对于本地还原，从准备的恢复磁带引导。
   c. 进行本地还原时，恢复过程将自动启动。

   对于网络还原，从 Ignite-UX 客户机引导并配置网络和 UI。

   进行网络还原时，从 Ignite-UX 服务器安装 Golden Image。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

以下先决条件适用:

必须在客户机上安装 Ignite-UX 文件集，以使 Ignite-UX 服务器能够与客户机通信，然后才能针对灾难准备系统。

确保 Ignite-UX 服务器上和客户机上的 Ignite-UX 文件集的修订版相同。使所有内容保持一致的最简单方式是从 Ignite-UX 服务器上生成的仓库中安装 Ignite-UX。通过在 Ignite-UX 服务器上运行以下命令，可以构造此仓库： pkg_rec_depot -f 。此命令可在 /var/opt/ignite/depots/recovery_cmds 下创建 Ignite-UX 仓库，该目录可以在客户机上由 swinstall 指定为用于安装 Ignite-UX 软件的源目录。

在客户机节点上安装 Ignite-UX 之后，可以使用 make_net_recovery 或 make_tape_recovery 在 Ignite-UX 服务器上使用 GUI 创建恢复归档。

使用 make_tape_recovery 创建存档

1. 确保将备份设备连接到 HP-UX 客户机。
2. 通过执行以下命令，启动 Ignite-UX GUI： /opt/ignite/bin/ignite & 。
3. 右键单击客户机图标，然后选择“创建磁带恢复存档 ”。
4. 如果有多个设备连接到 HP-UX 客户机，则选择一个磁带设备。
5. 选择要加入存档中的卷组。
6. 现在将开始磁带创建过程。通过右键单击客户机图标并选择 Client Status ，检查 Ignite-UX 服务器上的状态和日志文件。

> **注意**Ignite-UX 建议使用 90m DDS1 备份磁带，以确保磁带适用于任何 DDS 驱动器。

使用 make_net_recovery 创建存档

使用 make_net_recovery 创建恢复存档的过程与使用 make_tape_recovery 几乎相同。此命令的优点是不需要在本地连接备份设备，因为默认情况下恢复存档存储在 Ignite-UX 服务器上。

1. 通过执行以下命令，启动 Ignite-UX GUI: /opt/ignite/bin/ignite &
2. 右键单击客户机图标，然后选择“创建磁带恢复存档” 。
3. 选择目标系统和目录。确保有足够的空间可存储压缩后的存档。
4. 选择要加入存档中的卷组。
5. 现在将开始存档创建过程。通过右键单击图标并选择 Client Status ，检查 Ignite-UX 服务器上的状态和日志文件。

> **注意**使用 Ignite-UX 可以根据压缩的存档文件创建可引导的存档磁带。请参阅《Ignite-UX Administration Guide》中的 Create a Bootable Archive Tape via the Network 一章。

恢复 HP-UX 客户机

有 3 种不同的方法可使用手动灾难恢复 (MDR) 恢复 HP-UX 客户机：

- 使用 Golden Image 进行恢复
- 从可引导备份磁带进行恢复
- 从网络进行恢复

使用 Golden Image 进行恢复

通过应用 Golden Image（位于网络上的 NFS 共享上）可恢复 HP-UX 客户机。

在客户机上

完成以下步骤：

1. 更换故障硬件。
2. 从 Ignite-UX 服务器引导 HP-UX 客户机： boot lan.IP-address Ignite-UX server install.
3. 显示“欢迎使用 Ignite-UX”屏幕时，选择**安装 HP-UX**。
4. 从“GUI 选项”屏幕中选择 **Ignite-UX 服务器上运行的远程图形界面**。
5. 对“网络配置”对话框作出回应。
6. 系统现在已为远程 Ignite-UX 服务器控制的安装做好准备。

在 Ignite-UX 服务器上

完成以下步骤：

1. 在 Ignite-UX GUI 中右键单击客户机图标，然后选择**安装客户机 - 新安装**。
2. 选择要安装的 Golden Image，检查设置（网络、文件系统、时区...），然后单击**开始**。
3. 通过右键单击客户机图标并选择**客户机状态**，可以检查安装进度。
4. 安装结束之后，使用标准 Data Protector 还原过程还原其他用户和应用程序数据。

从可引导备份磁带进行恢复

使用 make_tape_recovery 命令创建可引导备份磁带。

完成以下步骤：

1. 更换故障硬件。
2. 确保将磁带设备在本地连接到受影响的 HP-UX 客户机，并插入含有要还原的存档的介质。
3. 从准备的恢复磁带引导。为此，请在 boot admin 菜单中键入 SEARCH ，获得所有可用的引导设备的列表。确定哪一个是磁带驱动器，然后键入 boot 命令： boot hardware path 或 boot Pnumber 。
4. 此时将自动启动恢复过程。
5. 恢复成功完成之后，使用标准 Data Protector 还原过程还原其他用户和应用程序数据。

从网络进行恢复

可以从位于 Ignite-UX 服务器上的恢复归档文件通过网络引导目标系统。按照有关如何使用 Golden Image 执行恢复的说明进行操作，并确保为安装选择了所需的存档。

使用系统恢复工具 (make_tape_recovery、make_net_recovery)

使用与 Ignite-UX 捆绑的系统恢复工具，可从磁盘故障中快速轻松地恢复。系统恢复工具的恢复存档仅包括必要的 HP-UX 目录。但是，还可以在存档中加入其他文件和目录 (例如其他卷组或 Data Protector 文件和目录) 以加快恢复过程。

make_tape_recovery 可创建针对系统自定义的可引导恢复 (安装) 磁带，并支持无人看管的灾难恢复，具体方法是将备份设备直接连接到目标系统，并从可引导恢复磁带启动目标系统。在创建存档和恢复客户机期间，备份设备必须从本地连接到客户机。

make_net_recovery 可通过网络在 Ignite-UX 服务器或其他任何指定的系统上创建恢复存档。从由 Ignite-UX make_boot_tape 命令创建的可引导磁带启动或系统直接从 Ignite-UX 服务器引导之后，可以跨越子网恢复目标系统。直接从 Ignite-UX 服务器启动的过程可以借助 Ignite-UX bootsys 命令自动化，也可以在引导控制台上以交互方式指定启动过程。

使用系统恢复工具的常规步骤包括：

1. **阶段 0**
   a. 在 Ignite-UX 服务器上使用 Ignite-UX GUI 创建 HP-UX 客户机的恢复存档。
2. **阶段 1** 和 **2**
   a. 用替换磁盘替换故障磁盘。
   b. 对于本地还原，从准备的恢复磁带引导。
   c. 进行本地还原时，恢复过程将自动启动。

      对于网络还原，从 Ignite-UX 客户机引导并配置网络和 UI。

      进行网络还原时，从 Ignite-UX 服务器安装 Golden Image。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

以下先决条件适用:

必须在客户机上安装 Ignite-UX 文件集，以使 Ignite-UX 服务器能够与客户机通信，然后才能针对灾难准备系统。

确保 Ignite-UX 服务器上和客户机上的 Ignite-UX 文件集的修订版相同。使所有内容保持一致的最简单方式是从 Ignite-UX 服务器上生成的仓库中安装 Ignite-UX。通过在 Ignite-UX 服务器上运行以下命令，可以构造此仓库： pkg_rec_depot -f 。此命令可在 /var/opt/ignite/depots/recovery_cmds 下创建 Ignite-UX 仓库，该目录可以在客户机上由 swinstall 指定为用于安装 Ignite-UX 软件的源目录。

在客户机节点上安装 Ignite-UX 之后，可以使用 make_net_recovery 或 make_tape_recovery 在 Ignite-UX 服务器上使用 GUI 创建恢复归档。

使用 make_tape_recovery 创建存档

1. 确保将备份设备连接到 HP-UX 客户机。
2. 通过执行以下命令，启动 Ignite-UX GUI： /opt/ignite/bin/ignite & 。

3. 右键单击客户机图标，然后选择“创建磁带恢复存档 ”。
4. 如果有多个设备连接到 HP-UX 客户机，则选择一个磁带设备。
5. 选择要加入存档中的卷组。
6. 现在将开始磁带创建过程。通过右键单击客户机图标并选择 Client Status ，检查 Ignite-UX 服务器上的状态和日志文件。

> 注意Ignite-UX 建议使用 90m DDS1 备份磁带，以确保磁带适用于任何 DDS 驱动器。

使用 make_net_recovery 创建存档

使用 make_net_recovery 创建恢复存档的过程与使用 make_tape_recovery 几乎相同。此命令的优点是不需要在本地连接备份设备，因为默认情况下恢复存档存储在 Ignite-UX 服务器上。

1. 通过执行以下命令，启动 Ignite-UX GUI: /opt/ignite/bin/ignite &
2. 右键单击客户机图标，然后选择“创建磁带恢复存档” 。
3. 选择目标系统和目录。确保有足够的空间可存储压缩后的存档。
4. 选择要加入存档中的卷组。
5. 现在将开始存档创建过程。通过右键单击图标并选择 Client Status ，检查 Ignite-UX 服务器上的状态和日志文件。

> 注意使用 Ignite-UX 可以根据压缩的存档文件创建可引导的存档磁带。请参阅《Ignite-UX Administration Guide》中的 Create a Bootable Archive Tape via the Network 一章。

磁盘传递灾难恢复（DDDR）

磁盘传递灾难恢复有两种可能的方法。可以使用正常运行的 Data Protector 客户机系统，并在连接到此客户机时创建新磁盘。此外，可以使用辅助磁盘，而不使用其他正常运行的客户机。需要在灾难之前收集足够的数据才能正确地对磁盘进行格式化和分区。

概述

使用装有最小化操作系统（其上配置有网络并安装了 Data Protector 代理）的辅助磁盘（可以随身携带）执行 UNIX 客户机的磁盘传递。

确保已执行准备一章中提及的所有常规准备步骤。对 UNIX 客户机使用辅助磁盘的常规步骤包括：

1. **阶段 1**
   a. 用替换磁盘替换故障磁盘，将辅助磁盘连接到目标系统，然后使用辅助磁盘上安装的最小化操作系统重新启动系统。
   b. 手动对这些磁盘进行重新分区，重新建立存储结构并使替换磁盘可引导。
2. **阶段 2**
   a. 使用标准 Data Protector 还原过程将原始系统的引导磁盘还原到替换磁盘（使用**还原到**选项）。
   b. 关闭系统并删除辅助磁盘。如果您使用的是热插拔硬盘驱动器，则无需关闭系统。
   c. 重新启动系统。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

以下限制适用：

- 应在与目标系统相同硬件级别的系统上准备辅助磁盘。

- 群集环境恢复可能与标准过程有所不同。根据群集环境的配置，可能需要对环境执行额外的步骤和修改。
- 不支持 RAID。

完成以下步骤：

1. 为灾难恢复做准备。
2. 安装和配置磁盘。
3. 还原系统数据。

为 UNIX 客户机的磁盘传递灾难恢复做的准备

要做好准备而使灾难恢复成功，应遵照与常规准备过程相关的说明以及特定方法要求。必须提前准备，以便快速高效地执行灾难恢复。有关受支持操作系统的详细信息，请参阅 。

为磁盘传递灾难恢复做的准备包括：

- 收集备份规范的信息
- 准备辅助磁盘
- 准备备份规范（使用 pre-exec 脚本）
- 执行备份

在客户机系统上执行灾难恢复之前，必须进行所有这些准备过程。

一次性准备

如果在 pre-exec 命令过程中收集信息，则应在灾难恢复计划中记录这些文件的位置，以便在发生灾难时可以找到这些信息。此外，应考虑版本管理（每个备份有一组“辅助信息”）。

还应在每个客户机系统上建立 minimal activity（经过修改的 init 1 run-level）状态，以便准备其进行一致的备份，并因此避免恢复之后出现问题。有关详细信息，请参见操作系统文档。

HP-UX 示例

- 从 /sbin/rc1.d to /sbin/rc0.d 移动某些终止链接，并补充对引导部分的更改。终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统上配置了 rpcd（在 /etc/rc.config.d/dce 文件中配置 RPCD=1 选项)。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1 (FS_mounted, hostname_set, date_set, syncer_running)
- 网络必须正在运行
- 运行的进程： network 、 inetd 、 rpcd 、 swagentd

Solaris 示例

- 从 /etc/rc1.d to /etc/rc0.d 移动某些终止链接，并补充对引导部分的更改。终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统中配置了 rpcbind 。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1
- 网络必须正在运行
- 运行的进程： network, inetd, rpcbind

AIX

无需任何操作，因为用于准备辅助磁盘的 alt_disk_install 命令可确保一致的磁盘映像，而不必进入最低限度系统活动的状态。

准备辅助磁盘

如果要使用辅助磁盘，则需要首先准备它。每个单元和平台仅需要一个可引导辅助磁盘。该磁盘必须包含操作系统和网络配置，且必须可引导。

备份系统

准备好备份规范之后，应执行备份过程。定期重复此过程，或至少在每次系统配置有更大更改之后，尤其是在物理或逻辑卷结构方面发生任何更改之后重复此过程。

为 UNIX 客户机的灾难恢复创建备份规范

要为 UNIX 客户机的灾难恢复配置备份规范，请修改现有规范，或用指定的 pre-exec 和 post-exec 脚本创建新规范。

完成以下步骤：

提供将执行以下操作的 pre-exec 脚本：

- 收集有关环境的所有必要信息，并将其存储在稳妥之处以备灾难恢复时使用。这些信息包括：
  - 系统的物理和逻辑存储结构
  - 当前逻辑卷结构 (例如在 HP-UX 系统中，使用 vgcfgbackup 和 vgdisplay -v)
  - 群集配置数据、磁盘镜像和条带化
  - 文件系统和装载点概述 (例如在 HP-UX 系统中，使用 bdf 或 /etc/fstab 的副本)
  - 系统分页空间信息 (例如在 HP-UX 系统中， swapinfo 命令的输出)
  - I/O 结构概述 (例如在 HP-UX 系统中，使用 HP-UX 系统中的 ioscan -fun 和 ioscan -fkn)
  - 客户机网络设置

也可以将数据的紧急副本放入备份本身内。如果是这样，则请在实际恢复之前提取信息。

- 从系统中注销所有用户。
- 关闭所有应用程序，除非单独备份应用程序数据（例如使用联机数据库备份）。
- (可选) 限制通过网络访问系统，以便在备份运行时无人可登录系统 (例如在 HP-UX 系统中，覆盖 inetd.sec 并使用 inetd -c)。
- 如果需要，进入最低限度系统活动的状态 (例如在 HP-UX 系统中，使用 sbin/init 1； wait 60 ；检查是否达到 run-level 1)。注意，这是经过修改的“init 1”状态。

提供将系统还原到标准运行级别、重新启动应用程序等等的 post-exec 脚本。

在 Cell Manager 上使用 pre-exec 和 post-exec 脚本为客户机配置备份规范。其中应包括所有磁盘。

执行此备份过程并定期重复执行该过程，或者至少在每次发生重大系统配置更改时，尤其是逻辑卷结构发生任何更改（例如，在 HP-UX 上使用 LVM）时执行此过程。

使用 DDDR 安装和配置 UNIX 客户机

灾难发生之后，应首先为故障客户机安装和配置新磁盘（阶段 1）。

以下先决条件适用:

- 需要用新硬盘更换受影响的磁盘。
- 应在与目标系统相同硬件级别的系统上准备辅助磁盘。
- 辅助磁盘应包含相关的 UNIX 操作系统和 Data Protector 代理。
- 应有要恢复的客户机的有效完整备份。

完成以下步骤：

1. 将故障磁盘替换为类似大小的新磁盘。
2. 将辅助磁盘（包含所需的操作系统和 Data Protector 客户机）连接到系统，并将其作为引导设备。
3. 从辅助操作系统引导。
4. 如果适用，则重新构造逻辑卷结构（例如，在 HP-UX 系统中使用 LVM）。对非根卷组使用备份数据 (例如使用 HP-UX 系统中的 vgcfgrestore 或 SAM)。
5. 此外，创建要在修复的磁盘上还原的根卷组 (例如使用 HP-UX 系统中的 vgimport)。它在还原过程中不像是根卷组，因为正在运行辅助磁盘中的操作系统。
6. 使用相关的 UNIX 命令使新磁盘可引导。
7. 在备份期间，根据辅助存储设备上保存的数据重新构造任何其他存储结构，如镜像、条带、Serviceguard 等等。
8. 创建文件系统，并根据备份中数据的需要装载这些文件系统。使用相似但并非原始的装载点名称 (例如 /etc_restore 对于 /etc 等等)。
9. 删除要还原的装载点中的任何文件；这些装载点必须为空。
10. 开始还原系统数据。

使用 DDDR 还原系统数据 (UNIX 客户机)

可以将系统还原为上次成功执行备份时的状态。首先应安装和配置 UNIX 客户机（阶段 1）。

以下先决条件适用:

- 应安装并配置相关的操作系统。
- 应安装 Data Protector。
- 应有要恢复的客户机的有效完整备份。
- 还原所需的介质应可用。

完成以下步骤：

阶段 2

1. 启动 Data Protector 用户界面，然后打开到 Data Protector Cell Manager 的连接。
2. 将包含辅助磁盘的系统导入单元。
3. 选择要从中还原的备份版本。

4. 使用选项“还原为” new_mountpoint 将所有必需的装载点还原到系统，包括 (未来的) 根卷。

   备份中的根卷还原为“已修复磁盘”上的根卷。任何内容都不还原到辅助磁盘上当前运行的辅助操作系统。

5. 关闭并重新启动刚还原的系统。
6. 断开辅助磁盘与系统的连接。
7. 从新的（或已修复的）磁盘重新启动系统。

阶段 3

8. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

一键式灾难恢复 (OBDR)

一键式灾难恢复用于恢复 Data Protector 客户机。

一键式灾难恢复 (OBDR) 是一种适用于 Linux Data Protector 客户机的 Data Protector 自动恢复方法，尽可能减少用户干预。

备份时，OBDR 将自动收集所有相关的环境数据。备份期间，临时安装和配置 DR OS 所需的数据打包在单个大型 OBDR 映像文件（恢复集）中，并存储在备份磁带上。灾难发生时，OBDR 设备（能够模拟 CD-ROM 的备份设备）用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。

然后，Data Protector 运行并配置灾难恢复操作系统 (DR OS)，对磁盘进行分区和格式化，最后使用 Data Protector 将原始操作系统还原为备份时的原样。

重要说明每次硬件、软件或配置更改之后都要执行新的备份。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

OBDR 过程根据所选的恢复范围恢复卷。

可按照 Data Protector 标准还原过程恢复所有剩余卷。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Windows 客户机使用一键式灾难恢复方法的常规步骤包括：

1. **阶段 1**

   从恢复磁带引导并选择恢复范围。

2. **阶段 2**

   根据您所选的恢复范围，系统将自动还原所选的卷。

   关键卷（引导分区和操作系统）始终会被还原。

3. **阶段 3**

   按照标准还原过程还原所有剩余分区。

重要说明建议限制对 OBDR 引导介质的访问。

以下各节将介绍有关在 Windows 系统上执行一键式灾难恢复的要求、限制、准备和恢复。

要求

- 在要允许使用此方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复组件。此外，必须在将准备 DR OS 映像的系统上安装自动灾难恢复组件。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 装有 Data Protector 的卷应至少有 800 MB 的可用空间。此空间是创建临时映像所必需的。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。

- 在 SAN 引导配置中，确保目标系统上的以下项目与原始系统上的一致。
  - 本地 HBA 的 BIOS 参数
  - SAN 磁盘 LUN 数目
- 在多路径 SAN 磁盘配置中，目标系统磁盘的 LUN 和 WWID 必须与原始系统上的一致。

以下限制适用：

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 不支持 USB 磁带存储设备。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION/SYSTEMRECOVERYDATA 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp。但是，如果您手动更新现有的备份规范，则系统将不会设置这一排除。要成功备份，请排除 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 文件夹。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：
  - fio-status – 列出所有 Fusion IO 磁盘的状态。
  - fio-format [path] – 执行 Fusion IO 磁盘的低级格式化。
  - fio-attach [path] – 将 Fusion IO 磁盘连接到系统。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为一键式灾难恢复做准备
2. 恢复操作系统
3. 还原用户数据。

增强型自动灾难恢复 (EADR)

增强型自动灾难恢复 (EADR) 用于恢复 Data Protector Cell Manager 和客户机。

Data Protector 为 Linux Data Protector Cell Manager 和客户机提供增强型灾难恢复过程。

备份时，EADR 将自动收集所有相关的环境数据。在整个客户机系统的完整备份期间，对于单元中的每个已备份客户机，临时安装和配置 DR OS 所需的数据打包在单个大型恢复集文件中并存储在备份磁带上（以及可选存储在 Cell Manager 上）。

除此映像文件以外，对磁盘进行正确分区和格式化所需的阶段 1 启动文件（P1S 文件）存储在备份介质和 Cell Manager 上。灾难发生时，增强型自动灾难恢复向导用于从备份介质还原恢复集（如果其在完整备份期间未保存在 Cell Manager 上）并将其转换为灾难恢复 CD ISO 映像。可以使用任何 CD 刻录工具将 CD ISO 映像录制到 CD 上并用于引导目标系统。

启动 DR OS 映像后，Data Protector 将自动对磁盘进行格式化和分区，最后用 Data Protector 将原始系统恢复到备份时的状态。

重要说明

- Micro Focus 建议限制对备份介质、恢复集文件、SRD 文件和灾难恢复 CD 的访问。
- 使用 omnikeytool -export *keyFileName* [-password] 命令加密并导出的备份不支持灾难恢复。使用 omnikeytool -export *keyFileName* 命令导出密钥，而无需 -password 选项。有关更多信息，请参见 omnikeytool 命令页面。
- 跨多个介质的备份不支持 AES 加密的灾难恢复备份和还原。这适用于所有设备类型。
- 即使目标系统中可用的 NIC 少于源系统中的可用 NIC，使用 NIC 聚合的 EADR 恢复也是成功的。以下是此类 NIC 负载均衡的列表:
  - 激活备份
  - XOR (异或)
  - 广播
  - 动态链路聚合
  - 传输负载均衡 (TLB)
- 默认情况下，通过 EADR 磁盘分区大小调整支持，可以将源系统中磁盘的原始分区调整为新替换的磁盘大小。仅在以下情况下受支持:
  - 该磁盘是非 LVM 磁盘
  - 该磁盘具有单一分区，该分区具有以下属性:
    - 分区类型为非 LVM
    - 分区样式为 MBR 或 GPT
    - 分区具有 ext4/xfs 文件系统
  - 新替换的磁盘大小大于源系统中的原始磁盘
    无论该分区主机上的数据如何 (/boot, /home, /var, /tmp or user data)，都会调整磁盘分区的大小。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Linux 客户机使用增强型自动灾难恢复方法的常规步骤包括：

1. **阶段 1**
   a. 更换故障硬件。
   b. 从灾难恢复 CD 或 USB 闪存驱动器引导目标系统并选择恢复的范围。这是完全无人看管的恢复。
2. **阶段 2**
   a. 根据您所选的恢复范围，系统将自动还原所选的卷。关键卷（引导卷、根卷以及包含 Data Protector 安装和配置的卷）始终会被还原。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

重要说明提前为任何必须首先还原的关键卷（尤其是 DNS 服务器、Cell Manager、介质代理客户机、文件服务器等等）准备好 DR OS 映像。

提前为 Cell Manager 恢复准备好包含加密密钥的可移动介质。

以下各节将介绍与 Linux 客户机的 EADR 相关的要求、限制、准备步骤和恢复过程。

要求

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置（扇区重新映射）。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 备份时引导分区上还需要另外 200 MB 的可用磁盘空间。如果没有这些磁盘空间，则灾难恢复将失败。
- 在 EADR 准备期间，安装 Data Protector 所在的卷必须至少具有 800 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 系统的 BIOS 必须支持可引导 CD 扩展（如 El-Torito 标准所定义），并且必须支持通过 INT13h 功能 XXh 使用 LBA 寻址对硬盘驱动器进

行读/写访问。可以在系统的用户手册中或通过在引导之前检查系统设置而检查 BIOS 选项。

- 在 UEFI+Secureboot ON 模式下用于保护系统二进制文件的加密密钥在 RHEL 版本 8.0 到 8.5 之间是不同的。确保介质创建主机操作系统版本与 DA 客户机备份系统相同，以便创建 ISO 映像并在 UEFI+secureboot ON 模式下成功启动。
- 必须在系统上安装模块 dmsquash-live ，才能成功进行 EADR 备份。此模块是 dracut-live 包的一部分，默认情况下此包不会作为操作系统版本 8.x 安装的一部分进行安装。确保从操作系统 ISO 映像或 DVD 安装此包。
- 确保在 Cell Manager 的管理员组中添加以下用户以成功进行联机 EADR 恢复:

在 Windows 客户机中：
Type = Windows, name = Administrator, domain/group = <domain/group of DR client>, client = <DR client>
Type = Windows, name = SYSTEM, domain/group = NT AUTHORITY, client = <DR client>

在 Linux 客户机中:
Type = UNIX, name = root, Unix group = root, client = <DR client>

以下限制适用：

- 增强型自动灾难恢复 (EADR) 和一键式灾难恢复 (OBDR) 仅在 Linux 系统上可用。
- 必须在 Linux 系统上创建 Linux 系统的 DR ISO 映像。不可以在其他系统（Windows 系统、HP-UX 系统、Solaris 系统）上创建 DR ISO 映像。该限制不适用于更新 SRD 文件或其他任务。
- 如果某个装载点名为 CONFIGURATION 且包含目录 SystemRecoveryData ，则不会备份目录 SystemRecoveryData 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID，从而导致灾难恢复失败。
- 不支持自定义内核安装或配置，仅支持随分发提供的原始内核。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 。但是，如果您手动更新现有的备份规范，则系统将不会设置这一排除。要成功备份，请排除 /opt/omni/bin/drim/log 和 /opt/omni/bin/drim/tmp 文件夹。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：
  - fio-status – 列出所有 Fusion IO 磁盘的状态。
  - fio-format [path] – 执行 Fusion IO 磁盘的低级格式化。
  - fio-attach [path] – 将 Fusion IO 磁盘连接到系统。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs（多种 btrfs raid 配置），因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 /etc/fstab 文件。需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。这同样适用于 GRUB 配置，因此请避免 UUID。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

> **注意**
>
> Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。父对象与其快照之间的整体写时复制 (COW) 关系会丢失。因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 /etc/fstab 文件中的 subvolid（请参阅《btrfs 文档》）装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 subvolid 不需要与备份期间的相同。尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

> **注意**
>
> 使用 fstab 中的 subvol 选项而不是 subvolid。

- 不支持使用基于以太网的光纤通道 (FCoE) LUN 和基于以太网的光纤通道 (FCoE) SAN 引导对系统执行 EADR。
- 连接有外部 USB 驱动器的系统支持备份和恢复。但 USB 驱动器上的数据无法备份或恢复。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。

完成以下步骤：

1. 为增强的自动灾难恢复做准备
2. 准备灾难恢复 CD
3. 恢复 Cell Manager 和客户机系统
4. 还原用户数据。

为增强的自动灾难恢复做的准备（Windows 和 Linux）

要做好准备而使灾难恢复成功，请遵照与所有灾难恢复方法的常规准备过程相关的说明，然后再执行本主题中列出的步骤。必须提前准备，以便快速高效地执行灾难恢复。应特别注意 Cell Manager 的灾难恢复准备。

> **重要说明**请在灾难发生之前准备灾难恢复。

在选择此灾难恢复方法前，请考虑以下要求和限制：

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。
- 在 Windows Server 2008 及更高版本中，至少有一个卷必须为 NTFS 卷。
- 用于灾难恢复的所有必要数据的备份可能需要大量可用空间。通常 500 MB 便足够，最高可能需要 1 GB，具体取决于操作系统。
- 如果可引导 USB 设备连接到 Windows 客户机，则 CONFIGURATION 对象的备份可能会失败。定义 omnirc 选项 OB2_USE_SYSTEM_BOOT_VOL=1 以将系统卷设置为引导卷。
- 在 DR OS 映像创建期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- 确保已启用自动装载功能。自动装载功能可确保所有卷（没有装载点）都处于联机状态。如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- 在群集环境中，如果每个群集节点上的总线地址枚举相同，则可以成功备份群集节点。这表示需要：
  - 群集节点主板硬件相同
  - 两个节点上的 OS 版本（Service Pack 和更新）相同
  - 总线控制器的数量和类型相同
  - 必须在相同的 PCI 主板插槽中插入总线控制器。
- 在备份时应当激活操作系统。否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Server 2008 和更高发布的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包 (ADK): Data Protector 将检查 WAIK/ADK 版本，如果没有适当的版本可用，将中止映像创建。
  - **Windows 7、Windows Server 2008 和 2008 R2**
    - 适用于 Windows Server 2008 R2 SP1 的 Windows 自动安装工具包 (AIK) 补充
  - **Windows 8 和 8.1、Windows Server 2012 和 2012 R2**
    - Windows 8.1 更新的评估和部署工具包 (ADK)，版本 1.1
  - **Windows 10、Windows Server 2016**
    - Windows 10 的评估和部署工具包 (ADK)，版本 1703
  - **Windows 10、Windows Server 2019**
    - Windows 10 的评估和部署工具包 (ADK)，版本 1809
    - Windows PE ADK 加载项，版本 1809

- 对于从可引导 USB 设备进行的灾难恢复，请确保：
  - USB 存储设备的大小应至少为 1 GB
  - 目标系统支持从 USB 设备引导。较旧的系统可能需要更新 BIOS，否则可能完全无法从 USB 存储设备启动。
- 要为 Windows Server 2008 和更高版本的 Windows 系统创建可引导网络映像，必须满足以下条件:
  - 在目标系统上，已启用网络适配器以通过 PXE 协议进行通信。此系统的 BIOS 应与 PXE 协议兼容。
  - 已经在 Windows Server 2008 和更高版本的 Windows 系统上安装并配置 Windows 部署服务 (WDS) 服务器。WDS 服务器必须为 Active Directory 域的成员或 Active Directory 域的域控制器。
  - 具有活动范围的 DNS 服务器和 DHCP 服务器正在网络中运行。
- 要备份位于 Windows Server 2008 和更高版本上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。
- 在为 Linux 客户机创建恢复 ISO 映像的过程中，恢复介质创建主机必须安装 **squashfs 工具**和 **mkisofs**，才能成功创建恢复 ISO 映像。

以下限制适用：

- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 您可以在所有受支持的 Windows 平台上创建可引导 USB 驱动器
- 仅可在 Windows Server 2008 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows Server 2008 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 不支持 Windows Server 2012 存储空间。
- 请勿选择属于检查点重新启动备份会话的备份对象版本。
- 选择对象复制作为恢复源时，需遵守以下规则：
  - 只能选择完整备份对象的副本用于恢复。
  - 仅在从卷的列表中创建卷恢复集时才能选择对象副本。不支持会话。
  - 不支持介质副本。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。
- 在脱机还原期间，稀疏文件将还原为其完整大小。这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs（多种 btrfs raid 配置），因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 /etc/fstab 文件。需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。这同样适用于 GRUB 配置，因此避免用于 root 设备的 UUID，并按名称更换设备。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

  > **注意**
  >
  > Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。父对象与其快照之间的整体写时复制 (COW) 关系会丢失。因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 /etc/fstab 文件中的 subvolid（请参阅《btrfs 文档》）装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 subvolid 不需要与备份期间的相同。尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

  > **注意**

使用 fstab 中的 subvol 选项而不是 subvolid。

磁盘和分区配置

- 不支持动态磁盘（包括从 Windows NT 升级而来的镜像集）。
- 驻留在 Windows 群集中的共享动态磁盘不支持 EADR。
- 如果系统保留卷驻留在动态磁盘上，在 Data Protector GUI 中，卷不由黄色图标指示，而是指示为绿色图标。
- 通过动态磁盘执行灾难恢复时，在启动 EADR 之前需要清除所有磁盘。
- EADR 会话之后，将重新创建所有卷，但只有恢复范围内的卷能够还原。
- 新磁盘的大小必须等于或大于崩溃的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12（包括 EISA）和 0xFE 的供应商特有分区。
- 恢复使用 Intelligent Provisioning 工具 (1.4 和 1.5 版本) 部署的操作系统可能会由于错误的 MBR 分区信息而失败。注意: 这可能属于产品声明。
- 稀疏文件被还原为其完整大小。这可能会导致目标卷空间用尽。
- 不支持物理磁盘不完全属于存储池的存储空间配置。

常规准备

1. 执行完整的客户机系统备份。建议备份整个客户机，如若不然，您至少需要选择以下关键卷和对象：

   - 引导和系统卷
   - Data Protector 安装卷
   - CONFIGURATION 对象所在的卷
   - Active Directory 数据库卷（如果使用 Active Directory 控制器）
   - 仲裁卷（如果使用 Microsoft 群集服务器）

   在客户机完整备份期间，恢复集和 P1S 文件存储在备份介质上和（恢复集可选）Cell Manager 上。

   注意事项：

   ***Windows Server 2008 及更高版本*:**

   - 请确保同时备份存在的系统卷。
   - 可以通过使用 VSS 写入程序的磁盘映像备份来备份逻辑卷。VSS 磁盘映像备份可确保卷在备份过程中保持未锁定状态，并可由其他应用程序访问。必须使用常规文件系统备份来备份 IDB 和 CONFIGURATION 对象以及未装载的卷或作为 NTFS 文件夹装载的卷。

   ***Windows Server 2012 及更高版本*:**

   - 使用磁盘映像备份在以下情况下备份卷:
     - 重复卷

       在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。磁盘映像还原会保持卷的大小。
     - 使用复原文件系统 (ReFS) 的卷

   ***Microsoft 群集服务器*:**

   - 一致的备份包括 (在相同的备份会话中):
     - 所有节点
     - 管理虚拟服务器（由管理员定义）
     - 如果将 Data Protector 配置为群集感知应用程序，则包括 Cell Manager 虚拟服务器和 IDB。

     以上各项应包含在相同的备份会话中。
   - *群集共享卷：*执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。

     必须卸载虚拟硬盘 (VHD) 以确保一致性。
   - 执行备份之后，在 MSCS 中合并所有节点的 P1S 文件，以使每个节点的 P1S 文件都包含关于共享群集卷配置的信息。

     如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。如果要恢复 Cell Manager 或如果无法与 Cell Manager 建立连接，则需要该密钥。

   ***Windows Server 2008 和更高版本的 Windows Server 上的 Active Directory*:**

   - 如果您的 Windows Server 是 Active Directory 大小超过 512 MB 的域控制器，则需要修改客户机备份的备份规范: 在源页中，展开 CONFIGURATION 对象，并清除 ActiveDirectoryService 和 SYSVOL 项的复选框。

     > **注意**
     >
     > Active Directory 和 SYSVOL 将仍作为系统卷（C:\）备份的一部分进行备份。默认情况下，它们分别位于 C:\Windows\NTDS 和 C:\Windows\SYSVOL。

2. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复:

   ```
   omnicc –secure_comm –configure_for_dr <hostname_of_client_being_recovered> -overwrite
   ```

3. 联机恢复客户机之后，在 Cell Manager 上运行以下命令:

   omnicc –secure_comm –configure_peer <client_host_name>

4. 灾难发生之后，使用 EADR 向导将 DR 映像转换为灾难恢复 CD ISO 映像。

   ***Windows Server 2008 及更高版本*:** 或者使用 DR OS 映像代替灾难恢复 CD，创建可启动网络映像或可启动 USB 驱动器。

5. 使用支持 ISO9660 格式的任何 CD 录制工具在 CD 上录制灾难恢复 CD ISO 映像。此灾难恢复 CD 随后可用于引导目标系统并自动还原关键卷。

6. 执行灾难恢复测试计划。

7. 在 Windows 系统上，如果在启动后某些服务或驱动程序无法运行，则可能需要手动编辑 kb.cfg 文件。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备。

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：

  omnicc –secure_comm –configure_for_dr <cell_manager_hostname>

- 恢复完成之后，在介质主机上运行以下命令：

  omnicc –secure_comm –configure_peer <cell_manager_hostname>

- 定期备份 IDB。IDB 会话不应早于文件系统会话。
- 在安全位置（而非在 Cell Manager 上）存储 Cell Manager 的 SRD 文件。
- 提前为 Cell Manager 准备灾难恢复操作系统映像。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv（Windows 系统）或 /var/opt/omni/server/export/keys/DR-ClientName-keys.csv（UNIX 系统），其中 ClientName 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

将恢复集保存到 Cell Manager

在进行完整客户机备份期间，恢复集打包在单个大型文件中，并存储在备份介质上和（可选）Cell Manager 上。如果计划在 Cell Manager 上录制灾难恢复 CD，则将恢复集文件保存到 Cell Manager 会很有用，这是因为从硬盘获取恢复集比从备份介质还原要快得多。

如果在备份期间将恢复集保存到 Cell Manager，则系统会将其保存到默认的 Data Protector P1S 文件位置。

要更改默认位置，请指定一个新的全局选项 EADRImagePath = valid_path（例如 EADRImagePath = /home/images 或 EADRImagePath = C:\temp）。

请参阅《Data Protector 帮助》索引: “全局选项, 修改”。

> **提示**如果在目标目录中没有足够的可用磁盘空间，则可以创建装载点（Windows 系统）或另一个卷的链接（UNIX 系统）。

将备份规范中所有客户机的恢复集文件保存到 Cell Manager

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。
4. 在"结果区域"中，单击**选项**。
5. 在**文件系统选项**下，单击**高级**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Server 2008 及更高版本:** 在 **WinFS 选项**页中，选择**检测 NTFS 硬链接**，选中**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

   “WinFS 选项”选项卡

将备份规范中特定客户机的恢复集文件保存到 Cell Manager

要仅为备份规范中的特定客户机复制恢复集文件，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范 (创建该备份规范 - 如果尚未执行此操作)。
4. 在"结果区域"中，单击**备份对象摘要**。
5. 选择要将其恢复集文件存储在 Cell Manager 上的客户机，并单击**属性**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Server 2008 及更高版本:** 在 **WinFS 选项**页中，选中**检测 NTFS 硬链接**和**使用卷影复制**选项并清除**允许回退**选项。请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

准备 DR OS 映像

灾难发生之前，应准备一个要录制在灾难恢复 CD 上或保存到可引导 USB 驱动器的 DR OS 映像，它随后可用于增强的自动灾难恢复。或者，也可以准备可引导的网络映像。

请注意，必须在将准备 DR OS 映像的系统上安装 Data Protector 自动灾难恢复组件。

每次硬件、软件或配置更改之后都必须根据新的恢复集准备好一个新的灾难恢复 OS 映像。

为必须首先恢复的任何关键系统提前准备 DR OS 映像，尤其是网络正常工作所需的系统（DNS 服务器、域控制器、网关等）、Cell Manager、介质代理客户机和文件服务器等。

建议对含有 OS 映像的备份介质和灾难恢复 CD 或 USB 驱动器的访问权限进行限制。

完成以下步骤：

1. 在 Data Protector 上下文列表中，单击“还原”。
2. 在“范围窗格”中，单击**任务**，然后单击**灾难恢复**以启动灾难恢复向导。
3. 在结果区域中，从**要恢复的主机**下拉列表中选择要为其准备 DR OS 映像的客户机，然后单击**验证**以验证该客户机。

   > **注意**
   >
   > 经过验证的客户机将添加到**要恢复的主机**下拉列表中。

4. 在**恢复介质创建主机**下拉列表中，选择要在其上准备 DR OS 映像的客户机。默认设置下，该客户机与为其准备 DR OS 映像的客户机一样。您在其上准备 DR OS 映像的客户机必须安装有相同 OS 类型（Windows、Linux），并且必须已安装“磁带客户机”。
5. 使**增强的自动灾难恢复**保持选中状态，并选择要从备份会话还是从卷列表构建卷恢复集。默认情况下，选择**备份会话**。

   单击“下一步”。
6. 具体取决于所选的恢复集构建方法：

   - 如果选择了备份会话，则应选择主机备份会话；如果是 Cell Manager，则选择 IDB 会话。
   - 如果选择了“卷”列表，则应为每个关键对象选择相应的对象版本。

   单击“下一步”。
7. 选择恢复集文件的位置。默认情况下，**从备份还原恢复集文件**处于选中状态。

   如果在备份期间已在 Cell Manager 上保存了恢复集文件，则应选择**指向恢复集文件的路径**并指定其位置。单击“下一步”。
8. 选择映像格式。可用的选项如下：

   - **创建可引导的 ISO 映像**: DR ISO 映像 (默认情况下为 recovery.iso)
   - **创建可引导 USB 驱动器**：可引导 USB 驱动器上的 DR OS 映像
   - **创建可引导的网络映像**: 可用于网络引导的 DR OS 映像 (默认情况下为 recovery.wim)
9. 如果创建的是可引导 ISO 映像或可引导网络映像，请选择要将创建的映像放置到的目标目录。

   如果要创建可引导的 USB 驱动器，请选择要在其中放置所创建的映像的目标 USB 驱动器或磁盘编号。

   > **重要说明**
   >
   > 在创建可引导的 USB 驱动器时，该驱动器上存储的所有数据将丢失。

10. 也可选择设置密码来防止对 DR OS 映像进行未授权的使用。锁图标指示是否设置了密码。

    单击**密码**打开“密码保护映像”对话框并输入密码。要删除密码，清除字段内容即可。
11. **Windows Server 2008 及更高版本**:

    查看并修改（如果需要）插入 DR OS 映像中的驱动程序的列表。

可以使用此选项将缺少的驱动程序添加到 DR OS 中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

> **重要说明**
>
> 在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要插入 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

12. 单击**完成**以退出向导并创建 DR OS 映像。
13. 如果要创建可引导的 CD 或 DVD，可使用支持 ISO9660 格式的刻录工具，将 ISO 映像刻录在 CD 或 DVD 上。

使用 EADR 恢复 Linux 系统

只有在完成所有准备步骤后，才能成功执行 Linux 系统的增强型自动灾难恢复。如果要恢复 Cell Manager，将先从内部数据库的备份映像将该内部数据库还原，然后从卷和 CONFIGURATION 对象的备份映像将卷和 CONFIGURATION 对象还原。

以下先决条件适用:

- 需要用新硬盘更换受影响的磁盘。
- 您应当具有要恢复的整个系统的有效完整文件系统备份（客户机备份）。
- 为了对 Cell Manager 进行灾难恢复，您应当具备有效的“内部数据库”备份映像，它应当比文件系统备份映像新。
- 需要灾难恢复 CD。

完成以下步骤：

阶段 1

阶段 3

1. 除非要执行脱机灾难恢复操作，否则向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector admin 帐户:

   > **注意**
   >
   > 灾难恢复过程只能由 root 用户执行。

   - 类型： root
   - 组\域: root
   - 客户机：正在恢复的系统的临时主机名

     在恢复阶段 1 期间向系统分配临时主机名。您可以在恢复阶段 2 之前切换到另一个 shell 检索该主机名，然后运行 hostname 命令。

   添加用户帐户
2. 从原始系统的灾难恢复 CD 引导客户机系统。
3. 显示以下消息时按 **Enter**：按 Enter，以便从恢复 CD 引导。
4. 首先将 DR OS 加载到内存中，然后显示范围菜单。选择恢复范围。有四种不同的恢复范围和两个其他选项：
   - Reboot：不执行灾难恢复，但重新启动计算机。
   - Default Recovery：恢复 /boot 和 / (根) 卷，以及 Data Protector 安装及配置文件所在的所有卷 (/opt、 /etc 和 /var)。所有其他磁盘均未进行分区和格式化，可在阶段 3 中使用。
   - Minimal Recovery：仅恢复 /boot 和 / (根) 卷。
   - Full Recovery：恢复所有卷，而非仅恢复关键卷。
   - Show Recovery Scope [Yes]：加载“恢复范围”屏幕。
   - Run shell：运行 Linux shell。可以将其用于高级配置或恢复任务。
5. **阶段 2**
6. 此时将显示灾难恢复向导。要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。要继续执行灾难恢复，选择**继续进行还原**。

   > **注意**请确保 Cell Manager 和介质 (备份) 主机可访问。否则，可能需要修改 NIC 和 MAC 地址。

7. 如果灾难恢复备份经过加密，并且您要恢复 Cell Manager 或无法访问 Cell Manager 的客户机，则将显示以下提示：

   Do you want to use AES key file for decryption [y/n]?

   按 **y**。

   确保客户机上存在密钥库（DR-ClientName-keys.csv）（例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器），并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。

8. 如果 SRD 文件中的信息并非最新（例如，因为灾难之后更改了备份设备），并且要执行脱机恢复，则应在继续此过程之前编辑 SRD 文件。
9. 在联机恢复期间更改备份设备需要使用 omnidbutil -changebdev 命令。识别用于还原的备份会话和当前使用的备份设备。可使用 GUI 或 omnidb -session <SessionID> -detail 完成此操作。然后使用 omnidbutil -changebdev FromDev ToDev -session SessionID 替换旧设备。在 EADR 期间将自动使用新设备。
10. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。

    请注意，Data Protector 将首先尝试执行联机还原。如果联机还原因任何原因而失败（如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager），则 Data Protector 将尝试执行远程脱机恢复。甚至如果远程脱机还原失败（例如，因为介质代理主机仅接受来自 Cell Manager 的请求），则 Data Protector 也将执行本地脱机还原。

11. 删除步骤 1 中从 Cell Manager 上 Data Protector admin 用户组创建的客户机的本地 Data Protector 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。
12. 如果要恢复 Cell Manager，则要使 IDB 一致。
13. 使用标准还原过程还原用户和应用程序数据。
14. 如果要执行群集中所有节点的灾难恢复，则需要其他步骤。

恢复后

灾难恢复完成后，使用以下命令重新生成证书：

- 在客户机上： omnicc -secure_comm -regenerate_cert [Hostname]
- 在 Cell Manager 上： omnicc -secure_comm -configure_peer {Hostname1 HostName2 ...]} [-accept_host]

相关任务

- 创建备份规范
- 备份磁盘映像
- 将完整 DR 映像保存到 Cell Manager
- 合并 MS 群集的 P1S 文件

为一键式灾难恢复做的准备（Windows 和 Unix）

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。提前准备，以便快速高效地执行灾难恢复。

重要说明请在灾难发生之前准备灾难恢复。

准备步骤

完成灾难恢复的常规准备之后，执行以下特定步骤以准备 OBDR。

1. 按照**不可追加**介质使用策略和**宽松**介质分配策略 (因为备份介质在 OBDR 备份期间进行格式化) 为 DDS 或 LTO 介质创建介质池。此外，将此介质池指定为 OBDR 设备的默认介质池。只有此类池中的介质可用于 OBDR。
2. 在要允许使用 OBDR 进行恢复的系统上本地执行 OBDR 备份。

   注意事项

   ***Windows Server 2008 及更高版本*:** 请确保备份所存在的系统卷（例如引导卷）。

   ***Windows Server 2012 (R2)*:** 使用磁盘映像备份在以下情况下备份卷:

   - 重复卷

     在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。磁盘映像还原会保持卷的大小。
   - 使用复原文件系统 (ReFS) 的卷

   ***Microsoft 群集服务器*:** 一致的备份包括 (在相同的备份会话中):

   - 所有节点
   - 管理虚拟服务器（由管理员定义）
   - 如果将 Data Protector 配置为群集感知应用程序，则为客户机系统的虚拟服务器。

   要使用 OBDR 方法在 MSCS 上自动还原所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点，以使共享磁盘卷在 OBDR 备份期间不会由另一个节点锁定。也就是说无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

   ***群集共享卷*:** 执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。必须在单独的设备上执行备份，因为只有在不可追加介质上才可以执行 OBDR 备份。

   必须卸载虚拟硬盘 (VHD) 以确保一致性。

   如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。如果无法建立和 Cell Manager 之间的连接，您将需要密钥。
3. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复：

   ```
   omnicc –secure_comm –configure_for_dr <hostname_of_client_being_recovered>
   ```
4. 联机恢复客户机之后，在 Cell Manager 上运行以下命令:

   ```
   omnicc –secure_comm –configure_peer <client_host_name> -overwrite
   ```
5. 执行灾难恢复测试计划。
6. 在 Windows 系统上，如果在系统启动后某些服务或驱动程序无法运行，则可能必须手动编辑 kb.cfg 文件。

编辑 kb.cfg 文件

kb.cfg 文件位于 Data_Protector_home\bin\drim\config 目录中，用于存储 %SystemRoot% 目录中的驱动程序文件位置的相关信息。此文件的用途是提供一种灵活的方法，使 Data Protector 可以在 DR OS 中包括驱动程序（和其他需要的文件），以使系统采用与引导相关的特定硬件或应用程序配置。默认 kb.cfg 文件已包含行业标准硬件配置所需的所有文件。

例如，某些驱动程序的功能分散到多个单独的文件中，驱动程序需要所有这些文件才能正常工作。有时，如果未在 kb.cfg 文件中逐个列出所有驱

动程序文件，则 Data Protector 无法识别这些驱动程序文件。在这种情况下，DR OS 中将不包括这些驱动程序文件。使用 kb.cfg 文件的默认版本创建和执行测试计划。如果 DR OS 无法正常不引导或无法访问网络，则可能需要修改此文件。

如果要备份这些驱动程序，则以适当的格式将相关文件的信息添加至 kb.cfg 文件，如 kb.cfg 文件开头的说明所述。编辑文件的最简单方式是复制和粘贴现有行，并将其替换为相关信息。

请注意，路径分隔符为 "/" (正斜杠)。忽略空格，但引号中的路径名除外，因此相关条目可分散在多行中。还可以添加开头为 "#" (磅) 符号的注释行。

编辑完 kb.cfg 文件之后，将其保存到原始位置。然后，执行另一个客户机完整备份，将添加的文件包含在恢复集中。

重要说明由于系统硬件和应用程序的配置任务繁重，因此无法为所有可能的配置提供“即用型”解决方案。因此可以修改此文件以包括驱动程序或其他文件，风险自担。

警告建议创建并执行测试计划，以确保编辑 kb.cfg 文件之后灾难恢复可正常运行。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv (Windows 系统) 或 /var/opt/omni/server/export/keys/DR-ClientName-keys.csv (UNIX 系统)，其中 ClientName 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

创建一键式灾难恢复的备份规范

必须创建一键式灾难恢复 (OBDR) 备份规范，才能准备好 OBDR 引导磁带。

以下先决条件适用:

- 添加 OBDR 设备前，为 DDS 或 LTO 介质创建一个采用不可追加介质使用策略和宽松介质分配策略的介质池。必须选择所创建的该介质池作为 OBDR 设备的默认介质池。
- 此设备必须在本地连接到要允许使用 OBDR 进行恢复的系统。
- 在要允许使用 OBDR 方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复和用户界面组件。
- 必须在要允许使用 OBDR 进行恢复的系统上本地创建备份规范。

提示为了能够使用 OBDR 方法自动还原 MS 群集中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。实际上无法收集足够的信息为由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。

此备份规范属一键式灾难恢复方法所独有。默认情况下，会将必需卷备份为文件系统。但是，在 Windows Server 2008 及更高版本中，可选择通过 VSS 写入程序将逻辑卷备份为磁盘映像。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。要将逻辑卷备份为磁盘映

像，必须修改为 OBDR 创建的备份规范。

创建 OBDR 的备份规范

完成以下步骤：

1. 在 Data Protector 上下文列表中，单击“备份”。
2. 在范围窗格中，单击**任务**，然后单击**一键式灾难恢复向导**。
3. 在“结果区域”中，从下拉列表中选择要为其执行 OBDR 备份（在客户机上本地）的客户机，然后单击**下一步**。
4. 此时已选择需要备份的关键卷。单击“下一步”。

   > **重要说明**重要卷由系统自动选择，并无法取消选择。选择要保留的任何其他分区，因为在恢复过程中 Data Protector 将从系统中删除所有分区。

5. 选择要用于备份的本地设备或驱动器。只能选择一个设备或驱动器。单击“下一步”。
6. **Windows Server 2008 或更高版本:**

   查看并修改（如果需要）插入 DR OS 映像中的驱动程序的列表。

   可以使用此选项将缺少的驱动程序添加到 DR ISO 映像中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

   （可选）选择备份选项。

   > **重要说明**在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要添加 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

   Linux：选择备份选项。

   单击“下一步”。
7. （可选）安排备份。单击“下一步”。
8. 在“备份摘要”页中，查看备份规范设置，然后单击**下一步**。

   无法更改以前选择的备份设备或备份规范相互之间的先后顺序。仅可删除 OBDR 非必需备份对象，并且只能查看常规对象属性。也可以更改备份对象说明。
9. 将经过修改的备份规范保存为 OBDR 备份规范，以使其成为原始的一键式灾难恢复格式。(可选) 可使用“保存并计划”选项计划备份。
10. 1. 单击“启动备份”以交互方式运行备份。此时将显示“启动备份”对话框。单击“确定”开始备份。

       如果备份为加密备份，则 omnisrdupdate 实用程序将自动导出加密 ID，此操作作为 post-exec 命令执行。

系统的可引导映像文件（包含安装和配置临时 DR OS 所需的所有信息）将写在磁带的开头，以使其可引导。

> **重要说明**每次硬件、软件或配置更改之后执行新的备份并准备好可引导的备份介质。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

修改 OBDR 备份规范以使用磁盘映像备份

完成以下步骤：

1. 在范围窗格中，单击已创建的 OBDR 备份规范。当系统询问您是否要将其视为 OBDR 备份规范或视为普通的备份规范，单击**否**。

   > **注意**当将一个 OBDR 备份规范保存为普通备份规范之后，该备份规范仍然可以用于 OBDR。

2. 在“备份对象摘要”页面中，选择要将其备份为磁盘映像的逻辑卷，然后单击**删除**。

   > **注意**只能备份逻辑卷。应使用文件系统备份来对配置对象、未装载或装载为 NTFS 文件夹的卷执行备份。

3. 单击“手动添加”以打开向导。
4. 在“选择备份对象”页中，单击**磁盘映像对象**选项，然后单击**下一步**。
5. 在“常规选择”页中，选择要用磁盘映像进行备份的客户机，并提供相应的描述信息。单击“下一步”。

   > **注意**对于每个磁盘映像对象，描述信息必须是唯一的。使用一个描述性名称，例如 [Disk Image C] for C: volume。

6. 在“常规对象选项”属性页中，将数据保护设置为**无**。单击“下一步”。

   > **注意**当将数据保护功能设置为**无**时，磁带内容可由更新的 OBDR 备份覆盖。

7. 在“高级对象选项”属性页中，可以指定磁盘映像对象的高级备份选项。单击“下一步”。
8. 在“磁盘映像对象选项”属性页中，指定磁盘映像中要备份的部分。使用以下格式：

   \\.\DriveLetter: ，例如： \\.\E:

   > **注意**当卷的名称被指定为驱动器号时，不会在备份过程中锁定该卷。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

9. 单击**完成**退出向导。
10. 在“备份对象摘要”页中，检查备份规范的摘要。指定为磁盘映像的逻辑卷应属于“磁盘映像”类型。单击“应用”。

使用 OBDR 恢复 Linux 系统

只有在完成所有准备步骤后，才能成功执行 Linux 系统的一键式灾难恢复 (OBDR)。

以下先决条件适用:

- 需要用新硬盘更换受影响的磁盘。
- 应有一个可引导 OBDR 备份介质，其中含有要恢复的客户机的所有关键对象。必须在客户机上本地执行 OBDR 备份。
- 需要一个在本地连接到目标系统的 OBDR 设备。

完成以下步骤：

阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，向 Cell Manager 上的 admin 用户组添加具有以下属性的 admin 帐户:
   - 开始还原
   - 还原到其他客户机
   - 作为 root 还原

   > **注意**灾难恢复过程只能由 root 用户执行。

2. 将包含映像文件和备份数据的磁带插入 OBDR 设备中。
3. 关闭目标系统，并关闭磁带设备的电源。
4. 打开目标系统的电源，并在其初始化时，按磁带设备上的“弹出”按钮，并打开该设备的电源。
5. 首先将 DR OS 加载到内存中，然后显示范围菜单。选择恢复范围。有四种不同的恢复范围和两个其他选项：
   - Reboot：不执行灾难恢复，但重新启动计算机。
   - Default Recovery：恢复 /boot 和 / (根) 卷，以及安装和配置所在的所有卷 (/opt 、 /etc 和 /var)。所有其他磁盘均未进行分区和格式化，可在阶段 3 中使用。
   - Minimal Recovery：仅恢复 /boot 和 / (根) 卷。
   - Full Recovery：恢复所有卷，而非仅恢复关键卷。
   - Full with Shared Volumes：恢复所有卷，包括在备份时锁定的共享卷。
   - Run shell：运行 Linux shell。可以将其用于高级配置或恢复任务。

   阶段 2

6. 此时将显示灾难恢复向导。要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。选择“继续进行还原”以继续执行灾难恢复操作。
7. 如果灾难恢复备份已加密，并且要恢复其 Cell Manager 无法访问的客户机，将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库 (DR-ClientName-keys.csv)（例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器），并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。

8. 如果 SRD 文件中的信息并非最新（例如因为灾难之后更改了备份设备），并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
9. 然后， 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。

   请注意，将首先尝试执行联机还原。如果联机还原因任何原因而失败 (如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager)，则将尝试执行远程脱机恢复。如果远程脱机还原失败（如因为介质代理主机仅接受来自 Cell Manager 的请求），则 将执行本地脱机还原。

10. 从 Cell Manager 上的 admin 用户组中删除在第 1 步创建的客户机本地帐户，除非灾难恢复之前 Cell Manager 上已存在该帐户。

    阶段 3

11. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤（例如编辑 SRD 文件）。
12. 使用标准还原过程还原用户和应用程序数据。

维护安装

本主题描述了修改备份环境配置的常用步骤。查看下列各节以了解以下信息:

Data Protector 维护模式

在 Cell Manager 上执行维护任务期间，应阻止对内部数据库进行写入操作，需要 Data Protector 进入维护模式。此类任务包含升级 Data Protector 安装、安装补丁和重要修补程序、升级硬件或操作系统。在本章中，只有特定的步骤需要使用维护模式。但事实上，维护模式同样适用于整个文档在其他部分描述的任务。

进入维护模式过程可自动启动一系列任务，例如停止调度程序、重命名备份规范目录、中止正在运行的进程和释放锁定的资源。单个单元、MoM 和群集环境中支持维护模式。

启动维护模式

维护模式可以由具有管理权限的用户通过命令行界面进行启动。要启动维护模式，请执行以下命令：

- 在单个单元中：
  omnisv -maintenance GracefulTime
- 在 MoM 环境中：
  omnisv -maintenance -mom

Cell Manager 指示运行会话一次全部停止，同时 MoM 环境中的单元逐一进入维护模式。

要自定义 Cell Manager 进入维护模式的方式，请修改相应的全局选项。 MaintenanceModeGracefulTime 选项反映了留给 Data Protector 服务中止正在运行的会话的秒数，而 MaintenanceModeShutdownTime 选项则反映了等待会话中止所需要的秒数。两个选项的默认值均为 300。如果使用 GracefulTime 选项，则它将覆盖 MaintenanceModeGracefulTime 全局选项。如果在执行此选项后恢复会话仍在运行，则维护模式初始化失败。

如果 MoM 环境中任何单元未能进入维护模式，模式会恢复。

要检查 Data Protector 是否以维护模式运行，请通过执行 omnisv -status 或检查 GUI 状态栏来查看 CRS 服务状态。请注意，GUI 只有连接到 Cell Manager 时才能可靠地显示维护模式，这有时可能会导致即使在 Cell Manager 切换回正常模式后状态栏上依旧显示维护模式。

在维护模式期间，Cell Manager 拒绝所有将数据写入内部数据库的操作，例如创建新设备、备份和还原会话或其预览、清除、复制和合并会话。

在群集环境中，维护模式处于活动状态时只能执行手动群集的相关活动，例如关闭群集包、停止 Data Protector 服务，或者手动装载卷。

维护模式处于活动状态时允许所有只读 IDB 操作。Data Protector 服务均已启动并正在运行。当 Cell Manager 处于维护模式时，只有具有管理 Data Protector 用户权限的用户可以连接到单元或 MoM。

退出维护模式

要使用 CLI 退出 Cell Manager 上的维护模式，请执行:

- 在单个单元中：
  omnisv -maintenance -stop
- 在 MoM 环境中：
  omnisv -maintenance -mom_stop

处于 MoM 环境中时，单个单元不能退出维护模式。只能从 MoM 服务器调用 MoM 维护。

要使用 GUI 退出维护模式，请执行以下操作：

- 在“上下文列表”中，选择**客户机**。
- 在“操作”菜单中，单击“停止维护模式”

恢复正常模式后，您可以重新启动中止的会话。要运行中止后的会话，请执行以下操作：

1. 在“上下文列表”中，单击**内部数据库**。
2. 在“范围窗格”中，展开“会话”
3. 右键单击会话，然后从上下文菜单中选择**重新启动失败的对象 (Restart Failed Objects)**

拒绝的会话只能在默认 Data Protector 日志文件目录中的 maintenance.log 文件中记录，因此无法重新启动。

以下两个示例显示了已中止和拒绝会话的 maintenance.log 条目：

```
10.5.2013 10:52:45 OMNISV.2492.9936 ["/cli/omnisv/omnisv.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2 会话已中止 - 宽限期已过期! 会话 ID: 2013/05/10-8 会话类型: 0 datalist: large_backup 开始日期: 2013-05-10 10:52:45 所有者: JOHN.JOHNSON@company.com 10.5.2013 10:48:45 CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":142] X.99.01 b2 CRS 处于维护模式 - 会话已被拒绝 会话 ID: R-2013/05/10-200 会话类型: dbsm 会话描述: 数据库 开始日期: 2013-05-10 10:48:45 所有者: .@ pid=0
```

将群集感知客户机导入到单元

在群集感知客户机上本地安装 Data Protector 软件后，将代表“群集感知”客户机的虚拟服务器导入到 Data Protector 单元。

先决条件

- 将 Data Protector 安装在所有群集节点上。
- 所有群集包必须正在群集内运行。

Microsoft 群集服务器

要将 Microsoft 群集服务器客户机导入到 Data Protector 单元，请完成以下步骤:

1. 在 Data Protector 中，切换到“客户机”上下文。
2. 在范围窗格中，右键单击 **MS 群集**，然后单击**导入群集**。
3. 键入代表要导入的群集客户机的虚拟服务器的名称，或浏览网络以选择虚拟服务器。
   Data Protector 允许基于虚拟服务器的 IP 地址或主机名导入客户机群集。如果在使用 IP 地址导入客户机群集的过程中出现任何问题，请在导入期间使用虚拟服务器的主机名。
4. 单击“下一步”。
5. 单击**完成 (Finish)** 以导入群集客户机。
6. 为导入的客户机设置用户帐户。请参阅配置用户。

提示:要导入特定的群集节点或虚拟服务器，请在“范围窗格”中右键单击其群集并单击“导入群集节点”或“导入群集虚拟服务器”。

其他群集

要将 **Serviceguard** 或 **Veritas** 群集客户机导入到 Data Protector 单元，请完成以下步骤:

1. 在 Data Protector Manager 中，切换到客户机 上下文。
2. 在“范围窗格”中，右键单击“客户机”然后单击“导入客户机”。
3. 键入虚拟服务器的主机名（如应用程序群集包中所指定），或浏览网络以选择要导入的虚拟服务器（仅限 Windows GUI 中）。
   选择**虚拟主机**选项指明这是一个群集虚拟服务器。
4. 单击**完成 (Finish)** 以导入虚拟服务器。
5. 为导入的客户机设置用户帐户。请参阅配置用户。

提示要在群集节点的本地磁盘上配置数据备份，需要导入代表 Data Protector 客户机的群集节点。

从单元导出客户机

从 Data Protector 单元导出客户机意味着从 Cell Manager 上的 IDB 中删除其引用，而不从客户机卸载软件。这可以使用 Data Protector GUI 来完成。

如果您要执行以下操作，则可以使用导出功能：

1. 要将客户机移动到其他单元
2. 要从不再属于网络一部分的 Data Protector 单元配置中删除客户机
3. 希望解决有关许可的问题
   通过从单元导出客户机，许可证将对其他某个系统可用。

先决条件

在导出客户机前，请检查以下内容：

- 客户机的所有实例都已从备份规范中删除。否则，Data Protector 将尝试备份未知的客户机，而此部分备份规范将会失败。
- 客户机没有已连接和配置的备份设备或磁盘列阵。导出系统后，Data Protector 不再能够使用原单元中的备份设备或磁盘列阵。

导出客户机

使用 Data Protector GUI 导出客户机

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，单击“客户机”，右键单击要导出的客户机系统，然后单击“删除”。
3. 此时会询问您是否要同时卸载 Data Protector 软件。单击“否”以导出客户机，然后单击“完成”。

客户机将从“结果区域”的列表中删除。

注意: 如果 Cell Manager 安装在与要导出的客户机相同的系统上，则无法导出或删除 Data Protector 客户机。但是，可以从仅安装了客户机和安装服务器的系统中导出客户机。在这种情况下，安装服务器也从单元中删除。

Microsoft Cluster Server 客户机

从 Data Protector 单元导出 Microsoft 群集服务器客户机

Microsoft Cluster Server 客户机

从 Data Protector 单元导出 Microsoft 群集服务器客户机

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开“MS 群集”，右键单击要导出的群集客户机，然后单击“删除”。
3. 此时会询问您是否要同时卸载 Data Protector 软件。单击**否 (No)** 仅导出群集客户机。
   群集客户机将从“结果区域”的列表中删除。

提示：要导出特定的群集节点或虚拟服务器，请在“范围窗格”中右键单击群集节点或虚拟服务器并单击“删除”。

用户验证和 LDAP

应在企业用户管理基础设施中结合将 Data Protector 作为企业系统进行身份验证和授权的功能。此连接允许向企业用户目录中配置的用户和组授予访问 Data Protector 用户界面的权限。

将在安全连接上执行用户身份验证，并将轻型目录访问协议 (LDAP) 用作基础技术。因此，用户可以使用其企业凭据访问 Data Protector 服务，而不需要维护单独的密码。此外，可以在企业目录中将管理员或操作员保留为组，从而符合已建立的授权和审批流程。

使用 Java 身份验证和授权服务 (JAAS) 登录模块在 Data Protector 嵌入式应用程序服务器 (AppServer) 的安全域中配置 LDAP 集成。可选的 LDAP 登录模块可提供 LDAP 身份验证和授权服务，可将这些服务通过必需的 Data Protector 登录模块映射到 Data Protector 权限。如果未配置 LDAP 集成，Data Protector 将按照以前版本中的流程运行。

Data Protector 使用登录模块堆栈中的登录模块对用户进行身份验证。当用户使用 Data Protector GUI 连接到 Cell Manager 时，用户身份验证将由以下登录模块执行:

1. LDAP 登录模块：对照现有 LDAP 服务器对用户凭据进行身份验证，例如用户名和密码。请参阅配置 LDAP 登录模块。
2. Data Protector 登录模块：对照 Data Protector 用户列表和 Web 访问密码对用户凭据进行身份验证。请参阅向 LDAP 用户授予权限。
3. 执行 LDAP 初始化和配置所需的所有步骤后，还可以检查配置。请参阅检查 LDAP 配置。
4. (可选) 将配置从不安全的 LDAP 修改为 LDAPS。请参阅安全地配置 LDAP。

> **注意**
>
> 当在 Data Protector 中将用户或客户机配置为允许其以典型方式访问 CLI 时，Data Protector GUI 不使用 LDAP 功能，且将不显示登录对话框。

配置 LDAP 登录模块

要配置 LDAP，需要满足以下先决条件:

- Cell Manager (AppServer) 必须能够与 LDAP 服务器通信 (通过端口 389/TCP (对于 LDAP) 或通过端口 636/TCP (对于 LDAPS))。
- 当配置 LDAPS 时，强烈建议首先配置并测试 LDAP。这可以作为 Data Protector GUI 配置过程的一部分来完成。
- LDAP 用户必须分配到 Data Protector 用户组 (直接分配或使用 LDAP 组) 并配置登录名 (userPrincipalName 属性，例如 user@testlab.net)。

> **注意**
>
> - 在 MoM 环境中配置 LDAP 登录模块时，请确保在每个 Cell Manager 上执行上述步骤。MoM 环境中的每个 Cell Manager 需具有相同的 LDAP 登录模块配置。
> - 从 Data Protector 10.04 (和更早版本) 升级到它时，可能需要重新创建 LDAP 配置。

要配置 LDAP 登录模块，请执行以下步骤:

1. 在上下文菜单中，单击“用户”，然后在“操作”菜单下选择“LDAP 配置”。

   将显示“LDAP 配置”窗口，其中包含现有 LDAP 配置信息。如果未配置 LDAP，则可以配置新的 LDAP 服务器。

2. 指定或编辑以下字段的值:

名称	描述	值
供应商	LDAP 服务器供应商	将 LDAP 服务器供应商指定为 ActiveDirectory。
名称	LDAP 配置名称	指定 LDAP 配置的名称。
LDAP 服务器	LDAP 服务器主机名或 IP 地址	指定 LDAP 服务器主机名或 IP 地址。
LDAP 端口	LDAP 服务器上的端口	指定 LDAP 服务器要使用的端口号。默认端口号为 389。在 GUI 中不配置 LDAPS。在最后一步完成所需的更改。
用户 DN	用户所在的 LDAP 树的完整 DN。此 DN 为 LDAP 用户的父项。	指定含有用户的 LDAP 树的 DN。例如：CN=Users,DC=mytestlab,DC=net 。
绑定 DN	用于与 LDAP 服务器初始绑定的用户	指定 LDAP 用户的 DN，以供 Keycloak 用于访问 LDAP 服务器。例如：CN=bindDN,CN=Users,DC=mytestlab,DC=net 。
绑定凭据	绑定 DN 用户的密码	指定绑定 LDAP 用户的密码。
测试连接	测试 LDAP 服务器连接	检查是否可以使用指定的服务器主机名/IP 地址和端口号连接到 LDAP 服务器。
测试身份验证	测试 LDAP 服务器身份验证	检查是否可以使用指定的“绑定 DN”和“绑定凭据”连接到 LDAP 服务器。**注意:** 如果已配置 LDAPS，则失败。如果需要，可以从 Keycloak 执行测试。

3. 单击“添加”以新建 LDAP 配置，或单击“修改”以确认对现有配置的更改。

删除 LDAP 配置

要删除现有 LDAP 配置，请执行以下步骤:

1. 在上下文菜单中，单击“用户”，然后在“操作”菜单下选择“LDAP 配置”。

   将显示“LDAP 配置”窗口，其中包含现有 LDAP 配置信息。

2. 单击“删除配置”以删除现有 LDAP 配置。在出现提示时确认。

向 LDAP 用户授予权限

只有获授 Data Protector 权限的 LDAP 用户才能连接到 Cell Manager。配置 LDAP 登录模块后，可以向 LDAP 用户/组授予所需的 Data Protector 权限。

要授予 Data Protector 权限，请执行以下步骤:

1. 启动 Data Protector GUI，然后向 LDAP 用户授予 Data Protector 权限。
2. 向 Data Protector 用户组添加 LDAP 用户。
3. 使用 LDAP 凭据登录。

向 Data Protector 用户组添加 LDAP 用户

要将 LDAP 用户添加至 Data Protector 用户组，请执行以下操作:

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开“用户”，然后右键单击要添加 LDAP 用户的用户组。
3. 单击**添加/删除用户**打开向导。
4. 在“添加/删除用户”对话框的“手动”选项卡中，提供以下详细信息:
   - **类型**：选择 LDAP。
   - 当将“LDAP 用户”添加为“实体”时，以用户主体名称格式指定“名称”，例如 username@mytestlab.net 。
   - 当将“LDAP 组”添加为“实体”时，以判别名称格式指定“名称”，例如 CN=DPAdmin,OU=DPLocal,OU=Groups,DC=mytestlab,DC=net 。
   - **描述**: 此项可选。
5. 单击**完成**退出向导。

使用 LDAP 凭据登录

要使用 LDAP 凭据登录，请执行以下步骤：

1. 启动 Data Protector GUI 并连接至 Cell Manager。仅对于未配置进行基于典型 Data Protector 的身份验证的用户，才会显示登录对话框。
2. 在 LDAP 身份验证屏幕上提供 LDAP 凭据以访问 Data Protector。LDAP 用户可以属于任何可用的 Data Protector 用户组。

检查 LDAP 配置

以下过程讲解如何检查是否为特定 LDAP 用户或组正确设置了用户权限，方法是从 Web 浏览器中查询 Data Protector 登录提供程序服务 getDpAcl 。

要获取指定用户的 Data Protector 访问控制列表 (ACL)，请执行以下步骤：

1. 使用浏览器连接 Data Protector 登录提供程序 Web 服务。
2. 浏览器可能会提示您接受服务器证书。单击**接受**确认请求。
3. 将显示一个对话框，提示您提供登录凭据。提供之前使用 Data Protector 配置的有效 LDAP 用户名和密码。
4. 浏览器将返回以下访问控制列表 (ACL)： https://<server>:7116/dp-loginprovider/restws/dp-acl
5. 使用此 ACL 检查分配权限与为对应 Data Protector 用户组指定的 Data Protector 用户权限是否匹配。

安全地配置 LDAP

要安全地配置 LDAP，请按照下列步骤操作:

1. 从 LDAP 服务器导入 SSL 证书。
2. 将不安全的 LDAP 身份验证重新配置为 LDAPS。

注意**:** 使用 LDAP 组配置的用户不会在 Data Protector GUI 中列出。由于 LDAP 配置是直接通过 Keycloak 完成的，用户会在 Keycloak 数据库中自动同步，因此不会在“用户” 上下文中单独列出。

从 LDAP 服务器导入 SSL 证书

1. 使用 Cell Manager 上的 openssl s_client -connect <LDAP Server>:636 从 LDAP 服务器获取 SSL 证书。
2. 创建临时证书文件 C:\Temp\ldap_cert.pem 或 /tmp/ldap_cert.pem ，然后复制步骤 1 中 BEGIN CERTIFICATE 到 END CERTIFICATE 之间的行。
3. 从 Cell Manager 上的 javax.net.ssl.trustStore 获取信任库的位置，并从 standalone.xml 中的 javax.net.ssl.trustStorePassword 值获取密码。可以在 Windows 的 %DP_SDATA_DIR%Config\Server\AppServer\standalone.xml 和 Linux Cell Manager 的 /etc/opt/omni/server/AppServer/standalone.xml 中找到。
4. 使用步骤 3 中的值将您在步骤 1 中生成的 LDAP 服务器证书导入到 AppServer 信任库中。该命令位于 Windows 的 "%DP_HOME_DIR%jre\bin\keytool" -importcert -keystore "trustStoreLocation" -alias "ldap" -file C:\Temp\ldap_cert.pem -storepass trustStorePassword 和 Linux Cell Manager 的 /opt/omni/jre/bin/keytool -importcert -keystore trustStoreLocation -alias "ldap" -file /tmp/ldap_cert.pem -storepass trustStorePassword 中。
5. 使用 omnisv -restart 重新启动 Data Protector AppServer hpdp-as 或 Data Protector 服务。

将 LDAP 身份验证重新配置为 LDAPS

1. 如果 DpKeycloakUser 的密码未知，请运行以下命令重置该密码：omniusers -resetpass -name DpKeycloakUser -pass Password_123
2. 在浏览器 https://localhost:7116/auth/admin/DataProtector/console 中打开 Keycloak 管理控制台，然后修改 LDAP 的设置以使用 LDAPS。使用步骤 1 中的以下登录凭据连接 Keycloak 控制台。
3. 修改 LDAP 属性:
    1. 单击“用户联合”，在已配置的 **Ldap** 提供程序上选择“编辑”
    2. 将“连接 URL” 从 http 修改为 https，并将端口从 389 更改为 636，然后使用“测试连接”按钮验证证书是否已加载且服务器有所响应。
    3. “保存”设置。
4. 重新启动 Data Protector AppServer。

证书生成实用程序

X.509 证书生成实用程序 (omnigencert.pl) 可生成证书颁发机构 (CA) 和服务器证书。它负责执行以下任务：

- 设置单级 root CA
- 生成 CA 和服务器证书
- 创建用于存储密钥、证书、配置和密钥库文件所需的目录结构
- 在 CM 上的预定义位置中存储所生成的证书
- 生成 Web 服务角色的属性文件

仅管理员用户 (Windows) 和 root 用户 (UNIX) 可运行 omnigencert.pl 实用程序。

将 omnigencert.pl 实用程序以脚本形式开发，并随 Cell Manager (CM) 安装套件一起安装。作为 CM 安装过程的一部分，首先运行此脚本，然后生成证书并将其存储在预定义的位置。

omnigencert.pl 脚本存在于以下位置：

- Windows： %Data_Protector_home%\bin
- UNIX： /opt/omni/sbin

如果需要，Data Protector 管理员可在安装后随时运行此实用程序，以使用新的密钥对或 CA 安装重新生成证书。但是，并非必须对基于证书的身份验证过程使用由此实用程序生成的证书。您可以改为使用现有的 CA 安装，以生成所需的证书。

语法

作为 Cell Manager 安装过程的一部分，此实用程序最初由安装程序执行，并生成所需证书并将其存储到预定义的位置。

此实用程序仅限管理员使用，并用于通过使用新密钥对（即使包括新 CA 安装）重新生成证书。Windows 平台上的“管理员”用户和 UNIX 平台上的 "root" 用户可执行此脚本。

omnigencert.pl 脚本存在于以下位置：

- Windows： %Data_Protector_home%\bin
- Unix： /opt/omni/sbin

可使用以下语法和选项运行 omnigencert.pl 实用程序: **使用情况**

```
[-no_ca_setup] [-server_id ServerIdentityName] [-store_password KeystorePassword] [-cert_expire CertificateExpireInDays] [-ca_dn CertificateAuthorityDistinguishedName] [-server_dn ServerDistinguishedName] [-server_san]
```

omnigencert.pl 实用程序支持多个选项，在生成证书的同时提供灵活性。如果未指定选项，此实用程序将使用默认值生成证书。

omnigencert.pl 实用程序支持以下选项：

选项	描述
-no_ca_setup	为现有 CA 安装生成服务器证书。如果 CA 安装不存在，则此选项无效。
-server_id	指定服务器证书的判别名称 (DN) 部分中的公用名称 (CN) 实体的值。此选项的默认值是 CM 完全限定的域名 (FQDN)。
-store_password	定义密钥库或信任库 (在其中保存服务器证书，包括其密钥) 的密码。如果未提供此选项，将使用默认密码创建库。
-cert_expire	定义所生成的证书的有效期限（以天为单位）。此选项的默认值为 8760 天（24 年）。
-ca_dn	定义 CA 的 DN 字符串。DN 格式如下所示：“CN=<value>, O=<value>, ST=<value>, C=<value>” CN = 公用名称，O= 组织名称，ST= 州名称，C= 国家名称。O、ST 和 C 参数的默认值如下所示：CN = CA <CM 服务器的 FDQN 名称> O = HEWLETT-PACKARD ST = CA C= US

-server_dn	定义服务器证书的 DN 字符串。DN 格式如下所示：“CN=<value>, O=<value>, ST=<value>, C=<value>” CN = 公用名称，O= 组织名称，ST= 州名称，C= 国家名称。O、ST 和 C 参数的默认值如下所示：CN = <CM 服务器的 FDQN 名称> O = HEWLETT-PACKARD ST = CA C= US
-server_san	指定服务器证书中的使用者替代名称 (SAN)。但是，在 Cell Manager 安装期间生成的服务器证书在 SAN 部分中具有 DNS 类型的条目。这些 SAN 条目将基于 Cell Manager 中的可用 IP 数量自动生成。要覆盖服务器证书中默认情况下自动生成的 SAN 条目，请在使用证书生成实用程序生成证书时指定该选项。 支持 DNS 和 IP 类型的 SAN 条目。 此选项的值格式如下所示： santype:value,santype:value 每个 SAN 条目由逗号 (",") 分隔，且包括两个部分：1) SAN 类型，2) SAN 类型的值。 **示例：** dns:iwf1112056.dprdn.hpe.com , dns:iwf1113456.dprnd.hpe.com ip:15.218.1.100, ip:15.218.1.200, ip:15.218.1.155 dns:iwf1112056.dprnd.hpe.com, ip:15.218.1.100

注意: 此实用程序不支持以下选项组合：

- -server_id 和 -server_dn
- -no_ca_setup 和 -ca_dn。

示例

以下各节列出了用于在 Windows 和 UNIX 上运行 omnigencert.pl 实用程序的示例命令。

omnigencert.pl 脚本存在于以下位置：

- Windows： %Data_Protector_home%\bin
- Unix： /opt/omni/sbin

Windows 和 UNIX 命令

任务	Windows 命令	

使用默认值设置 CA 并生成 CA 和服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl	/opt/
使用指定的公用名称值设置 CA 并生成 CA 和服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id	/opt/
使用指定的存储密码设置 CA 并生成 CA 和服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -store_password	/opt/
使用指定的证书有效期限设置 CA 并生成 CA 和服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -cert_expire	/opt/
通过默认值生成将使用现有 CA 安装(在安装过程中创建)的服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup	/opt/
使用指定的 DN 设置 CA 并生成 CA 和服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -ca_dn -server_dn	/opt/
使用指定的 DN 和现有 CA 设置生成服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn	/opt/
使用 SG-CLUSTER 环境中的现有 CA 证书生成服务器证书	1。从文件 <DP_DATA_DIR>\Config\Server\AppServer\standalone.xml 中的属性 keystore-password 检索现有密码。 2。从以下目录检索 **PGOSUSER** 值: \server\idb\idb.config。 3.使用如下所示的群集虚拟系统名称运行 omnigencert.pl 实用程序: %Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -store_password existing_keystor_passwd	1。从 2。从 **PGO** 值: /etc/ 3.使用 /opt/ store
在 SG-CLUSTER 环境中生成 CA 和服务器证书	1。从文件 <DP_DATA_DIR>\Config\Server\AppServer\standalone.xml 中的属性 keystore-password 检索现有密码。 2。从以下目录检索 **PGOSUSER** 值: \server\idb\idb.config。 3.使用如下所示的群集虚拟系统名称运行 omnigencert.pl 实用程序: %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id cm_virtual_name.domain.com -store_password existing_keystor_passwd	1。从 2。从 **PGO** 值: /etc/ 3.使用 omni 实用程 /opt/ exist

为特定的 Cell Manager 服务器生成含 DNS 类型的 SAN 条目的服务器证书。	%Data_Protector_home%\bin\ perl.exe omnigencert.pl -no_ca_setup -server_dn iwf11160123.dprnd.hpe.com -server_san "dns:iwf11160123.dprnd.hpe.com,dns:iwf11160123.dp.hpe.com"	/opt/ /perl "dns
为 特定的 Cell Manager 服务器生成含 IP 类型的 SAN 条目的服务器证书。	%Data_Protector_home% \bin\perl.exe omnigencert.pl -no_ca_setup-server_dn 15.218.1.100 -server_san “ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125,ip:15.218.1.116”	/opt/ "ip:1
为特定的 Cell Manager 服务器生成含 DNS 和 IP 类型的 SAN 条目的服务器证书	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn iwf111206.dprnd.hpe.com -server_san"dns:iwf111206.dprnd.hpe.com,iwf111206.hpe.com,ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125, ip:15.218.1.116"	/opt/ _san "dns

目录结构

以下部分列出了用于存储证书的目录。

Windows 目录	Unix 目录	描述
ProgramData\Omniback\Config\Server\certificates	/etc/opt/omni/server/certificates	包含 CA 证书文件，cacert.pem ，其中包含 CA 公钥。
ProgramData\Omniback\Config\Server\certificates\ca	/etc/opt/omni/server/certificates /ca	包含 CA 功能所需的配置、输入和其他文件。
ProgramData\Omniback\Config\Server\certificates\ca\keys	/etc/opt/omni/server/certificates /ca/keys	包含 CA 私钥文件，cakey.pem。
ProgramData\Omniback\Config \Server\certificates\server	/etc/opt/omni/server/certificates /server	包含两种类型的库：密钥库和信任库。这些库由 Java 实用程序和密钥工具创建，用于保护服务器证书及其密钥。这些库通过库密码进行保护。包括以下库： ca.truststore server.keystore server.truststore
ProgramData\Omniback\Config\Server\AppServer	/etc/opt/omni/server/AppServer	包含由此实用程序创建的属性文件。除以下属性文件外，此目录还包括其他一些文件： • jce-webservice-roles.properties • dp-webservice-roles.properties

覆盖现有的证书

要用由现有 CA 安装生成的证书覆盖现有证书 (在 CM 安装期间由实用程序生成)，可使用以下选项之一:

- 覆盖现有密钥库和信任库文件中的证书
- 通过新建密钥库和信任库文件覆盖证书

重新生成证书或使用新证书后，必须重新启动 CM 上的 Data Protector 服务。必须在执行任何将使用证书的操作前完成此步骤，因为重新启动此服务将确保新证书生效。

覆盖现有密钥库和信任库文件中的证书

要覆盖现有密钥库和信任库文件中的证书，请完成以下任务：

- 替换现有服务器库文件
- 替换 CA 证书

替换现有服务器库文件

要替换现有服务器库文件，请继续执行以下步骤:

1. 从 standalone.xml 文件中的属性 keystore-password 检索现有密码。
   Windows
   - <DP_DATA_DIR>\Config\Server\AppServer\standalone.xml

   UNIX
   - /etc/opt/omni/server/AppServer/standalone.xml
2. 从现有服务器库文件中删除所有条目，这些文件位于:
   - Windows： ProgramFiles\Omniback\bin\jre
   - UNIX： /opt/omni/jre/lib/security
3. 使用 Java 密钥工具实用程序将生成的证书导入以下库：
   - 将服务器和 CA 证书导入 server.keystore
   - 将 CA 证书导入 server.truststore
   - 将 CA 证书导入到 jre\cacerst 密钥库 (默认密码必须为 **changeit**)

替换 CA 证书 要替换现有的 CA 证书，请继续执行以下步骤:

1. 请注意现有 CA 证书文件 cacert.pem 的权限，该文件位于:
   - Windows： ProgramData\Omniback\Config\Server\certificates
   - UNIX： /etc/opt/omni/server/certificates
2. 用生成的 CA 证书替换现有的 CA 证书文件 cacert.pem。

通过新建密钥库和信任库文件覆盖证书

要覆盖新密钥库和信任库文件中的证书，请完成以下任务：

- 替换现有服务器库文件
- 替换 CA 证书
- 使用库密码更新配置文件

注意: 必须为服务器库保留密码。

替换现有服务器库文件

要替换现有服务器库文件，请继续执行以下步骤:

1. 请注意现有 cacerts 存储文件的权限，该文件位于:
   - Windows： ProgramFiles\Omniback\bin\jre
   - UNIX： /opt/omni/jre/lib/security
2. 删除服务器库文件。
3. 创建具有相同文件名和权限的库。
4. 使用 Java 密钥工具实用程序将生成的证书导入以下库：
   - 将服务器和 CA 证书导入 server.keystore
   - 将 CA 证书导入 server.truststore
   - 将 CA 证书导入 ca.truststore
   - 将 CA 证书导入到 jre\cacerst 密钥库 (默认密码必须为 **changeit**)

Java 密钥工具实用程序位于:

- Windows： Program Files\Omniback\jre\bin
- UNIX： /opt/omni/jre/bin

替换 CA 证书

要替换 CA 证书，请执行以下步骤：

1. 请注意现有 CA 证书文件 cacert.pem 的权限，该文件位于：

- Windows： ProgramData\Omniback\Config\Server\certificates
- UNIX： /etc/opt/omni/server/certificates

1. 将现有 CA 证书文件 cacert.pem 替换为生成的 CA 证书。

使用库密码更新配置文件

要使用库密码更新配置文件，请执行以下步骤：注意: 只有在使用新密码创建了新库的情况下才需要执行此任务。

1. 使用创建 server.keystore 文件时使用的密钥库密码来更新 standalone.xml 配置文件。配置文件位于：**Windows**
   - ProgramData\OmniBack\Config\server\AppServer\standalone.xml
     UNIX
   - /etc/opt/omni/server/AppServer/standalone.xml
2. 在 standalone.xml 文件中，更新密钥库密码 (以粗体突出显示):
   <ssl>
   <keystore path="C:/ProgramData/OmniBack/Config/server/certificates/server/server.keystore" keystore-password="i5hLm57oFFwfw"/>
   </ssl>

管理 Data Protector 补丁

Data Protector 补丁通过支持服务提供，可从支持网站下载。

验证已安装哪些 Data Protector 补丁

您可以在单元中的系统上验证已安装哪些 Data Protector补丁。要在单元中的特定系统上验证已安装哪些 Data Protector 补丁，请使用 Data Protector GUI 或 CLI。

> 注意**:** 安装站点特定的补丁后，它将始终列在补丁报告中，即使以后的补丁已包括该补丁。

先决条件

- 要使用这个功能，应安装用户界面组件。

限制

- 补丁验证只能在同一单元的系统上检查已安装哪些补丁。

使用 GUI 验证 Data Protector 补丁

使用 Data Protector GUI 验证特定客户机上已安装哪些补丁

1. 在“上下文”列表中，选择“客户机”
2. 在“范围窗格 (Scoping Pane)”中，展开**客户机 (Clients)** 并选择单元中要验证已安装补丁的系统。
3. 在“结果区域”中，单击“补丁”打开“安装的补丁”窗口。
   如果在系统中找到了补丁，则验证返回每个补丁的级别和说明以及安装的补丁数。
   如果系统上没有 Data Protector 补丁，则验证将返回一个空列表。
   如果验证的系统不是单元的成员、不可用或发生错误，则验证将报告错误消息。
4. 单击**确定**关闭窗口。

使用 CLI 验证 Data Protector 补丁

要使用 Data Protector CLI 验证特定客户机上安装了哪些补丁，请执行 omnicheck -patches -host hostname 命令，其中 hostname 是要验证的系统的名称。

有关更多 omnicheck 命令的信息，请参见 omnicheck 手册页。

Data Protector 所需的补丁

有关 Data Protector 补丁，请参阅 https://softwaresupport.softwaregrp.com 了解最新信息。

Windows 系统补丁

对于运行 Windows 的系统，请联系 Microsoft Corporation 了解最新的 Microsoft Windows Service Pack。

HP-UX 系统补丁

有关运行 HP-UX 操作系统的系统补丁，请参见 http://h20565.www2.hpe.com/portal/site/hpsc 了解最新信息，或与响应中心联系以了解当前的补丁号。在寻求支持前，请先安装最新的补丁。列出的补丁可以由更新的补丁所替代。

建议定期安装适用于 HP-UX 的 Extension Software Package。其中涵盖了许多建议的补丁，下面列出的是其中一部分。请联系 Micro Focus 支持人员，了解当前版本的 HP-UX Extension Software Package。

HP-UX 11.31

Data Protector 需要以下 HP-UX 11.31 单个补丁：

补丁名称	硬件平台	描述
PHCO_38050	Itanium	pthread 库累计补丁
PHKL_38055	Itanium	调度程序累计补丁
PHSS_41179	Itanium	连接器和 fdp 累计补丁

SUSE Linux Enterprise Server 系统补丁

使用推荐的最新系统补丁，由 SUSE 提供。

Red Hat Enterprise Linux 系统补丁

使用推荐的最新系统补丁，由 Red Hat 提供。

其他受支持平台的补丁

使用推荐的由相关供应商提供的最新系统补丁。

安装补丁

Cell Manager 补丁可以本地安装。但是，修补客户机需要安装服务器。安装服务器安装补丁后，即可远程修补客户机。

> 注意**: 重要说明:** 在使用 Cell Manager (CS) 补丁修补 Cell Manager 之前，需使用 omnisv 命令停止 Data Protector 服务，然后在完成修复过程后重新启动。

要验证系统上安装的补丁类型，可以使用 Data Protector GUI 或 CLI。

在 Symantec Veritas Cluster Server 中配置的 Cell Manager 上安装补丁

为 Cell Manager 组件安装补丁（CS 补丁）时，必须先在每个节点本地应用该补丁。在 Symantec Veritas Cluster Server 上为群集感知的 Cell Manager 执行的修补程序类似于升级，但有以下例外:

- 必须跳过配置步骤。(即，不得执行 omniforsg.ksh。)
- 在补丁安装之前，不得启动 Data Protector 服务。

在本地安装好补丁后（如果需要），非 Cell Manager 组件和核心组件必须从已修补的安装服务器推动升级。这也是非群集感知 Cell Manager 的常规补丁安装程序。

管理站点特定补丁和热修复

站点特定补丁 (SSP) 和热修复 (HF) 将手动应用于受影响的客户机或 Cell Manager。

准备用于远程安装 SSP 或 HF 的安装服务器

Data Protector SSP 或 HF 包由支持提供。必须将 SSP 或 HF 包复制到位于以下位置的安装服务器仓库：

UNIX:/opt/omni/databases/vendor/ssphf

Windows：Data_Protector_program_data\depot\ssphf (例如: C:\ProgramData\Omniback\depot\ssphf)

注意: 修补程序以 ZIP 文件的方式提供。在安装服务器上使用 SSP 或 HF 之前，必须对这些文件进行解压缩。对于 Windows，可以将提取的 zip 文件复制到 Data_Protector_program_data\depot\ssphf。对于 Linux/UNIX，在将 SSP 或 HF 复制到安装服务器之后，必须在 Linux/UNIX 上对提取的 tar.gz 文件进行解压缩（使用 gzip）。安装服务器上预期的 SSP 或 HF 格式对于 Windows 系统为 ZIP，对于 Linux/UNIX 系统为 TAR。

要检查安装服务器上可用于远程安装的 SSP/HF 包，请执行以下操作：

- 在“上下文”列表中，选择“客户机”。
- 在“范围 (Scoping)”窗格中，展开**安装服务器 (Installation Servers)** 并选择单元中要进行 SSP/HF 推送安装的目标系统。
- 在“结果 (Results)”区域中，单击 **SSP 和 HF (SSPs and HFs)...** 打开 SSP/HF 弹出窗口。如果在系统中找到了 SSP/HF，则需要查看安装服务器上的 SSP/HF ID 和 SSP/HF 数量。
- 单击**确定**关闭窗口。

在客户机上安装站点特定补丁或热修复

在将 SSP/HF 包复制到安装服务器后，可以使用 Data Protector GUI 中提供的 SSP/HF 选择列表来选择用于安装的 SSP/HF。如果选择了 SSP/HF，则所有其他 Data Protector 组件将被禁止选中，因为一次只能安装一个 SSP/HF 包。SSP/HF 可提供各种 Data Protector 组件的二进制文件，只有已安装的 Data Protector 组件的二进制文件才会应用于系统。但由于所有适用的二进制文件都会应用于系统，因此 SSP/HF 包的状态仍显示为已安装。

注意: 也可以在 MoM-GUI 中进行 SSP/HF 包的远程安装。

SSP/HF 包的远程安装指的是在远程系统上部署 SSP/HF 包，提取包，并将适用的二进制文件复制到其目标位置。这样，它就不会处理替换在使用文件所需的特殊过程。

要在客户机上手动安装 SSP/HF，请执行以下操作：

- 将 SSP/HF 存档包复制到目标主机并进行提取。
- 停止 Data Protector 服务。只能停止受影响的服务或进程。
- 按以下方式应用 SSP/HF 二进制文件：
  - 将文件从提取的 SSP/HF 包复制到适用的目标位置。（仅复制为其安装 Data Protector 组件的文件）。
  - 将 CII_<SSPHFNAME> 复制到其相应的位置。
    例如：
    Windows：Data_Protector_program_data\config\Client\ssphf
    其他平台：\etc\opt\omni\client\ssphf

此外，还可以使用 ob2install 命令在客户机上安装 SSP/HF。有关 ob2install 命令的详细信息，请参阅 ob2install 手册页。

多数情况下，需要手动安装 SSP/HF 包，其中提供了所列的一些二进制文件:

- 单元服务器二进制文件 - 尤其是服务和会话管理器二进制文件。
- CORE 二进制文件 - Windows：Inet 服务二进制文件和编目消息。例如 OmniInet.exe、OmniEnu.dll 等等。
- GUI 二进制文件 - 当在需要应用此类 SSP/HF 的主机上使用 Data Protector GUI 时。

注意: 将禁止把组件添加到正在 MS 群集服务器上运行的群集感知的 Cell Manager，因为这样无法远程安装 SSP/HF，而必须手动将其应用于所有适用的群集节点。

恢复被 SSP/HF 替换的二进制文件

在远程安装 SSP/HF 二进制文件期间，当前文件进行备份并留在系统上供以后使用。

例如，

Windows：Data_Protector_program_data\tmp\ssphf\<SSPHFNAME>\<日期时间>

其他平台：/var/opt/omni/tmp/ssphf/<SSPHFNAME>/<DATE_TIME>。（确切的位置取决于平台）。

要恢复被 SSP/HF 推送安装替换的二进制文件，请考虑以下方法之一:

- 手动恢复已备份的二进制文件。
- 将受影响的组件重新安装到系统。（首选方法）
- 从 Data Protector GUI 升级系统。（客户机上下文）
- 从 Data Protector 安装向导执行修复操作。（仅适用于 Windows 系统）
- 安装任何其他 SSP/HF 包，其中包含了正在打包的作为将要替换的旧 SSP/HF 一部分的所有二进制文件。

每个 SSP/HF 推送操作都会在以下位置创建自己的日志，该日志可用于对失败的操作进行故障诊断:

Windows：Data_Protector_program_data\log\ssphf_install_<日期时间>.log **Unix:** /var/opt/omni/log/ssphf_install_<PID>.log (确切的位置取决于平台)

验证已安装的 SSP 或 HF

可以使用 Data Protector GUI 或 CLI 验证在单元中的系统上安装了哪些 Data Protector 站点特定补丁或热修复。

注意: 成功安装 SSP/HF 后，SSP 和 HF 将安装状态显示为“已安装”。在失败的情况下，将会恢复二进制文件，并且不列出此类 SSP/HF 的状态。

SSP/HF 的远程安装仅安装已在目标主机上安装的组件的二进制文件。SSP/HF 包可能显示以下状态之一:

- 已安装 - 已复制在系统上安装的 Data Protector 组件的所有 SSP/HF 二进制文件。
- 部分 - 未安装 SSP/HF 包中对应已在系统上安装的 Data Protector 组件的少量二进制文件。由于两种原因可能发生这种情况：

1. 如果安装了完整的 SSP/HF 包，SSP/HF 将被标记为“已安装”。但在某个时间点，如果来自原始安装的另一个 SSP/HF 或 Data Protector 组件被推送到系统，覆盖了 SSP/HF 提供的部分二进制文件，则这类包的状态将更改为“已部分安装”。
2. 如果 SSP/HF 包提供了多个 Data Protector 组件 (例如: da 和 ma) 的二进制文件，并且系统上仅安装了少数几个组件 (例如: da)，则将仅在系统上应用已安装组件的二进制文件 (即 da)。这类包的安装状态将显示为“已安装”。稍后，如果在系统上安装了 ma 组件，则该包的状态将变为“已部分安装”。
   注意: 如果 SSP/HF 包安装的所有二进制文件都被其他某些二进制文件替换，则这类 SSP/HF 不再被视为已安装，也不会显示在 SSP/HF 状态列表中。

要查看已更改的 SSP/HF 二进制文件列表，请执行以下操作：

- 使用调试选项运行 Inet 服务。
- 检查已安装的 SSP/HF 包的状态。
- 检查已更改的二进制文件的 Inet 日志。

使用 GUI 验证 SSP 或 HF 包

使用 Data Protector GUI 验证特定客户机上已安装哪些 SSP/HF:

- 在“上下文”列表中，选择“客户机”。
- 在“范围 (Scoping)”窗格中，展开**客户机 (Clients)** 并选择单元中要验证已安装 SSP/HF 的系统。
- 在“结果 (Results)”区域中，单击 **SSP 和 HF (SSPs and HFs)...** 打开 SSP/HF 弹出窗口。如果在系统上找到了 SSP/HF，验证操作将返回 SSP/HF ID 和每个 SSP/HF 的状态以及已安装的 SSP/HF 数量。
- 单击**确定**关闭窗口。

使用 CLI 验证 SSP 或 HF

要使用 Data Protector CLI 验证特定客户机上安装了哪些 SSP/HF，请执行 omnicheck -ssphf -host hostname 命令，其中 hostname 是要验证的系统的名称。

有关更多 omnicheck 命令的信息，请参见 omnicheck 手册页。

向客户机添加组件

This feature is available in the Premium Edition

可以在现有客户机和 Cell Manager 上安装其他 Data Protector 软件组件。组件可以从远程或本地添加。有关本地安装，请参阅更改 Data Protector 软件组件。对应的安装服务器必须可用。

Serviceguard 客户机

在 Serviceguard 群集环境中，请确保要添加组件的节点处于活动状态。

将 Data Protector 软件分发到 Data Protector 单元中的客户机上

1. 在 Data Protector Manager 中，切换到**客户机 (Clients)** 环境。
2. 在“范围窗格 (Scoping Pane)”中，展开“客户机 (Clients)”，右键单击某个客户机，然后单击**添加组件 (Add Components)**。
3. 如果配置了多个安装服务器，则选择要在其上安装组件的客户机的平台 (UNIX 或 Windows) 和要用于安装组件的安装服务器。单击“下一步”。
4. 选择要从中安装组件的客户机。单击“下一步”。
5. 选择要安装的 Data Protector 组件，如“选择组件”中所示。请注意，您只能选择一种介质代理。

如果已选择多个客户机，并且希望在各个客户机上安装不同组件，请单击“为各个客户机分别指定组件”，然后单击“下一步”。单独为每个客户机选择组件。

单击**完成 (Finish)** 开始安装。

更改 Data Protector 软件组件

本节描述了在 Windows、HP-UX、Solaris 和 Linux 系统中删除和添加 Data Protector 软件组件的步骤。

Data Protector 软件组件可在 Cell Manager 或客户机上使用 Data Protector GUI 添加。使用安装服务器功能远程安装选定组件。

Data Protector 组件可在 Cell Manager、安装服务器或客户机本地删除。

在 Windows 系统上

在 Windows 系统上添加或删除 Data Protector 软件组件。

仅当具有相同补丁级别的 Data Protector 安装仓库可用时，方可执行此过程。在某些情况下，需要设置安装仓库的路径，例如: **\\<DP_IS_SYSTEM>\Omniback\x8664**。

1. 在 Windows 控制面板中，单击**添加或删除程序/程序和功能**。
2. 选择 **HPE Data Protector 10.00**，然后单击“更改”。
3. 单击“下一步”。
4. 在“程序维护”窗口中，单击“修改”，然后单击“下一步”。
5. 在“自定义设置”窗口中，选择要添加的组件和/或取消选择要删除的软件组件。单击“下一步”。
6. 单击**安装 (Install)** 开始安装或删除软件组件。
7. 安装完成后，单击“完成”。

群集感知客户机

如果是在群集感知客户机上更改 Data Protector 软件组件，则必须在每个群集节点从安装包本地完成此操作。然后，必须使用 GUI 手动将虚拟服务器主机名导入到 Data Protector 单元中。

在 HP-UX 系统中

要删除组件，请使用 swremove 命令。

要删除 Data Protector 软件组件，请完成以下步骤：

- 以 root 身份登录并运行 swremove 命令。
- 双击“B6960MA, DATA-PROTECTOR”，然后双击“OB2-CM”，以显示 Data Protector 组件的列表。
- 选择要删除的组件。
- 在**操作**菜单中，单击**标记以删除**来标记要删除的组件。
- 标记完要删除的组件后，单击“操作”菜单中的“删除”，然后单击“确定”。

在标记要删除的 Data Protector 组件时，如果剩余组件无法正常操作，则会弹出“依赖性消息对话”框，显示有依赖性的组件列表。

Oracle Server 详情

在 Oracle Server 系统上卸载 Data ProtectorOracle Server 集成后，Oracle Server 软件仍链接到 Data ProtectorDatabase Library。您必须删除此链接，否则删除该集成后将无法启动 Oracle Server。有关详细信息，请参阅“Data Protector 集成”一节。

在 Linux 系统上

可以使用安装服务器功能添加新组件。在 Linux 系统上，某些 Data Protector 组件互相依赖，如果删除某一个，则无法正常操作。下表显示了组件及它们之间的依赖关系。

Linux 上的 Data Protector 软件组件依赖关系

组件	依赖
Cell Manager	
OB2-CC、OB2-DA、OB2-MA 和 OB2-DOCS	OB2-CORE 和 OB2-TS-CORE

OB2-TS-CS, OB2-TS-JRE, OB2-TS-AS, OB2-WS, OB2-JCE-DISPATCHER, OB2-JCE-SERVICEREGISTRY	OB2-CORE、OB2-TS-CORE 和 OB2-CC
安装服务器	
OB2-CORE-IS	OB2-CORE
OB2-CF-P 和 OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	OB2-CORE-IS、OB2-CF-P 和 OB2-TS-CFP
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP、OB2-CORE-IS、OB2-CF-P 和 OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

步骤

要从 Linux 系统中删除 Data Protector 组件，请完成以下步骤:

- 确保已终止所有 Data Protector 会话并退出 GUI。
- 输入命令 rpm | grep OB2 列出安装的所有 Data Protector 组件。
- 以与安装顺序相反的顺序，使用 rpm -e package name 命令删除步骤 2 中提到的组件并按提示继续。

在其他 UNIX 系统上

手动从 UNIX 系统 (而不是 HP-UX 或 Linux) 上的 Data Protector 客户机删除组件时，更新 /usr/omni/bin/install 路径中的 **omni_info** 文件。

对于每个删除的组件，请从 omni_info 文件中删除相关的组件版本字符串。

如果仅从 Data Protector 客户机中删除组件而没有从单元中导出客户机，则需要更新 cell_info 文件中的单元配置 (在 Cell Manager 上)。方法是在安装有单元控制台的单元中的系统上执行以下命令：

```
omnicc -update_host HostName
```

在 Data Protector 10.00 之后的版本中，内部 cell_info 文件的格式有所修改。

多宿主环境中的 **Data Protector**

Data Protector 多宿主环境指连接到多个网络的系统。在这样的环境中，Data Protector 可以使用专用网络进行通信。

配置

如果要将 Data Protector 通信配置为使用专用网络，请执行以下步骤:

1. 使用其备份主机名配置 Cell Manager 系统。有关配置的详细信息，请参考“附录 B:*系统准备和维护任务”中的“更改 Cell Manager”一节*。如果在进行 Cell Manager 全新安装时已配置备份网络，则跳过重新生成证书步骤。默认情况下，会为所有相应的主机名生成证书
2. 使用客户机的备份名导入客户机。

   以前导入的客户机:

   对于以前导入的客户机，可以将它们导出，然后使用备份名将它们导入，也可以在 cell_info 文件中直接编辑主机条目。cell_server 名称也必须与 cell_info 文件一起手动更新。因此，最好使用其备份名导出和导入客户机。

   新安装的客户机:

   对于新安装的客户机，使用其备份主机名导入客户机 (在客户机推送安装期间或稍后在导入操作时定义备份主机名)。

限制

- 如果正在重新配置现有的单元配置，则还应使用新的备份主机名更新受影响的备份规范，因为引入的新备份对象将破坏使用旧的首选主机名执行的备份的还原链。
- 一些安装操作 (如本地安装或群集系统导入) 会使用其首选主机名重新导入受影响的客户机，或仅为首选主机条目更新单元配置。
- 会话中报告的主机名通常反映首选主机名，而不是客户机导入单元时使用的名称。

验证安装

需要检查 Data Protector 软件组件是否在 Cell Manager 或客户机系统中正常运行时，可以使用 Data Protector 图形用户界面验证安装。

先决条件

必须具有适用于客户机系统类型 (UNIX 系统或 Windows 系统) 的安装服务器。

步骤

- 在“上下文列表”中，单击**客户机**。
- 在“范围窗格”中，展开“客户机”，右键单击 Cell Manager 或客户机系统，然后单击“检查安装”以打开向导。
- 此时将列出相同类型（UNIX 系统或 Windows 系统）的所有客户机系统。选择要验证其安装的客户机，然后单击**完成**开始验证。

验证的结果将显示在“检查安装”窗口中。

全局选项

全局选项包括一组用于定义整个 Data Protector 单元的行为的选项。这些选项以纯文本文件形式存储在 Cell Manager 上。

> **注意:** 大多数用户应能够操作 Data Protector，无需更改全局选项。

自定义全局选项

您可以修改现有全局选项的值或添加新选项。要设置 Data Protector 全局选项，请按如下方式编辑 全局文件

1. 使用文本编辑器打开位于 Cell Manager 系统以下位置的 全局选项文件:
   - **Windows**： <PROGRAMDATA>\Config\Server\Options 。
     例如： C:\ProgramData\OmniBack\Config\Server\Options
   - **Linux**： /etc/opt/omni/server/options 。
2. 要激活选项，请删除其名称前的 **#** 标记并设置所需值。
3. 以 Unicode 格式保存文件。

常用全局选项

以下列表包括最常用的全局选项。有关详细信息，请参阅 Cell Manager 系统上的全局选项文件:

全局选项	描述
MaxSessions	指定在单元中可同时运行的 Data Protector 会话（任何类型）的最大数。 默认值： 1000 。
MaxBSessions	指定在单元中可同时运行的 Data Protector 备份会话的最大数。 默认值： 100 。
MaxMAperSM	指定可同时在一个备份、对象复制、对象合并或还原会话中使用的 Data Protector 备份设备的最小数量。 默认值： 100 。
MaxDAperMA	指定 Data Protector 备份、对象复制和对象合并对话的最大磁盘代理并发 (设备并发) 数。 默认值： 32 。
DCDirAllocation	确定用于为新 DC 二进制文件选择 DC（详细编目）目录的算法： Fill in sequence 、 Balance size（默认）、 Balance number 。
MediaView	在介质管理上下文中更改字段及其顺序。
InitOnLoosePolicy	如果使用宽松介质策略，使 Data Protector 能够自动初始化空介质或未知介质。
DailyMaintenanceTime	确定日常维护任务在何时之后可以开始。默认值： 12:00 (中午)。
DailyCheckTime	确定日常检查在何时之后可以开始。默认值： 12:30 P.M. 。还可以禁用日常检查。
SessionStatusWhenNoObjectToCopy 和 SessionStatusWhenNoObjectToConsolidate	如果没有要复制或合并的对象，使您能够控制对象复制和对象整合会话的会话状态。 根据值集标记会话: • **0** 默认 会话标记为失败并显示严重错误。 • 1: 会话标记为成功并显示警告。 • 2: 会话标记为成功并显示正常消息。
SetInitialMediumProtection	确保对新介质的保护。将该值设为 1 ，以防止在不受保护的介质的备份或复制会话期间丢失数据。

DeleteUnprotectedMediaFreq	定义用于运行不受保护的介质删除操作的时间段。值的范围在 0 <= DeleteUnprotectedMediaFreq <= 24 之内。默认值为 1 。根据您希望介质维护发生的频率来编辑此选项的值。 根据设置值执行删除操作: • 0: 对于最小值，不执行操作。 • 1: 每天一次 (00:00)， • 2: 每天两次 (00:00、12:00)， • 3: 每天三次 (00:00、08:00、16:00)， • 4: 每天四次 (00:00、06:00、12:00、18:00)。 • 24: 对于最大值，每小时启动一次操作。 注意: • 对于具有 CMMDB 的 MoM 环境，取决于 CMMDB 服务器上设置的选项值，仅在 CMMDB 服务器上进行介质维护 (删除不受保护的介质)。 • 对于没有 CMMDB (带有 MMDB) 的 MoM 环境，根据每个 Cell Manager 服务器上设置的选项值，对所有 Cell Manager 进行介质维护。
DeleteUnprotectedMediaMinimumAge	确定要供 omnimm -delete_unprotected_media 删除的介质的最小老化程度。如果介质老化程度低于此值 (从创建时开始)，则 omnimm 将跳过它。默认值为 86400 。
IgnoreObjectLocalityForDeviceSelection	确定是否应跳过本地设备的排序和优先化。默认值为 0 。 如果设置为 1 ，则跳过并忽略本地设备的排序和优先化。
SmUseGreedyB2DExpansion	SmUseGreedyB2DExpansion =<会话类型> 使用情况： SmUseGreedyB2DExpansion = BSM（仅为 BSM 启用标志） SmUseGreedyB2DExpansion = RSM（仅为 RSM 启用标志） SmUseGreedyB2DExpansion = BSM,RSM（同时为 BSM 和 RSM 启用标志）

Omnirc 选项

omnirc 选项可用于覆盖仅影响配置这些选项的 Data Protector 客户机的行为的设置。但是，仅当您的操作环境需要并且 Micro Focus 支持人员建议这样做时才使用它们。

对于每个 Data Protector 客户机，在位于如下位置的 **omnirc** 文件中设置 **omnirc** 选项:

- **Windows 系统：** Data_Protector_program_data\OmniBack
- **Linux、HP-UX 和 Solaris:** /opt/omni/.omnirc
- **其他 UNIX 系统:** /usr/omni/.omnirc

如何使用 omnirc 选项？

1. 根据平台的不同，将 omnirc.tmpl 或 .omnirc.TMPL 模板分别复制到 omnirc 或 .omnirc 。

   对于 OpenVMS，将 OMNI$ROOT:OMNIRC.TMPL 复制到 OMNI$ROOT:OMNIRC 。

2. 在编辑模式下打开文件 omnirc 或 .omnirc 。

   > **注意:**在 **omnirc** 文件中为选项名称使用特殊字符时，请考虑使用操作系统支持的字符来设置环境变量。例如，Unix 客户机上的变量不能包含以下任何字符: Space Tab / : * " <> | 。

3. 通过从行中删除 "#" 标记来取消注释包含您要使用的选项的行。 为此选项设置所需的值。
4. 验证文件的权限。例如：在 Unix 系统上为 **omnirc** 文件设置的权限取决于您的 umask 设置，并且可能会阻止某些进程读取该文件。请将权限手动设置为 644。
5. 在修改 **omnirc** 文件的 Data Protector 客户机上重新启动 Data Protector 服务/后台程序。对 Unix 系统上的 CRS 后台程序强制执行此操作，对 Windows 系统上的 Data Protector CRS 和 Inet 服务建议执行此操作。仅当您删除条目或重命名文件时，才必须在 Windows 客户机上重新启动服务，在文件中添加或更改条目时则不需要。

有关在灾难恢复期间设置 **omnirc** 选项的信息，请参阅“Data Protector 灾难恢复”一节。

最常用的 omnirc 选项

以下列表包括最常用的 **omnirc** 选项。有关完整说明，请参阅 **omnirc** 文件。

omnirc 选项	描述
OB2_SHOW_BTRFS_MOUNTS	要显式备份装载的卷，您需要导出 **omnirc** 变量（OB2_SHOW_BTRFS_MOUNTS），它将强制 inet 发回所有卷。将 OB2_SHOW_BTRFS_MOUNTS 变量的值设置为 1 。
OB2_ENCRYPT_PVT_KEY	要对安全远程安装使用加密私钥，请在安装服务器上将此选项设置为 1 。默认值是 0 （未设置）。

OB2_ENCRYPT_MEDIUM_STRICT	使您能够控制在备份、对象整合、对象复制和自动化介质复制会话中是否使用基于驱动器的加密。仅当您在用户界面中为当前会话选择“基于驱动器的加密” 选项时，才会考虑该选项。
	
	将值设为 1 时:
	• 如果选定磁带驱动器不支持加密，则会话在默认情况下将中止。
	• 如果选定磁带驱动器支持加密，但其中的介质不支持加密:
	  ◦ 对于单独的磁带驱动器**:** Data Protector 发出装载请求。
	  ◦ 对于磁带库**:** Data Protector 检查库中所有可用介质的加密支持，否则它会发出装载请求。
	• 如果选定磁带驱动器及其中的介质都支持加密，则数据写入操作将在加密模式下执行。
	
	将值设为 0 时:
	• 如果选定磁带驱动器不支持加密，则数据写入操作将在非加密模式下执行。
	• 如果选定磁带驱动器支持加密，但其中的介质不支持加密，则数据写入操作将在非加密模式下执行。
	• 如果选定磁带驱动器及其中的介质都支持加密，则数据写入操作将在加密模式下执行。

OB2_ENCRYPT_FORCE_FORMAT	使您可以在使用 Data Protector 基于驱动器的加密时控制格式化行为。 基于值集: • **0** 默认中止格式化操作。 • **1:** 强制进行格式化操作。

OB2_AES_COMPATIBILITY_MODE	从使用 Data Protector 版本 (DP 7.03_108、8.14、8.14_209、8.14_210、9.03 和 9.04) 创建的 AES 加密备份中还原的数据没有作用。纠正此错误需要手动介入。 要还原使用 Data Protector 版本 (DP 7.03_108、8.14、8.14_209、8.14_210、9.03 和 9.04) 创建的 AES-256 软件加密备份，请在需要还原的客户机上的 **omnirc** 文件中将此选项设置为 1。 要还原使用其他 Data Protector 版本创建的 AES-256 软件加密备份，请将此选项设置为 0 (或) 从 **omnirc** 文件中删除此选项，然后重新启动该特定客户机上的 inet 后台程序。
OB2FORCEPOSTEXEC	使您能够强制执行 post-exec 脚本。 基于值集: • **0 (**默认值**):** 不强制执行 post-exec 脚本。 • **1:** 始终执行 post-exec 脚本，即使 pre-exec 脚本失败时亦如此。
OB2BLKPADDING_n	指定在初始化时写入介质的空块数。复制介质时，这有助于防止目标介质在数据复制完成之前用完空间。
OB2DEVSLEEP	加载设备时，更改每次重试之间的休眠时间。
OB2ENCODE	使您始终能够使用数据编码，无论在备份规范中是如何设置备份选项的。
OB2OEXECOFF	使您能够限制或禁用在特定客户机的备份规范中定义的任何对象 pre- 和 post-exec 脚本。
OB2REXECOFF	使您能够禁用特定客户机的任何远程会话 pre- 和 post-exec 脚本。
OB2CHECKCHANGETIME (Unix 系统特有)	定义何时对增量备份使用“最后一个 inode 更改”时间 。 三个有效值包括: • **0 :** 增量备份将仅备份已修改的文件，而不会检测到已移动的文件。 • **1 :** 除非将上述两个选项中的任何一个设置为修改**最后 inode 更改**时间的值，否则将检查**最后 inode 更改**时间（并检测移动的文件）。 • **2 :** 使用此设置，即使使用有问题的选项，磁盘代理也可以检测到移动的文件。 设置 OB2INCRDIFFTIME 变量并指定延迟期间 (等于备份的最大预期持续时间)。 默认值： 1
OB2INCRDIFFTIME (Unix 系统特有)	在为增量备份选中“最后一个 inode 更改”时间时，指定一个强制的“增量延迟”期间。此选项仅在 OB2CHECKCHANGETIME 选项为 2 时有效。
OB2RECONNECT_ACK	定义 Data Protector 应等待多长时间才能获得确认消息 (默认值为: 1200 秒)。如果代理在此时间内未获得确认，则假定套接字连接不再有效。
OB2RECONNECT_RETRY	定义 Data Protector 磁盘代理或介质代理在连接失败后应等待多长时间才能尝试重新连接。默认值： 600 秒。
OB2SHMEM_IPCGLOBAL	在同时安装了磁盘代理和介质代理的 HP-UX 客户机上，将此选项设为 1 ，以防在备份期间发生以下错误: Cannot allocate/attach shared memory (IPC Cannot Allocate Shared Memory Segment) System error: [13] Permission denied) => aborting
OB2VXDIRECT	为高级 VxFS 文件系统启用直接读取（不进行缓存），这样可以改进性能。
OB2ODIRECT_BACKUP	此选项将 Data Protector 配置为在打开文件进行读写时使用 O_DIRECT 标志，从而避免使用文件系统缓存。在 Linux 和 AIX 系统上，此选项仅适用于 FS 备份。 OB2ODIRECT_BACKUP=0|1 Default:0

OB2ODIRECT_RESTORE	此选项将 Data Protector 配置为在打开文件进行写入时使用 O_DIRECT 标志，从而避免使用文件系统缓存。由于未使用缓存，这可能会导致减慢还原速度。在 Linux 和 AIX 上，此选项仅适用于 FS 还原。根据 Data Protector 平台和集成支持矩阵，可以支持不同的文件系统。 OB2ODIRECT_RESTORE=0|1 Default:0
OB2ODIRECT_RESTORE_MINIMUM_SIZE	设置此选项后，仅当文件大小大于指定值时，还原才会使用 O_DIRECT 标志。 OB2ODIRECT_RESTORE_MINIMUM_SIZE =<min_file_size_in_bytes> Default:0
OB2_CLP_MAX_ENTRIES （Windows 系统特有）	设置 Windows NTFS 更改日志提供程序可以在内存中保存的条目数。更改日志提供程序使用的内存量取决于所有条目的文件名长度。 最少： 15 000 个条目 (这代表约 25 MB 的内存)。 默认值： 100 000 个条目 (大约 120 MB 的内存)。 如果将该数字更改为较小的值，以致于无法将所有条目都保存在内存中，则备份时间可能会增加。
OB2_CLP_CREATE_EI_REPOSITORY （Windows 系统特有）	指定在首次运行 Windows NTFS 更改日志提供程序时是否创建增强型增量存储库。将此选项设置为 1 可以创建增强型增量存储库。默认值： 0 (不创建)。如果设置此选项，将增加备份时间，因为会始终更新增强型增量存储库。但是，这支持回退到常规的增强型增量备份。
OB2_ENHINC_SQLITE_MAX_ROWS	指定增强型增量备份数据库（Windows、HP-UX 和 Linux 系统上的 SQLite）中可以存储在内部存储器缓存中的最大行数。如果备份包含大量 (数百万) 目录，则此选项用于通过增加在缓存中存储的最大行数来提高磁盘代理性能。
OB2SANCONFSCSITIMEOUT （Windows 系统特有）	设置与 sanconf 相关的操作的超时。在运行此命令之前，在受 sanconf 影响的所有客户机上设置该选项。默认值： 20 秒。
OB2PORTRANGE	动态分配侦听端口时，限制 Data Protector 使用的端口号的范围。通常设置此选项来支持通过防火墙进行单元管理。请注意，需要单独配置各个防火墙，并且指定的范围不影响 Inet 侦听端口。
OB2PORTRANGESPEC	限制特定 Data Protector 进程使用的端口号的范围。请注意，需要单独配置各个防火墙，并且指定的范围不影响 Inet 侦听端口。 对于端口范围配置的示例，请参阅《Data Protector 帮助》索引: “防火墙支持”。
OB2HSMBACKUPALL	要备份具有脱机属性的文件，请将此选项设置为 1。默认值为 0（未设置），因此备份过程将跳过所有具有脱机属性的文件。 当具有脱机属性的文件没有重分析点时，备份之前是否执行数据重新调用和重新水合取决于分层存储管理 (HSM) 产品。这可能导致高 I/O 流量和系统过载。有关详细信息，请参见 HSM 产品文档。 重分析点指的是考虑外部文件的位置。
OB2BMASTATISTICS	此变量用于测量备份统计信息和性能。 要启用此变量，请在所有介质代理主机上设置环境变量 OB2BMASTATISTICS = 2 并从系统中收集文件“bmastat.log”（介质代理：<OmniBack_home>\log)。 默认值： 0
OB2SGENABLED	SG 群集设置中不支持通过选项“使用已还原的数据库作为新的内部数据库”将已还原的 IDB 用作新的 IDB。您可以设置此 **omnirc** 变量，以提供在会话报告中将还原的 IDB 用作新 IDB 的过程。 默认值： 0

OB2_DISABLE_INF_TIMEOUT_MIRRORING	OB2_DISABLE_INF_TIMEOUT_MIRRORING = 0 或 1 默认值：0 如果设置为 1，则当会话中存在镜像设备时，还将考虑 SmMaIdleTimeout。
OB2SCRIPTOUTPUTTIMEOUT	备份 DA 使用此超时。对象 pre-exec 或 post-exec 脚本必须至少每 OB2SCRIPTOUTPUTTIMEOUT 分钟发送一些输出，否则将中止 DA。 默认：未设置
OB2_SAPHANA_PIPE_TIMEOUT	此超时值是所有以 backint 命名的管道的累积处理时间。如果 Data Protector 中的设备并发数为 **1**，backint 创建的管道数为 **n**，每个管道所用的处理时间为 **m**，则将超时设置为 **n * m**。 默认值：10 秒。 值 **0** 启用阻止行为（不建议这样做，因为这可能会导致残余进程）。如果此值为 **0**，将导致日志备份挂起。使用此变量，备份会话可能会恢复，以便 SAP HANA 后续的备份请求可以再次成功。
OB2CREATEFILEFLAGS	仅适用于Windows 介质代理。 OB2CREATEFILEFLAGS=0|1|2|3|WRITE_THROUGH|NO_BUFFERING|ALL 默认值：0 此变量用于将其他标志传递给服务器，以便服务器知道在写入数据之前不满足写请求，从而确定在 OS/驱动程序/硬件级别发生的 I/O 错误。受此变量影响的设备是：独立、介质库和文件库。 CreateFile() 的 FILE_FLAG_WRITE_THROUGH 标志使对该句柄的任何写操作都直接写入文件而不进行缓冲。直到将数据写入文件后，写调用才会返回。这也适用于远程写入。网络重定向器将 FILE_FLAG_WRITE_THROUGH 标志传递给服务器，以便服务器知道在将数据写入文件之前不满足写入请求。 FILE_FLAG_NO_BUFFERING 使这一概念更进一步，消除了所有预读文件缓冲和磁盘缓存，从而确保所有读取均来自文件，而不是任何系统缓冲区或磁盘缓存。请注意，设置这些标志可能会对性能产生影响，具体取决于磁盘缓存和空间碎片。 FILE_FLAG_WRITE_THROUGH 标志有时可能无效，因为 SATA 驱动程序可能会忽略刷新请求。文件系统不知道驱动程序在撒谎，因此它仍会在假定直写请求有效的前提下完成所有工作。 • **0** [无] - 未设置标志。 • **1** [WRITE_THROUGH] - 写入操作不会通过任何中间缓存，而是直接进入磁盘。 • **2** [NO_BUFFERING] - 正在打开文件或设备，没有用于数据读写的系统缓存。该标志不影响硬盘缓存或内存映射文件。 • **3** [ALL] - 两个标志均设置： WRITE_THROUGH 和 NO_BUFFERING。
OB2_SAPHANA_AUTOINCREMENT	该变量负责以下功能。 • **重复的对象**: 当计数器增量和对象启动由 BSM 自动完成时，将实现自动增量逻辑。 在 MSG_WAIT 上，使用新会话的计数器，以防止重复。 修改 SAP HANA，以在对象启动期间提供部分对象名称，并在 MSG_CONNECT 上从 BSM 检索全名。 • **对象限制**: 自动增量逻辑在对象启动期间检查计数器，并始终遵守该限制 (如果达到限制，则不会分配对象)。 此功能默认情况下已启用。 可以使用 **omnirc** 或参数文件变量来禁用它。 OB2_SAPHANA_AUTOINCREMENT=<0|1> 默认值：1。如果值为 1，则启用自动递增逻辑。如果值为 0，则禁用自动递增逻辑。
OB2_MSSQL_DISABLE_FULLBACKUP_VALIDATION	在 MSSQL 备份期间，如果将此变量设置为 0，它将检查是否有有效的完整 Data Protector 备份。 如果找不到有效的完整备份，它会将任何事务或差异备份转换为完整备份，以确保还原链不会中断并导致成功还原。如果设置为 1，它将禁用完整备份验证。 默认值：0
OB2_CLOUD_ENABLE_AWSSDK_LOGS	使用此变量来控制 AWS 开发工具包日志记录系统的详细程度。如果不使用此变量，则不会记录 SDK 日志。 下面是详细级别的范围映射: 1 - 29 错误；30 - 98 警告；99 - 198 信息；199 - 398 调试；399 及更高为跟踪。例如: **OB2_CLOUD_ENABLE_AWSSDK_LOGS = 1-98** 将打印所有错误和警告日志。 默认值：1-29
OB2_GLACIER_RESTORE_SLEEPTIME	使用此变量可设置从 AWS Glacier/DeepArchive 还原期间的睡眠时间 (秒)。在此时间内，该过程将一直等待，直到启动的作业完成。 如果您在睡眠时间内中止会话，则只有在睡眠时间结束后，会话才会中止。 Glacier 标准层的最大值 – 14400，Glacier 批量层的最大值 – 43200，DeepArchvie 标准层的最大值 – 43200，DeepArchvie 批量层的最大值 – 172800，Glacier 加速层的最大值 – 300 默认值：60

OB2_VEAGENT_VCENTER_CONNECTION_LIMIT	vCenter/ESX 服务器对一次可以打开的 HTTP 连接数量有限制。每个备份都会打开一个新连接，最终导致达到此连接限制。 可以使用此设置来计算要并行启动的安全线程数。 线程数 = 连接限制 - 10 % (至少一个线程) 请注意，这些连接之一将用于控制通信。 默认值：10
OB2_VEAGENT_VCENTER_CONNECTION_LIMIT_INCR	使用此变量来计算增量备份的连接限制。此变量类似于 OB2_VEAGENT_VCENTER_CONNECTION_LIMIT. 默认值：4
OB2_VEAGENT_DISK_CONCURRENCY	使用此变量来计算可并行启动的安全磁盘连接数。选择的磁盘来自任何正在运行的 VM 连接。磁盘连接数等于 VM 磁盘并发。 已启动的磁盘线程数 = VM 磁盘并发数 - 10 % (至少一个线程) 默认值： 10
OB2_VEAGENT_THREADED_DISK_BACKUP	使用此变量可以并行处理多个磁盘对象备份。要进行并行备份，请将变量设置为 1。要切换回顺序备份，请将其设置为 0。您只能将此变量用于 VMware 和 Hyper-V 备份。 默认值： 1
OB2_FORCE_OLD_DECR_MODE	要强制解密使用旧算法加密的驱动器，请在介质代理主机上将此选项设置为 1。默认值是 0。 建议您在对此 omnirc 变量进行更改时，在介质代理主机上重新启动 Data Protector INET 服务。
OB2_IMPORT_OPTIONS	OB2_IMPORT_OPTIONS = -protect {none | weeks n | days n | until Date | permanent | extend} [-expired_only] 默认: 未设置。 要为导入的介质强制设置新的保护期，请在 Cell Manager 上的 omnirc 文件中设置此变量。 您可以将保护期设置为几周、几天或直到特定日期。例如，以下值对导入的介质应用 30 周的保护。 OB2_IMPORT_OPTIONS=-protect weeks 30 要永久设置保护，请使用 **permanent** 选项。 要扩展之前设置的保护，请使用 **extend** 选项。 可选 " -expired_only " 参数仅对导入时已过期的介质应用指定的保护。

卸载 Data Protector 软件

如果您的系统配置更改，则可能要从系统中卸载 Data Protector 软件或删除部分软件组件。
卸载是从系统中删除所有 Data Protector 软件组件，其中包括 Cell Manager 计算机上的 IDB 对此系统的所有引用。但是，默认情况下，Data Protector 配置数据 (包括自签名证书) 会保留在系统中，因为将来升级 Data Protector 时可能需要这些数据。如果在重新安装后需要生成新证书，请按照《Data Protector 管理员指南》的 Data Protector 一节的“重新生成证书”中的步骤生成证书并将其分发给客户机。
要在卸载 Data Protector 软件后删除配置数据，请删除安装了 Data Protector 的目录。
如果 Data Protector 安装目录中有其他数据，请确保在卸载 Data Protector 前将这些数据复制到其他位置。否则，卸载过程中将删除这些数据。
从单元中卸载 Data Protector 软件需要以下步骤：

1. 使用 GUI 卸载 Data Protector 客户机软件
2. 卸载 Data Protector Cell Manager 和安装服务器

您也可以不用卸载 Cell Manager 或客户机即卸载 Data Protector 软件组件。
在 UNIX 上，还可以手动删除 Data Protector 软件。

先决条件

从计算机中卸载 Data Protector 软件前，请检查以下内容：

- 确保计算机的所有相关参考都已从备份规范中删除。否则，Data Protector 将尝试备份未知的系统，而此部分备份规范将会失败。
- 确保要卸载的系统上没有连接和配置备份设备或磁盘阵列。导出系统后，Data Protector 不再能够使用原单元中的备份设备或磁盘列阵。
- 在卸载之前，确保关闭所有未处理的 GRE 开机请求。此外，确保完成或中止正在进行中的实时迁移会话。

卸载 Data Protector 客户机

注意: 远程卸载过程要求为正在卸载其 Data Protector 软件的平台安装安装服务器。
在 Data Protector GUI 中远程卸载客户机

1. 在“上下文列表 (Context List)”中，切换到**客户机 (Clients)** 上下文。
2. 在“范围窗格”中，展开**客户机**，右键单击要卸载的客户机，然后单击**删除**。此时会询问您是否要同时卸载 Data Protector 软件。
3. 单击**是 (Yes)** 从客户机中卸载所有软件组件，然后单击**完成 (Finish)**。

客户机将从“结果区域”的列表中删除，Data Protector 软件将从硬盘中删除。
请注意，Data Protector 配置数据将保留在客户机系统中。要删除配置数据，请删除安装了 Data Protector 的目录。

卸载群集客户机

如果您的 Data Protector 环境中具有群集感知的客户机且要卸载它们，则必须在本地执行此操作。此过程与卸载 Cell Manager 或安装服务器的情况相同。
群集客户机将从“结果区域”的列表中删除，Data Protector 软件将从其硬盘中删除。
TruCluster
要卸载 TruCluster 客户机，请首先导出虚拟节点。然后从节点卸载 Data Protector 客户机。
OpenVMS 客户机
无法使用安装服务器远程删除 Data Protector OpenVMS 客户机。必须在本地卸载它。
从 OpenVMS 系统中卸载 Data Protector 客户机

1. 首先使用 Data Protector GUI 从 Data Protector 单元中导出相关的客户机。当询问是否要同时卸载 Data Protector 软件时，选择“否”。
2. 要删除实际的 Data Protector 客户机软件，请登录 OpenVMS 客户机上的 SYSTEM 帐户并执行以下命令：`$ PRODUCT REMOVE DP`。对于出现的提示请选择 YES 。重要说明：
   这将关闭 Data Protector 服务并删除 OpenVMS 系统上所有与 Data Protector 关联的目录、文件和帐户。

卸载 Cell Manager 和安装服务器

本节介绍从 Windows 和 Linux 系统上卸载 Data Protector Cell Manager 和安装服务器软件的步骤。

从 Windows 系统中卸载

从 Microsoft 服务器群集中卸载
从 Windows 系统中卸载 Data Protector 软件

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 在 Windows 控制面板中，单击**添加/删除程序**。
3. 根据您是否希望在系统上留下配置数据，将应用不同的操作：
   重要说明：如果卸载后在系统中保留 Data Protector 配置数据，以后又安装了低于所卸载版本的 Data Protector Cell Manager，请注意这些配置数据将不可用。要成功安装较低版本，请在安装期间选择将删除配置数据的选项。
   - 要卸载 Data Protector 并将 Data Protector 配置数据保留在系统中，请选择“Data Protector 10.00”并单击“删除”。
   - 要卸载 Data Protector 并删除 Data Protector 配置数据，请选择“Data Protector 10.00”，单击“更改”，然后单击“下一步”。在“程序维护”对话框中，选择“删除”。选择**永久删除配置数据**并单击**下一步**。
4. 卸载完成后，单击**完成**退出向导。

卸载在 Serviceguard 上配置的 Cell Manager 和/或安装服务器

如果您的 Cell Manager 和/或安装服务器是在 Serviceguard 群集上配置的，请执行以下步骤来卸载软件。
主节点
登录到主节点，并执行以下步骤：

```
vgchange -a y -q y vg_name
```

例如：

```
vgchange -a y -q y /dev/vg_ob2cm
```

1. 停止 Data Protector 包：

   ```
   cmhaltpkg PackageName
   ```

   其中 PackageName 表示群集包名称。
   例如：

   ```
   cmhaltpkg ob2cl
   ```

2. 停用卷组的群集模式：

   ```
   vgchange -c n vg_name
   ```

   （其中 vg_name 代表位于 /dev 目录的子目录中的卷组的路径名）。
   例如：

   ```
   vgchange -c n /dev/vg_ob2cm
   ```

3. 激活卷组：
4. 将逻辑卷装载为共享磁盘：

   ```
   mount lv_path shared_disk
   ```

   （其中 lv_path 代表逻辑卷的路径名，shared_disk 代表装载点或共享目录）。
   例如：

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

5. 使用 swremove 实用程序删除 Data Protector。
6. 删除软链接：

   ```
   rm /etc/opt/omni rm /var/opt/omni
   ```

7. 删除备份目录：

   ```
   rm -rf /etc/opt/omni.save rm -rf /var/opt/omni.save
   ```

8. 删除 Data Protector 目录及其内容：

   ```
   rm -rf /opt/omni
   ```

9. 卸载共享磁盘：

   ```
   umount shared_disk
   ```

   例如：

   ```
   umount /omni_shared
   ```

10. 停用卷组：

    ```
    vgchange -a n vg_name
    ```

    例如：

    ```
    vgchange -a n /dev/vg_ob2cm
    ```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 激活卷组：

   ```
   vgchange -a y vg_name
   ```

2. 装载共享磁盘：

```
mount lv_path shared_disk
```

3. 使用 swremove 实用程序删除 Data Protector。
4. 删除软链接：

```
rm /etc/opt/omni rm /var/opt/omni
```

5. 删除备份目录：

```
rm -rf /etc/opt/omni.save rm -rf /var/opt/omni.save
```

6. 删除 Data Protector 目录及其内容：

```
rm -rf /opt/omni
```

7. 删除共享文件系统中的目录：

```
rm -rf shared_disk /etc_opt_omni rm -rf shared_disk /var_opt_omni
```

例如：

```
rm -rf /omni_shared/etc_opt_omni rm -rf /omni_shared/etc_opt_omni
```

8. 卸载共享磁盘：

```
umount shared_disk
```

9. 停用卷组：

```
vgchange -a n vg_name
```

已将 Data Protector 从系统中完全删除。

卸载在 Symantec Veritas Cluster Server 上配置的 Cell Manager 和/或安装服务器

如果您的 Cell Manager 和/或安装服务器是在 Symantec Veritas Cluster Server 上配置的，请执行以下步骤来卸载软件。

主节点

登录到主节点，并执行以下步骤：

1. 使 Data Protector 应用程序资源脱机。
2. 禁用 Data Protector 应用程序资源。
3. 卸载 Data Protector。
4. 删除软链接：

```
rm /etc/opt/omni rm /var/opt/omni
```

5. 删除备份目录：

```
rm -rf /etc/opt/omni.save rm -rf /var/opt/omni.save
```

6. 删除 Data Protector 目录及其内容：

```
rm -rf /opt/omni
```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到辅助节点。
2. 卸载 Data Protector。
3. 删除软链接：

```
rm /etc/opt/omni rm /var/opt/omni
```

4. 删除备份目录：

```
rm -rf /etc/opt/omni.save rm -rf /var/opt/omni.save
```

5. 删除 Data Protector 目录及其内容：

```
rm -rf /opt/omni
```

6. 删除共享文件系统中的目录：

```
rm -rf shared_disk /etc_opt_omni rm -rf shared_disk /var_opt_omni
```

例如：

```
rm -rf /omni_shared/etc_opt_omni rm -rf /omni_shared/var_opt_omni
```

已将 Data Protector 从系统中完全删除。

从 Linux 系统中卸载

先决条件
使用 omnisetup.sh -bundlerem 命令删除已安装的所有 Data Protector 补丁包。
Cell Manager
适用于 Linux 的 Cell Manager 始终使用 omnisetup.sh 命令在本地安装。因此，必须使用 rpm 实用程序在本地将其卸载。
重要说明：
如果卸载后在系统中保留 Data Protector 配置数据，以后又安装了低于所卸载版本的 Data Protector Cell Manager，请注意这些配置数据将不可用。要成功安装较低版本，请在卸载后从系统中删除剩余的 Data Protector 目录。

要卸载 Data Protector Cell Manager，请按如下方式继续操作:

1. 确保已终止所有 Data Protector 会话并退出图形用户界面。
2. 输入 rpm -qa | grep OB2 命令，列出 Cell Manager 上安装的所有 Data Protector 组件。与 Cell Manager 关联的组件如下:

OB2-CORE	Data Protector 核心软件
OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-DISPATCHER	作业控制引擎调度程序
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。
OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式和 Data Protector 文档和 WebHelp 格式的 Data Protector 帮助。

如果系统上还安装了 Data Protector 客户机或安装服务器，则其他组件也将列出。

注意:
要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 rpm -e package name 命令删除上一步中提到的组件并按提示继续。

安装服务器

Linux 上适用于 UNIX 的安装服务器始终使用 omnisetup.sh 命令在本地安装。因此，必须使用 rpm 实用程序在本地将其卸载。

要卸载 Data Protector 安装服务器，请按如下方式继续操作:

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 输入 rpm -qa | grep OB2 命令，列出所有 Data Protector 组件和安装服务器系统上存储的远程安装包。

   与安装服务器关联的组件和远程安装包如下:

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装安装服务器，则已安装该软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器核心软件。
OB2-CFP	适用于所有 UNIX 平台的公用安装服务器核心软件。
OB2-TS-CFP	适用于所有 UNIX 平台的公用安装服务器技术堆栈软件
OB2-DAP	适用于所有 UNIX 系统的磁盘代理远程安装包。
OB2-MAP	适用于所有 UNIX 系统的介质代理远程安装包。
OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于所有 UNIX 系统的单元控制台远程安装包。

如果系统上安装了其他 Data Protector 组件，则其他组件也将列出。

注意:
要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 rpm -e package name 命令删除上一步中提到的组件并按提示继续。

在 UNIX 上手动删除 Data Protector 软件

卸载 UNIX 客户机前，应先将其从单元中导出。

Linux 系统

要手动从 Linux 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni rm -fr /etc/opt/omni rm -fr /opt/omni
```

Solaris 系统

要手动从 Solaris 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni rm -fr /etc/opt/omni rm -fr /opt/omni
```

其他 UNIX 系统

使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /usr/omni
```

设备和介质相关的任务

本主题提供有关任务的其他信息，这些任务包括设备驱动程序配置、管理 SCSI 机械手、维护 SCSI 环境等等。

在 Windows 系统上使用磁带和机械手驱动程序

Data Protector 支持默认情况下为连接到 Windows 系统的已启用磁带驱动器加载的本机磁带驱动程序。Data Protector 不支持为介质更换器 (机械手) 设备加载的 Windows 本机驱动程序。

在下面的示例中，4mm DDS 磁带设备连接到 Windows 系统。如果 4mm DDS 磁带设备连接到 Windows 系统并配置用于 Data Protector，则需要禁用为介质更换器设备加载的本机驱动程序。本节将介绍相关步骤。

磁带驱动程序

如果设备列在硬件兼容性列表 (HCL) 中，则 Windows 中通常带有驱动程序。HCL 是 Windows 支持的设备的列表，可在以下站点找到: http://www.microsoft.com/whdc/hcl/default.mspx。

计算机一启动，设备驱动程序就会自动为所有启用的设备加载。您不需要单独加载本机磁带驱动程序，但可以更新它。

更新或更换 Windows 系统上的本机磁带驱动程序

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在“管理工具”窗口中，双击“计算机管理”。单击**设备管理器 (Device Manager)**。
3. 展开磁带驱动器。要检查当前为设备加载了哪个驱动程序，请右键单击磁带驱动器，然后单击“属性”。
4. 选择“驱动程序”选项卡并单击“更新驱动程序”。然后在向导中可以指定是要更新当前安装的本机磁带驱动程序还是要将其替换为其他驱动程序。
5. 重新启动系统以应用更改。

   重要说明：如果已为 Data Protector 配置了不使用本机磁带驱动程序的设备，则必须对引用此特定磁带驱动器的所有配置的 Data Protector 备份设备重命名设备文件 (例如，从 scsi1:0:4:0 重命名为 tape3:0:4:0)。

机械手驱动程序

在 Windows 中，将为启用的磁带库自动加载机械手驱动程序。要在 Data Protector 中使用带库机械手，必须禁用各个驱动程序。

下面的示例中是使用 4mm DDS 磁带的 1557A 磁带库。

在 Windows 系统上禁用自动加载的机械手驱动程序 (ddsmc.sys):

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在“管理工具”窗口中，双击“计算机管理”。单击**设备管理器 (Device Manager)**。
3. 在“设备管理器 (Device Manager)”窗口的“结果区域 (Results Area)”中，展开介质更换器。
4. 要检查当前加载了哪个驱动程序，请右键单击“4mm DDS 介质更换器”，然后单击“属性”。
   选择“驱动程序”选项卡并单击“驱动程序详细信息”。

   要禁用本机机械手驱动程序，请右键单击“4mm DDS 介质更换器”，然后选择“禁用”。

在 Windows 系统上创建设备文件（SCSI 地址）

磁带设备文件名语法取决于为磁带驱动器加载了 (tapeN:B:T:L) 还是未加载 (scsiP:B:T:L) 本机磁带驱动程序。

使用本机磁带驱动程序的 Windows

要为连接到使用本机磁带驱动程序的 Windows 系统的磁带驱动器创建设备文件，请执行以下步骤：

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在“管理工具”窗口中，双击“计算机管理”。展开可移动存储，然后展开物理位置。右键单击磁带驱动器并选择“属性”。
3. 如果加载了本机磁带驱动程序，则设备文件名会显示在“常规”属性页中。否则，可在“设备信息 (Device Information)”属性页中找到相关信息。

磁光设备

如果将磁光设备连接到 Windows 系统，则在重新启动系统后会给设备分配一个驱动器字母。稍后会在创建设备文件时使用该驱动器字母。例如，E: 是为分配了驱动器字母 E 的磁光驱动器创建的设备文件。

在 HP-UX 系统上配置 SCSI 机械手

在 HP-UX 系统上，SCSI Pass-Through 驱动程序用于管理磁带库设备 (例如 12000e) 的 SCSI 控制器和控制设备 (也称为机械手或选择器)。带库中的控制设备负责将介质装入驱动器/从驱动器中取出介质以及将介质导入这种设备/从这种设备导出介质。

使用的 SCSI 机械手驱动程序的类型取决于硬件。配备 GSC/HSC 或 PCI 总线的系统具有名为 schgr 的 SCSI 自动更换器驱动程序，配备 EISA 总线的系统具有名为 sctl 的 SCSI Pass-Through 驱动程序，它已置于内核中。但是，用于配备 NIO 总线的服务器的 SCSI Pass-Through 驱动程序名为 spt。默认情况下，它安装在系统上而不置于内核中。

如果 SCSI 机械手驱动程序尚未链接到当前内核，则必须手动添加并将其分配给连接的磁带库的机械手。

下面的步骤说明了如何手动将 SCSI 机械手驱动程序添加到内核以及如何手动重建一个新的内核。

提示：在 HP-UX 平台上，还可以使用 System Administration Manager (SAM) 实用程序构建内核。

使用 /opt/omni/sbin/ioscan -f 命令，检查是否已将 SCSI 机械手驱动程序分配给要配置的库。

在上面的 SCSI Pass-Through 驱动程序 (sctl) 的状态中，可以看到分配给 Exabyte 磁带设备的控制设备的 sctl SCSI Pass-Through 驱动程序。相应的硬件路径 (H/W Path) 是 8/12.2.0。（SCSI=2，LUN=0）

此外，还有一个磁带驱动器连接到同一 SCSI 总线，但是控制该磁带驱动器的驱动程序是 stape。相应的硬件路径 (H/W Path) 是 8/12.1.0。（SCSI=0，LUN=0）

重要说明：SCSI 地址 7 总是由 SCSI 控制器使用，虽然相应的行可能不显示在 ioscan -f 命令的输出中。在本示例中，控制器由 sctl 管理。

在 SCSI Pass-Through 驱动程序 (spt) 的状态中，以看到一个已连接的磁带设备，其机械手由 spt SCSI Pass-Through 驱动程序控制。该特定设备是 12000e 磁带库设备，使用 SCSI 地址 4 并通过 H/W Path 52 连接到 SCSI 总线。相应的硬件路径是 52.4.1。机械手正确分配给 spt SCSI Pass-Through 驱动程序。

如果 sctl、spt 或 schgr 驱动程序没有分配给机械手，则必须将机械手的 H/W Path 添加到 system 文件的驱动程序声明中并重建内核。请执行以下步骤。

以下步骤说明如何手动将 SCSI 机械手驱动程序添加到内核，将其分配给机械手，然后手动重建新的内核:

1. 以 root 用户身份登录并切换到 build 目录：
   cd /stand/build
2. 从现有内核创建新系统文件：
   cd /stand/build
3. 检查哪个 SCSI 机械手驱动程序已置于当前内核中。在 /stand 目录中，执行以下命令：
   grep SCSIRoboticDriver system
   其中 SCSIRoboticDriver 可以是 spt、sctl 或 schgr。如果该驱动程序已置于当前内核中，则系统将显示相应的行。
4. 使用编辑器将驱动程序声明：
   driver H/W Path spt
   到 /stand/build/system 文件，其中 H/W Path 是设备的完整硬件路径。对于上例中的 12000e 磁带库，请输入:
   driver 52.4.1 spt
   对于连接到同一系统的多个库，必须使用相应的硬件路径为每个库机械手添加一个驱动程序行
   配置 schgr 驱动程序时，请将以下行附加到驱动程序声明中：
   schgr
5. 输入 mk_kernel -s./system 命令以构建新内核。
6. 使用其他名称保存原始的旧系统文件，并将新系统文件改为原始名称，这样它便成为当前系统文件：
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
7. 使用其他名称保存旧内核，并将新内核改为原始名称，这样它便成为当前内核：
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
8. 输入以下命令从新内核重新启动系统：
   shutdown -r 0
9. 重新启动系统后，使用以下命令验证已作的更改:
   /usr/sbin/ioscan -f command

在 HP-UX 系统上创建设备文件

先决条件

创建设备文件前，备份设备应已连接到系统。使用 /usr/sbin/ioscan -f 命令，检查设备是否正常连接。使用 /usr/sbin/infs -e 命令，自动为某些

备份设备创建设备文件。

如果在系统初始化（启动进程）期间或运行 infs -e 命令后没有创建对应于特定备份设备的设备文件，则必须手动创建这些设备文件。管理库控制设备（库机械手）所需的设备文件就是这种情况。

我们来看一个为连接到 HP-UX 系统的 12000e 库设备的机械手创建设备文件的示例。磁带驱动器的设备文件已在系统重新启动后自动创建，而控制设备的设备文件必须手动创建。

在 SCSI Pass-Through 驱动程序 (spt) 的状态中，可以查看选定 HP-UX 系统上的 ioscan -f 命令的输出。

SCSI 总线接口由 scsi1 系统驱动程序控制。这是 SCSI NIO 接口。要访问 SCSI NIO 总线上的库机械手，必须使用已安装并分配给使用硬件路径 52.4.1 的 12000e 磁带设备的机械手的 spt SCSI Pass-Through 驱动程序。

注意: 如果不使用基于 SCSI NIO 的总线接口，则不需要 spt 驱动程序而使用 sctl 驱动程序。

要创建设备文件，需要知道 SCSI Pass-Through 驱动程序的主号字符和次号字符，它与使用的 SCSI Pass-Through 驱动程序无关。

要获取属于 spt 的主号字符，请运行系统命令:
lsdev -d spt

在本示例中 (请参阅已连接设备的列表)，命令报告主号字符为 75。

要获取属于 sctl 的主号字符，请运行系统命令：
lsdev -d sctl

在本示例中，命令报告主号字符为 203。

无论使用哪种 SCSI Pass-Through 驱动程序，次号字符都具有以下格式：
0xIITL00
II-> ioscan -f 输出报告的 SCSI 总线接口 (非设备) 的实例编号位于第二列，标有 I。在本示例中，实例编号是 0，所以必须输入两位十六进制数 00。

T-> 库机械手的 SCSI 地址。在本示例中，SCSI 地址是 4，所以必须输入 4。

L-> 库机械手的 LUN 编号。在本示例中，LUN 号是 1，所以必须输入 1。00-> 两位十六进制的零。

创建设备文件

以下命令用于创建设备文件：
mknod /dev/spt/devfile_name c Major # Minor #
通常 spt 的设备文件位于 /dev/spt 或 /dev/scsi 目录中。在这种情况下，我们将控制设备文件命名为 /dev/spt/SS12000e。
因此，在 /dev/spt 目录中创建名为 SS12000e 的设备文件的完整命令是：
mknod /dev/spt/SS12000e c 75 0x004100
如果为 sctl 创建名为 SS12000e 且位于 /dev/scsi 目录的设备文件，则完整命令是：
mknod /dev/scsi/SS12000e c 203 0x004100

设置 SCSI 控制器的参数

通过 Data Protector 可更改设备的块大小，这可能需要在某些 SCSI 控制器上进行附加配置。

在 Windows 系统上，通过编辑 Adaptec SCSI 控制器及某些使用 Adaptec 芯片组的控制器的注册表值来设置 SCSI 控制器的参数：

1. 设置以下注册表值：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aic78xx\Parameters\Device0\MaximumSGList
2. 输入包含 4 kB 块数量的 DWORD 值再加一。
   MaximumSGList = (OBBlockSize in kB / 4) + 1
   例如，要启用 260 kB 的块大小，MaximumSGList 必须至少是 (260 / 4) + 1 = 66。
3. 重新启动系统。

注意: 该注册表值设置块大小的上限。设备的实际块大小必须使用设备配置的 Data Protector GUI 进行配置。

在 HP-UX 系统上查找未使用的 SCSI 地址

连接到 HP-UX 系统的备份设备是通过必须对每个物理设备都存在的设备文件来访问和控制的。必须先找出仍未使用、对新设备可用的 SCSI 地址（端口），才能创建设备文件。

在 HP-UX 系统上，/usr/sbin/ioscan -f 系统命令用于显示已占用的 SCSI 地址的列表。因此，/usr/sbin/ioscan -f 命令的输出中未列出的地址就是仍未使用的地址。

在本示例中，只有一个 SCSI 总线，使用 H/W Path 52。在该总线上，可以使用 SCSI 地址 0 和 3，因为它们没有显示在列表中。

在 HP-UX 系统上 ioscan -f 命令的输出中，可以查看选定 SCSI 总线上已被占用的 SCSI 地址:

- SCSI 地址 1 被 SCSI 磁盘占用
- SCSI 地址 2 被 CD-ROM 占用
- SCSI 地址 4，LUN 0，被磁带驱动器占用
- SCSI 地址 4，LUN 1，被磁带库机械手占用
- SCSI 地址 5 被 SCSI 磁盘占用
- SCSI 地址 6 被 SCSI 磁盘占用
- SCSI 地址 7 被 SCSI 控制器占用

虽然默认情况下 SCSI 地址 7 被 SCSI 控制器占用，但是它没有列出。

所有设备的 S/W State 值都设置为 CLAIMED，H/W Type 值都设置为 H/W DEVICE，这说明设备当前已连接。如果 S/W State 列中有 UNCLAIMED 值或 H/W Type 列中有 NO-HW 值，则说明系统无法访问该设备。

SCSI 地址 4 被磁带库占用，其中磁带驱动器在 LUN 0，机械手在 LUN 1。驱动器由 tape2 驱动程序控制，机械手由 spt SCSI Pass-Through 驱动程序控制。通过描述可以看到，该设备是 12000e 库；很容易就在 SCSI 库中认出它，因为它对磁带驱动器和机械手使用相同的 SCSI 地址，但是使用不同的 LUN。

整个 SCSI 总线由 scsi1 接口模块控制。

在 Solaris 系统上查找未使用的 SCSI 目标 ID

连接到 Solaris 系统的备份设备是通过设备文件访问和控制的。该设备文件是当备份设备已连接且客户机系统和备份设备通电时，由 Solaris 操作系统在目录 /dev/rmt 中自动创建的。

但是，在连接备份设备前，必须检查可用的 SCSI 地址并将备份设备的地址设置为尚未分配的地址。

要在 Solaris 系统上列出可用的 SCSI 地址，请完成以下步骤:

1. 按“停止”和“A”停止系统。
2. 在 ok 提示窗口中运行 probe-scsi-all 命令：
   probe-scsi-all
   系统可能要求您先启动 reset-all 命令，再执行 probe-scsi-all 命令。
3. 要返回正常操作，请在 ok 提示窗口中输入 go：
   go

在列出可用地址并选择一个用于备份设备后，必须先更新相关的配置文件，然后再连接和启动设备。请参见下一节获取更新配置文件的相关说明。

在 Solaris 系统上更新设备和驱动程序配置

更新配置文件

以下配置文件用于设备和驱动程序配置。必须先检查（必要时编辑）它们，然后才能使用连接的设备：

- st.conf
- sst.conf
  st.conf: 所有设备

  在每个连接了磁带设备的 Data Protector Solaris 客户机上，都需要此文件。对于连接到该客户机的每个备份设备，它必须包含相应的设备信息和一个或多个 SCSI 地址。对于单驱动器设备，需要单个 SCSI 条目；对于多驱动器库设备，需要多个 SCSI 条目。

1. 在客户机上检查未使用的 SCSI 地址（如上一节所述），并为要连接的设备选择一个地址。
2. 在备份设备上设置所选的 SCSI 地址。
3. 关闭客户机系统。
4. 连接备份设备。
5. 首先打开设备，然后再打开客户机系统。
6. 按停止 (Stop) 和 A 停止系统。
7. 在 ok 提示窗口中输入 probe-scsi-all 命令：
   probe-scsi-all
   这会提供连接的 SCSI 设备的相关信息，包括新连接的备份设备的正确设备 ID 字符串。
8. 返回到正常运行：

go

9. 编辑 /kernel/drv/st.conf 文件。Solaris st（SCSI 磁带）驱动程序使用该文件。它包含 Solaris 正式支持的设备列表以及适用于第三方设备的配置条目集。如果使用支持的设备，则应该可以连接和使用设备而无需进一步配置。否则，应将以下类型的条目添加到 st.conf 中：
   - 磁带配置列表条目（和磁带数据变量定义）。文件中有带注释的示例条目。如果适用，您可以使用其中一个条目，或进行修改以满足您的需要。

   该条目必须位于文件中第一个 name= 条目之前，且格式要求如下: tape-config-list= " Tape unit ", " Tape reference name ", " Tape data" ; 其中:

Tape unit	磁带设备的供应商和产品 ID 字符串。必须按照设备制造商文档所述正确指定该条目。
Tape reference name	您选择的名称，系统将通过该名称识别磁带设备。您提供的名称不会更改磁带产品 ID，但是系统启动后，该参考名称将显示在系统识别的外围设备列表中。
Tape data	参考一系列其他磁带设备配置项目的变量。也必须按照设备制造商文档所述指定该变量定义。

例如：

```
tape-config-list="Quantum DLT4000", "Quantum DLT4000", "DLT-data"; DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

第二个参数 0x38 将 DLTtape 磁带类型指定为"其他 SCSI 驱动器"。这里指定的值应在 /usr/include/sys/mtio.h 中定义。

注意: 请确保 tape-config-list 中的最后一个条目以分号（;）结尾。

- 对于多驱动器设备，目标条目如下：

```
name="st" class="scsi" target=X lun=Y;
```

其中:

X	是分配给数据驱动器（或机械手装置）的 SCSI 端口。
Y	是逻辑单元值。

例如：

```
name="st" class="scsi" target=1 lun=0; name="st" class="scsi" target=2 lun=0
```

通常在 st.conf 中仅对驱动器要求目标条目，对机械手装置不要求，它在其他目标上。这些设备的条目通常在 sst.conf 文件中提供（请参见下文）。但是，某些设备 (例如 24x6) 将机械手装置视为与其他驱动器类似。在这种情况下，需要具有相同目标的两个条目（一个用于驱动器，一个用于机械手），但是这两个条目必须具有不同的 LUN。
例如：

```
name="st" class="scsi" target=1 lun=0; name="st" class="scsi" target=1 lun=1
```

sst.conf: 库设备

在每个连接了多驱动器库设备的 Data Protector Solaris 客户机上，都需要此文件。一般来说，它需要每个连接到客户机的库设备机械手装置的 SCSI 地址条目 (也有例外，例如上一节中提到的 24x6)。

1. 将 sst 驱动程序（模块）和配置文件 sst.conf 复制到要求的目录：
   - 对于 32 位操作系统：

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

   - 对于 64 位操作系统：

     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /sst $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

2. 编辑 sst.conf 文件并添加以下条目：
   name="sst" class="scsi" target=X lun=Y;
   其中:

X	是机械手装置的 SCSI 地址。
Y	是逻辑单元。

例如：
name="sst" class="scsi" target=6 lun=0;

3. 将驱动程序添加到 Solaris 内核：
   add_drv sst

创建和检查设备文件

设置配置文件和安装驱动程序后，可按以下步骤创建新的设备文件：

1. 从 /dev/rmt 目录中删除所有现有的设备文件：
   cd /dev/rmt rm *
2. 输入以下命令以关闭系统：
   shutdown -i0 -g0
3. 重新启动系统：
   boot -rv
   boot 命令中的 r 开关启用内核编译并包括创建用于与磁带设备通信的设备特殊文件。v 开关启用系统启动文件的详细模式显示。启用详细模式后，系统应通过显示您在 /devices 目录配置启动阶段选择的 Tape reference name 字符串来表明设备已连接。
4. 请输入以下命令以验证安装：
   mt -t /dev/rmt/0 status
   该命令的输出取决于配置的驱动器。它与以下内容类似：
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention residual= 0 retries= 0 file no= 0 block no= 0
5. 系统重新启动完成后，可以使用命令 ls -all 检查已创建的设备文件。对于带库设备，该命令的输出可能是：

/dev/rmt/0hb	适用于第一个磁带驱动器
/dev/rmt/1hb	适用于第二个磁带驱动器
/dev/rsst6	适用于机械手驱动器

在 Windows 系统上查找未使用的 SCSI 目标 ID

在 Windows 系统上确定未使用的 SCSI 目标 ID（SCSI 地址）

1. 在 Windows 控制面板中，单击“SCSI 适配器”。
2. 对于列表中每个连接到 SCSI 适配器的设备，检查其属性。双击设备名称，然后单击**设置 (Settings)** 打开属性页。

   记住分配给设备的 SCSI 目标 ID 和 LUN（逻辑单元号）。这样可以找出哪些 SCSI 目标 ID 和 LUN 已被占用。

在 330fx 库上设置 SCSI ID

为机械手和驱动器选择未使用的 SCSI ID 后，可以使用带库设备的控制面板对它们进行检查和配置。**示例** 如果有库模型 330fx，则可以按如下步骤找到配置的 SCSI ID:

1. 从 READY 状态中，按“下一步”，此时将显示 ADMIN*。
2. 按 **Enter**，此时将提示您输入密码。请输入密码。
3. 此时将显示 TEST*，按“下一步”直到显示 SCSI IDs *。
4. 按 **Enter**。此时将显示 VIEW IDs* 。
5. 按 **Enter**。此时将显示 JKBX ID 6 LUN 0。
6. 按“下一步”。此时将显示 DRV 1 ID 5 LUN 0。
7. 按“下一步”。此时将显示 DRV 2 ID 4 LUN 0，等等。

多次按“取消 (CANCEL)”可返回到 READY 状态。

连接备份设备

以下是将备份设备连接到 HP-UX、Solaris、Linux 或 Windows 系统的常规步骤。

1. 选择将连接备份设备的客户机。
2. 在选定系统上安装介质代理。
3. 确定可供设备使用的未使用的 SCSI 地址
   - 如果连接到 HP-UX 系统，请检查所需驱动程序是否已安装并置入当前内核中。
   - 如果连接到 Solaris 系统，请检查是否已为要安装的设备安装所需驱动程序和更新配置文件。
   - 如果连接到 Windows 客户机，则可以加载或禁用本机磁带驱动程序，这取决于 Windows 系统版本。如果为已在 Data Protector 中配置的设备加载了本机磁带驱动程序且不使用本机磁带驱动程序，请确保对参考此特定设备的所有配置的 Data Protector 逻辑设备重命名设备文件名（例如，从 scsi1:0:4:0 重命名为 tape3:0:4:0）。
4. 在设备上设置 SCSI 地址 (ID)。根据设备类型，此操作通常可使用设备上的开关完成。有关详细信息，请参见设备自带的文档。注意: 在安装有 Adaptec SCSI 适配器并连接到 SCSI 设备的 Windows 系统上，必须启用 Host Adapter BIOS 选项，这样系统发出 SCSI 命令时才不会出现问题。
   要设置 Host Adapter BIOS 选项，请在系统启动期间按 Ctrl+A 进入“SCSI 适配器”菜单，然后选择“配置/查看 Host Adapter 设置”>“高级配置”选项并启用 Host Adapter BIOS。
5. 首先，打开设备和计算机，等待启动过程完成。验证系统是否正确识别新的备份设备。
   Windows 系统： 如果使用 devbra 实用程序，则可以验证系统是否正确识别新的备份设备。在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。
   在 devbra 命令的输出中，您将发现对于每个已连接且正确识别的设备都有以下行：

   ```
   备份设备规范 硬件路径 介质类型 ..... 例如，以下输出： HP:C1533A tape3:0:4:0 DDS ... ...
   ```

   意味着 DDS 磁带设备 (已加载本机磁带驱动程序) 具有驱动器实例编号 3，已连接到 SCSI 总线 0、SCSI 目标 ID 4 和 LUN 编号 0。或者，以下输出：

```
HP:C1533A scsi1:0:4:0 DDS ... ...
```

意味着 DDS 磁带设备 (未加载本机磁带驱动程序) 已连接到 SCSI 端口 1、SCSI 总线 0，磁带驱动器具有 SCSI 目标 ID 4 和 LUN 编号 0。

HP-UX 系统： 运行命令 /usr/sbin/ioscan -fn 显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的设备及其正确的 SCSI 地址。

如果在系统启动过程中没有自动创建设备文件，则应当手动创建。

Solaris 系统： 在 /dev/rmt 目录中运行 ls -all 命令显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的设备及其正确的 SCSI 地址。

Linux 系统： 在 /dev/rmt 目录中运行 ls -all 命令显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的设备及其正确的 SCSI 地址。

AIX 系统： 运行命令 lsdev -C 显示连接的设备列表（包括相应的设备文件）。

硬件压缩

大多数新型备份设备都提供了内置的硬件压缩功能，在设备配置过程中创建设备文件或 SCSI 地址时可启用该功能。有关详细步骤，请参阅《Data Protector 帮助》。

使用软件压缩而禁用硬件压缩时，数据由磁带客户机压缩并以压缩的形式发送到介质代理。如果使用软件压缩，则压缩算法可能会占用磁带客户机系统中大量的资源，但是这减小了网络负载。

硬件压缩由从介质代理客户机收到原始数据并以压缩模式将其写入磁带的设备来完成。硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数据较少。

要在 Windows 系统上启用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加“C”，例如：scsi:0:3:0C（如果加载磁带驱动程序，则为 tape2:0:1:0C）。如果设备支持硬件压缩，则会使用硬件压缩，否则将忽略 C 选项。

要在 Windows 系统上禁用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加 “N”，例如：scsi:0:3:0:N。

要在 UNIX 系统上启用/禁用硬件压缩，请选择正确的设备文件。有关详细信息，请参见设备和操作系统文档。

下面的步骤

至此，您应该已连接备份设备，这使您能够配置备份设备和介质池。有关进一步的配置任务的详细信息，请参阅《Data Protector 帮助》索引: “配置, 备份设备”。

系统上必须安装有介质代理。

以下章节将介绍如何将 Standalone 24 磁带设备、12000e 库和 DLT 库 28/48 插槽连接到 HP-UX 和 Windows 系统。

连接 24 独立设备

24 DDS 备份设备是一种基于 DDS3 技术的独立磁带驱动器。

连接到 HP-UX 系统

将 24 独立设备连接到 HP-UX 系统

1. 检查所需驱动程序 (stape 或 tape2) 是否已安装并置入当前内核中。
2. 确定可供磁带驱动器使用的未使用的 SCSI 地址。
3. 在设备上设置 SCSI 地址 (ID)。使用设备背面的开关。有关详细信息，请参见设备自带的文档。
4. 首先，打开设备和计算机，等待启动过程完成。
5. 验证系统是否正确识别新连接的磁带驱动器。使用 ioscan 实用程序：
   ```
   /usr/sbin/ioscan -fn
   ```
   显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。驱动器的设备文件已在启动过程中创建。

下面的步骤

正确连接设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接到 Windows 系统

将 24 独立设备连接到 Windows 系统

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址（目标 ID）。
2. 在设备上设置 SCSI 地址 (ID)。使用设备背面的开关。有关详细信息，请参见设备自带的文档。
3. 首先，打开设备和计算机，等待启动过程完成。
4. 验证系统是否正确识别新连接的磁带驱动器。在 Data Protector 命令目录中，执行 devbra -dev 命令。
   在 devbra 命令的输出中，应包含 24 独立设备的新连接的磁带驱动器。

下一步？

正确连接设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接 DAT 自动加载器

12000e 和 DAT24x6 库都有一个存储库 (带六个磁带盒)、一个驱动器和一个用于将磁带盒移入/移出驱动器的机械手臂。这两个带库还具有内置的脏磁带检测功能。

连接到 HP-UX 系统

将 12000e 库设备连接到 HP-UX 系统

1. 在自动加载器背面，将模式开关设置为 6。
2. 检查所需驱动程序 (stape 或 tape2) 是否已安装并置入当前内核中。
3. 检查所需 SCSI Pass-Through 驱动程序（sctl 或 spt）是否已安装并置入当前内核中。
4. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。
   注意: 12000e 库使用与磁带驱动器和机械手相同的 SCSI 地址，但是使用不同的 LUN 编号。
5. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。
6. 首先，打开设备和计算机，等待启动过程完成。
7. 验证系统是否正确识别新连接的磁带驱动器。使用 ioscan 实用程序
   /usr/sbin/ioscan -fn
   显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。
8. 驱动器的设备文件已在启动过程中创建，而机械手的设备文件必须手动创建。
9. 验证系统是否正确识别为带库机械手新创建的设备文件。运行 ioscan 实用程序：
   /usr/sbin/ioscan -fn
   在该命令的输出中应包含新创建的设备文件。

下面的步骤

正确连接库设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接到 Windows 系统

将 12000e 库设备连接到 Windows 系统

1. 在自动加载器背面，将模式开关设置为 6。
2. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。
3. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。
   注意: 12000e 库使用与磁带驱动器和机械手相同的 SCSI 地址，但是使用不同的 LUN 编号。
4. 首先，打开设备和计算机，等待启动过程完成。
5. 验证系统是否正确识别新连接的磁带驱动器和机械手。在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。
   在 devbra 命令的输出中，应包含 12000e 库设备的新连接的磁带驱动器和机械手。

下面的步骤

正确连接库设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接 DLT 库 28/48 插槽

DLT 库 28/48 插槽是用于要备份 80-600 GB 的企业环境的多驱动器库。它具有四个 DLT 4000 或 DLT 7000 驱动器、多个数据通道、一个邮件插槽和一个条形码读取器。

连接到 HP-UX 系统

将 DLT 库 28/48 插槽库设备连接到 HP-UX 系统

1. 检查所需驱动程序（stape 或 tape2）是否已安装并置入当前内核中。
2. 检查所需 SCSI Pass-Through 驱动程序（sctl 或 spt）是否已安装并置入当前内核中。

3. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。
   注意: DLT 库 28/48 插槽具有四个磁带驱动器和机械手，因此需要五个未使用的 SCSI 地址以防同时使用所有磁带驱动器。磁带驱动器和机械手必须使用不同的 SCSI 地址。
4. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。
5. 打开设备和计算机，等待启动过程完成。
6. 验证系统是否正确识别新连接的磁带驱动器。使用 ioscan 实用程序
   /usr/sbin/ioscan -fn
   显示连接的设备列表（包括相应的硬件路径和设备文件），其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。
7. 驱动器的设备文件已在启动过程中创建,而机械手的设备文件必须手动创建。
8. 验证系统是否正确识别为带库机械手新创建的设备文件。使用 ioscan 实用程序：
   /usr/sbin/ioscan -fn
   在该命令的输出中应包含新创建的设备文件。

下面的步骤

正确连接 DLT 库 28/48 插槽库设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接到 Solaris 系统

对于此示例，假设两个驱动器将分配给 Data Protector。

在 Solaris 系统上配置 C5173-7000 库设备

1. 将 sst 驱动程序（模块）和配置文件 sst.conf 复制到要求的目录：
   - 对于 32 位操作系统：

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

   - 对于 64 位操作系统：

     ```
     $cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9 /sst $cp /opt/omni/spt/sst.conf /usr/kernel/drv /sparcv9/sst.conf
     ```

2. 将驱动程序添加到 Solaris 内核：
   add_drv sst
3. 从 /dev/rmt 目录中删除所有现有的设备文件：
   cd /dev/rmt rm *
4. 按“停止”和 A 停止系统。
5. 在出现 " ok " 提示时运行 probe-scsi-all 命令，以检查哪些 SCSI 地址可用。
   ok probe-scsi-all
   系统可能会要求您先启动 reset-all 命令，再执行 probe-scsi-all 命令。
   在此例中，端口 6 用于 SCSI 控制设备，端口 2 用于第一个驱动器，端口 1 用于第二个驱动器，LUN 是 0。
6. 返回到正常运行：
   ok go
7. 将 st.conf 配置文件复制到要求的目录：
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   st.conf 文件存在于每个 Solaris Data Protector 客户机上并包含每个连接到客户机的备份设备的 SCSI 地址。
8. 编辑 /kernel/drv/st.conf 文件并添加以下行：

   ```
   tape-config-list= "QUANTUM DLT7000", "Digital DLT7000", "DLT-data3"; DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;
   name="st" class="scsi" target=1 lun=0; name="st" class="scsi" target=2 lun=0; name="st" class="scsi" target=6 lun=0;
   ```

   这些条目分别为驱动器 1、驱动器 2 和机械手驱动器提供 SCSI 地址。

9. 编辑 sst.conf 文件 (在复制 sst 驱动程序 (模块) 和配置文件 sst.conf 时复制到要求的目录)，并添加以下行: name="sst" class="scsi" target=6 lun=0;
   注意: 该条目必须与 st.conf 文件中机械手驱动器的条目匹配。
10. 关闭客户机系统，并连接库设备。
11. 首先打开库设备，然后打开客户机系统。
    现在系统将启动并自动为机械手驱动器和磁带驱动器创建设备文件。使用命令 ls -all 可以列出这些设备文件。在此例中：

/dev/rmt/0hb	适用于第一个磁带驱动器
/dev/rmt/1hb	适用于第二个磁带驱动器
/dev/rsst6	适用于机械手驱动器

下一步？

正确连接 DLT 库 28/48 插槽库设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接到 Windows 系统

将 DLT 28/48 插槽库设备连接到 Windows 系统

1. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址（目标 ID）。

2. 在设备上设置 SCSI 地址（目标 ID）。有关详细信息，请参见设备自带的文档。
   注意: DLT 库 28/48 插槽具有四个磁带驱动器和机械手，因此需要五个未使用的 SCSI 地址以防同时使用所有磁带驱动器。磁带驱动器和机械手必须使用不同的 SCSI 目标 ID。
3. 首先，打开设备和计算机，等待启动过程完成。
4. 验证系统是否正确识别新连接的磁带驱动器和机械手。在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。在 devbra 命令的输出中，应包含 DLT 库 28/48 插槽库设备的新连接的磁带驱动器和机械手。

下面的步骤

正确连接 DLT 库 28/48 插槽库设备后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的带库设备配置 Data Protector 备份设备的相关说明。

连接 Seagate Viper 200 LTO Ultrium 磁带驱动器

Seagate Viper 200 LTO Ultrium 磁带驱动器是一种用于要备份 100-200 GB 的企业环境的独立设备。

连接到 Solaris 系统

在 Solaris 系统上配置 Seagate Viper 200 LTO Ultrium 磁带驱动器

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址。运行 modinfo 或 dmesg 命令查找使用中的 SCSI 控制器和已安装的 SCSI 目标设备：
   dmesg | egrep “target” | sort | uniq
   应得到以下输出：

   ```
   sd32 at ithps0: target 2 lun 0 sd34 at ithps0: target 4 lun 0 st21 at ithps1: target 0 lun 0 st22 at ithps1: target 1 lun 0
   ```

   注意: 在将 Viper 200 LTO 设备连接到 Solaris 系统时，建议使用 glm 或 isp SCSI 控制器。另建议使用 Ultra2 SCSI 或 Ultra3 SCSI 控制器。
2. 编辑 /kernel/drv/st.conf 文件并添加以下行：

   ```
   tape-config-list= “SEAGATE ULTRIUM06242-XXX” , “SEAGATE LTO” , \ “SEAGATE_LTO”; SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \ 0x00, 1;
   ```

3. 关闭客户机系统，并连接设备。
4. 依次打开设备和客户机系统。
   现在系统将启动并自动为磁带驱动器创建设备文件。使用命令 ls -all 可以列出这些设备文件。

下一步？

正确连接 Seagate Viper 200 LTO Ultrium 磁带驱动器后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。

连接到 Windows 系统

在 Windows 系统上连接 Seagate Viper 200 LTO Ultrium 磁带驱动器

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址（目标 ID）。
2. 在设备上设置 SCSI 地址（目标 ID）。有关详细信息，请参见设备自带的文档。
3. 首先，打开设备和计算机，等待启动过程完成。
4. 验证系统是否正确识别新连接的磁带驱动器和机械手。在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。在 devbra 命令的输出中，应包含 Seagate Viper 200 LTO Ultrium 磁带驱动器的新连接的磁带驱动器。

下面的步骤

正确连接 Seagate Viper 200 LTO Ultrium 磁带驱动器后，请参阅《Data Protector 帮助》索引: “配置, 备份设备”了解为新连接的设备配置 Data Protector 备份设备的相关说明。
注意: 在 Data Protector 中配置 Seagate Viper 200 LTO Ultrium 磁带驱动器时，请确保设置了压缩模式。方法是在驱动器的 SCSI 地址后指定 C 参数，例如：
scsi2:0:0:0C

选项

本主题包含 Data Protector 的所有常规选项的列表。

- 选项：未完全创建快照式克隆则最多推迟磁带备份 X 分钟
- 选项：描述
- 选项：说明 - 介质池
- 选项：卸载应用程序系统上的文件系统
- 选项：在复本生成之前卸除应用程序系统上的文件系统
- 选项：显示统计信息
- 选项：不检查中止 ID
- 选项：不检查已用的会话时间
- 选项：会话后弹出介质
- 选项：启用 Magic Packet
- 选项：启用可恢复的恢复
- 选项：仅启用受保护对象的选择
- 选项：以读取/写入模式启用备份系统
- 选项：估计持续时间
- 选项：硬件压缩
- 选项：导入副本作为原件
- 选项：增量
- 选项：增量 1
- 选项：在备份完成之后保留复本 (SA)
- 选项：级别(通知)
- 选项：在备份期间锁定文件
- 选项：日志记录
- 选项：MAC 地址
- 选项：MU 编号 (特定于 P9000 XP 的选项)
- 选项：箱盒支持
- 选项：每个存储的最大连接数量
- 选项：最大重写次数
- 选项：介质池
- 选项：介质类型
- 选项：在会话结束时
- 选项：在会话开始时
- 选项：移动繁忙文件
- 选项：将自由介质移至自由池
- 选项：不覆盖
- 选项：非权威
- 选项值：无
- 选项：轮换的复本数量
- 选项：重试次数（Windows 特有选项）
- 选项：在客户机上
- 选项：选择原始设备
- 选项：所有权
- 选项：路径
- 选项：池名称
- 选项：post-exec（备份会话）
- 选项：post-exec（备份对象）
- 选项：pre-exec（备份会话）
- 选项：pre-exec（备份对象）
- 选项：prealloc 列表
- 选项：为备份 (重新同步) 准备下一镜像磁盘
- 选项：主
- 选项：公共
- 选项：重新连接已断开的连接
- 选项：成功复制后回收失败的源对象的数据和编目保护
- 选项：冗余级别
- 选项：将打开的锁定文件报告为（Windows 特有选项）
- 选项：重新启动应用程序命令行
- 选项：还原目录的共享信息（Windows 特有选项）
- 选项：备份系统上安装路径的根目录
- 选项：脚本
- 选项：查看私有对象
- 选项：单个消息级别
- 选项：快照源
- 选项：快照类型
- 选项：使应用程序命令行停止/静默
- 选项：存储大小软配额 (GB)
- 选项：切换会话所有权
- 选项：如果尚未同步，则同步磁盘
- 选项：超时
- 选项：跟踪复本以用于即时恢复 (P9000 XP 磁盘阵列系列选项)
- 选项：跟踪即时恢复的复本
- 选项：使用直接库访问 (特定于 SAN 的选项)
- 选项：使用自由池
- 选项：使用锁名称
- 选项：使用复制
- 选项：使用与应用程序系统上相同的装载点
- 选项：有效期(月)
- 选项：BDACC
- 选项：DATALIST
- 选项：MODE
- 选项：OWNER
- 选项：PREVIEW

选项：分配 - 宽松

如果选择了此选项，则 Data Protector 将接受池中任意合适的介质（介质不得处于差状况或不受保护）。

此选项可以与**首先分配未格式化的介质**选项组合使用。

如果将全局选项 InitOnLoosePolicy 设置为 1（默认值为 0），则自动初始化 (格式化) Data Protector 无法识别的介质。对于堆栈器设备（这些设备按顺序加载介质）或如果不希望无人看管备份因指定介质不可用而失败，建议采用此策略。

选项：块大小(KB)

设备接收数据时，使用设备类型特有（DDS、LTO）的块大小处理数据。通过从下拉列表中选择一个值或手动键入甚至更高的值，可以在备份设备的“高级选项”中设置块大小。Data Protector 支持从 8 kB 到 1024 kB 的块大小。

在使用更大的块大小之前，请检查当前主机适配器所支持的块大小。对于由 NDMP 控制的设备，请检查 NDMP 服务器所支持的块大小（记录大小）。

请注意，Data Protector 只能向用相同块大小写入的介质进行追加。

默认值：**QIC**：32 KB **其他设备类型和型号**: 256 kB

选项：全部记录

这是默认的日志记录级别。有关所备份的文件和目录的所有详细信息 (名称、版本和属性) 都记录到 IDB 中。

可以在还原之前浏览目录和文件，此外还可以查看文件属性。Data Protector 可以在恢复特定文件或目录时快速定位磁带。

选项：不记录任何内容

选择此日志记录级别时，不会将有关所备份的文件和目录的任何信息（名称和版本）记录到 IDB 中。还原之前，将无法搜索和浏览文件和目录。

选项：软件压缩

使用此选项可压缩由磁带客户机读取的数据。以压缩格式将数据写入介质，此格式减少备份所需的介质数，并在某些情况下改进备份性能。默认情况下，不选择此选项。

由于双重压缩仅会降低性能而不会产生更好的压缩结果，因此如果硬件提供内置的硬件压缩功能，请不要使用此选项。

可以使用自定义压缩库而非由 Data Protector 提供的那些库。请注意，更改压缩库后应执行完整备份。

选项：分配 - 严格

如果选择了此选项，则 Data Protector 需要特定的介质。必须已将该介质格式化 (初始化) 以用于 Data Protector。Data Protector 在备份会话期间不自动格式化介质。

如果介质的均衡使用优先于方便使用，以及带库中有设备既包含 Data Protector 介质也包含非 Data Protector 介质，则应采用此分配策略。选择严格分配策略可防止意外覆盖非 Data Protector 介质。

选项：将 POSIX 硬链接作为文件进行备份

这是 UNIX 文件系统特有的选项。此选项介绍 Data Protector 如何备份硬链接。

默认情况下，不选择此选项。以链接形式备份硬链接时，Data Protector 将遍历目录树两次。这样使 Data Protector 可估计备份的大小，但是这需要花费额外的时间。仅用文件内容备份一个硬链接，而所有其他硬链接都以硬链接形式备份。

如果选择此选项，则 Data Protector 对于每个硬链接都将备份整个文件内容。Data Protector 仅遍历文件系统树一次，因此显著加快了备份过程。当目录中没有硬链接时，请使用此选项。当选择此选项时，Data Protector 无法估计备份的大小或显示所完成备份的百分比。

选项：CRC 检查

CRC 检查是一种增强的校验和功能。选择此选项后，备份期间将向介质写入循环冗余校验和 (CRC)。通过 CRC 检查，可在备份之后验证介质。Data Protector 在还原期间重新计算 CRC，并将它与介质上的 CRC 相比较。验证和复制介质或验证对象时也使用此过程。默认情况下，不选择此选项。

可以对备份、对象复制和对象合并操作指定此选项。

选项：并发

通过并发，可以有多个磁盘代理同时写入一个备份设备。这样有助于 Data Protector 保持设备流式传送，因为设备接收数据所能达到的速度超过磁盘代理发送数据所能达到的速度。来自这些磁盘代理的数据交错存放在介质上。最大并发值为 32。

Data Protector 对所有支持的设备都提供默认并发。用于备份 Microsoft Exchange Server 数据的设备的最大设备并发对于直接连接到 Exchange Server 系统的设备为 2，对于远程连接到 Exchange Server 系统的设备为 1。

指定可同时写入设备的磁盘代理数。可以对备份、对象复制和对象合并操作指定此选项。

选项：不使用存档属性 (特定于 Windows 的选项)

如果未选择此选项（使用存档属性），则 Data Protector 在备份文件之后会使用存档属性作为增量备份的标准，还会清除该文件的存档属性。当文件的内容、属性、名称或位置更改时，系统将自动设置存档属性。

如果无法清除存档属性，则报告错误。这会影响未来的增量备份，这样将备份文件，即使其尚未更改也是如此。备份具有写保护的可移动介质时，可能会发生这种情况。

如果 VSS 用于分级增量备份，则文件将在执行初始备份时进行备份，但是在下次执行同级或更低级的备份时将不会进行备份。分级增量备份不应与存档位配合使用。

在 ZDB 的情况下，将清除复本中的存档属性，并且不会反映在源卷上。因此，在下一次增量 ZDB 会话中，当创建新复本后，将再次设置存档属性，并且将备份相应的文件，即使其可能尚未更改也是如此。此类文件的数量可能会持续增加，尽管已选择增量备份类型，也可以执行完整备份。要增强增量 ZDB 行为，请选择此选项。

如果选择了此选项，则 Data Protector 忽略存档属性，并使用其他标准检测（如文件的修改时间）更改的文件。

默认：未选择。

选项：完整

如果选择了此选项，则备份所选的全部对象，即使从上一次备份以来没有更改也是如此。

完整备份的优点是安全（在一个备份会话中备份所有数据），并可以更快速、更简单地还原（仅需最新完整备份的介质）。

缺点是完成完整备份需要更多时间，并在介质上和在 IDB 中占用更多空间，因为可以多次备份文件的相同版本。

选项：负载均衡

默认情况下，Data Protector 自动协调设备的负载（使用情况），以便均匀地使用这些设备。负载均衡通过调整备份到每个设备的对象数量优化设备使用情况。由于在备份时自动完成负载均衡，因此不需要管理向设备分配对象，这样所有已分配的设备在备份会话期间保持繁忙。指定用于此会话的设备，Data Protector 就会动态分配这些设备。

如果不选择负载均衡，则要选择哪个设备将用于备份规范中的每个对象，而 Data Protector 将只使用指定的设备。

最小 启动会话所需的最小可用设备 (未由其他 Data Protector 会话使用并经许可能够使用的设备) 数。如果可用设备比此处指定的少，则将会话排入队列。默认值：1.

最大 Data Protector 在会话中将同时使用的最大可用设备数。默认值：5.

选项值：记录文件

选择此日志记录级别时，将有关所备份的文件和目录的详细信息（名称和版本）都记录到 IDB 中。

可在还原之前浏览目录和文件，而 Data Protector 可以在还原特定文件或目录时在磁带上快速定位。这些信息不会占用太多空间，因为并非所有文件详细信息（文件属性）都记录到数据库中。

选项：网络负载

选择会话的网络负载。

将此选项设置为“中”或“低”可减少运行 Data Protector 时网络上的负载。这样可防止数据传输阻止其他用户使用网络，但会增加会话完成所需的时间。

默认值：高。

选项：报告级别

此选项定义将在备份或恢复会话期间为对象报告的错误的级别。报告级别为：**Warning**、**Minor**、**Major** 和 **Critical**。报告所选级别及更高级别的错误。例如，通过将级别设置为**轻微**，仅在“消息”字段中报告轻微、重大和严重错误。默认情况下，级别设置为 **Warning**。始终报告 **Normal** 级别的消息。

IDB 中存储的每备份系统的消息数限制为 3000。

选项：使用 - 不可追加

如果选择此选项，则只能将数据从一个备份会话写入此特定介质。尝试将备份会话追加到此介质将导致发出装载请求。您需要响应装载请求。

选项：使用卷影复制

如果要使用 Microsoft Volume Shadow Copy Service (VSS) 执行时间点备份，则选择此选项。使用 VSS 可以创建卷的卷影复制备份和文件的精确时间点副本，包括所有打开的文件。这意味着 VSS 机制在准备卷影复制卷时，完成所有挂起的输入/输出操作，保留传入写请求。这样，在创建卷影副本时，文件系统级别上的所有文件都是关闭的，并且未锁定。此选项仅适用于 Windows 系统，默认情况下处于选中状态。

在 Windows 系统上，如果为备份选择了整个卷并且为该卷选择了此选项，则在相应的 VSS 写入程序可用时，Data Protector 还可以在备份之前，确保每个 Windows Server 角色的数据或在卷上存储其数据的第三方应用程序的数据保持一致。为文件系统备份选择整个客户机系统时，也会产生相同的行为。

在为灾难恢复目的配置 Windows 系统的备份规范时，必须选择此选项，否则备份数据可能无法用于灾难恢复。

选项：分配顺序

一系列连续数字，定义 Data Protector 按照哪种顺序选择将新数据写入其中的 DC 目录，但前提是有效的 DC 目录分配策略是 Fill in sequence（ DCDirAllocation 全局选项设置为 0 ）。要使用的第一个 DC 目录应具有最低的分配序列号。

默认值：（值与现有 DC 目录数相匹配）

选项：备份目录的共享信息 (特定于 Windows 的选项)

指定将备份目录的共享信息。默认情况下，选择此选项。

如果备份目录时在网络上共享该目录，则还原之后也将共享该目录。如果不希望在还原之后共享此类目录，请在还原数据时清除**还原目录的共享信息**选项。

选项：检测 NTFS 硬链接

此选项允许检测 NTFS 硬链接。默认情况下，Data Protector 不检测 NTFS 硬链接，并以文件形式备份硬链接。这样可显著提高备份性能，但文件在介质上占用的空间较多。不保留原始结构，并在还原时以文件形式还原硬链接。请注意，通常 Windows 中不使用 NTFS 硬链接，因此一般不需要启用此选项。但是，如果您要在稍后执行灾难恢复，则必须启用此选项。

默认：未选择。如果已选择用于备份的 CONFIGURATION/SystemRecoveryData 对象 (灾难恢复所需)，则在创建备份规范时会自动选择。

如果使用增强型增量模式，该选项不可用。

选项：检测不洁驱动器

选择此设备选项可指示 Data Protector 使用设备的不洁驱动器功能。Data Protector 以两种方式处理不洁驱动器：

如果设备没有清洗介质存储库，则 Data Protector 发出“cleanme”请求。通过插入清洗磁带并确认“cleanme”请求，清洗不洁驱动器。

如果设备支持清洗磁带并且配置了清洗插槽，则设备发出“不洁驱动器”状态的信号时，Data Protector 将自动插入清洗磁带。

选项：磁盘代理缓冲区

Data Protector 介质代理和磁带客户机在数据传输期间使用内存缓冲区。这些内存分为许多缓冲区。缓冲区大小是介质代理在其缓冲区中可容纳的磁带客户机块数。可以指定 1 到 32 的值。

磁带客户机块的默认数为 8。

选项：不保留访问时间属性

打开、读取或锁定文件（发生在备份期间）后，文件的访问时间属性将更改。如果未选择此选项，则在备份之后，Data Protector 将文件的访问时间属性重置为其在备份之前的值。但是，在 UNIX 系统中，这种重置访问时间属性也会修改文件的更改时间。

在 UNIX 系统上，如果选择此选项（不保留访问时间属性），则 Data Protector 还可以使用文件的更改时间（inode 修改时间）作为增量备份的标准。因此，在增量备份中备份名称、位置或属性更改的文件。

访问时间将用 VSS 保留。

默认：未选择。

选项：故障转移时不重新启动备份

不重新启动备份。这是默认选项。

选项：基于驱动器的加密

选择此选项可允许对备份进行硬件加密，这样可防止在介质存储和传输期间未经授权访问数据。数据经过压缩、加密和格式化，因此在写入介质之前受到全面保护。

选项值：编码

通过 Data Protector，可以对文件系统和磁盘映像数据进行编码，以防止其他人在数据通过网络传输时访问这些数据。对数据进行编码，然后再通过网络传输这些数据并将其写入介质。默认情况下，不选择此编码选项。

Data Protector 提供一个以共享 C 程序带库实现的简单内置 XOR 算法。由于 Data Protector 向具有数据编码模块的接口提供由磁带客户机使用的 API，因此可以代替您自己的内部数据编码算法，以获得更大的安全性。为此，请编写自己的数据编码模块，将其编译到带库中，并用新库代替默认的 Data Protector 带库。请注意，更改编码库后应执行完整备份。

选项：增强型增量备份

选择此选项可启用增强型增量备份。与传统的增量备份不同，增强型增量备份可以可靠地检测并备份名称、位置和属性发生更改的文件。它还是后续对象合并（合成备份）的先决条件。

选择此选项之后，在执行完整备份之后，增量备份将仅以增强模式运行。

要在下一次备份中运行增强备份，尽管计划的下一次备份为增量备份，也要将全局选项 EnhIncrPromoteToFullIfNoEnhFull 设置为 1 ，这样会将下一次备份提升为完整备份。

选项：强制操作

使用此选项以便格式化（初始化）Data Protector 可识别的其他格式（tar、OmniBack I 等等）的介质或已由另一个应用程序使用的介质，或重新格式化 Data Protector 介质。

直到取消保护后，才会格式化含有受保护数据的 Data Protector 介质。

选项：增量 1-9

（可用的增量级别对于特定的集成有所不同。）

Incr1-9（也称为分级增量备份）仅备份从下一个更低级别的上一次受保护备份以来所做的更改。例如，Incr1 保存上次完整备份以来的所有更改，而 Incr5 备份保存上次 Incr4 备份以来的所有更改。Incr1-9 备份永不引用现有的 Incr 备份。如果没有受保护的完整备份，则 Data Protector 将改为启动完整备份。

增量备份的优点是完成备份所需的时间较少（备份的数据量较小），并且在介质上和 IDB 中占用的空间也较小。

缺点是还原起来更加复杂，因为通常需要从上一次完整备份以来用过的所有介质。

选项：增量

增量备份（Incr、Incr 1、Incr 2 等等）仅包括自从上一次完整或增量备份以来修改的数据。增量备份速度更快，并且需要的介质更少，但由于通常需要从上一次完整备份以来使用过的所有介质，因此使所有数据的还原更加复杂。

选项值：记录目录

选择此日志记录级别时，将有关所备份的目录的所有详细信息（名称、版本和属性）都记录到 IDB 中。

还原之前只能浏览目录。但是，在还原期间，Data Protector 仍执行快速定位，因为文件位于磁带上接近其实际所在目录的地方。此选项适用于许多文件为自动生成的文件系统，如新闻和邮件系统。

选项：空间不足

一个数量，定义 DC 目录在什么情况下被视为已满。实际上，它定义 DC 目录的实际大小与所配置的最大大小之间允许的最小差异。当达到此阈值时，Data Protector 使用由有效的分配策略定义的下一个 DC 目录启动。此外，此选项还定义 DC 目录驻留的卷所需的最小可用空间量。Data Protector 需要此空间来日志记录备份到 IDB 的文件和目录的名称。当上一个 DC 目录的可用空间低于该数量时 (意味着所有其他 DC 目录被视为已满)，Data Protector 将自动切换到“无日志”日志记录级别。

Data Protector 建议使用当前最大 DC 目录大小的 10% 或 15% 作为该选项的适当值。

默认值：2,048 MB (2 GB)。

选项：最大文件数

一个数值，限制可以同时存在于 DC 目录上的 DC 二进制文件数。对于每个用于备份的 Data Protector 介质，都会创建一个 DC 二进制文件。当备份介质被覆盖时，其相应的 DC 二进制文件将被删除，并将创建一个新的 DC 二进制文件。

默认值：100 000。

选项：最大大小

限制 DC 目录中 DC 二进制文件的总大小的数量。

默认值：204 800 MB (200 GB)。

介质条件 - 中

此介质状态意味着已达到寿命或使用次数的阈值的 95% 至 100%。

选项：介质条件 - 好

此介质状态意味着尚未达到寿命或使用次数的阈值的 95%。

介质条件 - 差

此介质状态意味着已超出寿命或使用次数的阈值，或介质上已发生读/写错误。Data Protector 不会使用状况为差的介质进行备份。

如果介质因设备错误而被标为差，则可以验证介质以检查和更改其状况。

选项：永久

此备份保护选项提供永久保护。这意味着永久保护数据防止被覆盖。

选项：保护

通过此选项，可为所备份的数据设置保护期，以防止数据被覆盖。默认值为**永久**。其他值为：

无: 不提供任何保护。在下次启动对文件库的写入操作/备份之前，介质将被删除。

直到: 表示直到指定日期才能覆盖介质上的数据。对数据的保护将在所选日期的中午停止。

天: 表示在指定的天数内不能覆盖介质上的数据。

周: 表示在指定的周数内不能覆盖介质上的数据。

选项：成功复制后更改数据和编目保护

选择此选项以为对象复制会话中涉及的源对象更改数据和目录保护期。更改期间仍将从源对象创建时应用。

源介质上不再有受保护的对象时，可以覆盖介质。

选项：重新扫描

如果选择此选项，则在启动备份之前，Data Protector 更新存储库信息。在插槽中手动更改介质顺序或输入并弹出介质时，这会很有用。

选项：重新启动所有对象的备份

Data Protector 重新启动完整备份会话。此选项可用于文件系统和集成备份（如 Oracle）。

选项：重新启动失败对象的备份

Data Protector 仅重新启动故障转移时失败的对象的备份。这最大限度地减少了备份时间，可防止在某些对象的备份已经完成时发生故障转移，因为 Data Protector 不会重新启动这些对象。此选项仅适用于文件系统备份，并且是首选选项。当重新启动失败的备份时，备份会使用新的会话 ID 重新启动。

选项：段大小(MB)(S)

选择介质上数据段的大小。

段大小影响还原和导入介质的速度。较小的段大小在介质上需要其他空间，因为每个段都有快速搜索标记。其他快速搜索标记导致更快还原，因为介质代理可以快速定位包含还原数据的段。另一方面，对于更小段，有更多目录段，这些段使导入介质更慢。

默认段大小取决于介质类型。可以指定的最小值是 10。最佳段大小取决于设备中使用的介质类型和要备份的数据类型。可以通过将介质的本机容量 (以 MB 为单位) 除以 50 来计算。例如，本机容量为 6 TB (6000000 MB) 的 LTO7 驱动器的最佳段大小将为 120000 MB。

选项：分割镜像/快照备份

如果要在镜像/快照创建之后将镜像/快照数据流式传送到磁带，并且还在备份后保存在磁盘阵列上，则选择**到磁盘+磁带**。

如果要在备份之后将镜像/快照数据保留在磁盘阵列上，但不在镜像/快照创建之后流式传送到磁带，则选择**到磁盘**。

选项：使用 - 可追加

如果选择此选项，则备份会话使用的第一个介质包含从上一个备份会话备份的数据，因此会使用介质上的剩余空间。如果在同一个备份会话期间需要其他介质，则会使用空的或取消保护的介质。

如果池中有多个可用的可追加介质，将使用最早写入的介质。

通过此介质使用策略，备份类型（完整或增量备份）可以在介质上以任何顺序组合。

追加介质可以节省介质空间，但降低了操纵介质的灵活性，因为一个介质可能包含来自几个备份会话的数据。

对于文件库不建议使用可追加介质使用策略。此外，如果使用文件库执行对象复制或对象合并，则不支持可追加策略。需要使用不可追加介质使用策略。

选项：用法 - 仅对于增量可追加

如果选择此选项并执行增量备份，则备份会话使用的第一个介质包含从上一个备份会话备份的数据，因此会使用介质上的剩余空间。如果在同一个备份会话期间需要其他介质，则会使用空的或取消保护的介质。

如果池中有多个可用的可追加介质，将使用最早写入的介质。

此介质使用策略将创建包含一个完整备份并且后跟许多增量备份的介质。

选项：使用本机文件系统更改日志提供程序(如果有)

如果选择此选项，将使用 Windows NTFS 更改日志提供程序（如果可用）执行增强的或传统的增量备份。在此情况下，将使用 Windows 更改日记生成自上次完整备份以来已修改的文件的列表，而不执行文件树遍历。

此选项不适用于非 Windows 平台。

选项值：**AES 256 位**

选择此选项可进行软件加密以保护数据。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。

但是，如果出于数据安全考虑选择了 AES-256，则磁带客户机将切换到联邦信息处理标准 (FIPS) 模式来进行数据加密。

选项：小于此时间则中止

发生故障转移并且启动 omniclus 命令后，如果会话运行时间小于此选项中指定的分钟数，则 Data Protector 中止该会话。

选项：大于此时间则中止

发生故障转移并且启动 omniclus 命令后，如果会话运行时间大于此选项中指定的分钟数，则 Data Protector 中止该会话。

选项：如果镜像磁盘尚未同步，则中止会话

选择**为备份(重新同步)准备下一镜像磁盘**时可用。

如果当前 ZDB 会话中要使用的复本卷至少有一个为镜像（或镜像副本），则此选项可用。相反，Data Protector 将视作已选择**尚未同步时同步磁盘**。

如果已选择此选项，并且当前 ZDB 会话中要使用的卷复本至少有一个未与对应的源卷处于“配对”状态，则会话将失败。

默认：未选择。

选项：将目录添加到装载路径

通过此选项，可以单独控制所创建的各个装载点。在创建路径过程中使用会话 ID 时，这样可保证各个装载点唯一。

这些选项定义用“备份系统上装载路径的根目录”选项指定的目录中将创建哪些子目录。

示例

根目录： c:\mnt

应用程序系统： app.comp.com

备份会话 ID： 2008-02-22-4

应用程序系统上的装载路径： E:\disk1.

如果选择**主机名**： c:\mnt\app.comp.com\E\disk1

如果选择**主机名 + 会话 ID**（默认）： c:\mnt\app.comp.com\2008-02-22-4\E\disk1

如果选择**会话 ID**： c:\mnt\2008-02-22-4\E\disk1

如果选择**会话 ID + 主机名**： c:\mnt\2008-02-22-4\app.comp.com\E\disk1

选项：备份后保留复本 (Data Protector 选项)

如果配置“ZDB 到磁带”，则选择此选项，以在零宕机时间备份会话之后将复本保留在磁盘阵列上。复本将变成复本集的一部分（为 **MU 编号**选项指定一个值）。除非**跟踪复本以用于即时恢复**的其他选项处于选中状态，否则复本*不* 可用于即时恢复。

如果未选择此选项，则会在会话结束时删除复本。

此选项会在**跟踪复本以用于即时恢复**选项处于选中状态时自动选择而且无法更改。

默认：选择。

选项：分配 - 首先分配未格式化的介质

如果选择**宽松**分配策略，则有此选项可用。

如果选择了此选项，则 Data Protector 将在释放 Data Protector 介质和中等介质之前、但仍在预分配顺序 (如果指定) 之后选择未格式化的介质用于备份，并且可追加 (如使用策略中所设置)。

如果未选择此选项，则 Data Protector 将在空闲 Data Protector 介质之后以及在预分配顺序（如果指定）之后选择未格式化的介质进行备份，并且可追加（如使用策略中所设置）。在未格式化的介质之后只能选择中等介质。

如果 Data Protector 是唯一一个使用带库的应用程序，并且希望均衡使用所有介质，则建议选项此选项。

选项：允许回退

在基于卷影复制服务（**VSS**）文件系统备份期间创建卷影副本失败时，默认情况下备份也将失败。如果希望在创建卷影副本失败时 **VSS** 文件系统备份作为正常的文件系统备份继续进行，则指定此选项。

在为灾难恢复目的配置受支持 Windows 系统的备份规范时，需要取消选择“允许回退”选项，否则备份数据可能无法用于灾难恢复。

选项：应用程序系统

运行应用程序的系统。在群集环境中，指定虚拟服务器主机名（而非物理节点主机名）。

选项：异步读取 (特定于 Windows 的选项)

如果选择了此选项，则磁带客户机将从磁盘执行异步读取，而不使用 Windows 缓存管理器。同时对相同文件启动并发读取。可以通过设置前缀为 OB2DAASYNC 的 omnirc 选项微调此行为。

如果未选择此选项，则从磁盘执行同步读取。

默认：未选择。

选项：权威

这是 Windows Server 特有的一个选项，用于处理 Active Directory 还原。还原之后不更新 Active Directory 数据库，并且还原的数据将覆盖目标中的现有数据。只有在还原会话完成之后通过从命令提示符下运行 ntdsutil.exe 才能执行权威还原。

选项：自动选择设备

当没有原始设备可供恢复或对象副本使用时，此选项适用。选择此选项可使 Data Protector 能够自动将不可用的设备替换为针对还原或对象副本选择的、并且设备标记与原始设备相同的其他设备。如果没有足够的设备可供替换原始设备，则启动还原或对象副本时设备将少于备份期间使用的设备。

默认情况下，Data Protector 首先尝试使用原始设备。如果未选择原始设备用于还原或对象副本，则考虑全局选项。要优先使用备用设备或干脆不用原始设备，请修改全局选项 AutomaticDeviceSelectionOrder 。

对于 Data Protector SAP MaxDB、DB2 UDB、Microsoft SQL Server 和 Microsoft SharePoint Server 2010/2013 集成，请确保可用设备数等于或大于备份期间所用的设备数。

默认：选择。

选项：在目标装载点自动卸除文件系统

如果装载点在使用中（例如，可能仍然装载之前会话中涉及的卷）并且已选择此选项，则 Data Protector 会尝试卸载装载的文件系统。

如果未选择此选项且装载点在使用中，或者已选择此选项但卸载操作失败，则会话操作将失败。

默认：未选择。

选项：**Business Copy P9000 XP**

选择此选项可为采用 P9000 XP 磁盘阵列系列配置的 Business Copy P9000 XP 配置 ZDB 备份规范。

默认：选择。

选项：备份文件的大小

可以指定要备份文件的大小。可以备份**所有大小**（默认）的文件、**大于**、**小于**某个大小或在指定大小**范围**（以 KB 为单位）内的文件。

选项：备份保护

指定对于所备份数据的保护期，以防备份被覆盖。

选项：备份大小软配额 (GB)

输入备份大小软配额 (GB)。如果在删除重复数据之前，数据的大小超过所设置的配额，则会话将显示一则警告，但数据仍将写入存储。该配额对备份、复制和对象合并会话有效。

如果备份大小配额小于存储大小配额，将显示一则警告并且存储大小配额将无效。

如果设置为 0 或字段为空，则说明未设置配额。

默认：未设置。

选项：备份系统

将向其复制（备份）数据的系统。在 ZDB 到磁盘+磁带和 ZDB 到磁带会话中，将备份数据从此系统复制到备份设备。

选项：备份系统

将向其备份数据的系统。在群集环境中，指定虚拟服务器主机名 (而非物理节点主机名)。

在 EMC GeoSpan for MSCS 环境中，选择活动节点的备份系统。故障转移之后，选择当前活动节点的备份系统，然后保存备份规范。

选项：条码读取器支持

如果设备和介质可以处理条码，则可以选择此选项以使用条码功能。

选项：组合 (Continuous Access P9000 XP + Business Copy P9000 XP)

选择此选项可为 P9000 XP 磁盘系列组合配置 Continuous Access P9000 XP + Business Copy P9000 XP 配置 ZDB 备份规范。

默认：未选择。

选项：Continuous Access P9000 XP

选择此选项可为采用 P9000 XP 磁盘阵列系列配置的 Continuous Access P9000 XP 配置 ZDB 备份规范。

默认：未选择。

选项：编目保护

目录保护决定有关备份数据的信息在 IDB 中保留多久。如果无编目保护，仍可还原数据，但不能在 Data Protector GUI 中浏览这些数据。

无: 不提供任何保护。

直到: 表示直到指定的日期才能覆盖 IDB 中的信息。对信息的保护在所选日期当天的中午停止。

天: 表示在指定的天数内不能覆盖 IDB 中的信息。

周: 表示在指定的周数内不能覆盖 IDB 中的信息。

与数据保护相同: 表示在数据受保护的时期保护有关 IDB 中备份数据的信息。

选项：检查内部数据库

此选项指示 Data Protector 在备份之前快速执行内部数据的一致性检查。这种类型的一致性检查将检测 IDB 内部的主要不一致。如果检测到这样的不一致，将不创建 IDB 备份映像，而且会话将失败。这可防止在 Cell Manager 受到灾难打击而且不存在具有一致 IDB 的备份映像的情况下丢失数据。

强烈建议使该选项保持选中状态。

默认：选择。

选项：检查中止 ID

创建备份规范时，可以指定备份规范的应用程序标识号或中止 ID。用 omniclus 实用程序创建脚本时可以使用此 ID，而当启动 omniclus 命令时将检查中止 ID，并仅中止影响 Cell Manager 上负载的会话。

选项：将完整 DR 映像复制到磁盘

如果在备份期间将灾难恢复映像保存到 Cell Manager，则将以文件名 ClientName.img 存储到默认 Data Protector P1S 文件目录。如果要在 Cell Manager 上准备灾难恢复 CD ISO 映像，则此选项很有用，因为从磁盘获取 DR 映像比从备份介质快许多。

选项：延迟(分钟)(D)

指定执行设备的装载请求脚本之前的延迟（以分钟为单位）。延迟是从发出装载请求到执行脚本时的分钟数。如果已指定装载请求脚本，则必须设置此选项。

选项：未完全创建快照式克隆则最多推迟磁带备份 X 分钟

此选项仅在选择快照式克隆作为快照类型时可用。

通过推迟向磁带复制数据直到克隆过程完成为止（ZDB 到磁带、ZDB 到磁盘 + 磁带），防止应用程序数据访问时间变长，并减少磁盘阵列上的负载。还可定义最大等待时间。达到指定的时间后，在任何情况下将启动到磁带的备份（即使克隆过程尚未完成）。

默认：选择，90 分钟。

选项：描述

备份规范的额外说明性文字为可选，但有助于辨别备份规范。其中可以包含任意字符，最大长度可以达到 80 个字符（包括空格）。

选项：描述

额外的说明性文字为可选，但建议加入这些文字以便于辨别。其中可以包含任意字符，最大长度可以达到 80 个字符（包括空格）。

选项：卸载应用程序系统上的文件系统

选择此选项可在创建复本之前卸载应用程序系统上的文件系统，随后重新装载这些文件系统。此外，如果选择整个物理磁盘（位于 Windows 系统上）或整个磁盘或逻辑卷（位于 UNIX 系统上）作为磁盘映像备份规范中的备份对象，则选择此选项将卸载这些对象上的所有文件系统，然后再重新装载这些文件系统。如果无法卸载其中任意文件系统，则备份会话将失败。

如果集成的应用程序（例如，Oracle Server）完全控制将进行备份的每个物理驱动器、磁盘或逻辑卷上的数据 I/O，则不需要卸载操作。在这种情况下，可以使此选项保持清除状态。

默认：未选择。

选项：在复本生成之前卸除应用程序系统上的文件系统

选择此选项可在创建复本之前卸载应用程序系统上的文件系统，随后重新装载这些文件系统。此外，如果选择整个物理磁盘（位于 Windows 系统上）或整个磁盘或逻辑卷（位于 UNIX 系统上）作为磁盘映像备份规范中的备份对象，则选择此选项将卸载这些对象上的所有文件系统，然后再重新装载这些文件系统。如果无法卸载其中任意文件系统，则备份会话将失败。

如果集成的应用程序（例如，Oracle Server）完全控制将进行备份的每个物理驱动器、磁盘或逻辑卷上的数据 I/O，则不需要卸载操作。在这种情况下，可以使此选项保持清除状态。

默认：未选择。

选项：显示统计信息

启用此选项后，Data Protector 将报告所备份或还原的每个对象的统计信息（如大小和性能）。可以在监视器窗口中查看这些信息。默认情况下，禁用此选项。

选项：不检查中止 ID

启动 omniclus 命令后，不检查备份规范的中止 ID。

选项：不检查已用的会话时间

启动 omniclus 命令后，不检查已用会话时间。

选项：会话后弹出介质

使用此选项可在完成备份或还原会话之后从设备中弹出介质。这是一项安全功能，有助于防止其他应用程序意外覆盖介质。默认情况下，不弹出介质。

如果以前已选择**可追加**介质使用策略，则不要启用此选项；否则，Data Protector 将根据介质分配策略和设备类型发出装载请求。

选项：启用 **Magic Packet**

如果客户机支持此选项，则选择此选项可启用远程开机。

选项：启用可恢复的恢复

如果选择了此选项，则 Data Protector 将在还原会话期间创建检查点文件。如果还原会话失败，并且要使用 Data Protector 还原会话功能恢复会话，则需要检查点文件。

默认: 已选择 (可以使用全局选项 ResumableRestoreDefault 更改默认值)。

选项：仅启用受保护对象的选择

如果选择此选项，则只能为复制选择具有数据保护的对象。没有数据保护的对象的复选框为灰色。

选项：以读取/写入模式启用备份系统

此选项适用于 UNIX 系统，并且只能针对 UNIX 系统进行更改。在 Windows 系统中，不能以只读模式装载文件系统。

选择此选项可启用对备份系统上的卷组和文件系统的读/写访问权限。为便于备份，以只读模式激活备份系统卷组和装载文件系统即可。对于其他任务，可能需要读/写模式。

请注意，选择了此选项后，当备份系统处于联机状态时可以对复本进行修改。因此，从此类复本中还原的数据包含所有潜在修改。

默认值：

Windows 系统：已选择。

UNIX 系统未选择。

选项：估计持续时间

估计会话的持续时间以确定计划在日历中的显示方式。

选项：硬件压缩

大多数当代的备份设备都提供内置的硬件压缩。设备从介质代理客户机收到原始数据，然后以压缩模式将这些数据写入磁带。硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数据较少。

如果设置了此选项，则 Data Protector 向设备发送使用硬件压缩的指示。

如果从下拉列表中选择 SCSI 地址，则 Data Protector 将自动确定此设备能否使用硬件压缩。

在 Windows 中，如果检测不成功并因此手动输入 SCSI 地址，则在 SCSI 地址的结尾添加 C 字符，例如：scsi:0:3:0C（如果加载了磁带驱动程序，则为 tape2:0:1:0C）。如果设备支持硬件压缩，则会使用硬件压缩，否则将忽略 C 选项。

要在 Windows 系统上禁用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加 N，例如：scsi:0:3:0N。

在 UNIX 系统中，通过选择硬件压缩设备文件启用硬件压缩。

对于多路径设备，要单独为每个路径设置此选项。

对于设备链，对每个地址（UNIX 系统中为设备文件）都要设置此选项。

选项：导入副本作为原件

在因覆盖或丢失而没有原始介质可用，要导入副本并使其成为原件时，请使用此选项。

此选项还适用于 MCF 文件中与介质相关的目录数据副本。

选项：增量

Incr 仅备份从上一次受保护备份以来的更改，无论该备份是完整备份或增量备份。

增量备份的优点是完成备份所需的时间较少（备份的数据量较小），并且在介质上和 IDB 中占用的空间也较小。

缺点是还原起来更加复杂，因为通常需要从上一次完整备份以来用过的所有介质。

选项：增量 1

增量 1 或差异备份将备份从上次完整备份以来所做的更改。此备份类型将恢复链限制为最多两个元素，但由于从完整备份以来所做的更改不断积累，因此备份可能变得很大。

选项：在备份完成之后保留复本

如果配置“ZDB 到磁带”，则选择此选项，以在零宕机时间备份会话之后将复本保留在磁盘阵列上。复本成为复本集的一部分（为**旋转的副本数**选项指定一个值）。除非“跟踪复本以用于即时恢复”这一附加选项处于选中状态，否则复本不可用于即时恢复。

如果未选择此选项，则会在会话结束时删除复本。

此选项会在**跟踪复本以用于即时恢复**选项处于选中状态时自动选择而且无法更改。

选项：让备份系统处于启用状态

此选项只在选择了**在备份完成之后保留副本**选项时可用。

如果选择此选项，在会话结束后，文件系统保持装载，卷组保持已导入且处于活动状态（UNIX 系统），目标卷仍然存在。在这种情况下，可以将备份系统用于数据仓库用途，但不能用于即时恢复。如果复本必须在之后重新使用（删除、循环出或用于即时恢复），则 Data Protector 会自动连接到备份系统，卸载文件系统，隐藏目标卷并清除备份系统中的相关逻辑结构。这时，如果文件系统未装载到当前备份系统，则 Data Protector 无法执行适当的清理作业，并会中止操作或即时恢复会话。

如果未选择此选项，则 Data Protector 会在 ZDB 会话结束后卸载文件系统，导出卷组（UNIX 系统）并隐藏备份系统中的目标卷。

选项：级别(通知)

可以对特定事件触发的通知指定严重性级别。属性的严重性按如下顺序递增：

Normal

警告

Minor

重大

严重

选项：在备份期间锁定文件

Windows OS：此选项定义如何在备份会话期间处理文件。如果选择，则将在备份会话期间锁定文件，这样可阻止备份期间修改或访问这些文件。使用强制锁定。默认情况下，不选择此选项。

Linux OS：此选项定义如何在备份会话期间处理文件。如果选择此选项，则 Data Protector 将在备份会话期间对文件读取锁定，防止其他进程在备份期间进行写入锁定。系统将使用建议锁定，这是因为我们不建议采用强制性锁定。这样一来，其他进程均可忽略锁定并修改文件的内容。默认情况下，不选择此选项。

选项：日志记录

日志记录级别决定在备份、对象副本或对象合并期间写入 IDB 的关于文件和目录的详细信息量。请注意，无论使用何种日志记录级别，都可以还原数据。

不同的日志记录级别设置会影响 IDB 增大、备份速度、对象副本或对象合并以及浏览数据进行还原的便利程度。

Data Protector 提供四个日志记录级别：**全部记录**、**记录文件**、**记录目录**和**不记录任何内容**。

日志记录级别对磁盘映像备份不可用。对于 B2D 设备，仅**无日志**和**全部记录**级别可用。

选项：MAC 地址

客户机中用于远程开机功能的网络适配器的硬件地址。

选项：MU 编号 (特定于 P9000 XP 的选项)

此选项仅在选择采用 P9000 XP 磁盘阵列系列配置的 Business Copy P9000 XP 时可用。

此选项定义了复本或复本集的镜像单元 (MU) 编号，Data Protector P9000 XP 代理根据该复本集循环选择在零宕机时间备份会话中使用的复本。对于镜像复本和快照，可为相同源卷创建的最大副本数量是不同的。这两个限制都由 P9000 XP 磁盘阵列系列存储系统施加。

您可以指定一个或多个非负整数、这些数字的一个或多个升序范围，或者这两者的任意组合。使用逗号作为分隔符。示例：

5

7-9

4,0,2-3

如果已指定序列，该序列不会定义复本的使用顺序。

默认值： 0 (未指定任何内容)。

选项：箱盒支持

通过此选项，可将一组介质用作一个称为箱盒的单位。与这些介质配合使用的备份设备必须支持箱盒，如 XPDAT 24x6 或 12000e。可以对要用于特定设备的介质池设置此选项。

配置新介质池时，可以设置此选项。

选项：每个存储的最大连接数量

限制可以连接到每个存储的介质代理的数量。

如果未选择此选项，则不限制连接数。

默认：未选择。

选项：最大重写次数

介质的使用情况定义为对介质的重写次数。介质数超过重写次数的阈值后，就会将该介质标为差。DDS 介质的默认阈值为 100 次重写。对于所有其他类型的介质，默认值为 250 次重写。

选项：介质池

此选项可为备份选择一个特定的介质池。如果不定义，则将使用设备定义中的默认介质池。

可以对备份、对象复制和对象合并操作指定此选项。

选项：介质类型

Data Protector 支持各种介质类型，如磁带、磁光、文件和 LTO 介质。

选择介质类型时，Data Protector 将估计目标介质池的介质上的可用空间。

选项：在会话结束时

此选项决定了 ZDB 会话结束后 Data Protector 处理镜像克隆复制链接的方式。它提供两个选项：

同步

选择此项可以在镜像克隆快照创建后，让 Data Protector 在 ZDB 会话中涉及的镜像克隆与相应的原始卷之间还原复制链接的*已同步*状态。

选择此项的好处是可以为**在会话开始时**选项选择**如果碎片化，则进行同步**选项。原因是，如果在创建镜像克隆快照后立即同步，则同步所需的时间通常短得多，而且不只是在下一个 ZDB 会话中的镜像克隆快照创建之前同步。

保持断开

选择此项可以在镜像克隆快照创建后，让 Data Protector 在 ZDB 会话中涉及的镜像克隆与相应的原始卷之间的复制链接保持*已断开*状态。

如果选择此项，则会自动选择**在会话开始时**选项的**如果碎片化，则进行同步**，而**如果碎片化，则中止**选项将不可用。

默认值：同步。

选项：在会话开始时

原始存储卷与其镜像克隆之间的复制链接可以处于不同的状态。因为 Data Protector 可以创建镜像克隆快照，所以镜像克隆与相应的原始存储卷之间的复制链接必须为*已同步*状态。

此选项提供两种选择：

如果断开，则进行同步

如果选择此项，即使在 ZDB 备份规范中选择的存储卷与其镜像克隆之间的复制链接在会话开始时为*已断裂*，也可以运行 ZDB 会话。在这种情况下，Data Protector 会在开始镜像克隆快照创建前，还原每个此类复制链接的已同步状态。

如果断开，则中止

选择此项让 Data Protector 在 ZDB 备份规范中选择的存储卷与其镜像克隆之间的复制链接为*已断开*时，中止 ZDB 会话。

如果选择此项，则会自动选择**在会话结束时**选项的**同步**，而**保持碎片状态**选项将不可用。

默认值：如果碎片化，则进行同步。

选项：移动繁忙文件

如果应用程序正在使用磁盘上的某个文件，当还原要替换此文件时，即与此选项相关。此选项仅适用于因应用程序或其他进程使用而被操作系统锁定的文件。此选项与**保持最新**或**覆盖**选项一起使用。默认情况下，禁用此选项。

在 UNIX 系统上，Data Protector 将繁忙文件从 filename 移至 #filename（在文件名前面添加井号）。应用程序将继续使用繁忙文件，直到其关闭该文件为止。随后，将使用还原的文件。

在 Windows 系统上，该文件还原为 filename.001 。所有应用程序都继续使用旧文件。重新引导系统后，旧文件将替换为还原的文件。

在 Linux 系统中，不支持此选项。

选项：将自由介质移至自由池

如果选择了此选项，则自动定期从常规池中将空闲介质分配回自由池。

默认选择。

选项：不覆盖

如果选择了此选项，则保留磁盘上存在的文件。这意味着它们不会被备份中这些文件的其他版本覆盖。仅从备份还原当前不存在的文件。默认情况下，禁用此选项。

不支持使用冲突处理选项“不覆盖”执行备份链形式 (完整、差异、增量、...) 的还原操作。

选项：非权威

在使用标准复制技术还原之后更新 Active Directory 数据库。**非权威**复制模式是默认选项。

选项值：无

此数据安全选项不提供任何保护。默认情况下，数据安全设置为“无”。

选项：轮换的复本数量

此选项仅在选择“在备份完成之后保留复本”选项时可用。

在 ZDB 会话期间，Data Protector 会创建一个新复本并将其保留在磁盘阵列中，直至达到**循环的复本数**选项所指定的值。在那之后，删除最旧的复本，然后创建一个新复本。

标准快照和无容量快照的数量受到存储系统的限制。Data Protector 不限制旋转的复本的数，但是如果超出限制，会话将失败。

选项：重试次数（Windows 特有选项）

输入 Data Protector 将尝试备份打开文件的次数。

选项：在客户机上

在下拉列表中，选择将执行特定的 pre-exec 或 post-exec 命令的客户机系统。

选项：选择原始设备

当目前没有原始设备可供还原或对象副本使用时，此选项适用。选择此选项可指示 Data Protector 等待所选设备变为可用。

这是 Data Protector SAP MaxDB、IBM DB2 UDB、Microsoft SQL Server 和 Microsoft SharePoint Server 2010/2013 集成的首选选项。

默认：未选择。

选项：所有权

This page is still under development. No published version is available at this time.

选项：路径

This page is still under development. No published version is available at this time.

选项：池名称

This page is still under development. No published version is available at this time.

选项：**post-exec**（备份会话）

This page is still under development. No published version is available at this time.

选项：post-exec（备份对象）

通过此选项，可以输入一个要在备份单独的备份对象之后执行的命令。

备份对象的命令可位于运行磁带客户机的系统上的任何目录中。但是，对于客户机备份，它们必须位于 Data_Protector_home\bin（Windows 系统）、 /opt/omni/lbin（HP-UX、Solaris 和 Linux 系统）或 /usr/omni/bin（其他 UNIX 系统）中。

如果命令位于 Data_Protector_home\bin（Windows 系统）、 /opt/omni/lbin（HP-UX、Solaris 和 Linux 系统）或 /usr/omni/bin 目录（其他 UNIX 系统）中，则只输入文件名，否则请指定完整路径名。

在 Windows 系统中，请注意，如果目录名称大于 8 个字符，则在引号中书写文件名，或以简短的 8.3 MS-DOS 兼容形式书写路径名。如果使用引号 ("") 指定路径名，则不要使用反斜杠和引号的组合 (\")。如果需要在路径名末尾使用尾随的反斜杠，则使用双反斜杠 (\\)。

请注意，Windows 系统中仅支持扩展名为 .bat 、 .exe 和 .cmd 的 post-exec 脚本。要运行扩展名不受支持（例如 .vbs ）的脚本，请创建批处理文件（ .bat ）以启动该脚本。然后配置 Data Protector，将批处理文件作为 post-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

选项：**pre-exec**（备份会话）

通过此选项，可以输入一个要在启动备份进程之前执行的命令。默认情况下，在 Cell Manager 系统上执行 pre-exec 命令。此命令必须返回成功，Data Protector 才能进行备份。

在 Cell Manager 上，这些脚本必须位于默认 Data Protector 目录中。在 Cell Manager 以外的系统上，这些脚本必须位于默认的 Data Protector 管理命令目录中。

对于位于默认的 Data Protector 管理命令目录中的脚本，请仅指定文件名，否则要指定脚本的完整路径名。

请注意，在 Windows 系统中，如果目录名称大于 8 个字符，则在引号中书写文件名，或以简短的 8.3 MS-DOS 兼容形式书写路径名。如果使用引号 ("") 指定路径名，则不要使用反斜杠和引号的组合 (\")。如果需要在路径名末尾使用尾随的反斜杠，则使用双反斜杠 (\\)。

请注意，Windows 系统中仅支持扩展名为 .bat、.exe 和 .cmd 的 pre-exec 脚本。要运行扩展名不受支持 (例如 .vbs) 的 pre-exec 脚本，请创建批处理文件 (.bat) 以启动该脚本。然后配置 Data Protector，将批处理文件作为 pre-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

选项：**pre-exec**（备份对象）

通过此选项，可以输入一个要在备份单独的备份对象之前执行的命令。此命令（或脚本）必须返回成功，Data Protector 才能进行备份。

用于备份对象的命令（或脚本）在运行磁带客户机的客户机系统上执行。在 Windows 系统上，脚本必须位于 Data_Protector_home\bin 目录或其子目录中。在 Unix 系统上，脚本必须位于 in /opt/omni/lbin 目录或其子目录中。

请注意，Windows 系统中仅支持扩展名为 .bat 、 .exe 和 .cmd 的 pre-exec 脚本。要运行扩展名不受支持 (例如 .vbs) 的 pre-exec 脚本，请创建批处理文件 (.bat) 以启动该脚本。然后配置 Data Protector，将批处理文件作为 pre-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

选项：**prealloc** 列表

prealloc 列表是按指定顺序用于备份的介质的一个子集。

将 prealloc 列表和严格介质分配策略与备份设备配合使用时，Data Protector 要求设备中介质的顺序对应于 prealloc 列表中指定的顺序。如果介质以此顺序不可用，则 Data Protector 发出装载请求。如果未在此列表中指定任何介质，则使用 Data Protector 分配过程分配介质。

可以对备份、对象复制和对象合并操作指定此选项。

选项：为备份（重新同步）准备下一镜像磁盘

只有当下一个 ZDB 会话中要使用的复本卷至少有一个为镜像（或镜像副本）时，此选项才可用。反之，Data Protector 就像未选择此选项一样运行。

如果选择此选项，当前 ZDB 会话结束时，在下一 ZDB 会话中使用的复本的所有卷会与相应的源卷列为成对状态：镜像将重新同步,要用于快照存储的卷将被清空。

如果未选择此选项，则下一 ZDB 会话中使用的复本的卷在当前 ZDB 会话结束时保持不变。

如果未选择此选项，则会自动选择**如果尚未同步，则同步磁盘**选项，而**如果尚未同步镜像磁盘，则中止会话**选项不可用。

默认：选择。

选项：主

“主”复制模式可使 NT 目录服务联机，并用于还原 FileReplicationService 以及 Active Directory 服务。复制共享的所有复制合作伙伴丢失时，必须使用此选项。对于证书服务器和 Active Directory 服务器，**主**与**权威**作用相同。

选项：公共

如果已选择此选项，则允许所有其他用户查看和还原此备份规范中指定的数据。默认情况下，对于文件系统备份，仅管理员和创建备份的 Data Protector 用户可以查看和还原数据。

选项：在备份之后重新建立链接（EMC Symmetrix 特有选项）

在备份之后在应用程序和镜像的设备之间重新建立链接。如果禁用此选项，则在备份之后保持拆分链接（在这种情况下，可以在备份系统上使用镜像的设备）。在启动下一个备份之前，使用选项**在备份之前重新建立链接**可以同步磁盘。

默认：选择。

选项：在备份之前重新建立链接（EMC Symmetrix 特有选项）

在备份之前同步磁盘以维护数据完整性（如果禁用在备份之后重新建立链接或使用保持拆分链接的 EMC 命令，则可能为必需的）。

默认：未选择。

选项：重新连接已断开的连接

如果设置了此选项，则万一发生短期网络问题，Data Protector 将尝试

- 重新连接 Backup Session Manager 和磁带客户机或介质代理（控制连接）或
- 在备份期间尝试重新连接磁带客户机和介质代理，如果启用了对象镜像，则尝试重新连接介质代理（数据连接）

默认情况下，Data Protector 尝试重新连接 600 秒。可以在 omnirc 选项 OB2RECONNECT_RETRY 中修改此超时时段。

重新连接功能仅在备份期间对网络问题起作用。

默认情况下，不选择此选项。

选项：成功复制后回收失败的源对象的数据和编目保护

选择此选项以在源介质上删除失败对象的数据和目录保护。将不在对象复制会话中复制失败的对象。介质上不再有受保护的对象时，可以覆盖介质。

选项：冗余级别

选择用于目标卷的存储冗余级别（Vraid 类型），或为应该使用的源卷指定相同的冗余级别。如果创建标准快照或无容量快照，所选的冗余级别应该等于或低于用于源卷的级别。否则，会应用与源卷相同的冗余级别。每个源卷的冗余级别会单独检查。

使用不同 Vraid 类型卷的存储冗余级别和由此产生的存储可靠性如下所示减少：

- Vraid6
- Vraid1
- Vraid5
- Vraid0

默认值：与源相同。

选项：将打开的锁定文件报告为（Windows 特有选项）

打开的锁定文件由其他应用程序独占打开或锁定，如数据库或字处理器。

此选项为 Data Protector 尝试备份时打开和锁定的文件设置报告级别。根据选择哪个选项，它会将此类文件报告为警告消息（默认设置）、minor 错误或不报告任何消息。

选项：重新启动应用程序命令行

如果在此选项中指定了一个命令，在复本创建后，会立即在应用程序系统中调用该命令。一个使用示例是恢复不与 Data Protector 集成的应用程序操作。

命令必须位于应用程序系统上默认的 Data Protector 管理命令目录中。请勿在此选项中指定命令的路径。

选项：还原目录的共享信息（Windows 特有选项）

指定将还原目录的共享信息。默认情况下，选择此选项。

还原备份目录时网络上共享的目录时，如果选择此选项，则在还原之后，还将共享目录（前提是创建备份时选择了**备份目录的共享信息**选项）。

选项：备份系统上安装路径的根目录

此选项仅在**使用与应用程序系统上相同的装载点**点选项处于未选中状态时可用。

指定将在其下装载复本的文件系统的根目录。

装载文件系统的确切位置取决于如何定义**将目录添加到装载路径**选项。

对于 SAP R/3 集成，此选项不适用（所创建的装载点始终与应用程序系统上的相同）。

默认值：

Windows 系统： c:\mnt

UNIX 系统： /mnt

选项：脚本

指定此设备的装载请求脚本。有此设备的装载请求时，执行装载请求脚本。可以使用此脚本为响应装载请求执行自动操作。操作是除了系统上显示的标准装载请求对话框以外的操作。要配置无人看管的备份时，这会很有用。此选择可选，但如果输入装载请求脚本，则还必须输入装载请求延迟。

选项：查看私有对象

此用户权限允许用户查看和还原备份为私有的对象。

会话

在此页中，可以指定要在报告输出中显示的消息级别。

消息级别

选择消息级别以筛选显示的消息。显示所选级别及更高级别的消息。

选项：单个消息级别

“监视器”窗口中显示的具有所选严重性级别或更高级别的消息的所有备份会话都将触发此通知。属性的严重性按如下顺序递增：

Normal

警告

Minor

重大

严重

选项：快照源

此选项提供两种选择：

原始卷

选择此项以创建所选存储卷的快照。请注意，如果会话开始时所选存储卷（原始卷）的镜像克隆存在于磁盘阵列上，则 ZDB 会话会失败。

如果选择此快照源，则**在会话开始时**选项和**在会话结束时**选项不可用。

镜像克隆

选择此项以创建所选存储卷的镜像克隆的快照。如果 ZDB 会话开始时无任何所选存储卷（原始卷）的镜像克隆存在，则 Data Protector 会自动创建它们。请注意，如果会话开始时原始卷的快照存在于磁盘阵列上，则 ZDB 会话会失败。

如果选择此快照源，则**快照式克隆**快照类型不可用。

默认值：原始卷。

选项：快照类型

无容量快照: 创建快照，但不预先分配磁盘空间。

标准快照: 创建快照，同时预先分配磁盘空间。

快照式克隆: 创建源卷的克隆。此快照类型只有在选择**原始卷**作为快照源时才可以使用。

默认值：Vsnap。

选项：拆分 post-exec（EMC Symmetrix 特有选项）

在应用程序系统上的默认 Data Protector 管理命令目录中创建可选的“拆分 post-exec”命令。拆分之后在应用程序系统上执行此命令，并用于重新启动不与 Data Protector 集成的应用程序。

如果“拆分 pre-exec”命令失败，“拆分 post-exec”也不会执行。因此，需要在“拆分 pre-exec”命令中实现清理过程。

如果 ZDB_ALWAYS_POST_SCRIPT omnirc 选项设置为 1，则“拆分 post-exec”在已设置的情况下始终执行 (默认是 0)。

选项：拆分 **pre-exec**（**EMC Symmetrix** 特有选项）

指定可选的“拆分 pre-exec”命令。在应用程序系统上默认的 Data Protector 管理命令目录中创建此命令。拆分链接之前在应用程序系统上执行“拆分 pre-exec”命令。例如，将其用于停止应用程序。

如果不执行由此选项设置的命令，则不中止备份会话。

选项：使应用程序命令行停止/静默

如果在此选项中指定了一个命令，会在创建复本前在应用程序系统中调用该命令。一个使用示例是停止不与 Data Protector 集成的应用程序。

命令必须位于应用程序系统上默认的 Data Protector 管理命令目录中。请勿在此选项中指定命令的路径。

如果命令失败，则不会调用在选项**重新启动应用程序命令行**中指定的命令。因此，可能需要在通过**使应用程序命令行停止/静默**指定的命令中实现清理过程。如果 omnirc 选项 ZDB_ALWAYS_POST_SCRIPT 设置为 1，则始终调用在“重新启动应用程序命令行”选项中指定的命令。

选项：存储大小软配额 (GB)

输入存储大小软配额 (GB)。如果存储中的重复删除的数据大小超过所设置的配额，则会话将显示一则警告，但数据仍将写入存储。该配额对备份、复制和对象合并会话有效。

如果存储大小配额大于备份大小配额，将显示一则警告并且存储大小配额将无效。

默认：未设置。如果设置为 0 或字段为空，则说明未设置配额。

选项：切换会话所有权

此用户权限允许用户指定在其下启动备份的备份规范的所有者。默认情况下，所有者是启动备份的用户。计划的备份在 Linux Cell Manager 上和 Windows 系统上的 Cell Manager 帐户下作为 hpdp 启动。如果启用了“启动备份规范”用户权限，则此用户权限是合适的用户权限。

选项：如果尚未同步，则同步磁盘

在 P9000 XP 阵列上，主卷 (源卷) 及其对应辅助卷 (目标卷) 必须处于 PAIR 状态才能实现 Data Protector 零宕机时间备份: 镜像必须同步，要用于快照存储的卷必须为空。

如果清除了**为备份(重新同步)准备下一镜像磁盘**，则此选项会自动选择且无法更改。

如果选择此选项，当前 ZDB 会话开始时，在下一 ZDB 会话中使用的复本的所有卷会与相应的源卷列为成对状态：镜像将重新同步,要用于快照存储的卷将被清空。

默认：选择。

选项：超时

输入 Data Protector 在重新尝试备份打开的文件或繁忙的文件之前等待的时间量（以秒为单位）。

选项：跟踪复本以用于即时恢复 (P9000 XP 磁盘阵列系列选项)

此选项仅在选择采用 P9000 XP 磁盘阵列系列配置的 **Business Copy P9000 XP** 时可用。选择此选项可以执行“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，并且将复本保留在磁盘阵列上以实现即时恢复。

如果不选择此选项，则无法使用在此会话中创建或重用的复本执行即时恢复。

如果选择此选项，请不要手动重新同步受影响的镜像并且不要清空用于快照存储的卷。否则，将不可能执行即时恢复。

默认：选择。

选项：跟踪即时恢复的复本

此选项只在选择了**在备份完成之后保留副本**选项时可用。

选择此选项可以执行“ZDB 到磁盘”或“ZDB 到磁盘 + 磁带”会话，并且将复本保留在磁盘阵列上以实现即时恢复。还要为**旋转的复本数**选项指定值。

如果不选择此选项，则无法使用在此会话中创建或重用的复本执行即时恢复。

选项：使用直接库访问 (特定于 SAN 的选项)

默认情况下，将库机械手设备配置为仅属于一个主机。通过**使用直接库访问**选项，每个系统能够将控制命令直接发送到库机械手。在多个系统操作同一库的情况下，必须同步此通信。必须在介质代理客户机上创建 libtab 文件，此功能才能正常工作。

如果为多路径库启用了直接访问库功能，则无论配置了什么路径顺序，都会首先使用本地路径（目标客户机上的路径）来控制库机械手。

选项：使用自由池

选择此选项时，池将链接到从下拉列表中选择的自由池，以便共享空闲介质。条件因素从自由池继承。默认情况下，清除此选项。

要创建具有所选介质类型默认属性的新自由池，请输入一个新名称，这样会自动创建新自由池。

选项：使用锁名称

设备锁名称可以防止 Data Protector 同时使用具有不同名称的同一物理设备。**使用锁名称**选项可以在备份或还原会话期间锁定设备。在此字段中，为正在配置的设备输入锁名称。

例如，如果使用一个物理设备配置两个备份设备，则必须对这两个设备使用相同的锁名称。

选项：使用复制

如果选择此选项，则数据会从一个设备复制到另一个设备，该过程不通过介质代理客户机，而是直接从一个备份设备到另一个设备。

默认：未选择。

选项：使用与应用程序系统上相同的装载点

如果应用程序系统也是备份系统（单主机配置），则此选项不可用。

如果选择此选项，则用于在备份系统上装载复本文件系统的装载点路径与在应用程序系统上装载源卷文件系统的装载点路径相同。

如果装载点已使用，则会话会失败。对于这类情况，必须选择**在目标装载点自动卸除文件系统**选项才能使会话成功。

Windows 系统：驱动器号必须提供，否则会话会失败。

默认：未选择。

选项：有效期(月)

介质老化的计算方式是自从初始化介质以来经过的月数。一旦介质超过月数阈值，则会将该介质标记为低劣。默认阈值为 36 个月。

选项：**BDACC**

磁盘代理设置其退出代码 (零表示成功) 并将该代码复制到 BDACC 环境变量。可以在 post-exec 命令中检查此变量，从而使 post-exec 命令依赖于磁带客户机的成功终止。

选项：**DATALIST**

备份规范名称。

选项：**MODE**

备份操作类型，比如完整、增量、增量 1，等等。

选项：**OWNER**

会话的所有者。在指定所有者时所使用的格式应当与内部数据库中使用的格式相同（区分大小写）：

Windows 系统： DOMAIN\Username@Hostname

UNIX 系统： Username.Group@Hostname

选项：**PREVIEW**

如果预览正在运行，则此变量设置为 1（一）。如果备份正在运行，则设置为 0（零）。使用此变量可以修改命令，以便仅在备份期间而不是在预览期间执行它们。默认情况下，不对预览执行 pre-exec 或 post-exec 命令。可以通过设置全局选项 ExecScriptOnPreview 启用它们。

选项：**RESTARTED**

如果这是重新启动的备份会话，则此变量设置为 1 ，否则设置为 0 。post-exec 脚本可以使用此变量防止在 SMEXIT 变量等于 0 (零) 时出现额外重新启动。

选项：SESSIONID

此变量用于标识完成的会话并记录在内部数据库中。无法使用它预览会话 (使用 SESSIONKEY)。

选项：SESSIONKEY

此变量用于标识正在运行的会话。例如，如果存在某种错误，可以在启动备份会话之前将其中止。

选项：SMEXIT

会话管理器的退出代码与 omnib 命令的退出代码相同。只能将此变量与 post-exec 命令一起使用。在 SMEXIT 值的说明中，“代理”一词可能指磁盘代理、介质代理或应用程序代理。

选项：备份保护

指定对于所备份数据的保护期，以防备份被覆盖。

选项：完整

如果选择了此选项，则备份所选的全部对象，即使从上一次备份以来没有更改也是如此。

完整备份的优点是安全（在一个备份会话中备份所有数据），并可以更快速、更简单地还原（仅需最新完整备份的介质）。

缺点是完成完整备份需要更多时间，并在介质上和在 IDB 中占用更多空间，因为可以多次备份文件的相同版本。

选项：增量

增量备份（Incr、Incr 1、Incr 2 等等）仅包括自从上一次完整或增量备份以来修改的数据。增量备份速度更快，并且需要的介质更少，但由于通常需要从上一次完整备份以来使用过的所有介质，因此使所有数据的还原更加复杂。

全局选项

一组选项，用于定义整个 Data Protector 单元的行为。这些选项存储在 global 中，这是 Cell Manager 中的一个纯文本文件，位置如下:

- Windows： <PROGRAMDATA>\Config\Server\Options 。示例： C:\ProgramData\OmniBack\Config\Server\Options 。
- Linux： /etc/opt/omni/server/options 。

选项：对卷备份进行重复数据删除

此选项允许 Data Protector 可靠地备份启用了 Windows 本机重复数据删除的卷。在文件系统优化过程中，通过重复数据删除过程更改的文件不会备份在增量备份中。如果为非 Windows 本机重复数据删除卷选择此选项，则会将其忽略。

如果已为使用“增强型增量备份”选项配置的备份启用此选项，则再次运行完整备份以可靠地备份启用了 Windows 本机重复数据删除的卷。

默认：未选择。

Use

This section provides information on tasks to be performed by the Data Protector user. The following topics are included:

User interfaces

This topic introduces the following user interfaces that Data Protector provides to administer and manage the backup environment and tasks:

- Data Protector graphical user interface (GUI)
- Data Protector command line interface (CLI)

Graphical user interface

Use the graphical user interface on a supported Windows system (Cell Manager or Data Protector Client) to administer your complete backup environment from a single system. You can manage multiple backup environments from the same system. When you install the Data Protector Cell Manager on a supported Windows system, the GUI installs by default. However, the Data Protector architecture gives you flexibility of installing and using the Data Protector user interface on any supported Windows client.

For ease of operation, install the GUI on multiple systems to allow multiple administrators access Data Protector through their local consoles. Before you start using the Data Protector GUI on a client system, add the system user to an appropriate Data Protector user group on the Cell Manager.

> **Note:** Displaying international characters in file names and session messages requires specific setup and configuration. See Customize language settings in the GUI.

Command line interface

Use the command line interface on Windows and Unix systems. The command line interface (CLI) follows the standard Linux format for commands and options and provides complete Data Protector functionality. You can use these commands in scripts to speed up your commonly performed tasks. For information about supported Data Protector command, see Introduction to CLI.

Related topics

- Elements of the Data Protector GUI
- Customize language settings in the GUI
- Change the character encoding in the Data Protector GUI
- Start the Data Protector GUI

Customize language settings in the GUI

Handling file names in a heterogeneous environment (different operating systems with different locale settings in one cell) is a significant challenge. File names that have been backed up with some locale settings and then viewed or restored using different locale settings, require a specific setup to be displayed correctly.

The following prerequisites apply for the GUI system:

- Install the appropriate fonts for the selected coded character set on the Data Protector GUI system. For example, to see Japanese characters in the GUI running on an European system, install Japanese fonts.

Limitations

- There are minor differences between the implementations of character encoding conversion on Windows and UNIX operating systems. Some characters cannot be mapped correctly if the Data Protector GUI is run on a different platform as the client being configured. However, only a few characters could be displayed incorrectly, which will not affect your backups or restores.

Complete the following steps:

1. In the Context List, click **Backup**, **Monitor**, **Restore**, **Reporting**, or **Internal Database**.
2. In the View menu, click **Encoding**.
3. Select the character encoding that was used on the system on which the backed up files were created.

Related topic

- Change the character encoding in the Data Protector GUI

Change the character encoding in the Data Protector GUI

All files can be backed up and restored regardless of the character encoding used. However, in heterogeneous environments (for example, a Windows Cell Manager with UNIX client or the opposite, with different locales on systems) the file names or backup objects and session messages may not display correctly. To correctly display international characters in file names and session messages, the proper encoding has to be selected in the Data Protector GUI.

You can modify the custom character encodings displayed in the Data Protector GUI. The appropriate locales or code page conversion tables must be installed on the system with the Data Protector GUI installed.

As a prerequisite, make sure that the code page conversion table for your character encoding is installed:

1. In the Windows Control Panel, double-click **Regional and Language Options**.
2. Click the **Region**, choose the **Formats** tab, and under Current format browse to the desired code page conversion table and install it if needed.

Follow the steps below to change a custom character encoding:

1. In the Data Protector GUI, in the File menu, click **Preferences**.
2. Click the **Encoding** tab.
3. In the Encoding description text box, type the desired code page conversion table name. You can list six different code page conversion tables regarding to your needs.

   For example, type the name ANSI/OEM Korean over the name Japanese Shift-JIS.

   > **Tip** Click **Load defaults** to replace the current encoding values with the defaults.

4. In the Value text box, depending on the operating system and on the type of Data Protector GUI that you are using, type the character encoding code which will be used when the character encoding is selected.

   For example, if you have chosen to replace Japanese Shift-JIS with ANSI/OEM Korean, type the value 949 over the value 932.

   > **Note** You can find a list of the character encoding codes for Windows systems at http://msdn.microsoft.com/en-us/library/system.text.encoding.aspx.

5. Restart the Data Protector GUI for the changes to take effect.

Related topic

- Customize language settings in the GUI

Start the Data Protector GUI

To start the Data Protector GUI on a Windows system, go to:

Start > **Programs** > **Data Protector** > **Data Protector Manager**

Alternatively, run the command `manager`.

To specify the Cell Manager you want to connect to, run:

```
manager -server Cell_Manager_Name
```

Context-specific options for this command enable you to start one or more Data Protector contexts. To start the Data Protector Backup and Restore contexts, run:

```
manager -backup -restore
```

For more information, see Section 5: Miscellaneous in the CLI Reference or the `omnigui` man page.

Home Context

Home context provides a unified way to access the **Dashboard**, **Reports**, and **Scheduler**. In addition, you can also configure settings for Scheduler, Reports, and Telemetry from the Home context.

The top right corner of the Home context displays the following details:

- The status of the Cell Manager. For example, **Running**. The status can be one of the following - Running, Not Running, and Stopped.
- The name of the current user and the host name of the Cell Manager in the following format: <username>@<Cell manager host name>

The following prerequisites must be met to access the Home context:

- **Browser recommendation**: To access the different functionalities available from Home context, the system must have a web browser installed. See the latest Support Matrix for browser recommendations.
- **Security settings**: When launching Home Context Web pages, the following **Security Alert** window appears.

  This window appears if the certificate is not added to the root trust store, and therefore the connection is flagged as untrusted .To avoid viewing this warning message, complete the following steps:

  1. Copy the file cacert.pem from Cell Manager to any temporary directory in the Cell Console client. The cacert.pem file is available at the following location in the Cell Manager:
     - Windows: %DP_SDATA_DIR%\Config\Server\certificates
     - Linux/HP-UX: /etc/opt/omni/server/certificates
  2. On the Cell Console client, open the command prompt and run the following command:

     ```
     certutil -addstore root cacert.pem
     ```

     This command adds the certificate to the root trust store.
  3. Restart the Data Protector GUI.

Configure Settings for Scheduler and Telemetry

Follow these steps:

1. Go to **Home** context and click Settings in the top-right corner.
2. Click the required tab (Scheduler or Telemetry) and configure the settings.

View Logs for Home context

Follow these steps to view logs for the Home context:

1. Go to **Home** context and click Settings in the top-right corner.
2. Click **Logs.** All the logs related to the Home context are displayed. After the log size reaches 5 MB, the existing logs are cleared and the new logs start getting displayed on this page.
3. *Optional*. Click **Clear Logs** to clear the existing logs, click **Refresh** to reload the logs or click **Copy** to copy logs to the clipboard.

Dashboard

The dashboard page provides user an overview of the Cell Manager instance including details such as total data protected, clients available, storage devices, licenses installed, and so on.

Access the Dashboard

To access the Dashboard page, click **Home** Context Menu in the GUI, and then click **Dashboard** in the top pane.

Dashboard

The dashboard page is divided into 9 different categories:

- Clients
- Total Data Protected
- Devices
- Alerts
- Sessions
- Users
- Data Backed Up
- Licenses
- Systems

The Dashboard page also displays the name of the current user and the host name of the Cell Manager at the top right corner in the following format:

<username>@<Cell manager host name>

Clients

Clients lists all the currently configured clients along with the hostname, operating system, version and total data protected. Click **More** to view the following information:

- **Hostname**: This column lists the hostnames of all the configured clients. It also lists hostname of the Edge Server if Office 365 component is installed. You can sort the hostname column in ascending or descending order based on your preference.

  When you click on a row, the information on **Installed Components** and **Data Protected Details** is displayed in the right pane. The backup is displayed as chart where different application backups are shown. If you click on a row containing a VMware host or an Edge Server, **Installed components** and **Data Protected Details** are displayed as *No installed components* and *No data backed up* respectively.

- **Platform**: This column lists all the operating systems used by the clients. In the top pane, there are additional filters to filter clients based on Platform, Version, or Hostname.
- **Version**: This column lists the version number of the Cell Manager or the client.
- **Data Protected**: This column lists the total data backed up on each client. The protected data for the client does not automatically update when you load the page. However, the protected data value gets updated during the daily maintenance schedule. In case of VMware clients, the data protected on each VMware host is displayed as "**-**". However, you can view the consolidated data protected on all the VMware hosts under **Data Protected Details** section in the right pane.

Total Data Protected

The total data protected on the Cell Manager. Click **More** to view the data in the form of chart with the amount of data backed up for the respective data type (for example, filesystem).

Note: The total protected data displayed here is not the latest. It is derived from the the daily maintenance schedule.

Devices

Lists the top three device types configured on the Cell Manager. For example, File Library and Smart Cache. Click **More** to view the following information:

- **Device name**: This column lists the names of the devices. You can sort this in ascending or descending order based on your preference.
- **Hostname**: The columns lists the hostname of the device or the media server. You can sort this in ascending or descending order based on your preference. You can filter the devices based on the Hostname or Type by using the filters provided in the top pane.
- **Type**: This column lists the device type of the storage devices.
- **Subtype**: This column lists the media format types.
- **Pool name**: This column lists all the media pools of the storage devices.

Alerts

The number of alerts generated in the last 24 hours under each of these categories -**Critical**, **Major**, and **Warnings**.

Sessions

The number of sessions in the last 24 hours under each of these categories -**Completed**, **Failed**, and **Aborted**.

Users

The number of users configured under each of the top three user groups.

Data Backed Up

The data backed up in the last 24 hours for Applications, Windows FS, and Unix FS.

Licenses

The number of licenses installed on Cell Manager. Click **More** to view the following categories:

- **Online Licenses**: Online License is a licensing mechanism that allows you to obtain licenses for a period of time.
- **Capacity Licenses**: Capacity License is a licensing mechanism that allows you to obtain licenses based on the amount of data you back up.

Note:

- Starting with Data Protector 2018.11, the capacity calculations are performed for 90 days prior to the current date.
- For premium and capacity licenses, data does not automatically update when you load the page. However, the license value gets updated during the daily telemetry schedule.

Systems

The number of systems configured in the environment based on the operating system. The categories displayed are **Windows**, **Unix**, and **Others**. The Others category includes VMware vCenter, VMware ESXi, Hyper-V, H3C CAS, NDMP server, OpenVMS, and macOS clients.

Telemetry

The Data Protector Telemetry Client service collects the data from the Data Protector Cell Manager through Application Server and uploads telemetry data to Data Protector support for further analysis.

Access the Telemetry page

To access the Telemetry page, select **Home** Context Menu in the GUI, click **Settings** in the top right corner and then click **Telemetry**.

The Telemetry Client service is a Windows and Linux service which is deployed on Cell Console (CC) client. The service page displays Data Protector Telemetry Client service where the user can start or stop the service.

Data Protector collects the following high-level information for telemetrics:

- Component information - Data Protector components and its versions. It also gathers information on the host OS version.
- Devices or Media Servers - the details associated to a client in the Cell Manager that includes the device usage size attached, name of the device, library name, device type, and pool name where the media is placed.
- Device usage size – The usage size of the device.
- Capacity Based Licensing (CBL) - CBL is leveraged to gather information on capacity.
- Traditional license categories - It gathers information about the licenses installed per host and available licenses.
- Client usage - The information is collected for each client. This information includes: hostname, application name and total size of data backed up.
- Storage usage - Total data backed up on the device.

The following prerequisites apply:

- The Telemetry Client service deployed on CC must be proxy configured to communicate with support backend server.
- When configuring telemetry, the customer name and proxy information should be available.

> **Note** The customer related internal information is gathered, but the host information is masked. The Cell Manager performance is not impacted during the collection of telemetry data.

Limitation:

- The Telemetry Client service is supported only on Windows x64 and Linux x64 operating system.

How Telemetry works?

During telemetry registration, the information is stored in the IDB. Any Windows host where the Data Protector CC component is installed is a suitable telemetry client. Depending on the configured frequency of upload, the Cell Console (CC) client checks the IDB settings and fetches the telemetry data from the Cell Manager and uploads the data to the backend server.

If the service is offline during the collection process, then telemetry upload does not happen at that time. When service is online, then the client becomes eligible to upload the telemetry data.

In a cell, if there are multiple telemetry clients then only one client performs the upload to the backend according upload frequency. IDB is updated with the upload status and time.

From telemetry clients, if a proxy is required to access the external network then you need to specify the proxy parameters. This can be ignored if a direct connection is possible.

Subscribe to Telemetry

The customer can subscribe or unsubscribe to the telemetry updates from the Telemetry page.
To subscribe to the telemetry updates, enter the following fields in the Telemetry page:

- **Customer Name** [Mandatory]: Name of the customer.
- **Frequency of data collection**: The user can select the frequency in which the data can be collected, that is: Daily, Weekly, Monthly and Quarterly.
- **Proxy Address** [Optional]: The address of configured proxy server.
- **Port** [Optional]: The port of the proxy server.
- **Username** [Optional]: Username to connect to the proxy server.
- **Password** [Optional]: Password for the given user name.

After entering the above fields and selecting the frequency of data collection, accept the terms and conditions and click **Subscribe**.

Note If you are using Windows telemetry client to connect to Linux Cell Manager, you must create a Data Protector user under Admin group with username as **SYSTEM**, domain or group as **NT AUTHORITY**, and client system as <*Hostname-of-Windows-client*> to be able to transfer telemetry data. The <*Hostname-of-Windows-client*> is the hostname of the client system configured for telemetry data upload.

Scheduler

Use the Scheduler to automate various operations such as, backup, copy, consolidation, verification, reporting and media copy at periodic intervals. The unattended background execution of operations eliminates the need of manually repeating a schedule whenever you want to run an operation.

Scheduler types

There are two types of schedulers in Data Protector:

- Basic Scheduler
- Web-based Scheduler

Data Protector provides an option to use both the Basic Scheduler and the Web-based Scheduler at the same time. However, both the schedulers are independent of each other.

Basic Scheduler and Web-based Scheduler - a comparison

The table below provides a comparison of Basic Scheduler and Web-based Scheduler:

Feature	Basic Scheduler	Web-based scheduler
Daily/Weekly/Monthly	Y	Y
Every Hour/Minute	Manual edit	Y
Priorities	N	Y
Timezones	N	Y
Monthly overview	Y	Y
Duration	N	Y
Conflict handling	N	Y
X-Day of Month/Year	Manual edit	Y
Editable schedules	Manual edit	Y
Schedule cloning	Manual edit and copy	Y
Secure editing	N	Y
REST API	N	Y
Individual enable/disable	N	Y

Scheduler tips

- To simplify scheduling, Data Protector provides backup specifications for group clients. All clients configured in one backup specification are backed up at the same time in a single backup session. Be sure to have sufficient media and devices to run unattended backups smoothly.
- When the scheduled backup is started, Data Protector tries to allocate all the needed resources, such as licenses, devices, and access to IDB. If one of the needed resources is not available, the session is marked as queued. Data Protector will try to find the needed resources for the queued session once every minute until the time-out period is reached. Once Data Protector finds the resources, one of the queued sessions is started. The queued sessions are not started in the order they are displayed.
- To prevent Cell Manager overload, a maximum of up to five backup sessions can be started at the same time. If more are scheduled at the same time, the sessions are queued. This limit can be modified using the `MaxBSessions` global option. On the other hand, the concurrently invoked sessions that fall above the maximum configurable limit are not started, and relevant errors are logged into the Data Protector Event Log.
- For each individual or periodic scheduled backup, you can specify the following options: Backup type (full or incremental), Network load, and Backup protection. With split mirror or snapshot backup, in the case of ZDB to disk or ZDB to disk+tape (instant recovery enabled), you specify the Split mirror/snapshot backup option.
- For split mirror and snapshot backups, the backup type is ignored (it is set to full).
- Each backup specification can be scheduled multiple times with different option values. Within one backup specification, you can schedule both ZDB to disk and ZDB to disk+tape, and specify a different data protection period for each individual or periodic scheduled backup.
- Data and catalog protection settings determine the period that data is kept on a medium (data protection) and in IDB (catalog protection).
- When applying a backup template, the schedule settings of the template override the schedule settings of the backup specification. After applying the template, you can still modify the backup specification and set a different schedule.
- When Backup and Copy sessions are started, they require memory to be allocated as they are resource intensive, especially on the Media Agent servers. So, you need to ensure that multiple backup and copy sessions do not start at the same time. For example, if you need to start nine backup specifications at approximately 6 PM, you need to start the first three backups at 5.45 PM, the next three at 6 PM, and the last three backups at 6.15 PM. Instead of scheduling all the nine backup specifications to start at 6 PM.
- When the scheduled backup is started, Data Protector tries to allocate all needed resources, such as licenses, devices, and access to the IDB. If one of the needed resources is not available, the session is queued while Data Protector is trying

to get the needed resources for the queued session every minute until the time-out period is reached. The time out can be modified by changing the SmWaitForDevice global option. When Data Protector gets the resources, the queued sessions are started. The queued session may not be started in the order they are displayed.

Basic Scheduler

Data Protector allows you to configure unattended backups by scheduling backups of your systems at specific times. The configuration and your scheduling policies can significantly influence the effectiveness and performance of your backup. You can schedule backups up to a year in advance. Periodic backups do not have a defined time limit.

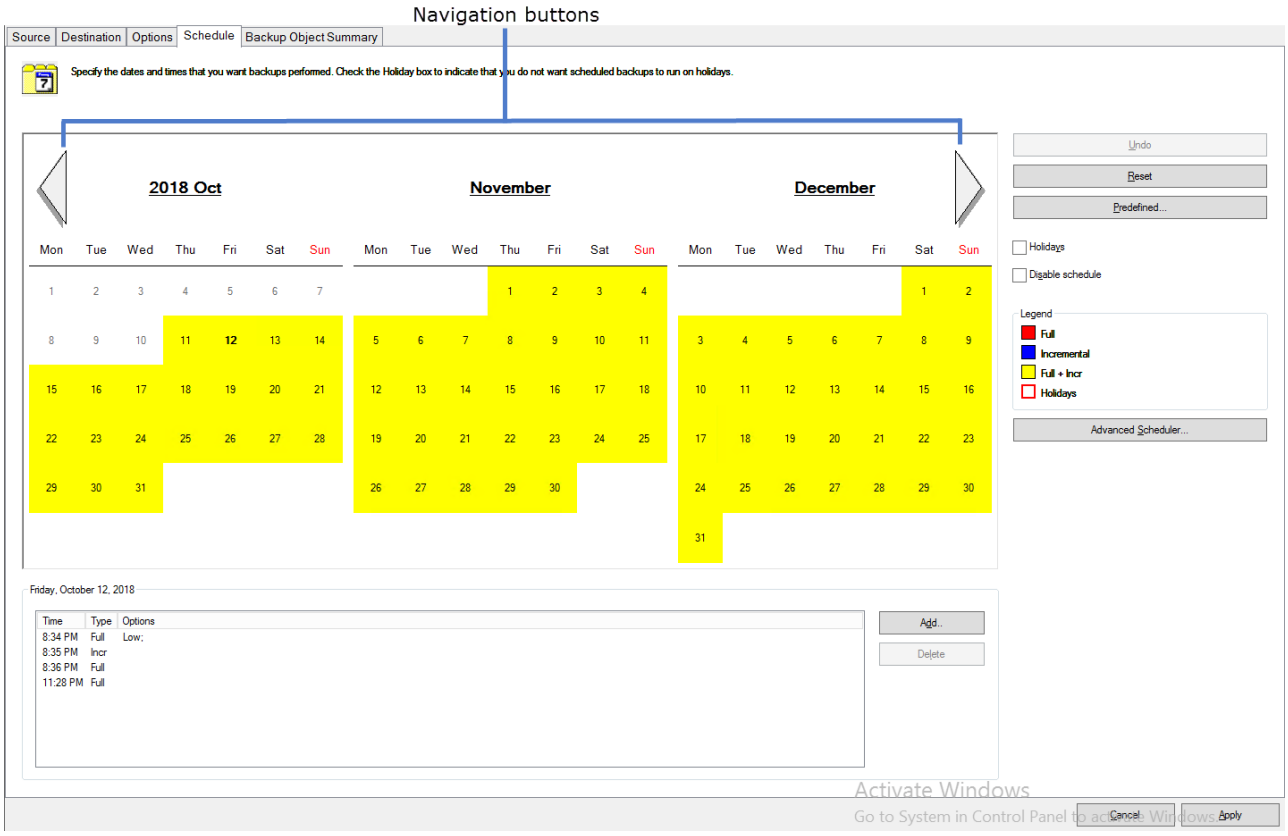
How to access the Basic Scheduler page?

To access the Scheduler page, click **Backup** in the context list, double-click the **Backup Specification** in the Scoping Pane, and then click the **Schedule** tab. Similarly, follow the same process to access the **Schedule** tab in case of other scheduling tasks like object copying, object consolidation, object verification, reporting, and media copying.

Use the following links to understand the Scheduler UI, and how to create and edit schedules in Data Protector.

- Basic Scheduler user interface
- Basic Scheduler options
- Basic Scheduler tasks

Basic Scheduler user interface



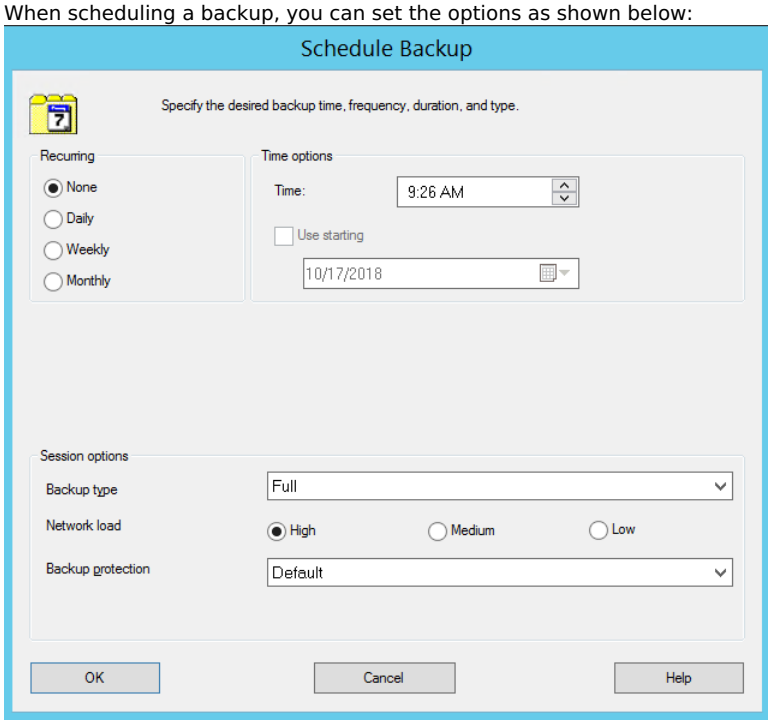
The controls are explained in the table below:

Control	Description
Undo	Reverses the last action.
Reset	Resets the schedule.

Control	Description
Predefined	Selects one of the available predefined backup schedules: • **daily intensive**: Data Protector runs a full backup at midnight and two additional incremental backups at 12:00 (noon) and 18:00 (6 P.M.) every day. • **daily full**: Data Protector runs a full backup every day at 21:00 (9 P.M.). • **weekly full**: Data Protector runs a full backup every Friday and Incr1 backups every day from Monday to Friday at 21:00 (9 P.M.). • **fortnight full**: Data Protector runs a full backup every second Friday. Between these backups, Data Protector runs Incr1 backups every Monday to Thursday, all at 21:00 (9 P.M.). • **monthly full**: Data Protector runs a full backup on the first of every month, an Incr1 backup every week, and an incremental backup every other day.
Holidays	Select this option if you do not want backups to run on holidays. By default, Data Protector runs backups on holidays.
Disable schedule	Select this option to prevent the scheduled backups from being performed, or deselect it to enable the schedule.
Legend	The colors that represent the types of scheduled backups in the calendar. • Red represents Full backup • Blue represents Incremental backup • Yellow represents Incremental+Full backup • White with a red border represents holidays.
Add	Schedules a backup on the date selected in the calendar.
Delete	Removes the backup selected in the list below the calendar.
Navigation buttons	The **Previous** navigation button on the left displays the calendar view of the previous month. The **Next** navigation buttons on the right displays the calendar view of the next month. The schedule for each day is highlighted against each date.

Basic Scheduler options

When scheduling a backup, you can set the options as shown below:



The controls are explained in the table below:

Control	Description
Recurring options	Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Control	Description
Time options	**Time:** Selects the time for the backup to start. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity option. **Use starting:** This option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.

Session options	Specify the following for the scheduled backup:
	
	• Backup types:
	  ◦ Full: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.
	  ◦ Incremental: If this option is selected, it backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup.
	• Network load: Set this option to **Medium** or **Low** to reduce the load on the network when running Data Protector. The default selection is **High**.
	• Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten.

Basic Scheduler tasks

You can perform the following tasks using the Basic Scheduler:

- Create a schedule
- Customize the schedule calendar

Create a schedule

Complete the following steps to schedule a backup. Similarly, follow the same procedure for object copy, object consolidation, verification, reporting and media copy to create a schedule.

1. Click **Backup** in the Context List.
2. Expand **Backup Specifications** in the Scoping Pane, and then expand the type of backup specification (for example, Filesystem). All saved backup specifications are displayed.
3. Double-click the appropriate backup specification and click the **Schedule** tab. The Schedule page is displayed.
4. Scroll through the calendar by clicking the single forward or back arrow to choose the month in which you want to schedule your backup.
5. Right-click the date on which you want to run the backup, and click **Schedule** to display the Schedule Backup dialog box.
6. Specify the **Recurring** options.
   - Set the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.
7. Set the time for the backup to start in the **Time Options**. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity option.
   The **Use starting** option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.
8. Set the **Session options**.
   - **Backup types**:
     - **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.
     - **Incremental**: If this option is selected, it backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup.
   - **Network load**: Set this option to Medium or Low to reduce the load on the network when running Data Protector. The default selection is High.
   - **Backup protection**: Specify the time period of protection of the data you back up to prevent the backup from being overwritten.
     In the case of ZDB to disk+tape or ZDB to disk (instant recovery enabled), specify the **Split mirror/snapshot backup** option.
9. Click **OK**.
10. Repeat steps 4 to 9 for all backups that you want to schedule.
11. Click **Apply** to save the changes.

> **Note** To modify schedule options for individual backups, perform steps 5 through 9.

Customize the schedule calendar

You can customize the appearance of the calendar that is used for scheduling various tasks, such as a backups, automated

media copying, and report generation.

You can customize the calendar when scheduling one of the scheduled operations, or when reviewing the schedule. After you have opened the Schedule property page of the scheduled operation, do the following:

1. In the Schedule property page, right-click a month name and select the required option from the pop-up menu.
   - **Fonts**: Select this option to customize The **Title**, **Weekday names**, and **Calendar days**.
   - **Dimensions**: Select this option to specify calendar dimensions.
     - **Calendar minimum size**: Set the minimum width and height of the months. Use the preferred unit. You can choose between millimeters and pixels. The default width and height are 59 and 49 mm respectively.
     - **Calendar title percentage**: Set the size of the month titles. The default is 22 percent.
2. Customize the calendar as required and click **OK**.

Handle scheduler conflicts

When scheduling periodic backups, it can happen that the chosen backup start time is already occupied by another scheduled backup in the same backup specification. In that case, Data Protector prompts you that there are scheduling conflicts, and asks if you wish to continue.

- If you click **Yes**, the new schedule will be applied where possible (on the days when the time slot is still free).
- If you click **No**, the new schedule will be discarded.

Backup during holidays

You can set different holidays by editing the Holidays file that resides in the default Data Protector server configuration directory.

By default, Data Protector runs backups on holidays. If you want to change the default behavior, consider the following example. If the date January 1 is registered as a holiday, Data Protector will not back up on that date. If you have scheduled a full backup for January 1st and an incremental for January 2nd, Data Protector will skip running the full backup on January 1st but will run the incremental backup scheduled for January 2nd. The incremental backup will be based on the last full backup.

It is generally not recommended to skip backups on holidays.

Consider the following when editing or adding new entries in the Holidays file:

- The first number in each line indicates the consecutive day of the year. The value is ignored by Data Protector, but it must be set between 0 and 366. You can set it to 0 to indicate that the number does not correspond to the date that follows it.
- The date is specified as Mmm d, where Mmm is the three-letter abbreviation of the month and d is day of month as a number (for example, Jan 1). Note that the month must be specified in English, regardless of your locale.
- The description of the holiday is optional and is currently not used by Data Protector.
- Data Protector only reads the following file name:
  - **Unix**: /etc/opt/omni/server/Holidays
  - **Windows**: \ProgramData\OmniBack\Config\Server\Holidays
- The `Holidays` file will be updated with the current year's holidays
- The `Holidays` file will be loaded with AppServer once everyday at the time of daily maintenance
- The `Holidays` file will be analysed every time the `omnitrig` reads schedules.
- For the AppServer, the log file which contains the result from **Holiday upload** should be mentioned.

Regardless of the year specified at the top of the file, the holidays specified in the file are always used as-is and must be edited manually if the holidays do not occur on the same dates each year. If you are not using the Holidays option for the scheduler, you can remove or comment out the entries in the Holidays file to prevent confusion in case of accidental use of a Holidays file that is out of date or has not been customized for your country or company specific requirements.

Limitations

The following limitation apply to the Basic Scheduler:

- The Basic Scheduler only supports the 12-hour time format.
- For all type of specifications in the **Scoping pane**, the values for **Scheduled** and **Backup Type** column appear as `n/a` in the **Results Area**, even if the specification is scheduled.
- The Scheduler uses the backup type option that was specified during backup specification creation. Also, you cannot reconfigure the backup type during the schedule creation or schedule migration.
- All schedules are displayed in the calendar in the time zone of the Cell Manager system. If you specified a backup or object operation session for a different time zone than that of the Cell Manager, the session will run at the specified time in the specified time zone.

Web-based Scheduler

The Web-based Scheduler provides a refined user interface and simplified and easy-to-use web controls, which provides easier schedule management. You can set the data protection, recurrence pattern, and fix conflicts using a single Scheduler wizard. Use the Scheduler to automate various operations such as, backup, object consolidation, verification, and copying, media copy, at periodic intervals. The unattended background execution of operations eliminates the need of manually repeating a schedule whenever you want to run an operation.

The Web-based Scheduler displays time in 12-hour or 24-hour time format based on the locale configuration of the user. For example, if the user locale is German, time is displayed in 24-hour format and if the user locale is English (United States), time is displayed in 12-hour format.

Web-based Scheduler options

Based on the specification type, you can set the following schedule options:

- Backup type: The type of backup. For example, full or incremental.
- Network load: The network load for the session. Setting this option to**Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users, but increases the time required for the session to complete.
- Data protection: The time period of protection for the data you backup to prevent the backup from being overwritten.
- Recurrence pattern: The frequency at which the schedule must run.

Additionally, the new Scheduler includes the following features:

Schedule exclusion during holidays

You can set different holidays by editing the Holidays file that resides in the default Data Protector server configuration directory.

By default, Data Protector runs backups on holidays. If you want to change the default behavior, consider the following example. If the date January 1 is registered as a holiday, Data Protector will not backup on that date. If you have scheduled a full backup for January 1 and an incremental for January 2, Data Protector will skip running the full backup on January 1 but will run the incremental backup scheduled for January 2. The incremental backup will be based on the last full backup.

Consider the following when editing or adding new entries in the `Holidays` file:

- The first number in each line indicates the consecutive day of the year. The value is ignored by Data Protector, but it must be set between `0` and `366`. You can set it to `0` to indicate that the number does not correspond to the date that follows it.
- The date is specified as `Mmm dd`, where `Mmm` is the three-letter abbreviation of the month and `dd` is day of month as a number (for example, `Jan 1`). Note that the month must be specified in English, regardless of your locale.
- The description of the holiday is optional and is currently not used by Data Protector.
- Data Protector only reads the following file name:
  - **Unix**: /etc/opt/omni/server/Holidays
  - **Windows**: \ProgramData\OmniBack\Config\Server\Holidays
- The `Holidays` file will be updated with the current year's holidays
- The `Holidays` file will be loaded with AppServer once everyday at the time of daily maintenance
- The `Holidays` file will be analysed every time the `omnitrig` reads schedules.
- For the AppServer, the log file which contains the result from**Holiday upload** should be mentioned.

Regardless of the year specified at the top of the file, the holidays specified in the file are always used as-is and must be edited manually if the holidays do not occur on the same dates each year. If you are not using the **Holidays** option for the Scheduler, you can remove or comment out the entries in the `Holidays` file to prevent confusion in case of accidental use of a `Holidays` file that is out of date or has not been customized for your country or company specific requirements.

Handle schedule conflicts

When scheduling periodic backups, it can happen that the chosen backup start time is already occupied by another scheduled backup in the same backup specification. In that case, Data Protector Schedule wizard shows you that there are scheduling conflicts. You can either redefine the recurrence pattern, or allow the Scheduler to set the schedule on the days when the time slot is still free. Based on the time slot availability, the following values are set as schedule status:

- Active: The schedule has no conflicts, and will run at the scheduled time.
- Overlapped: The schedule is in conflicting state, but free time slots are available for the selected date, when the schedule can be run.
- Inactive: The schedule is in conflicting state, and there are no free slots available on the selected date, when the schedule can run.
- Disabled: The schedule has explicitly been disabled by the user.

Note: If a scheduled backup specification is running, and the same backup specification is triggered again while the current schedule is already running, the second backup specification is ignored, and is not queued to be run later. For example, if 50 backup specifications are running, and are still in queued state; and in a 15 minute interval, the same backup specifications are triggered again, the new triggers are ignored. However, if the backup that is scheduled first is deleted, the conflicting backup will get activated automatically and will be displayed on the UI.

How to access the Web-based Scheduler page?

To access the Scheduler page, click **Home** Context Menu in the GUI, and then click **Scheduler** in the top pane. All schedules for the selected date, including disabled schedules, are listed on the Scheduler page. Use the following links to understand the Scheduler UI, and how to create and edit schedules in Data Protector.

Web-based Scheduler user interface

The following table describes the various controls that appear on the Web-based Scheduler UI:

Control	Description
Calendar	Displays the calendar. You can select a date in the calendar to view all the schedules for that day.
Navigation Buttons	The **Previous** and **Next** navigation buttons that enable you to move the date back and forward, and view the list of schedules for the selected date.
Filter	Allows you to open or close the Filter panel in the left pane. You can filter schedules based on the Specification name, Applications, Specification type, and Status. To search for a specification schedule, select the required criteria and click **Apply**. To clear the filter criteria, click **Reset**. If one or more filters are applied, the filter icon changes to
New	Opens the Create New Schedule wizard, and allows you to create a new schedule.
Enable	Enable one or more selected schedules. You can use this option to enable the entire series and not a single instance.
Disable	Disable one or more selected schedules. You can use this option to disable the entire series and not a single instance. If you disable a schedule, the schedule appears in gray color. Disabling a schedule does not impact any currently running schedules.
Delete	Deletes one or more selected schedules. After you click Delete, the following options are displayed: • **Delete** - Click to delete the instance of the schedule. • **Delete Schedules** - Click to delete all the schedules in the series.
Missed Job Execution	Displays a list of all the missed job executions and allows you to run or delete missed jobs.
Day View	Lists all schedules for the selected date, including disabled schedules. Click a**Schedule Name** in the Day view to view details of a specific schedule or edit, disable, or delete the schedule. To view all the available schedules for a specification, click **Specification Name**. Click the required schedule to view details, edit, disable, or delete the schedule.
Expand	This option is available in the Day view for minutely and hourly schedules. You can use this option to expand the list of schedules.
Collapse	This option is available in the Day view for minutely and hourly schedules. You can use this option to collapse the list of schedules. This option makes it easier to maintain a clutter-free day view , especially when a large number of schedules are listed.
Edit	Opens the Edit Schedule wizard.

Day View

The Day view on the Scheduler page lists all schedules for the selected date, including disabled schedules. You can click **Calendar** to select a date or use the Navigation buttons to move to the next or previous date.

It consists of the following columns which you can resize and sort based on your requirement:

- **Time:** Start time of the schedule.
- **Specification name:** Name of the specification for which the schedule is created.
- **Specification type:** Specification type for which the schedule is created. Each specification type is indicated by a specific color. For example, a Backup specification is marked with Blue color.
- **Schedule name:** Name of the schedule.
- **Backup type:**Type of the backup. For example, Full, Incremental, and so on.
- **Type:** Type of objects being backed up by the schedule.
- **Status:** Status of the schedule - Enabled or Disabled.
- **Edit:** Allows you to edit a schedule.

Filter schedules in a day view

You can use the Filter icon to open or close the Filter panel in the left pane. You can filter schedules based on the following:

- **Specification name:** This drop-down list contains the name of specifications for which schedules are created. You can either select from the drop-down list or type a specification name. As you start typing, all the names that match the text string are listed. You can then select the required specification name.
- **Application Name:** This drop-down list contains a list of the available application types. You can either select from the

drop-down list or type an application name. As you start typing, all the names that match the text string are listed. You can then select the required application name.

- **Specification type:** You can filter schedules based on the specification type used when creating a schedule. You can filter the schedules based on one or more of the following Specification types.
  - Backup
  - Verification
  - Consolidation
  - Copy
  - Media
  - Report
- **Status** - You can filter schedules based on the status. The available options are **Enabled** or **Disabled**.

After specifying the filter criteria, click **Apply** to apply the filters and refresh the page. To clear all the filters and refresh the page, click **Reset**.

Web-based Scheduler tasks

You can perform following tasks using the Web-based Scheduler.

- Create a schedule
- Edit an existing schedule
- View a schedule
- Enable and disable a schedule
- Configure schedule execution on holidays
- Set a schedule on a specific date and time
- Configure a recurring schedule
- Configure debugging
- Create a maintenance job
- Manage Missed Executions

Important You cannot reset schedules in the web-based Scheduler.

Create a schedule

The steps below show how to create a schedule for a specification type. The options available to you in the schedule wizard are based on the types of specification you choose.

1. In the Context Menu click **Home**, and then click **Scheduler** in the top pane. The Scheduler page opens.
2. Click + **New** in the top-right corner of the Scheduler page. The Create New Schedule page opens.
3. Select the specification for which you want create a schedule. To select a specification, you can either browse through the specification types or search for a specification by typing the specification name in the Search box. You must type minimum three characters to start the search. As you start typing, all the specifications that match the text string are listed.
   - For Backup Specification and Object Operation specification types, the Search displays results in the following format: Specification name (Application Type)
   - For Reporting and Media Copy, the results are displayed in the following format: Specification name (Specification Type)

   The name of the selected specification is displayed at the bottom of the wizard.
   To schedule a replication session, configure the object copy specification as **Use Replication**, and then schedule the copy specification.
   Note:
   - You cannot use this wizard to schedule a template.
   - The Search option is not applicable for Templates.
   - Starting with Data Protector 2019.12 release, Predefined schedules are not supported.

   Click **Next**.
4. In the **Properties** section, specify the properties for the schedule:
   - Specify a name for your schedule in the **Schedule Name** text box. The schedule name is pre-populated with <SpecificationType>-<ApplicationType>-<SpecificationName>. For example: Backup-oracle-iwf1114089_server Copy-dailybackups_storeonce
   - Select the **Backup Type**. For example, Full, Incremental, and so on.
   - Select the protection level from the **Data Protection Type** drop-down list. Protection level determines how long the information about the backed up data is kept in the IDB. If there is no catalog protection, you can still restore your data, but you cannot browse for it in the Data Protector GUI. Select from one of the following options:
     - None: Provides no protection.
     - Default: The information about backed up data in the IDB is protected as long as the data is protected.
     - Until: The information in the IDB cannot be overwritten until the specified date. Protection for the information stops at midnight on the chosen day.
     - Days: The information in the IDB cannot be overwritten for the specified number of days.
     - Weeks: The information in the IDB cannot be overwritten for the specified number of weeks.
     - Permanent: The information in the IDB is available permanently.
   - By default, the schedule is enabled. Turn OFF the **Schedule Activation** option to disable the schedule.
   - Turn ON the **Do not execute on Holidays** option if you do not want the operation to run on holidays. **Note**: To specify different days as holidays, edit the Holidays file. For more information about the Holidays file, see *Schedule*

exclusion during holidays section on this page.
- In the **Advanced options**, specify the **Network Load**. Setting this option to Medium or Low reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. **Note**: Starting with Data Protector 2019.12 release, setting **Priority** for the schedules is not supported.
- Turn ON the **Debug** option if you want to enable the debug logs for this schedule. Specify the debug file name in the **File Name** text box. By default, the debug files are stored in the `C:\ProgramData\OmniBack\tmp` folder and `/var/opt/omni/log` folder for Windows and Linux respectively. Select the range for debug logs in the **From** and **To** text box; the maximum value can be set as 900.

5. In the **Recurrence** section, specify the recurrence pattern. specify how often the backups should occur. Select the pattern and frequency from the following options:
   - **Once**: The schedule runs on the specific date only once. You can select the start date and time when the schedule must run. The start date is created in the time zone of the Cell Manager. The time zone field is non-editable.
   - **Minute(s)**: The schedule runs recursively after selected minutes in the specified time range. You can select the schedule frequency from the Every <value> Minute(s) field. The available values are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 minutes. For example, a recurrence value of 15 Minute(s) results in the schedule running every 15 minutes in the selected time range. You can also select the days on which this schedule must run.
   - **Hour(s)**: The schedule runs recursively after selected hours in the specified time range. You can select the schedule frequency from the Every <value> Hour(s) field. The available values are 1, 2, 3, 4, 6, 8, 12 hours. For example, a recurrence value of 2 Hour(s) results in the schedule running every 2 hours in the selected time range. You can also select the days on which this schedule must run.
   - **Day(s)**: The schedule runs regularly at the specified time. The schedules can be run on a weekday (Monday-Friday) or everyday. You can specify the schedule frequency using the Every <value> Day(s) field. For example, a recurrence value of 4 results in the schedule running every fourth day. You can select the start date and time when the schedule must run.
   - **Week(s)**: The schedule runs weekly on the specified day. You can specify the schedule frequency using the Every <value> Week(s) field. For example, a recurrence value of 2 results in the schedule running every two weeks on the selected day. You can select the start date and time when the schedule must run.
   - **Month(s)**: The schedule runs monthly on the specified day of the month. You can select the schedule frequency using the Every <value> month(s) field. The available values are 1, 2, 3, 4, 6, 12 months. For example, a value of 2 results in the schedule running every second month on the selected day. You can also set the schedule on a monthly day. For example: The schedule can be run every 1st Monday of the month. The schedule can be run every 1st Monday of every two months. The schedule can also run on last Sunday of the month. Select the **End of Recurrence** from one of the following options:
     - No End Date: Select if the backup is to recur indefinitely.
     - End Date: Select if the schedule must end on a specific date. The end date occurs in the same time zone as the start date. The **End of Recurrence** option is not available if you select **Once**.
6. Click Next to go to the **Summary** page. The Summary page displays a summary of the schedule. For example, you can see the specification name for which the schedule is created, the type of backup (Full/Incremental) that must be performed, the type of schedule, and so on.
7. Review all the schedule options. If there are schedule conflicts, the **Conflicts Found** option is shown as **Yes**, and you cannot complete the schedule creation task until you perform one of the following:
   - Redefine the schedule recurrence pattern. Click Previous to go back to the **Recurrence** page.
   - Turn ON the **Fill free slots** option. This option is available only if free time slots are available for the selected date. If there are no free time slots, you must redefine the schedule recurrence pattern.

> **Note** Conflicts are not handled for Minute(s) and Hour(s) recurrence type.

Click **Clone schedule** if you want to create a copy of the schedule. Click **Finish** to create the schedule.

Edit an existing schedule

You can edit a schedule either from the Backup context or from the Scheduler page.

Edit an existing schedule from the Backup context

The steps below show how to edit a schedule for a backup specification. The options available to you in the schedule wizard are based on the types of specification you choose.

> **Note** If you modify any of the following options for a schedule, the schedule is deleted, and a new schedule is created with the new values. This new schedule is moved to the end of the queue, and based on the time slot availability, status is applied.
>
> - Start Date
> - End Date
> - Time zone
> - Recurrence Pattern
> - Every nth value
> - Holidays

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then expand the appropriate type of backup specification (for

example, **Filesystem**). All saved backup specifications are displayed.
3. Right-click the appropriate backup specification and click **Edit Web Schedule**. The Scheduler page opens. All available schedules for the backup specification are listed in the right pane.
4. Click the schedule that you want to edit and click **Edit**. The **Edit Schedule** wizard opens.
5. Modify the required options and click **Finish**.

Edit a schedule from the Scheduler page

Follow these steps:

1. Go to **Home** context > **Scheduler**.
2. Do one of the following:
   1. Click **Specification name** to display all schedules configured for that specification, select the required schedule, and click **Edit**.
   2. Click **Schedule name** and click **Edit**. The **Edit Schedule** wizard opens.
3. Modify the required options and click **Finish**.

View a schedule

To view all schedules for a specification, click **Specification name** in the day view . All schedules for that specification are shown in the right pane.

To view details of a specific schedule, click the **Schedule name** in the day view.

The following details about the schedule are displayed in the right pane:

- Name: The name of the schedule.
- Specification: The name of the specification for which the schedule is created.
- Specification Type: The specification type for which the schedule is created.
- Data Protection: The data protection type selected for the schedule.
- Recurrence: The recurrence pattern set for the schedule.
- Network Load: The current values set for the load on the network when running Data Protector.

Enable and disable a schedule

By default, the schedule is enabled when added, but you can disable it, leaving the schedule settings intact for later use. Disabling backup schedules does not influence currently running backup sessions. The steps in this procedure show how to disable and enable a single or multiple schedules for a backup specification. The options available to you in the schedule wizard are based on the types of specification you choose. Perform the following steps to disable or enable schedules:

1. In the Context Menu click **Home**, and then click **Scheduler** in the top pane. The Scheduler page opens.
2. Click the Calendar icon. The calendar is displayed.
3. Select a day from the calendar. All the schedules set for the day are displayed.
4. Select a schedule and click **Disable**. You can also disable multiple schedules. Similarly, select one or more schedules and click **Enable** to enable the schedules.

Configure schedule execution on holidays

By default, Data Protector runs schedules on holidays. You can change this behavior by selecting the **Holidays** option. The backup on holidays is not performed until you deselect this option. The steps in this procedure show how to enable and disable a schedule for a backup specification on holidays. The options available to you in the schedule wizard are based on the types of specification you choose.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then expand the type of backup specification (for example, **Filesystem**). All saved backup specifications are displayed.
3. Right-click the backup specification for which you want to disable or enable backup schedule during holidays and, then **Edit Web Schedule**. The Scheduler page opens. All schedules available for the backup specification are visible in the right pane.
4. Click the schedule you want to edit, and then click the **Edit** icon. The Schedule wizard opens.
5. In the Properties section, turn **ON** the **Do not execute on Holidays** slider to prevent the operation from being performed on holidays. Turn **OFF** the slider if you want the operation to be performed on holidays.
6. Click **Next**. The Recurrence page opens.
7. Verify the recurrence pattern, and click **Next**. The Summary page opens.
8. Review the schedule options, and click **Finish**.

Configure a non-recurring schedule

The steps below show how to set a schedule for a backup specification on a specific date and time. The options available to you in the schedule wizard are based on the types of specification you choose.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then expand the appropriate type of backup specification (for example, **Filesystem**). All saved backup specifications are displayed.
3. Right-click the appropriate backup specification and click **Edit Web Schedule**. The Schedule page opens. All available schedules for the backup specification are listed in the right pane.
4. Click the schedule you want to edit, and then click the **Edit** icon. The Schedule wizard opens.
5. In the **Recurrence** section, select **Once**, and then specify the start date and the time when the backup must start. You can also specify the backup duration, and click **Next**.
6. Review the schedule options in the Summary page, and click **Finish**.
   If you schedule a backup in a time slot that is already occupied by a scheduled backup, the new scheduled backup overrides the previous one.

Configure a recurring schedule

You can create a schedule such that it starts at a specific time and date, and repeats as per the defined pattern. For example, you can schedule a full backup to take place every Friday at 21:00 for the next six months. Complete the following steps:

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, and then expand the appropriate type of backup specification (for example, **Filesystem**). All saved backup specifications are displayed.
3. Right-click the appropriate backup specification, and then click **Edit Web Schedule**. The Schedule wizard opens.
4. Go to the **Properties** section. In the **Schedule Name** text box, enter a name for the new schedule. Select a backup type (Full or Incremental; some other backup types are available for specific integrations), backup protection, and network load. Click **Next**. The Recurrence page opens.
5. Under **Recurrence Pattern**, select the pattern and frequency from the following options:
   - **Once**: The schedule runs on the specific date only once. You can select the start date and time when the schedule must run.
   - **Minute(s)**: The schedule runs recursively after selected minutes in the specified time range. You can select the schedule frequency from the Every <value> Minute(s) field. The available values are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 minutes. For example, a recurrence value of 15 Minute(s) results in the schedule running every 15 minutes in the selected time range. You can also select the days on which this schedule must run.
   - **Hour(s)**: The schedule runs recursively after selected hours in the specified time range. You can select the schedule frequency from the Every <value> Hour(s) field. The available values are 1, 2, 3, 4, 6, 8, 12 hours. For example, a recurrence value of 2 Hour(s) results in the schedule running every 2 hours in the selected time range. You can also select the days on which this schedule must run.
   - **Day(s)**: The schedule runs regularly at the specified time. The schedules can be run on a weekday (Monday-Friday) or everyday. You can specify the schedule frequency using the Every <value> Day(s) field. For example, a recurrence value of 4 results in the schedule running every fourth day.

     You can select the start date and time when the schedule must run.
   - **Week(s)**: The schedule runs weekly on the specified day. You can specify the schedule frequency using the Every <value> Week(s) field. For example, a recurrence value of 2 results in the schedule running every two weeks on the selected day.

     You can select the start date and time when the schedule must run.
   - **Month(s)**: The schedule runs monthly on the specified day of the month. You can select the schedule frequency using the Every <value> month(s) field. The available values are 1, 2, 3, 4, 6, 12 months. For example, a value of 2 results in the schedule running every second month on the selected day. You can also set the schedule on a monthly day. For example, the schedule can be run every 1st Monday of the month. It can also run, for example, every 1st Monday of every two months.
6. Specify the range of recurrence from the following options, and click **Next**.
   - Start: The initial date of the schedule. Specify the date, time-zone, and time when the schedule must start.
   - End of recurrence: The date when the final schedule must run. Select **No end date** if the schedule must run indefinitely.

   > **Note** If you set the recurring to 2 or more (for example, every 2 weeks on Saturday) without setting the starting date, the first backup may not be scheduled on the first possible date that matches your selection (for example, it will be scheduled on the second Saturday) due to the Data Protector scheduling algorithm.
7. Review the schedule options in the Summary page, and click **Finish**.
   If there are scheduling conflicts, Data Protector notifies you so that you can modify the schedule.

Configure debugging

You can enable or disable debug logs for a schedule by using the Schedule wizard.

The steps in the following procedure show how to enable debug logs for a schedule that is set for a backup specification. The options available to you in the schedule wizard are based on the types of specification you choose.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then expand the appropriate type of backup specification (for example, **Filesystem**). All saved backup specifications are displayed.
3. Right-click the appropriate backup specification and click **Edit Web Schedule**. The Scheduler page opens. All available schedules for the backup specification are listed in the right pane.
4. On the Scheduler page, click **Edit** icon for the schedule, for which you want to enable the debug logs and go to **Properties** page.
5. Expand **Advanced options** and turn ON the **Debugging** option to enable the debug logs for this schedule. Specify the debug file name in the **File Name** text box. By default, the debug files are stored in the C:\ProgramData\OmniBack\tmp folder. Select the range for debug logs in the **From** and **To** text box; the maximum value can be set as 900.

   Click **Next**. The Recurrence page opens.

6. Review the options, and then click **Next**. The Summary page opens.
7. Review all the schedule options. Click **Finish** to save the schedule.

Create a maintenance job

Complete the following steps to create a one-time maintenance job.

1. In the Context Menu click **Home**, and then click **Settings** in the top-right corner. Maintenance Job window is displayed.
2. Toggle the Quartz Status switch to **Paused** to pause all the scheduled jobs or **Running** to run the scheduled jobs.
3. Set the maintenance job start time and specify the duration the maintenance job has to run.
4. Toggle the **Trigger Skipped Schedules** switch to **Yes** to run the jobs paused during the maintenance job or **No** to skip running the jobs stopped during maintenance job.
5. Click **Save** to create a new maintenance job.

Edit a maintenance job

Complete the following steps to edit the maintenance job.

1. In the Context Menu click **Home**, and then click **Settings** in the top-right corner. Maintenance Job window is displayed.
2. Edit or change the following in the Maintenance Job window:
    1. Toggle the Current Status switch to **Paused** to pause all the scheduled jobs or **Running** to run the scheduled jobs.
    2. Edit the maintenance job start time and specify the duration the maintenance job has to run.
    3. Toggle the **Trigger Skipped Schedules** switch to **Yes** to run the jobs paused during the maintenance job or **No** to skip running the jobs stopped during maintenance job.
3. Click **Save** to save the modified maintenance job.

Delete a maintenance job

Complete the following steps to delete the maintenance job.

1. In the Context Menu click **Home**, and then click **Settings** in the top-right corner. Maintenance Job window is displayed.
2. Click **Delete** to delete the maintenance job. The Delete option is enabled only after maintenance schedules are created.

Manage Missed Executions

Missed executions are the sessions, scheduled using Scheduler, that failed due to a Cell Manager downtime, schedule not being configured properly, or backup specification being removed.To manage missed executions, you need the `Start backup specification` permission.

To list all the missed executions, complete the following steps:

1. In the Context List, click **Home** and then click **Scheduler** in the top pane. The Scheduler page opens.
2. Click **Missed Job Executions**.

    A table is displayed listing all the missed executions.

> **Note** The sessions that failed to execute due to maintenance mode are not treated as missed jobs, so they do not appear in the table.
>
> With Data Protector 2018.11 (10.20) onwards, only the missed jobs for the last 31 days will be listed.

Limitations and known issues

The following limitation exists with the Web-based Scheduler:

- The Web-based Scheduler provides only a day view of the schedules. Monthly view is not supported.
- Starting DP 2019.12 release, Predefined schedules are not supported.
- For the start date is of a schedule, the time zone of the Cell Manager is considered. The time zone field is non-editable.
- Starting with Data Protector 2019.12 release, setting **Priority** for the schedules is not supported.
- For all type of specifications in the **Scoping pane** in **Backup context**, the values for **Scheduled** and **Backup Type** column appear as `n/a` in the **Results Area**, even if the specification is scheduled.
- With the Web-based Scheduler, you cannot schedule a backup specification of the type `disk+tape` as `disk only`. The Scheduler uses the backup type option that was specified during backup specification creation. Also, you cannot reconfigure the backup type during the schedule creation or schedule migration.

  However, during migration, the old schedules created using basic scheduler are migrated as-is. For example, in Data Protector 9.0x, if a backup specification was created as `disk+tape` backup, and scheduled as `disk` only; post-migration, the schedule runs as `disk only`, the way it was configured in the basic schedule file.
- The Cell Manager and the GUI should be in the same time zone.
- The schedules added in previous versions of Data Protector did not have a name attribute associated with them. As a result, after migration, the name for the migrated schedules appears as **...** (series of three dots/ellipsis symbol). You can edit these schedule and provide a name to the schedule.

- During upgrade, yearly schedules configured in earlier versions of Data Protector will not be migrated to the latest version of Data Protector.
- While upgrading to the latest Data Protector version, the start date is not replicated for recurring schedules. Instead, the new Scheduler in the latest Data Protector version, considers the migration date as the start date for the recurring schedules.
- In versions prior to the latest Data Protector version, if the start date for a recurring schedule of the type Every x Day(s) was not set during the schedule creation; then, while upgrading Data Protector to the latest version, the new Scheduler considers the migration date as the start date for these recurring schedules.
- The schedules with -exclude option are not migrated in the new scheduler. You have to recreate these schedules manually.

Migrate schedules

Data Protector gives you an option to use both the Basic Scheduler and the Web-based scheduler to create schedules independently. The following table provides information on what happens when you upgrade to the the latest version of Data Protector from the earlier versions.

Upgrade path	Migration
New installation	• Basic Scheduler template schedules and holidays will be reintroduced.
Upgrade from Data Protector 8.x or 9.x to Data Protector 2018.11 or later versions.	• Schedules created using the Advanced Scheduler will be migrated to the Web-based Scheduler. • Schedules created using the Basic Scheduler will not get migrated. • Basic Scheduler template schedules and holidays will be reintroduced.
Upgrade from Data Protector 10.x to Data Protector 2018.11 and later versions.	• Basic Scheduler template schedules and holidays will be reinstated.
Upgrade from Data Protector 8.x or 9.x to 10.x to Data Protector 2018.11 and later versions.	

Migrate schedules

The following sections provide options to migrate schedules between the two schedulers.

Basic Scheduler to Web-based Scheduler

Use the `omnidbutil -migrate_schedules` option to migrate from Basic Scheduler to Web-based Scheduler. Schedules created using the Basic Scheduler will migrate to the Web-based Scheduler. The schedules which fail to migrate will remain with the Basic Scheduler and will be triggered as usual.

Web-based Scheduler to Basic Scheduler

Use the `omnidbutil -reinstate_legacy_schedules` option to reinstate schedules to the Basic Scheduler. All the schedules created using Basic Scheduler that were migrated will migrate back to the Basic Scheduler and be removed from the Web-based Scheduler. All the new schedules created using the Web-based Scheduler will remain and be triggered in the Web-based Scheduler along with the schedules that failed to migrate.

Use the `omnidbutil -reinstate_legacy_schedules -force` option to delete all the schedules in the Web-based Scheduler and to recreate the earlier migrated basic schedules in the Basic Scheduler. All modifications made in the Web-based scheduler will be lost when you migrate back to the Basic Scheduler.

Note It is recommended to use the `-force` option to reinstate schedules from the Web-based Scheduler to the Basic Scheduler, when you have upgraded from Data Protector 8x or 9x to Data Protector 10x to the latest version. If this option is not used, the schedules created using the Web-based Scheduler will remain and be triggered in the Web-based Scheduler and will also be recreated in the Basic Scheduler. This will cause duplication of schedules in both the Schedulers.

Important

- Migration of schedules may take time depending on number of specifications and schedules configured in the customer environment.
- Schedules that are scheduled using advanced scheduler will get **paused** during the time of upgrade. All these paused schedules and schedules of the day prior to migration will get triggered immediately after upgrade.
- Disable the schedules before starting the upgrade, and enable these schedules after the upgrade is complete.
- The deleted schedule instances will not be migrated during the upgrade.
- The missed execution schedules will not be migrated during the upgrade.

During upgrade, all your existing schedule files are appended with `.migrate` suffix.

For example, in Data Protector versions prior to 2019.02, if you had a backup specification schedule with the name `WeeklyBackup`, the file name will be modified as `WeeklyBackup.migrate` during upgrade. If migration fails, the files are not renamed.

If the schedules are not migrated correctly, you may be asked to provide these `.migrate` files to Support for troubleshooting. Alternatively, you can manually run the following command to successfully migrate the existing schedules to the new Scheduler:

```
omnidbutil -migrate_schedules
```

The migrated schedule files are available at the following location:

Specification Type	Schedule path
Backup schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\schedules UNIX: /etc/opt/omni/server/schedules
Media copy schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\amoschedules UNIX: /etc/opt/omni/server/amoschedules
Integration schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\Barschedules UNIX: /etc/opt/omni/server/Barschedules
Copy operation schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\copylists\scheduled\schedules UNIX: /etc/opt/omni/server/copylists/scheduled/schedules
Consolidation operation schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\consolidationlists\scheduled\schedules UNIX: /etc/opt/omni/server/consolidationlists/scheduled/schedules
Verification operation schedule	Windows: Data Protector_program_data\OmniBack\Config\Server\verificationlists\scheduled\schedules UNIX: /etc/opt/omni/server/verificationlists/scheduled/schedules
Report group schedules	Windows: Data Protector_program_data\OmniBack\Config\Server\rptschedules UNIX: /etc/opt/omni/server/rptschedules

Known Issues

- The schedules added in previous versions of Data Protector did not have a name attribute associated with them. As a result, after migration, the name for the migrated schedules appears as **...** (series of three dots/ellipsis symbol). You can edit these schedule and provide a name to the schedule.
- During upgrade, yearly schedules configured in earlier versions of Data Protector will not be migrated to the latest version.
- While upgrading to the latest version, the start date is not replicated for recurring schedules. Instead, the new Scheduler in the latest version, considers the migration date as the start date for the recurring schedules.
- In versions prior to the latest version, if the start date for a recurring schedule of the type `Every x Day(s)` was not set during the schedule creation; then, while upgrading Data to the latest version, the new Scheduler considers the migration date as the start date for these recurring schedules.
- The schedules with `-exclude` option are not migrated in the new scheduler. You have to recreate these schedules manually.

Use Data Protector reports

Data Protector reports offers various reports that help you in managing and planning your backup environment. The Data Protector reports are customizable and provide information on the status of the last backup, object copy, object consolidation, or object verification, consumption of media in media pools, status of devices, etc.

Traditional reports

Data Protector traditional reports provide various information on your backup environment. For example, you can check the status of the last backup, object copy, object consolidation, or object verification, check which systems in your network are not configured for backup, check on the consumption of media in media pools, check the status of devices and more.

These reports can be accessed using the **Reporting context** in the Data Protector GUI.

You can configure reports and report groups using the Data Protector GUI or any Web browser with Java support. Report groups allow you to easily manage reports, to schedule the reports in the report group, and to define the criteria for grouping the reports in report groups.

For more information on traditional reports, see Traditional reports.

Integrated reports from Reporting Server

Data Protector integrated reports offers various reports that help you in managing and planning your backup environment. These reports are customizable and provide information on the status of the last backup, object copy, object consolidation, or object verification, consumption of media in media pools, status of devices, etc. You can download these reports in PDF, PNG, CSV, or JSON format. Data Protector displays these reports as bar graph, pie chart, or in tabular format.

These reports can be accessed using the **Home context > Reports** option in the Data Protector GUI.

Data Protector displays integrated reports as bar graph, pie chart, or in tabular format. The favorite icon in the Dashboard helps you select your favorite reports to be displayed in the Dashboard.

To use integrated reporting capability, install the reporting software on a Linux or Windows server that is not a Data Protector Cell Manager. The Data Protector integrated reports are available with Capacity, Express, or Premium license only. If you change license, un-register and re-register reporting software for the new license to take effect.

For more information on integrated reports, see Integrated reports.

Use Traditional reports

The traditional reports in Data Protector offers various information about your backup environment, such as the following:

- Status of the last backup, object copy, object consolidation, or object verification
- Systems not configured for backup in your network
- Consumption of media in media pools
- Status of devices

You can configure traditional reports and report groups using the Data Protector GUI or any Web browser with Java support. Report groups allow you to:

- Manage reports
- Schedule the reports in the report group
- Define the criteria for grouping the reports in report groups

About traditional reports

- You can gather various reports in a report group, which can be scheduled, started interactively, or triggered by a notification.
- Reports can be started using the Data Protector GUI, the Data Protector CLI, the Data Protector Scheduler, a notification event, or a post-exec script that includes a Data Protector CLI command that starts the report.
- Reporting is also available for a multiple-cell configuration when you use the **Manager-of-Managers** (MoM) functionality.
- Provides the output of the reports in various formats and can optionally display input parameters (selections), also.

Report parameters allow you to customize reports. Some parameters allow multiple selections. If no optional input parameters (optional selections) are specified when configuring a report, a default value is set, which is `all` in the case of objects and `no time limit` in the case of time frames. To configure a report or report group you need to provide:

- name for the report
- type of the report
- send method
- recipient(s)
- format

All other input parameters (selections) depend on the type of the report.

> **Note** The **VADP Reporting** feature is enabled by default. In order to disable it, set `EnableDPAforVM` global variable to `0`.

Traditional report formats

You can generate the Data Protector traditional reports in various formats.

If you start each report individually, the report displays in the Data Protector Manager and you don't have to choose the report format.

If you gather reports into report groups, you have to specify the format and the recipients of each report.

You can choose from the following report formats:

- **ASCII** - report generated as plain text.
- **HTML** - report generated in HTML format. This format helps in viewing the report using a web browser. For example, you can check if your systems have been backed up by clicking a link and viewing the report on the Intranet.
- **Short** - report generated as plain text displaying a summary of the most important information. This is the suggested format for broadcast messages.
- **Tab** - report generated with fields separated by tabs. This format helps if you plan to import the reports to other applications such as Microsoft Excel or to scripts for further analysis

The actual output of a report varies depending on the selected format. Only the Tab format displays all fields for all reports, other formats may sometimes display only selected fields.

Traditional report types

Depending on the information about your backup environment that you want to retrieve, you can generate various types of reports:

- Configuration reports
- Data Protector Internal Database (IDB) report
- Session specification reports
- Pools and media reports
- Sessions in timeframe reports
- Single session reports

Configuration reports

Configuration reports provide information such as the configuration of the Data Protector cell, devices not used for backup, and systems not configured for backup.

Configuration report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Cell Information	Lists the Data Protector cell-related information such as number of clients, backup specifications, media management server, and licensing server. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The **VADP clients** display the information on the Guest OS of the virtual machine. If the VM tools are installed and running, and VM is powered on, the Host information section of the output displays information, such as the operating system, IP address, or hostname. The VM hostname must display the DNS name if configured on the virtual machine. The VM hostname must display the IP address if VM has no DNS name and IPv4 is available. The VM hostname must display the VM name, if DNS name or IP address is not available (or) if the VM has only the IPv6 address.	none	none	all formats	cell_info
Client Backup	Lists information about the specified clients like: filesystems not configured, all objects, all objects with a valid backup and their backup times and average sizes. Note that Client Backup reports don't include information about application integration backup objects and backup specifications.	hostname	none	all formats	host
Clients not Configured for Data Protector	Lists clients in the selected domains that aren't part of the current cell. Note that generating this report can take some time depending on the condition of the network. This type of report cannot be aborted.	network range(s)	none	all formats	hosts_not_conf
Configured Clients not Used by Data Protector	Lists all configured clients that aren't used for backup and don't have any device configured.	none	none	all formats	hosts_unused
Configured Devices not Used by Data Protector	Lists configured destination devices that aren't used for backup, object copy, or object consolidation at all.	none	none	all formats	dev_unused
Licensing	Lists all licenses and the available number of licenses.	none	none	all formats	licensing
Look up Schedule	Lists all backup, object copy, object consolidation, or verification specifications that are scheduled to start in the next specified number of days, up to one year in advance.	number of days	none	all formats	lookup_sch

Data Protector Internal Database (IDB) report

IDB report provides information on the size of the IDB.

Important: The **Used** columns in this report show the percentage of used items for each IDB part. This figure is calculated as the current number of items divided by the number of maximum items for particular IDB part in percents. In case the number of items is unlimited, this figure is always 0%.

To find out whether certain parts of IDB are running out of space, you can additionally configure the IDB Space Low notification.

IDB report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
IDB Size	Provides a table that contains information about the Media Management Database, Catalog Database, Archived Log Files, Datafiles, statistics for Detail Catalog Binary Files directories, SMBF (msg directory), and low IDB disk space.	none	none	all formats	db_size

Session specification reports

Session specification reports provide information on backups, object copy, object consolidation or object verification, such as average size of backed up objects, schedule of sessions, filesystems not configured for backup, and so on.

Session specification report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Average Backup Object Sizes	Displays the average size of an object in the specified backup specification. It displays the size of the full and the incremental backup of the object. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The new object name format for **VADP clients** is as follows: <hostname>:/<vCenter>/<path>/<vmname> [<UUID>] Here, <hostname> is the DNS of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.	none	backup specification(s), backup specification group, number of days (counted from the moment of starting the report backwards)	all formats	dbobj_avesize_size
Filesystems Not Configured for Backup	Lists all disks (filesystems), that aren't configured in any of the selected backup specifications.	none	backup specification(s), backup specification group	all formats	fs_not_conf
Object's Latest Backup	Lists all objects in the IDB. For each object, it displays the last full and the last incremental backup time, the last full and the last incremental object copy time, and the last object consolidation time. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The new object name format for **VADP clients** is as follows: <hostname>:/<vCenter>/<path>/<vmname> [<UUID>] Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used. You can narrow the scope of objects listed using the backup specification filters and/or object creation time filter (see Optional Selections). However, consider the following particularities: • Objects of the Filesystem type (filesystem objects) that don't match the condition in the object creation time filter are listed anyway. However, in this case, their object creation time fields remain empty. • If you clear certain filesystem objects from a backup specification, these filesystem objects will not be included in the report even if the objects exist in the IDB. The above considerations aren't applicable for objects of the Bar type (integration objects).	none	backup specification(s), backup specification group, number of days (counted from the moment of starting the report backwards)	all formats	obj_lastbackup

Session specification report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Objects Without Backup	Lists all objects that are part of a backup specification and don't have a valid backup (successfully completed backup, the protection has not yet expired). This report is not available for backup specifications for integrations.	none	backup specification(s), backup specification group, number of days (counted from the moment of starting the report backwards)	all formats	obj_nobackup
Session Specification Information	Displays information about all selected backup, object copy, object consolidation, and object verification specifications, such as type (for example, IDB, MSESE, E2010), session type, session specification name, group, owner, and pre- and post-exec commands.	none	session specification(s), backup specification group	all formats	dl_info
Session Specification Schedule	Lists the next start time for each specified backup, object copy, object consolidation, and object verification specification up to one year in advance.	none	session specification(s), backup specification group	all formats	dl_sched
Trees in Backup Specifications	Lists all trees in the specified backup specification. It also shows names of drives and the name of a tree. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The report displays all the VM names for VMware objects.	none	backup specification(s), backup specification group	all formats	dl_trees

Pools and media pools reports

Pools and media pools reports provide information on media pools and used media.

Pools and media report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Extended List of Media	Lists all media matching the specified search criteria. For each medium, it provides information about the medium ID, medium label, media location, media condition, media protection, used and total space (MB), the time when the medium was last accessed, the media pool and media type, session specifications that have used the medium for backup, object copy, or object consolidation, as well as the session type and subtype.	none	session specification(s), backup specification group, description, location(s,) pool name(s), media type (**DDS**, **DLT**, and so forth), condition, expiration, timeframe, library device(s)	all formats	media_list_extended
List of Media	Lists all media matching the specified search criteria. For each medium, it provides information about the medium ID, medium label, media location, media condition, media protection, used and total space (MB), the time when the medium was last accessed, the media pool and media type.	none	description, location(s,) pool name(s), media type (**DDS**, **DLT**, and so forth), condition, expiration, timeframe, library device(s)	all formats	media_list
List of Pools	Lists all pools matching the specified search criteria. For each pool it provides information about the pool name, description, media type, total number of media, number of full and appendable media containing protected data, number of free media containing no protected data, number of poor, fair, and good media.	none	pool name(s), location(s), media type (**DDS**, **DLT**, and so forth), library device(s), timeframe	all formats	pool_list

Pools and media report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Media Statistics	Reports statistics on the media matching the search criteria. The following information is provided: number of media; number of scratch media; number of protected, good, fair, and poor media; number of appendable media; total, used, and free space on media.	none	description, location(s), pool name(s), media type (**DDS**, **DLT**, and so forth), condition, status, expiration, timeframe, library device(s)	all formats	media_statistics

Sessions in timeframe reports

Sessions in timeframe reports provide information on backup, object copy, object consolidation or object verification sessions that ran in a specified period of time.

Sessions in timeframe report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Client Statistics	Lists clients and their backup status statistics. Only the clients that match the search criteria are listed. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**, wherein the VM name is the client name.	timeframe	backup specification(s), backup specification group, hostname(s)	all formats	host_statistics
Device Flow	Graphically presents the usage of each device. A flow chart of the backup, object copy, and object consolidation sessions matching the search criteria is shown. If you set the RptShowPhysicalDeviceInDeviceFlowReport global option to 1, the same physical devices (presented by their lock names or serial numbers) are grouped together. If there is no lock name or serial number specified, the logical name is displayed.	timeframe	session specification(s), backup specification group	HTML	device_flow
Extended Report on Used Media	Provides extended information on destination media that have been used by backup, object copy, and object consolidation sessions in the specific time frame, as well as the session type and subtype.	timeframe	session specification(s), backup specification group	all formats	used_media_extended
List of Sessions	Lists all sessions and their statistics in the specified timeframe.	timeframe	session specification(s), backup specification group	all formats	list_sessions
Object Copies	Displays the number of valid copies of object version in the specified timeframe. The number of copies includes the original object version. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The new object name format for **VADP clients** is as follows: <hostname>:/<vCenter>/<path>/<vmname> [<UUID>] Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.	timeframe	session specification(s), backup specification group, number of copies	all formats	obj_copies
Report on Used Media	Lists destination media that have been used during the backup, object copy, and object consolidation sessions in the specified timeframe together with their statistics.	timeframe	session specification(s), backup specification group	all formats	used_media
Session Errors	Displays a list of error messages that occurred during a backup, object copy, object consolidation, or object verification session. The messages are grouped by client.	timeframe	session specification(s), backup specification group, hostname(s), message level	all formats	session_errors

Sessions in timeframe report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Session Flow	Graphically presents the duration of each session for the specified timeframe. A flow chart of the backup, object copy, object consolidation, and object verification sessions matching the search criteria is shown. Colors in the chart represent the following overall status of the sessions: • Red: Session failed or was aborted. • Green: Session completed successfully or completed with errors. • Yellow: Session completed with failures. • Blue: Session is queuing or a mount request is issued.	timeframe	session specification(s), backup specification group	HTML	session_flow
Session Statistics	Shows backup, object copy, or object consolidation status statistics in the selected timeframe.	timeframe	session specification(s), backup specification group	all formats	session_statistics

Single session reports

Single session reports provide detailed information on a specific session.

IDB report type	Description	Required selections	Optional selections	Supported formats	omnirpt option
Session Devices	Provides information about all destination devices that were used in the selected session.	session ID	none	all formats	session_devices
Session Media	Provides information about all destination media that were used in the selected session.	session ID	none	all formats	session_media
Session Object Copies	Displays the number of valid copies in a selected backup, object copy, or object consolidation session. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The new object name format for **VADP clients** is as follows: <hostname>:/<vCenter>/<path>/<vmname> [<UUID>] Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.	session ID	none	all formats	session_objcopies
Session Objects	Lists all backup, object copy, or object consolidation objects and their statistics that were part of a selected session. The **VADP** feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The Session Objects report displays the VM name and VM path.	session ID	none	all formats	session_objects
Session per Client	Provides information about each client that was part of the selected backup session. Using the **Generate multiple reports** option, this report can be split into smaller reports, one for each client. The VMware virtual machines are represented as Data Protector clients called **VADP clients**. The new object name format for **VADP clients** is as follows: <hostname>:/<vCenter>/<path>/<vmname> [<UUID>] Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.	session ID	message level	all formats	session_hosts
Single Session	Displays all relevant information about a single Data Protector backup, object copy, or object consolidation session.	session ID	message level	all formats	single_session

Reports Send Methods

You can choose among the following send methods when configuring or starting a report or a report group.

Broadcast message send method

The broadcast message send method lets you send a broadcast message with the output of the report to specified systems.

Broadcast messages can be sent (to Windows systems only) by specifying the system to which the broadcast message should be sent. Broadcast messages are limited to 1000 characters, so the short format is preferred.

Email send method

You can send an email with the output of the report to specified recipients. Make sure you provide the full email address of the recipient.

> **Important** Due to security features of Microsoft Outlook, using the email send method may cause the CRS service to stop responding. Alternatively, use email (SMTP) as the email send method.

- **On Windows systems:**

  To send an email report from a Windows system, you need to have a mail profile. You can either use an existing mail profile or create a new one, named OmniBack.

  To use an existing mail profile, add the following line to the Data Protectoromnirc file:

  ```
  OB2_MAPIPROFILE=existing_MAPI_profile_name
  ```

  The display of HTML email report on Windows depends on the email client settings. Many email clients display the report as plain ASCII text. To ensure the report displays correctly as HTML, open it in a Web browser.

- **On Unix systems:**

  The email subsystem has to be configured and running on a Unix system; no additional configuration is needed.

  Due to the operating system limitations, international characters in localized email reports can be displayed incorrectly on Unix systems, if they are passed between systems using a different locale.

Email (SMTP) send method

You can send an email with the output of the report to specified recipients using the SMTP protocol. Make sure you provide the full email address of the recipient. This is the recommended email send method.

By default, Data Protector sets the address of the SMTP server used for sending the reports to the Cell Manager IP address. To change the address, edit the SMTPServer global option. The SMTP server must be accessible from the Cell Manager system, but does not need to be part of the Data Protector cell.

- **On Windows systems**

  For information about configuring your existing Microsoft Exchange Server to support SMTP, see *Microsoft Exchange Server documentation*.

  The display of HTML email report on Windows depends on the email client settings. Many email clients display the report as plain ASCII text. To ensure the report displays correctly, open it in a Web browser.

- **On Unix systems**

  Due to the operating system limitations, international characters in localized email reports may display incorrectly on Unix if they are passed between systems using a different locale.

External send method

The external script send method allows you to process the output of the report in your own script. The script receives the output as standard input (STDIN). The recommended format for script processing is the tab format.

The script, which is located on the Cell Manager system, must reside in the /opt/omni/lbin (Linux systems) or Data_Protector_home\bin (Windows systems) directory. Provide only the name of the script, not the entire path.

Note that only .bat, .exe, and .cmd are supported extensions for external scripts on Windows systems. To run a script with an unsupported extension (for example, .vbs), create a batch file that starts the script. Then configure Data Protector to run the batch file as an external script, which then starts the script with the unsupported extension.

You can also use this delivery method to perform a scheduled eject of the specified media.

Log to file send method

Use this method to post a file with the output of the report to the Cell Manager system.

You have to specify the name of the file to which you want to post the report. The file will be overwritten if it exists.

SNMP send method

The SNMP trap send method allows you to send a report as an SNMP trap. The SNMP trap can be further processed by applications that use SNMP traps.

> **Note** The SNMP send method is appropriate only for reports that don't exceed the maximum size of the configured SNMP trap. Otherwise, the report gets fragmented.

- **On Windows systems**

  SNMP traps are sent to the systems configured in the Windows SNMP traps configuration. You need to configure Windows SNMP traps to use the SNMP send method on the Cell Manager.

- **On Linux systems**

  On a Linux Cell Manager, SNMP traps are sent to the systems configured in the report.

Configure and run report groups and reports

Configure report groups using the Data Protector GUI

You can run Data Protector traditional reports individually (interactively) or you can group them into report groups and then start the report group. You can add individual reports to an already configured report group. Mount Request Report and Device Error Report can be used only in a report group and aren't available as interactive reports.

Using the Data Protector GUI, a report group allows you to:

- Start all the reports at once (interactively).
- Schedule the group to start the reports at a specified time.
- Start the group when triggered by a notification.

To display the input parameters (selections) in the output of a report, select the **Show selection criteria in report** option in the Report wizard. This option is not available for reports that have no required or optional input parameters (selections). The output of the report displays only required parameters and optional parameters with changed default values.

Following are the prerequisites:

- You either have to be added in the `admin` user group or granted the Reporting and notifications user rights.
- The Data Protector user under whose account the `CRS` service is running shouldn't be removed. This user is configured by default at installation time. On a Windows Cell Manager, this is the user account used for the installation. On a Linux Cell Manager, this is the `root` user of the Cell Manager.

Configuration phases

- Configure a report group
- Add a report to a report group

Configure a report group

Complete the following steps to configure a report group:

1. In the Context List, select **Reporting**.
2. Right-click **Reports**, and then click **Add Report Group** to open the wizard.
3. Name the report group and then click **Next**.
4. Click **Finish** to add the report group and exit this wizard. You can now optionally perform the following tasks:
   - Schedule the report group: Right-click the report group, and click **Edit Schedule**. The Scheduler page opens.
   - Add reports to the report group: Right-click the report group, and click **Add Report**. Follow the Add Report wizard to add reports.

> **Tip** To trigger a report group by a notification, configure a report group and then configure the notification to use the Use Report Group send method.

Add a report to a report group

Complete the following steps:

1. In the Reporting context, expand **Reports**, right-click a report group, and click **Add Report** to open the Add Report

wizard. If configuring a report immediately after the report group configuration procedure, skip this step.

2. In the Results Area, select a type of report from the list.
3. In the Name text box, enter the name of the report and select a report in the Type drop-down list. Click **Next**.
4. The wizard options are available according to the selected report. For example, all wizard options available for the IDB Size report aren't available for the List of Media report. Click **Next** as many times as needed to reach the last page of the wizard.
5. In the Send method drop-down list, select a sending method for the report, then enter the recipient of the report in the Email address text box. In the Format drop-down list, select the format of the report. Click **Add** to add the recipient to the group of configured recipients.

   Repeat this step for any number of recipients.
6. Click **Finish** to add the report to the report group and exit the wizard.

Repeat this procedure for all the reports you want to add to a report group.

Run report groups using the Data Protector GUI

You can run all the reports in a report group together.

The following prerequisites apply:

- You have to be either added in the Admin user group or granted the Reporting and notifications user rights.
- The Data Protector user under whose account the `CRS` service is running shouldn't be removed. This user is configured by default at installation time. On a Windows Cell Manager, this is the user account used for the installation. On a Linux Cell Manager, this is the `root` user of the Cell Manager.

Complete the following steps:

1. In the Context List, select **Reporting**.
2. In the Scoping Pane, browse for and right-click the report group you want to start and then click **Start**.
3. Click **Yes** to confirm.

Run individual reports using the Data Protector GUI

You can run individual reports interactively or you can group them into report groups and then run all the reports in the report group together.

Mount Request Report and Device Error Report can only be used in a report group and aren't available as interactive reports.

The following prerequisites apply:

- You have to be in the Admin user group or have the Reporting and notifications user rights.
- The Data Protector user under whose account the `CRS` service is running shouldn't be removed. This user is configured by default at installation time. On a Windows Cell Manager, this is the user account used for the installation. On a Linux Cell Manager, this is the `root` user of the Cell Manager.

Complete the following steps:

1. In the Context List, select **Reporting**.
2. Click the **Tasks** tab below the Scoping Pane.
3. In the Scoping Pane, browse for the desired type of report and select a report to open the wizard.
4. The wizard options are available according to the selected report. For example, all wizard options available for the IDB Size report aren't available for the List of Media report. Click **Next** as many times as needed to reach the last page of the wizard.
5. At the end of the Report wizard, click **Finish** to display the output of the report.

Run reports and report groups using the Data Protector CLI

You can generate Data Protector reports using the command line interface (CLI). The CLI allows you to include Data Protector reports in other scripts you are using. You can generate individual reports, start report groups, define report formats and send methods.

The following prerequisites apply:

- You have to be either added in the Admin user group or granted the Reporting and notifications user rights.
- The Data Protector user under whose account the `CRS` service is running shouldn't be removed. This user is configured by default at installation time. On a Windows Cell Manager, this is the user account used for the installation. On a Linux Cell Manager, this is the `root` user of the Cell Manager.

Use the `omnirpt` command to generate reports.

Configure SNMP Traps

SNMP traps are sent to the systems configured in the `OVdests` configuration file. If correctly configured, you can see the status in the `omnisv -status` output.

omnisv -status ProcName Status [PID] ================================ crs : Active [2044] mmd : Active [2256] kms : Active [2368] hpdp-idb : Active [1684] hpdp-idb-cp : Active [1756] hpdp-as : Active [1660] omnitrig : Active omniinet : Active [2084] Sending of traps enabled for the following hosts: **monitoring1.domain.tld monitoring2.domain.tld** ================================ Status: All Cell Server processes/services up and running.

The OVdests configuration file may have one of more entries for monitoring systems to be notified. A white space is separating trap-dest: monitoring1.domain.tld and one entry per line.

```
trap-dest: monitoring1.domain.tld trap-dest: monitoring2.domain.tld
```

Modifications to the OVfilter configuration file allow to filter (not send) SNMP traps with a particular severity. If all available severities are included sending of SNMP traps based on session messages is completely disabled while sending SNMP reports is still available.

```
normal warning minor major critical
```

Windows SNMP Configuration

A Windows Cell Manager is using the Windows SNMP service to sent traps to the monitoring systems. Complete the following steps to finish the configuration:

1. Install the Windows SNMP services. For Windows Server 2012 and later:
    1. In the Start menu, right-click **Computer** and select **Manage**.
    2. Select **Features** and click **Add Features**.
    3. In the Features tree, select **SNMP Services** and then **SNMP Service**.
    4. Click **Next** and then **Install**.
2. Open **Control Panel**, **Administrative Tools**, **Services**.
3. Right-click **SNMP Service** and select **Properties**.
    1. Select the **Traps** tab. Enter public (value is mandatory) in the Community name text box and the FQDN of the monitoring system and the Cell Manager in the Trap Destinations text box.
    2. Select the **Security** tab. Under Accepted community names, select the community public (value is mandatory), click **Edit** and set Community rights to READ CREATE or READ WRITE. If you select the **Accept SNMP packets from these hosts** and make sure to specify the FQDN of the monitoring system and the Cell Manager.
    3. Confirm your changes.
4. From the %DP_HOME_DIR%\bin directory, run the omnisnmp.exe command. It creates an appropriate Data Protector entry in the System registry under CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents.
5. Restart the Windows SNMP service and verify the results.

This configuration sends SNMP traps based on the OVfilter. If the OVfilter is empty (nothing filtered) running a backup session sends a SNMP trap for each processed session message.

Configuration are logged in the debug.log on the Cell Manager.

```
Failed to send SNMP trap. Check SNMP service configuration.
```

SNMP Reports and Notifications

After configuring SNMP, you can configure reports and notifications using the SNMP Send method from the Reporting context in the GUI. If the reports and notifications are configured, a Windows Cell Manager sends the SNMP traps to the already configured trap destinations. Linux Cell Managers send SNMP traps to the systems configured in the notification or report.

Configure Secure SMTP

You can configure Data Protector to use secure SMTP protocol for reports and notifications that are configured with **Email (SMTP)** send method. When you configure Secure SMTP, it overrides (disables) any existing SMTP related configuration.

> **Note:** Support for Secure SMTP is available only in 64-bit Windows and 64-bit Linux operating systems.

Add configuration

1. To add secure SMTP configuration, run the following command:

    omnirpt -smtp_config -add -server_name <exchange_server_host_name> -user_name <exchange_user> -email_id <sender_email_address> [-server_port <port_number>]

    where:

    - exchange_server_host_name: Represents the host name of Microsoft Exchange Server. If SSL certificate verification is not disabled, the SSL certificate of the Exchange Server must contain this name in the CN or SAN of the certificate.
    - exchange_user: Represents the user account name corresponding to the email address configured in the exchange

server.
- sender_email_address: Represents the email address from which the DP reports and notifications triggers.
- port_number: Represents the secure SMTP port configured in the Exchange Server. Use this parameter only to specify a port number other than 587 (default port number).

For example: omnirpt -smtp_config -add -server_name system1234.mylab.net -user_name testuser -email_id testuser@labexchange.net -server_port 465

2. Enter the password for the specified user account and confirm the same when prompted.
3. Either configure or disable the SSL certificate verification of the SMTP server as desired:
   - **To verify the certificate of the SMTP server:**
     Copy either the CA certificate used to sign the SMTP server certificate or the self-signed certificate of SMTP server to the Cell Manager host. You must copy the certificate (in **PEM** format) in the following location:
     - **Windows:** *<DP_DATA_PATH>*|Config\client\certificates\smtp_cacert.pem
       Where *DP_DATA_PATH* by default refers to C:\ProgramData\OmniBack\. You can customize this path during the installation process.
     - **Linux:** /etc/opt/omni/client/certificates/smtp_cacert.pem
   - **To disable the SSL certificate verification of the SMTP server:**
     Set the OB2_DISABLE_SMTP_CACERT omnirc variable to 1.

Check configuration

To check the details of the existing secure SMTP configuration, run the following command:
omnirpt -smtp_config -list

Test connection

To test the connectivity with the configured SMTP server, run the following command:
omnirpt -smtp_config -test

A successful test confirms that the Data Protector can use the credentials to send reports/notifications. However, a failed test indicates that either the credentials or certificate configuration is incorrect.

Remove configuration

To remove the existing secure SMTP configuration, run the following command:
omnirpt -smtp_config -remove

SMTP Reports and Notifications

After configuring Secure SMTP, you can configure reports and notifications using the **Email (SMTP)** send method from the Reporting context in the GUI. See Notifications.

Use Reporting Server

Reporting Server offers integrated reports that help you in managing and planning your backup environment. You can access the integrated reports using the **Home context** > **Reports** option on the Data Protector GUI. The Data Protector integrated reports are customizable and provide information on the status of the last backup, object copy, object consolidation, or object verification, consumption of media in media pools, status of devices, etc. You can download these integrated reports in PDF, PNG, CSV, or JSON format.

Data Protector displays integrated reports as bar graph, pie chart, or in tabular format. The favorite icon in the Dashboard helps you select your favorite reports to be displayed in the Dashboard.

Integrated report types

Depending on the information about your backup environment that you want to retrieve, you can generate various types of integrated reports:

- Configuration reports
- Sessions in timeframe reports
- Pools and media reports
- Compliance reports
- Advanced reports
- Custom reports

Send reports

Reporting Server does not support scheduling reports. To send reports to the configured recipients, follow these steps:

1. Open the **Home** context and click **Reports**.
2. Select a report from the left pane, specify the required details and click **Generate**.
3. Click **Email** at the top right to send the report to the configured Email recipients.

Related Topic

For troubleshooting information about Reporting Server, see Troubleshoot Reporting Server.

Configuration reports

Configuration reports provide information on the configuration of the Cell Manager, on devices not used for backup, on systems not configured for backup, and so on. The following reports are categorized as Configuration reports:

Access Configuration reports

To access the Configuration reports, navigate to **Home Context** > **Reports** > **Configuration Reports**.

Transfer rate per backup specification report

The Transfer rate per backup specification report represents the average transfer rate or average speed for the backup specification(s) matching the specified search criteria on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Transfer Rate Per Backup Specification**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Specification
   - Speed Unit
3. Click **Generate** after changing the filters.
   - The Transfer rate per backup specification report displays as bar chart.
   - To generate the report in tabular format, click the table icon on the right.

The table shows details of backup specification, hosts backed up, target device and speed for the backup specifications. You can customize the display of the table by using the configurable parameters.

Average time per backup specification report

The Average time per backup specification report lists the average duration of all backup sessions run over the specified time frame for each backup specification on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Average Time Per Backup Specification**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Timeframe
3. Click **Generate** after changing the filters.
   - The Average time per backup specification report displays as a bar chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists details about the specification name, average duration in hours for all backup sessions involving the particular specification and the total amount of data backed up during those backup sessions expressed in GB. You can customize the display of the table by using the configurable parameters.

Media utilization report

The Media utilization report for a graphical view of average utilization rate (%) for the selected/all device(s) for the specified timeframe on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Media Utilization**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Media
   - Timeframe – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Device utilization report displays as a line chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists details like Media Name, Device Type, Date of device creation, Average Utilization rate (%) and Amount backed up (GB) for the selected/all device(s) for the specified timeframe on a particular/all cell manager(s). You can customize the display of the table by using the configurable parameters.

Number of backup versions report

The Number of backup versions report lists the count of backups performed by backup type (full, incremental, differential, etc.) belonging to selected backup specification for a particular/all cell manager(s). The report segregates the details in two separate sections for virtual and physical environments.

1. To generate the report, select **Configuration Reports > Number of Backup Versions**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Specification
   - Types of backups
3. Click **Generate** after changing the filters.
   - The Number of backup versions report displays as bar chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists the cell manager, the backup specifications belonging to that cell manager, the various types of backups that were performed using those backup specifications and the count of backup versions corresponding to each backup type. You can customize the display of the table by using the configurable parameters.

Transfer size report

The Transfer size report displays the average transfer size for the selected/all application type(s) and timeframe matching the specified search criteria on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Transfer size**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Time range – Number of Days/Weeks/Months/Years
   - Unit (of transfer size with options as KB/MB/GB/TB)
   - Object Type
3. Click **Generate** after changing the filters.
   - The Transfer size report displays as line chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists the Host name, Object name, Object size, amount of data written, application Object type and last used date for the selected application type(s) and timeframe matching the specified search criteria on a particular/all cell manager(s). You can customize the display of the table by using the configurable parameters.

Session status report

The Session status report displays the graphical view of sessions grouped by session type and session status matching the specified search criteria on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Session Status**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Session type
   - Session status
3. Click **Generate** after changing the filters.
   - The Session status report displays as donut chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists the Session ID, Session type, Mode, Session status, Start time and duration for all session type(s) and session status(s) matching the specified search criteria on a particular/all cell manager(s). You can customize the display of the table by using the configurable parameters.

Look up schedule report

The Look up schedule report lists all the specifications that are scheduled to start within the specified timeframe in search criteria for particular cell/all cell manager(s).

1. To generate the report, select **Configuration Reports > Look Up Schedule**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Timeframe – Number of Days/Weeks/Months/Year
   - Specification type
3. Click **Generate** after changing the filters.

Schedule overview report

The Schedule overview report lists the backups scheduled for specifications matching the specified search criteria for a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Schedule Overview**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Specification type
3. Click **Generate** after changing the filters.

Cell information report

The Cell information report identifies the number of clients available in the selected DP cell(s), backup specifications set for the cell(s), and other related details.

To generate the report, select **Configuration Reports > Cell Information**.

Object copy transfer rate report

The Object copy transfer report displays the information on average speed of data transfer for specific or across all object type(s) involved in copy sessions run for the specified timeframe on a particular/all cell manager(s).

1. To generate the report, select **Configuration Reports > Object Copy Transfer Rate**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Object type
   - Transferred in last – Number of Days/Weeks/Months/Years
   - Speed unit (MBps/GBps)
3. Click **Generate** after changing the filters.
   - The Object copy transfer rate report displays as line chart.
   - To generate the report in tabular format, click the table icon on the right.

The table shows details like Client name, Object type, Speed, Source Device name, Source backed up, Target device, Data written, Last used date and time for each object type(s) matching specified search criteria that has been involved in copy sessions over the specified timeframe on a particular/all cell manager(s). You can customize the display of the table by using the configurable parameters.

List of specifications report

The List of specifications report displays a card view of total count of specifications created till date for every specification type on a particular/all cell manager(s). It also represents how the total count of specifications per specification type is distributed across session statuses (Success/Failed/Warning).

1. To generate the report, select **Configuration Reports > List of specifications**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - App type (this filter is only for secondary view)
   - Session type
     - In case of primary view, this filter works by clicking on card.
     - In case of secondary view, this filter is present at the top.
   - Status
     - In case of primary view, this filter works by clicking on card where user is taken to the secondary view.
     - In case of secondary view, this filter is present at the top.
3. Click **Generate** after changing the filters.
   - The List of specifications report displays as card view.
   - To generate the report in tabular format, click the table icon on the right.

For user specified search criteria, Application / Object type(s), Session type(s), Session status(s) and cell manager(s), the table shows additional details like Specification Name, Client Name, Last Backup Time, Device, Amount Backed Up, Object Type, Specification Type, and Status. You can customize the display of the table by using the configurable parameters.

Data under protection report

The Data under protection report lists the total protected and unprotected data across all sessions till date for a particular/all cell manager(s). It also shows graphical view of how this total protected/unprotected data across all sessions till date is distributed among various application types.

1. To generate the report, select **Configuration Reports > Data under protection**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Object type
     - In case of primary view, this filter works when clicked on protected/unprotected data donuts and shows filtered data in Secondary view.
     - In case of secondary view, this filter is displayed at the top.
3. Click **Generate** after changing the filters.
   - The Data under protection report displays as multiple donut charts.
   - To generate the report in tabular format, click the table icon on the right.

The table lists details of exact amount of protected and unprotected data per object type(s) on the particular/all cell manager(s) matching the specified search criteria.

IDB Details report

The IDB details report provides information about IDB on when you need to perform some of the IDB maintenance tasks, such as extending the IDB size and reducing the IDB growth.

1. To generate the report, select **Configuration Reports** > **IDB Details**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Category
3. Click **Generate** after changing the filters. The IDB details report displays in tabular format.

Client Backup report

The Client backup report provides detailed information about mount point backup configuration and average size backed up. The report helps in identifying the mount points that do not have any backup specification configured.

1. To generate the report, select **Configuration Reports** > **Client Backup**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Client
   - Configuration Type
   - Unit (of average full back size of mount point in KB/MB/GB/TB)
3. Click Generate after changing the filters. The Client backup report displays in tabular format.

The table shows details like Client Name, Mount Point, Configuration Type, and Average Size for all the mount points of clients. If backup specifications are configured for mount point, Specfication Name and Trees are also shown for each client(s) matching specified search criteria on a particular/all Cell Manager(s). You can customize the display of the table by using the configurable parameters.

Clients not configured report

The Clients not configured report lists the clients in the selected domains that are not part of the current cell.

Complete the following steps to generate the Clients not configured report:

1. To generate the report, select **Configuration Reports > Clients Not Configured**.
2. Click **Generate**.

The Clients not configured report displays in cards format. You can customize the display of the cards by using the configurable parameters.

Licensing report

Licensing report lists the number of used licenses, available number of licenses, and if the system is in compliance in terms of over or under capacity based on the installed license type for a particular/all Cell Manager(s).

Complete the following steps to generate the Licensing report:

1. To generate the report, select **Configuration Reports > Licensing**.
2. (Optional) Select the **Cell Manager**.
3. Click **Generate**.

The Licensing report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Backup specification errors timeline report

The Backup specification errors timeline report displays a graphical view of the aggregated count of errors and warnings for the specified timeframe for a particular/all Cell Manager(s).

Complete the following steps to generate the Specification errors timeline report:

1. To generate the report, select **Configuration Reports > Backup specification errors timeline**.
2. (Optional) Select the **Cell Manager**, **Backup Specification** and the timeframe.
3. Click **Generate**.
    - Backup specification errors timeline report displays as stack line chart
    - To generate the report in tabular format, click the table icon on the right.

You can customize the display of the table by using the configurable parameters.

Configured devices not used report

The Configured devices not used report lists the destination devices that are not used for backup, object copy, or object consolidation for the specified time for a particular/all Cell Manager(s).

Complete the following steps to generate the Configured devices not used report:

1. To generate the report, Select **Configuration Reports > Configured Devices Not Used**.
2. (Optional) Select the **Cell Manager** and the timeframe.
3. Click **Generate**.

The Configured devices not used report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Session specific information report

The Session specific information report lists the session type, session specification name, its group, owner, pre and post execution commands for the selected session type for a particular/all Cell Manager(s).

Complete the following steps to generate the Specification errors timeline report:

1. To generate the report, select **Configuration Reports > Session Specific Information**.
2. (Optional) Select the **Cell Manager** and the **Session Type**.
3. Click **Generate**.

The Session specific information report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Sessions in timeframe reports

This feature is available in the Premium Edition

Sessions in timeframe reports provide session related statistics for specified timeframe like clients, destination media, utilization, session status, session errors etc. The following reports are categorized as Session in timeframe reports:

- Client statistics report
- Device flow report
- List of sessions report
- Media usage by sessions
- Object copies report
- Session flows report
- Session statistics report
- Report on used media
- Dedupe rate report
- Objects latest backup report
- Objects without backup report
- Average backup object size report
- Session specific schedule report
- Session errors report

Access Session and timeframe reports

To access the Session and timeframe reports, navigate to **Home Context** > **Reports** > **Session and Timeframe Reports**.

Session flows report

The Session flows report displays a graphical view of the duration of each session (successful, running, warning, and failed) for the specified timeframe on a particular/all cell manager(s).

1. To generate the report, select **Sessions in timeframe reports > Session Flows**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Specification
   - Timeframe – Number of Days/Weeks/Months/Years
   - Status
3. Click **Generate** after changing the filters.
   - The Session flow report displays as bar chart.
     The bar chart represents the distribution of session types over the timeframe specified in search criteria for a particular/all cell manager(s). The aggregated session type for the selected cell manager(s) is displayed on the top of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right.
     In the tabular format, this report also shows additional details on backup object, type, duration and end time of each session. You can customize the display of the table by using the configurable parameters.

Client statistics report

The Client statistics report displays a graphical view of clients list and their backup status statistics for the specified timeframe. Only the clients that match the search criteria are listed.

1. To generate the report, select **Sessions in Timeframe Reports > Client Statistics**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Client
   - Timeframe
3. Click **Generate** after changing the filters.
   - The Client statistics report displays as bar chart.
     The bars represent the amount of data written on each client within the timeframe matching the search criteria on a particular/all cell manager(s).
   - To generate the report in tabular format, click the table icon on the right.
     In the tabular format, this report also lists each client with count of files, object, and statuses within the timeframe matching the search criteria on a particular/all cell manager(s). You can customize the display of the table by using the configurable parameters.

List of sessions report

The List of session report lists the total count of sessions with status details for the specified timeframe matching the specified search criteria on a particular/all cell manager(s).

1. To generate the report, select **Sessions in Timeframe Reports > List of Sessions**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Session type
   - Timeframe
   - Status
3. Click **Generate** after changing the filters.
   - The List of sessions report displays as stacked bar chart.
     For the selected cell manager(s) with selected session type, the stacked bars represent the distribution of all session counts per status. The total count of session status aggregated for the selected session type(s) is displayed at the bottom of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right.
     For each session matching the specified search criteria, the table lists details about the session ID, session type, object, object type, and status. You can customize the display of the table by using the configurable parameters. The table view has multiple rows for single session type as there are multiple objects involved for a single session.

Session statistics report

The Session statistics report displays a graphical view of following for the specified timeframe in the search criteria on a particular/all cell manager(s):

- Consolidated count of media and objects
- Consolidated session count details like completed, failed, running, and pending.
- Amount of data written

1. To generate the report, select **Sessions in timeframe reports > Session Statistics**.
2. You can apply the following filters while generating the report:
   - Cell manager name
   - Session status
   - Time frame – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Session statistics report displays as line chart.
     This line chart represents the media and object count with amount of data written along with session statuses like completed, failed, running, and pending for the specified timeframe in search criteria on a cell/all cell manager(s).
   - To generate the report in tabular format, click the table icon on the right.
     For each session on a particular/all cell manager(s) belonging to the specification selected in the search criteria and involved in sessions whose session status matches the specified search criteria for the specified timeframe, the table lists the total count of data written in GB, media, object, and session status like completed, failed, running, and pending. You can customize the display of the table by using the configurable parameters.

Media usage by sessions

The Media used by Sessions report lists the detailed media usage information across all session types within the specified timeframe matching the search criteria for a particular/all cell manager(s). For each session type, this further shows the distribution by session status (success/failed) and media usage details corresponding to the same. Based on the view selected, this report also shows detailed information on media location, sessions, media usage, protection etc. for all media belonging to the specification, session type, status and timeframe specified in the search criteria.

1. To generate the report, select **Sessions in timeframe reports > Media Usage By Sessions**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Time frame
   - Specification (this filter is only for secondary view)
   - Session type (this filter is only for secondary view)
   - Session status (this filter is only for secondary view)
3. Click **Generate** after changing the filters.
   - The Media Used by Sessions displays as card view.
     The first row of cards represents total media usage across all session types for the selected timeframe specified in the search criteria for a particular/all cell manager(s). The second row of cards show the distribution by session status (success/failed) and media usage details corresponding to each session type.
   - To generate the report in tabular format, click the table icon on the right.
     For each medium on a particular/all cell manager(s) belonging to the specification selected in the search criteria and involved in sessions whose session type and status matches the specified search criteria over the timeframe matching the specified search criteria, the table shows detailed information on medium label, location, pool name, media type, protection, amount of total media available and media used, last accessed time, specification name, session ID, session type, session subtype and session status. You can customize the display of the table by using the configurable parameters.

Device flow report

The Device flow report displays a graphical view of the utilization of each device belonging to the session type(s) specified in the search criteria over the timeframe selected in search criteria for a particular/all cell manager(s).

1. To generate the report, select **Sessions in timeframe reports > Device Flow**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Time frame – Number of Days/Weeks/Months/Years
   - Session type
3. Click **Generate** after changing the filters.
   - The Device flow report displays as stacked bar chart.
     The stacked bars represent the distribution of total utilization of each device across various session types over the timeframe specified in search criteria for a particular/all cell manager(s). The aggregated utilization per session type across all devices of the selected cell manager(s) is displayed on the top of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right.
     In the tabular format, this report also shows additional details on utilization for each device matching the specified search criteria. For each device involved in sessions of the type matching the specified search criteria, the table lists the device name, session type, session date and time and the corresponding device utilization during that session. You can customize the display of the table by using the configurable parameters.

Object copies report

The Object copies report displays a graphical view of valid copies of object version for the specified timeframe on a particular/all cell manager(s). The number of copies includes the original object version. This report always displays the number of valid copies as one even when no object copies are created. This is because the backup of the object is treated as valid copy.

1. To generate the report, select **Sessions in timeframe reports > Object Copies**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Object type
   - Time frame – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Object copies report displays as bar chart.
     The bar chart represents the count of valid copies of object type for the timeframe specified in search criteria on a particular/all cell manager(s).
   - To generate the report in tabular format, click the table icon on the right.
     In the tabular format, this report also lists additional details of object version and object copy time. You can customize the display of the table by using the configurable parameters.

Report on used media

The Report on used media displays a graphical view on media utilization based on media type and timeframe matching the specified search criteria for a particular/all cell manager(s).

1. To generate the report, select **Sessions in Timeframe Reports > Report On Used Media**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Session type
   - Unit (KB/MB/GB/TB)
   - Time frame – Number of Days/Weeks/Months/Years
   - Media type
3. Click **Generate** after changing the filters.
   - The Report on used media report displays as line chart.
     This timeline chart represents the media utilization per device for the specified media type and involved in sessions of the specified session type over the timeframe specified in search criteria for a particular/all cell manager(s). The unit of media utilization (Y-axis) is customizable as per search criteria chosen by user.
   - To generate the report in tabular format, click the table icon on the right.
     For each medium on a particular/all cell manager(s) of the specified media type and involved in sessions of the specified session type over the timeframe specified in search criteria, the table shows detailed information on medium label, pool name, protection, amount of total media available and media used, last accessed time, media type and session type. You can customize the display of the table by using the configurable parameters.

Dedupe rate report

Dedupe rate report displays a graphical view of the specification(s) dedupe ratio for the selected period for a particular/all Cell Manager(s):

Complete the following steps to generate the Dedupe rate report:

1. To generate the report, select **Sessions in Timeframe Reports > Dedupe Rate**.
2. (Optional) Select the **Cell Manager**, **Specification**, and the timeframe.

3. Click **Generate**.
   - The Dedupe rate report displays as a line chart.
   - To generate the report in tabular format, click the table icon on the right.
     The table lists details like specification name, dedupe size, ratio, and target. You can customize the display of the table by using the configurable parameters.

Objects latest backup report

The Object latest backup report lists all objects in IDB. For each object, it displays the last full and the last incremental backup time, the last full and the last incremental object copy time, and the last object consolidation time for the selected period for a particular/all Cell Manager(s).

Complete the following steps to generate the Objects latest backup report:

1. To generate the report, select **Sessions in Timeframe Reports > Objects Latest Backup**.
2. (Optional) Select the **Cell Manager** and the timeframe.
3. Click **Generate**.
   - The Objects latest backup report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Objects without backup report

The Objects without backup report lists all objects that are part of a backup specification and do not have a valid backup for the selected period for a particular/all Cell Manager(s). A successfully completed backup or backup where the protection has not yet expired is considered a valid backup.

This Objects without backup report is not available for backup specifications for integrations.

Complete the following steps to generate the Objects without backup report:

1. To generate the report, Select **Sessions in Timeframe Reports > Objects Without Backup**.
2. (Optional) Select the **Cell Manager**, **Specification**, and the timeframe.
3. Click **Generate**.
   - The Objects without backup report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Average backup object size report

The Average backup objects size report displays the average size of an object in the specified backup specification. It displays the size of the full and the incremental backup of the object for the selected period for a particular/all Cell Manager(s).

Complete the following steps to generate the Average backup objects size report:

1. To generate the report, select **Sessions in Timeframe Reports > Average Backup Object Size**.
2. (Optional) Select the **Cell Manager**, **Specification**, **Unit**, and the time period.
3. Click **Generate**.
   - The Average backup objects size report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Session specific schedule report

The Session specific schedule report lists the next start time for each specified backup, object copy, object consolidation, and object verification specification up to one year in advance for a particular/all Cell Manager(s).

Complete the following steps to generate the Session specific schedule report:

1. To generate the report, select **Sessions in Timeframe Reports > Session Specific Schedule**.
2. (Optional) Select the **Cell Manager** and **Session Type**.
3. Click **Generate**.
   - The Session specific schedule report displays in tabular format. You can customize the display of the table by using the configurable parameters.

Session errors report

The Session errors report lists all the errors and their resolutions, if available, for each session for the specified timeframe on a particular/all Cell Manager(s).

Complete the following steps to generate the Session errors report:

1. To generate the report, select **Advanced Reports > Session Errors**.
2. (Optional) Select the **Cell Manager**, **Client Type**, and timeframe.
3. Click **Generate**.
   - The Session errors report displays in tabular format. To see the error message and its resolution, expand the session row by clicking the arrow icon on the left. You can customize the display of the table by using the configurable parameters.

Pools and media reports

Pools and Media reports provide information on media pools and used media. The following reports are categorized as pools and media reports:

Access Pools and media reports

To access the Pools and media reports, navigate to **Home Context** > **Reports** > **Pools and Media Reports**.

List of pools report

The List of pools report displays a graphical view of the following for the specified search criteria (media type) on a particular/all Cell Manager(s):

- Total number of media grouped by media pool
- Distribution of total media per media pool by media condition
- Distribution of total media per media pool by media usage

1. To generate the report, select **Pools and Media Reports > List of pools**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Media type
3. Click **Generate** after changing the filters.
   - The List of pools report displays as bar chart.
     The bars represent the aggregated count of media sliced and diced by media condition (good, fair, poor media) and media usage (appendable, full, and free media) for each pool belonging to the selected media type for a particular/all cell manager(s). Click the right arrow icon to see further details.
     The total count of media (by media condition and usage) aggregated over all pools for the selected media type and cell manager is displayed at the bottom of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right.
     For each pool matching the specified search criteria, the table lists the pool name, description, media type, the count of total media, number of full and appendable media containing protected data, number of free media containing no protected data, number of poor, fair and good media. You can customize the display of the table by using the configurable parameters.

Extended list of media report

The Extended list of media report lists all media matching the specified search criteria with detailed statistics on media usage for a particular/all Cell Manager(s).

1. To generate the report, select **Pools and Media Reports > Extended List of Media**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Media protection
   - Media condition
   - Session specification
   - Last accessed time
3. Click **Generate** after changing the filters.
   - The Extended list of media report displays as stacked bar chart.
     For the selected Cell Manager(s), selected session specification and media condition, the stacked bars represent the distribution of media by usage (used and unused space) for each media type belonging to that session specification. This trend can be seen based on the range of media protection and last accessed timeframe selected by the user.
     The total used media and total unused media aggregated over all media types belonging to selected session specification and matching the other search criteria is displayed at the bottom of the chart area of the report.

1.
   - To generate the report in tabular format, click the table icon on the right.

For each medium matching the specified search criteria, the table lists details about the medium ID, medium label, media location, media condition, media protection, used and total space, the time when the medium was last accessed, the media pool and media type, session specifications that have used the medium for backup, object copy, or object consolidation, as well as the session type and subtype. You can customize the display of the table by using the configurable parameters.

Media statistics report

The Media statistics report displays a graphical view of the following for the specified pool(s) matching search criteria on a particular/all cell manager(s):

- Status data for total media grouped as good media, fair media, and poor media
- Space data for total media grouped as used space and free space
- Protection data for total media grouped as protected media and unprotected media

1. To generate the report, select **Pools and Media Reports > Media Statistics**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Pool Name
   - Timeframe
3. Click **Generate** after changing the filters.
   - The Media statistics report displays as donut charts.
     The donuts represent the distribution of pool media condition (good/fair/poor media), distribution of space data (used/free space), distribution of protection data (protected/unprotected), for selected media pool(s) within in timeframe matching the search criteria on a particular/all cell manager(s).
   - To generate the report in tabular format, click the table icon on the right.
     The table lists all pool media matching the specified search criteria/filters. For each pool medium, it provides information about the number of media, number of protected, good, fair, and poor media, total, used, and free space on media. You can customize the display of the table by using the configurable parameters.

Media list report

The Media List report displays a graphical view on distribution by media condition (good/fair/poor media) for a selected media type or even a rolled-up distribution by media condition across all media types in a particular/all Cell Manager(s).

1. To generate the report, select **Pools and Media Reports > Media List Report**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Media type
   - Media condition
3. Click **Generate** after changing the filters.
   - The Media List report displays as doughnut chart.
     The charts show the distribution of media condition (good/fair/poor media) for a selected media type or even a rolled-up distribution of media condition across all media types for a particular/all cell manager(s).
   - To generate the report in tabular format, click the table icon on the right.
     The table lists all media matching the specified search criteria/filters. For each medium, it provides information about the medium ID, medium label, media location, media condition, media protection, used and total space, the time when the medium was last accessed, the media pool and media type. You can customize the display of the table by using the configurable parameters.

Media expiration summary report

The Media expiration summary report displays a graphical view on the total number of devices getting protection expired within the specified media expiration timeframe in a particular/all cell manager(s).

1. To generate the report, select **Pools and Media Reports> Media Expiration Summary**.
2. You can apply the following filters while generating the report:
   - Cell manager
   - Media expiring in – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Media Expiration Summary report displays as bar chart.
     The bars specify the total number of devices getting expired within the specified media expiration period for a particular/all cell manager(s). The bars are grouped on a daily/weekly/monthly/yearly basis , based on the unit of media expiration time selected by user.
   - To generate the report in tabular format, click the table icon on the right.
     Lists all media matching the specified search criteria/filters. For each medium, it provides information about the medium ID, medium label, media location, media pool, media type, and its expiration date. You can customize the display of the table by using the configurable parameters.

Compliance reports

The compliance reports help you ensure that all the compliance details are verified properly. The following reports are categorized as compliance reports:

Access Compliance reports

To access the Compliance reports, navigate to **Home Context** > **Reports** > **Compliance Reports**.

Recovery point objective report

The Recovery point objective (RPO) report lists the clients and application types along with their RPO status for a particular/all cell manager(s). The details also include the Specification name and the status of minimum, maximum and average RP and whether the RPO is met, breached or undefined.

To generate the RPO report, complete the following steps:

1. To generate the report, select **Compliance Reports > RPO**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Client
   - Application Type
3. Click **Generate** after changing the filters.
   - The RPO report displays in tabular format listing the RPO related details for each specified Cell Manager.

Recovery time objective report

The Recovery time objective (RTO) report lists the RTO status for a particular/all cell manager(s). The details include the status of minimum, maximum and average RT and whether the RTO is met, breached or undefined. To generate the RTO report, select **Compliance Reports > RTO**. The RTO report displays in tabular format listing the RTO related details for each specified Cell Manager.

Advanced reports

Advanced reports provide additional details that help you to have in-depth analysis of your backup environment. The following reports are categorized as Advanced reports:

Access Advanced reports

To access the Advanced reports, navigate to **Home Context** > **Reports** > **Advanced Reports**.

Advanced list of sessions report

The Advanced list of sessions report specifies detailed information on list of sessions by session types and specification name for the specified timeframe matching the search criteria on particular/Cell Manager(s). To generate the Advanced list of sessions report, complete the following steps:

1. To generate the report, select **Advanced Reports > Advanced List of Sessions**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Specification
   - Timeframe – Number of Days/Weeks/Months/Years
   - Session type
3. Click **Generate** after changing the filters.
   - The Advanced list of session report displays in tabular format. The table lists each session details like object type, mode, start and end time, duration for the specified time frame matching the search criteria for particular/all Cell Manager(s). You can customize the display of the table by using the configurable parameters.

Charge back report

The Charge back report lists the total usage of storage by clients and applications for the time frame specified in the search criteria for a particular/all Cell Manager(s). Complete the following steps to generate the Charge back report:

1. To generate the report, select **Advanced Reports > Charge Back**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Clients
   - Applications
   - Timeframe – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Charge back report displays in tabular format. The table lists each client name, application type, data backed up in GB for the specified time frame matching the search criteria for particular/all Cell Manager(s). You can customize the display of the table by using the configurable parameters.

Most unreliable backup specification report

The Most unreliable backup specification report lists the unreliable backup device details for the timeframe specified in the search criteria for a particular/all Cell Manager(s). Complete the following steps to generate the Most unreliable backup specification report:

1. To generate the report, select **Advanced Reports > Most Unreliable Backup Specification**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Backup Specification
   - Timeframe – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Most unreliable backup specification report displays as bar chart. The bars represent the count of failed sessions for the backup specification(s) for the specified timeframe matching the specified search criteria on a particular/all Cell Manager(s).
   - To generate the report in tabular format, click the table icon on the right. The table shows details of backup specification name, total sessions count, and failure sessions count for the specified timeframe matching the specified search criteria on a particular/all Cell Manager(s). You can customize the display of the table by using the configurable parameters.

Most unreliable client report

The Most unreliable client report lists the unreliable client details for the timeframe specified in the search criteria for a particular/all Cell Manager(s). Perform the following steps to generate the Most unreliable client report:

1. To generate the report, select **Advanced Reports > Most Unreliable Client**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Client
   - Timeframe – Number of Days/Weeks/Months/Years
3. Click **Generate** after changing the filters.
   - The Most unreliable client report displays as bar chart. The bars represent the count of failed sessions for each client for the specified timeframe matching the specified search criteria on a particular/all Cell Manager(s).
   - To generate the report in tabular format, click the table icon on the right. The table shows details of client name, failed sessions count and passed sessions count for the specified timeframe matching the specified search criteria on a particular/all Cell Manager(s). You can customize the display of the table by using the configurable parameters.

Session per time and status report

The Session per time and status report displays a graphical view of the consolidated sessions count based on their session status for the specified timeframe matching the search criteria for particular/all Cell Manager(s). To generate the Session success report, complete the following steps:

1. To generate the report, select **Advanced Reports** > **Session Per Time and Status**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Session Status
   - Timeframe
3. Click **Generate** after changing the filters.
   - The Session per time and status report displays as bar chart. The bars represent the count of sessions per status for the specified timeframe for particular/all Cell Manager(s). The aggregated session count per status is displayed at the bottom of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right. In the tabular format, this report also shows each session status, its count, and timestamp within the specified timeframe. You can customize the display of the table by using the configurable parameters.

Session success report

The Session success report displays a graphical view of percentage of successful sessions for the specified timeframe matching the search criteria for particular/all Cell Manager(s). Complete the following steps to generate the Session success report:

1. To generate the report, select **Advanced Reports** > **Session Success**.
2. You can apply the following filters while generating the report:
   - Cell Manager
   - Session Type
   - Specification
   - Timeframe
3. Click **Generate** after changing the filters.
   - The Session success report displays as bar chart. The bars represent the percentage count of successful sessions for each specification for the specified timeframe for particular/all Cell Manager(s). Click the right arrow icon to see further details.
   - The total percentage of successful sessions aggregated over all specifications is displayed on the top of the chart area of the report.
   - To generate the report in tabular format, click the table icon on the right. In the tabular format, this report also shows additional details on backup object, type, duration and end time of each session. You can customize the display of the table by using the configurable parameters.

Time since last successful backup report

The Time since last successful backup report lists the time of last successful backup of the selected specification(s). To generate the Time since last successful backup report, select **Advanced Reports** > **Time Since Last Successful Backup**. The Time since last successful backup displays as table listing each specification name and its start time.

Dedupe rate prediction report

Dedupe rate prediction report displays a graphical view of specification(s) current and future dedupe ratio for the selected timeframe for a particular/all Cell Manager(s):

Complete the following steps to generate the Dedupe rate prediction report:

1. To generate the report, select **Advanced Reports > Dedupe Rate Prediction**.
2. (Optional) Select the **Cell Manager**, **Specification**, and the timeframe.
3. Click **Generate**.
   - The Dedupe rate prediction report displays as a line chart.
   - To generate the report in tabular format, click the table icon on the right.

The table lists details like specification name, dedupe size, ratio, and target. You can customize the display of the table by using the configurable parameters.

Health assessment report

The Health assessment report displays a graphical view of the following on a particular/all Cell Manager(s):

- Data under protection (total protected and unprotected data across all sessions)
- Rolled-up distribution by media condition (good/fair/poor) across all media types
- Number of objects (with and without backup)
- Total count of sessions with status details

Complete the following steps to generate the Health assessment report:

1. To generate the report, select **Advanced Reports > Health Assessment**.
2. Click **Generate**.
    - The Health assessment report displays in donuts format.

Capacity used report

The Capacity used report displays a graphical view of the actual and predicted size of storage capacity used for the specified timeframe matching the search criteria for a particular/all cell manager(s). Complete the following steps to generate the Capacity used report:

1. To generate the report, select **Advanced Reports > Capacity Used**.
2. You can apply the following filters while generating the report:
    - Cell Manager
    - Units
    - Timeframe
    - Pool Name
3. Click **Generate** after changing the filters.
    - The Capacity used report displays as line chart. The line represents the size of storage capacity used and predicted size in GB.
    - To generate the report in tabular format, click the table icon on the right. In the tabular format, this report also lists the pool name and media creation date along with the utilization details for the specified timeframe. You can customize the display of the table by using the configurable parameters.

Transfer size prediction report

The Transfer size prediction report displays a graphical view of the actual and predicted transfer size of objects for the specified timeframe matching the search criteria for a particular/all cell manager(s). To generate the Session success report, complete the following steps:

1. To generate the report, select **Advanced Reports** > **Transfer Size Prediction**.
2. You can apply the following filters while generating the report:
    - Cell Manager
    - Units
    - Timeframe
    - Mode
3. Click **Generate** after changing the filters.
    - The Transfer size prediction report displays as line chart. The lines represent the size of existing objects in GB and the reduction in size after the transfer completion.
    - To generate the report in tabular format, click the table icon on the right. In the tabular format, this report also lists each transfer mode with object size and session date for the specified timeframe. You can customize the display of the table by using the configurable parameters.

Custom reports

In addition to the predefined reports, you can use the Data Protector GUI to create up to five custom reports for monitoring the backup environment based on your requirements. You can select these custom reports as favorite reports for displaying in the Dashboard. You can also download these reports or send them as predefined reports in email attachments.

Create custom reports

Perform the steps below to create custom reports:

1. Go to **Reports** > **Custom Reports** to select the required criteria for a customized report.
2. Click the "**+**" icon and complete the following:
    1. Report Information:
        1. **Report Name:** Enter a report name.
        2. **Category:** Select the relevant category from the drop-down list.
        3. **Description:** Enter a report description.
        4. Click **Next**.
    2. Data Set:
        1. Select the required data fields relevant to the category selected in the Report Information dialog. Select a minimum of one numeric and one text data set.
        2. Click **Next**.
    3. Layout:
       You can generate Custom reports for graphic view and tabular view.
        - For graphic view (selected by default):
            1. Select the relevant options from the **X-axis** (text fields) and **Y-axis** (numeric fields) drop-down lists to plot the graph.
            2. Select the type of Operation (Sum/Average) from the drop-down list.
        - For tabular view:
            1. Click the tabular icon.
            2. Select the relevant options for the filters (column headers).
3. Click **Finish**. The newly created custom report lists under the selected category in the left pane and you can do the following:
    - To view the newly created custom report, select it from the relevant category in the left pane.
    - To edit the custom report, select it from the Custom Report section, click the edit icon, and then modify the required details.
    - To delete the custom report, select it from the Custom Report section, and click the trash bin icon.

Set up data restore

A restore is a process that recreates the original data from a backup copy to a disk. This process consists of the preparation and actual restore of data and, optionally, some post-restore actions that make that data ready for use.

Depending on the platform, the way you specify these features and available options can vary.

Standard restore procedure

A standard restore procedure consists of several phases.

1. Select the data to restore
2. Select a specific backup version
3. Manage file conflicts
4. Select a device to restore from
5. Find media needed to restore
6. Preview and start a restore
7. Abort a restore

   Other settings are predefined according to the backup process, but can be modified.

To perform a restore you must have the appropriate user rights. These rights are defined according to the user group.

Select the data to restore

You can browse for data to restore in two possible ways: either from the list of the backed up objects or from the list of sessions. The difference is in the scope of directories and files presented for restore:

- **Restore objects** with a list of backed up objects classified by client systems in the cell and by different data types (such as Filesystem, Disk Image, Internal Database, and so on). You can browse all the directories, files and versions, which were backed up and are still available for restore.
- **Restore sessions** with a list of filesystem sessions with all objects backed up in these sessions. You can choose to view only sessions from the last year, last month, or last week. You can browse all objects that were backed up in this session (like any drives from all clients named in the backup specification), and all versions of this restore chain. By default, the entire restore chain of the selected directories or files is restored, but you can also restore data from a single session only.

In order to browse objects and select directories or specific files, the corresponding backups must have been done using a logging level of directory, filenames, or log all.

Select the data from the list of the backed up objects

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, expand the object and then select directories or files that you want to restore.

   By default, when you select a whole directory, only directories and/or files from the last backup session are selected for restore. Directories and files in the same tree structure that have not been backed up in the same backup session are shaded. If you want to restore the data from any other backup session, right-click the selected directory and click **Restore Version**. In the Backup version drop-down list, select the backup version that you want to restore from.

> **Tip** If you repeat the steps above and select data under more than one object (mountpoint or drive), you can perform a parallel restore.

Select the data from the list of the backup sessions

The following limitations apply:

- You cannot perform the restore of an online database integration from a specific backup session.
- You cannot use "Restore Sessions" mode to perform a restore from a copy session.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the **Restore Sessions** to display clients and then objects, backed up on a particular client. Click an object to open the object's property pages.
3. In the **Source** page, select directories and files to be restored.

   By default, the entire restore chain is restored (**Show full chain** is selected). To restore only data from this session, select **Show this session only**.
4. Specify the restore destination and set the restore options.
5. Click **Restore** to start the restore session.

Tip To perform a parallel restore, repeat steps 2 to 4 for additional objects before starting the restore.

Select a specific backup version

After selecting the data that you want to restore, you can select its backup version.

Select the backup version for each file or directory separately

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, Filesystem).
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select the object to restore. By default, the latest backup version is selected for restore.
5. Right-click the object and click **Restore Version**.
6. In the Backup version drop-down list, select the backup version that you want to restore. Click "**...**" if you need more information on the backup versions. The "**...**" button is available if the backup was performed using a logging level that logs attributes.
7. Click **OK**.

After you have selected a version for restore, only the files and directories from this version are shown as available for restore in the Source property page. Other files and directories are grayed and will not be restored.

Select the backup version for several files or directories simultaneously

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select multiple objects to restore. By default, the latest backup version is selected for restore.
5. Click the **Restore Summary** tab, select all objects, right-click the selection and then click **Select Version By Time**.
6. Click the **Select version by date and time** option, and select the day from the pop-up menu.
7. You can enter the time by clicking on the displayed time in the **Select version by date and time** drop-down list.
8. Under **Differences in backup time**, make any necessary adjustments in case there is no backup version corresponding to your date and time selection for any of the selected objects.
9. Under **If selected date and time doesn't match with selected criteria**, make any necessary adjustments in case there is no backup version corresponding to your date and time selection and to **Differences in backup time** correction for any of the selected objects.
10. Click **OK**.

After you have specified the criteria for restore, the backup versions corresponding to your selection are shown in the Source property page next to every object to be restored.

Manage file conflicts

You can choose how to resolve conflicts between the file version currently on the disk and the version from the backup.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select the disk, directories, or files to be restored.
5. Click the **Destination** tab and then, under File Conflict Handling, select one of the available options:
   - Keep most recent
   - No overwrite
   - Overwrite

Select a device to restore from

By default, Data Protector restores selected data with the same devices that were used during backup. However, you can select alternative devices for your restore.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, expand the object and then select what you want to restore.
5. Click the **Devices** tab to open the Devices property page.

   The devices that were used during backup are listed here.

   To restore your data with an alternative device, select the original device and click **Change**. In the Select New Device dialog box, select the alternative device and click **OK**. The name of the new device appears under Device Status. The new device will be used only for this session.

   For more information on a device, right-click the device and click **Info**.

   To edit data restore policies for AWS S3 Glacier and S3 Deep Archive Glacier, select the device and click S3 Retrieval Policies. By default, the Standard tier is selected with **Max retrieval rate** for data retrieval.

   Specify what Data Protector should do if the selected devices are not available during restore (for example, if they are disabled or already in use). Select either **Automatic device selection** or **Original device selection**.

Find media needed to restore

After selecting the data that you want to restore, you need to get a list of media containing the data. This is essential if you use standalone devices or if you keep media outside the library.

If an object version that you want to restore exists on more than one media set, you can influence the selection of the media set that will be used for the restore by setting the media location priority, or manually select the media set that will be used.

If you use synthetic backup, there is often more than one restore chain of the same point in time of an object. By default, Data Protector selects the most convenient restore chain and the most appropriate media within the selected restore chain.

Note Copies obtained using the media copy functionality are not listed as needed media. A medium copy is used only if the original medium (the medium that was used as a source for copying) is unavailable or unusable.

The following limitations apply:

- With some integrations, it is not possible to set the media location priority in the Restore context. The GUI does not

display the Media tab for these integrations.
- You cannot manually select the media set when restoring integration objects.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, expand the object and then select what you want to restore.
5. Click the **Media** tab to open the Media property page. The needed media are listed. For more information on a medium, right-click it and click **Info.**

   If an object version that you want to restore exists on more than one media set, all media that contain the object version are listed. The selection of the media set depends on the Data Protector internal media set selection algorithm combined with the media location priority setting.

   - To override the media location priority setting, select a location and click **Change priority**. Select a different priority for the location and click **OK**.
   - To manually select the media set from which you want to restore, click the **Copies** tab. In the Copies property page, select the desired object version and click **Properties**. Select the **Select source copy manually** option, select the desired copy from the drop-down list, and click **OK**.
6. If necessary, insert the media into the device.

Tip You can also list the media needed for restore, including media containing object copies of the selected objects, by clicking **Needed media** in the Start Restore Session dialog box. This dialog box appears when you start the restore.

Preview and start a restore

Ensure that the needed media is available or loaded in the device.

Preview is not available for the Data Protector Internal Database restore and the restore sessions of Data Protector application integrations.

Complete the following steps:

1. Select what you want to restore and specify options in the restore property pages, including the selection of the device to be used.
2. Check which media are required for the restore.
3. In the **Actions** menu, click **Preview Restore** if you want to preview it or **Start Restore** to actually start the restore process. You can also click **Preview** or **Restore** button on a **Property** page.
4. In the Start session wizard, review your selection and specify the **Report level**, **Network load**, and **Enable resumable restore** options.

The Restore Monitor shows the progress of the restore.

Abort a restore

Aborting a restore session stops the restore. Data processed before the session was aborted is restored to the specified location.

Complete the following step:

1. To abort a restore session, click **Abort** in the **Actions** menu.

Tip You can abort restore sessions from the Data Protector Monitor context.

Block-based restore procedure

The block-based restore option enables you to restore volumes that are backed up at a block level.

Complete the following steps to restore backed up volumes:

1. Select the volume to restore.

   You can browse for the volume to restore in two possible ways: either from the list of the backed up objects or from the list of sessions.

   To select the volume from the list of backup objects perform the following steps:

   a. In the **Context List**, click **Restore**.
   b. In the **Scoping Pane**, under **Restore Objects**, expand the appropriate data type (for example, **Block based Filesystem**).
   c. In the **Source** tab, select the volume you want to restore.

      By default, when you select the entire volume for restore, the volume from the last backup session is selected. If you want to restore the volume from any other backup session, right-click the selected volume and click **Restore Version**. In the Backup version drop-down list, select the backup version that you want to restore from.

   To select volume from the list of backup sessions, perform the following steps:

   a. In the **Context List**, click **Restore**.
   b. In the **Scoping Pane**, expand the **Restore Sessions** to display clients and then objects, backed up on a particular client. Click an object to open the object's property pages.
   c. In the **Source** tab, select the volume to be restored.

2. In the **Destination** tab, select either the **Restore to original location** or the **Restore to new location** option depending on where you want to restore the backup.
3. In the **Devices** tab, the devices used during the backup are listed. Select the device you want to restore from.

   To restore your volume with an alternative device, select the original device and click **Change**. In the Select New Device dialog box, select the alternative device and click **OK**. The name of the new device appears under Device Status. The new device will be used only for this session. For more information on a device, right-click the device and click **Info**.

   Specify what Data Protector should do if the selected devices are not available during restore (for example, if they are disabled or already in use). Select either **Automatic device selection** or **Original device selection**.
4. In the **Media** tab the needed media are listed. For more information on a medium, right-click it and click **Info.**

   If an object version that you want to restore exists on more than one media set, all media that contain the object version are listed. The selection of the media set depends on the Data Protector internal media set selection algorithm combined with the media location priority setting.

   - To override the media location priority setting, select a location and click **Change priority**. Select a different priority for the location and click **OK**.
   - To manually select the media set from which you want to restore, click the **Copies** tab. In the Copies property page, select the desired object version and click **Properties**. Select the **Select source copy manually** option, select the desired copy from the drop-down list, and click **OK**. If necessary, insert the media into the device.
5. In the **Actions** menu, click **Preview Restore Session** if you want to preview it or **Start Restore Session** to actually start the restore process. You can also click **Preview** or **Restore** button on a **Property** page.

   In the **Start session** wizard, review your selection and select the desired **Report level**, and **Network load** option**.** Select the **Enable resumable restore** option if you want to restart the failed restore session.

For more information on the restore procedure, see Standard restore procedure.

Block-based recovery procedure

The Block-based recovery option enables you to browse, select, and recover individual files and folders instead of restoring the entire block.

Block-based recovery using GUI

Complete the following steps to perform recovery of backed up data using Data Protector GUI:

1. Select data to recover.

   You can browse for data to recover in two possible ways: either from the list of the backed up objects or from the list of sessions. The difference is in the scope of directories and files presented for recovery.

   To select data from the list of backup objects perform the following steps:

   a. In the **Context List**, click **Restore**.
   b. In the **Scoping Pane**, under **Restore Objects**, expand the appropriate data type (for example, **Block Based Filesystem**).
   c. Expand the client system with the data you want to recover and then click the object that has the data. Select the individual files and folders that you want to recover.

   > **Note** When you select individual files and folders, a pop-up appears announcing the shift from Restore to Recovery mode.

   d. In the **Source** tab, select the directories or files that you want to recover.

      By default, when you select a whole directory, only the directories and/or files from the last backup session are selected for recovery. If you want to recover the data from any other backup session, right-click the selected directory and click **Restore Version**. In the Backup version drop-down list, select the backup version that you want to recover from.

   > **Note**
   > - Select files or directories before right-clicking them to use the **Restore As**/**Restore Into** option. The location field will be disabled if you right-click a file or directory without selecting it first.
   > - You can use the options **Restore Only** and **Skip** if you want to recover or skip files or folders which match a specific criteria. These options are mutually exclusive. If you specify both options with a value, then there will be no effect of these options.

   To select data from the list of backup sessions, perform the following steps:

   a. In the **Context List**, click **Restore**.
   b. In the **Scoping Pane**, expand the **Restore Sessions** to display clients and then objects, backed up on a particular client. Click an object to open the object's property pages.

   > **Note** If you select a session in either **running** or **aborted** or **completed with errors** state, the following warning message appears: "You have selected backup session that was not successfully completed. Browsing of files and folders from incomplete backup session is not allowed." Select another session for recovery.

   c. In the **Source** tab, expand the object and then select directories that you want to recover.

2. In the **Destination** tab, the following options are available for selection:

   - Target client
   - Restore to original location
   - Restore to new location

   You can choose how to resolve conflicts between the file version currently on the disk and the version from the backup.

   - Keep most recent
   - No overwrite
   - Overwrite

3. In the **Options** tab, the following restore options are available for selection:

   - Move busy files
   - Lock files during restore

- List restored volumes
- Restore time attributes
- Display statistical information
- Pre-exec
- Post-exec

4. In the **Devices** tab, the devices used during the backup are listed. Select the device you want to recover from.

   To recover your data with an alternative device, select the original device and click **Change**. In the ‘’’Select New Device’’’ dialog box, select the alternative device and click **OK**. The name of the new device appears under Device Status. The new device will be used only for this session. For more information on a device, right-click the device and click **Info**.

   Specify what Data Protector should do if the selected devices are not available during recovery (for example, if they are disabled or already in use). Select either **Automatic device selection** or **Original device selection**.

5. In the **Media** tab the needed media are listed. For more information on a medium, right-click it and click **Info.**

   If an object version that you want to recover exists on more than one media set, all media that contain the object version are listed. The selection of the media set depends on the Data Protector internal media set selection algorithm combined with the media location priority setting.

   - To override the media location priority setting, select a location and click **Change priority**. Select a different priority for the location and click **OK**.
   - To manually select the media set from which you want to recover, click the **Copies** tab. On the Copies property page, select the desired object version and click **Properties**. Select the **Select source copy manually** option, select the desired copy from the drop-down list, and click **OK**. If necessary, insert the media into the device.

6. In the **Actions** menu, click **Preview Restore Session** if you want to preview it or **Start Restore Session** to actually start the recovery process. You can also click **Preview** or **Restore** button on a **Property** page.

   In the **Start session** wizard, review your selection and specify the **Report level**, **Network load**, and **Enable resumable restore** options.

For more information on restore or recovery procedure, see Standard restore procedure.

Block-based recovery using CLI

Complete the following steps to perform recovery of backed up data using CLI:

1. Log in to any client with the Data Protector User Interface component installed.
2. Open the command prompt and change to the directory in which the omnir command is located.
3. Execute:

```
omnir -winfsblockbased <Client:MountPoint Label> -session <SessionID> -tree <TreeName...> [DATA_OPTIONS] -exclude PathName... -skip MatchPattern... -only MatchPattern... -as PathName -into PathName [FILESYSTEM_OPTIONS_BLOCKBASED] -touch -lock -[no_]overwrite | -merge -move_busy [GENERAL_OPTIONS]
```

For more information on these recovery options, see the omnir page.

Restore location

This feature is available in the Premium Edition

By default, Data Protector restores the data to the same client and directory from which it was backed up. You can change these default settings in the Destination property page by specifying where to restore the data to:

- with appropriate user rights you can restore to another client system
- you can restore to another directory

The general restore location can be set on a per-object basis.

Additionally, Data Protector offers you the **Restore As/Into** option to specify a different location for individual files and directories from the same backup object.

Select Restore location

After selecting the data that you want to restore, you can select the location to restore the data to. You can restore the data to another client system and change the directory path. This applies to the entire object to be restored.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type.
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select the object to restore.
5. Click the Destination tab and then, in the Target client drop-down list, select the client system that you want to restore on the new client. By default, Data Protector uses the original directory structure to restore: if the data was backed up from the `C:\temp` directory on system `A`, it restores the data to the `C:\temp` directory on system `B`.
6. You can change the directory path for your restore by selecting the **Restore to new location** option and then entering or browsing for a new anchor directory. The directory path at backup time is appended to the new anchor directory: if data was backed up from the `C:\sound\songs` directory and you enter `\users\bing` as a new path, the data is restored to the `C:\users\bing\sound\songs` directory.

Specify restore location for individual files and directories

You can specify an individual restore path for any directory or file within each object. The individual location specified under the **Restore As/Into** option overrides the location specified in the Destination property page.

This capability is available for the initially selected tree node (directory) and for tree nodes that are not hierarchically dependent on any already selected tree nodes. A selected tree node is indicated by a blue check mark, and a dependent tree node is indicated by a black check mark.

Restore into

Restore into appends the path from the backup to the new location selected here. The new location has to be an existing directory.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type.
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select the object to restore.
5. Right-click the specific file or directory and then click **Restore As/Into**.
6. Under the Destination tab, in the Restore drop-down list, select **Into**.
7. As an option on Windows systems, you can select another drive in the Drive text box to restore the data to. If you want to restore to another client system, click **Browse**.
8. In the Location text box, enter a new path for the file or directory. The original path is added to the new one: if the `colors.mp3` file was backed up from the `C:\sound\songs` directory and you enter `\users\bing` as a new path, the file is restored to the

C:\users\bing\sound\songs directory.
9. Click **OK**.

Restore as

Restore as replaces the path from the backup with the new location selected here. The destination path can be a new directory or an existing one. You can rename the files and directories as you restore them.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type.
3. Expand the client system with the data you want to restore and then click the object that has the data.
4. In the Source property page, select the object to restore.
5. Right-click the specific file or directory and then click **Restore As/Into**.
6. Under the Destination tab, in the Restore drop-down list, select **As**.
7. As an option on Windows systems, you can select another drive in the Drive text box to restore the data to. If you want to restore to another client system, click **Browse**.
8. In the Location text box, enter a new path for the file or directory. The original path is added to the new one. For example, if the colors.mp3 file was backed up from the C:\sound\songs directory and you enter \users\bing\colors.mp as a new path, the file is restored to the C:\users\bing directory.
9. Click **OK**.

> ⚠ **Caution** Consider the risk of deleting data with the Overwrite option enabled when:
>
> - specifying to restore under a name that already exists
> - entering an existing path without specifying the file or directory name.
>
> For example, when you enter a new path \users\bing in the Location text box to restore file colors.mp, but you didn't enter the name of the file, then colors.mp file will be restored as bing. What used to be the bing directory is deleted and substituted with the restored file.

Resume failed sessions

When a backup or restore session fails due to any of the following reasons, Data Protector allows you to resume the session:

- network connectivity
- fatal Disk Agent, Media Agent, or Session Manager errors
- fatal media errors such as torn tape
- abort command invoked from the GUI

Before resuming the session, you must ensure that the initial issue no longer exists. Also, Data Protector requires a resume point for resumption of the session. However, if the resume point isn't available, then Data Protector displays a message stating that the session can't be resumed due to unavailability of the resume point record. In such a scenario, you can choose to restart the session.

Data Protector can resume only the following sessions:

- Filesystem backup sessions (excluding NDMP backups)
- Filesystem restore sessions (excluding NDMP restores)
- Data Protector Oracle Server integration backup sessions
- Data Protector Oracle Server integration restore sessions

When you resume a failed session, Data Protector continues with the backup or restore right from where the session failed. The resumed session inherits all the options from the original session.

Filesystem backup sessions

The resume session functionality for filesystem backup sessions is based on the checkpoint file information that is written into the Internal Database. When a backup session fails, the last backed up file is marked as a checkpoint in the Internal Database. Thus, the backup session can continue from the point of failure when the session is resumed. The file at the point of failure is backed up from the beginning, while the remaining data is appended to the original backup session as its incremental backup. The resumed session automatically inherits the options of the original session.

In case the file marked as a checkpoint is deleted from the filesystem, the resume functionality can still determine what data has not been backed up yet. A failed backup session can be resumed multiple times until it is completed successfully.

In the graphical user interface, the session can be resumed using the context menu of the failed session. In command-line interface, the session can be resumed using the `omnib -resume` option.

The following limitations apply:

- Resume is not supported for disaster recovery.
- Objects backed up with OpenVMS backup client systems are not resumable.

Filesystem restore sessions

The resume session functionality for filesystem restore sessions is based on checkpoint files that are created during a restore session and contain information about which restore options are used in the session and which files have been successfully restored. As soon as a new file is restored, the corresponding checkpoint file is updated.

By default, the checkpoint files are created on both the Cell Manager and the destination client (the checkpoint file that contains information about restore options is created only on the Cell Manager).

On the Cell Manager, the checkpoint files are created in:

Windows systems: `\config\server\sessions\checkpoint`

UNIX systems: `/var/opt/omni/server/sessions/checkpoint`

On clients, the checkpoint files are created in the default Data Protector temporary files directory, within the `Checkpoint` subdirectory.

How the functionality works

When you resume a failed restore session, Data Protector reads information from the checkpoint files and continues with the restore from where the failed restore session left off. Actually, when you resume a restore session, its checkpoint files are moved to the checkpoint file directory of the resumed restore session, where they continue to be updated. Consequently, a failed restore session can only be resumed once. If you try to resume the failed session for the second time, the operation fails because its checkpoint files are no longer there.

Considerations:

- In cluster environments, ensure that the checkpoint files are created on a shared disk, so that both cluster nodes can access the files. To change the location for the checkpoint files, use the OB2CHECKPOINTDIR omnirc option. The option must be set on both cluster nodes and must point to the same directory.
- You can disable the creation of checkpoint files by clearing the option **Enable resumable restore** before you start a restore session (the option can be found in the Start Restore Session dialog box, at the end of the restore wizard). However, if such a restore session fails, you will not be able to resume it because the checkpoint files will be missing. Successfully completed sessions also cannot be resumed since Data Protector deletes the checkpoint files at the end of such sessions.
- A resumed restore session that did not complete successfully is also resumable. This is due to the fact that a resumed restore session inherits the checkpoint files of the original session. Consequently, it inherits all the restore options used in the original session, including the option **Enable resumable restore**.
- When a restore session is removed from the IDB (by default, a session is removed after 30 days), its checkpoint files are purged as well. Checkpoint files are also purged when you initialize the IDB using the omnidbinit command.
- If the No overwrite option was used to restore one or more objects in a failed session, the omnirc option OB2NOOVERWRITE_TRAVERSEDIROBJ must be set to 1 before you resume that session.

The following limitations apply:

- If a restore session failed because the destination client crashed, the resume session functionality may not work correctly. It all depends on whether or not the checkpoint files were successfully flushed from the memory to the disk when the client crashed.
- If a restore session failed right when hard-linked files were being restored, the resume session functionality may not be able to restore the remaining hard-linked files. This is due to the fact that, during backup, Data Protector backs up a hard-linked file only once. For other files that are hardlinked to it, it backs up only the reference to the file. Consequently, restore of hard-linked files is interconnected so the files must be restored all together. Note that this problem does not occur if the restore session fails before the hard-linked files start to be restored or after they have been successfully restored.
- Suppose you want to restore a tree that has been backed up in the following sessions: Full, Incr, and Incr. If the restore session fails because the tree backup object created in one of the backup sessions is not available (for example, the backup media used in the last Incr backup session are corrupted), you must provide the copy of that backup object. If such an object copy does not exist,

you cannot resume the failed restore session, even if a synthetic full backup of the missing backup object exists.

Resume failed sessions

Backup and restore sessions that failed (for example, due to network connectivity problems) can be resumed using the Data Protector resume session functionality. When you resume a failed session, Data Protector continues with the backup or restore, starting right where the failed session left off.

You either have to be in the Data Protector Admin user group or have the Data Protector Monitor user right.

Complete the following steps:

1. If you are using an ordinary Cell Manager, in the Context List, click **Internal Database**. If you are using a Manager-of-Managers, in the Context List, select **Clients** and expand **Enterprise Clients**. Select a Cell Manager with the problematic session. From the Tools menu, select **Database Administration** to open a new Data Protector GUI window with the Internal Database context displayed.
2. In the Scoping Pane, expand **Internal Database** and click **Sessions**. A list of sessions is displayed in the Results Area. Status of each session is denoted in the Status column.
3. Right-click a failed session, and select **Resume Session**.

Advanced restore tasks

You can control a restore in many ways. Data Protector offers a set of the advanced restore tasks for the Windows and UNIX system.

Following are the prerequisites:

- To perform a restore you need to have the appropriate user rights. These rights are defined according to the user group.
- You have to consider the standard restore procedure before proceeding.

Advanced restore tasks

Advanced restore tasks include specifying rarely used options or taking some actions that do not follow the standard restore procedure. To restore the data you will still have to perform most of the standard restore steps.

The way you follow the standard restore procedure depends on the advanced task you want to perform. For example, you can restore your data without browsing. In this case, you need to specify the desired files in a different way, but can still follow the standard restore procedure in other steps.

Skip files for restore

Data Protector allows you to skip files that were backed up, but you do not wish to restore. By using wildcard characters you can skip files matching a specific pattern.

Skipping files for restore is not supported with Data Protector server integration.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, select the directory that you want to restore.
5. Right-click the directory and then click **Properties**.
6. Click the **Skip** tab.
7. In the text box, enter the file name or the criteria used to match the files to be skipped (for example, *.mp3) and then click **Add**. In this example, no mp3 files would be restored. To use more criteria, repeat this step.
8. Click **OK**.

Select only specific files (matching) for restore

Data Protector allows you to restore only those files from the backup that match a specific pattern. By using wildcard characters, you can specify the pattern to be used.

This functionality is not supported with Data Protector NDMP server integration.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type (for example, Filesystem).

3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, select the directory that you want to restore.
5. Right-click the directory and then click **Properties**.
6. Click the **Restore Only** tab.
7. In the text box, enter the file names or enter the criteria to match the files to be restored, for example, `*.mp3`, and then click **Add**. This will restore only `mp3` files. For more criteria, repeat this step.
8. Click **OK**.

Select open files for restore

By default, Data Protector does not restore the files that are in use by some other application (open files). You can restore open files following the steps below.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, expand the object and then select what you want to restore.
5. Click the **Options** tab, and then select the **Move busy files** option.

Deny access to files during restore

By default, Data Protector does not lock files during restore. You can change this default behavior.

Complete the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, expand the object and then select what you want to restore.
5. Click the **Options** tab, and then select the **Lock files during restore** option.

Search for a file to restore

If you do not know the full path of a file that you want to restore, you can search for the file in the IDB, provided that the logging level at backup time was set to Log Files or Log All. You can search for files and directories using the **Restore by Query** task if you know at least a part of the file name.

Perform the following steps:

1. In the Context List, click **Restore**.
2. Click the **Tasks** navigation tab at the bottom of the Scoping Pane. The predefined restore tasks are listed in the Scoping Pane.
3. Click **Restore by Query** to open the wizard.
4. Specify a part of the file name, using wildcard characters.

   For example, type `*.exe` to search for all backed up files with this extension.

   When specifying non-ASCII characters, ensure that the current encoding in the Data Protector GUI and the encoding that was used when the file was created match. Otherwise, Data Protector will not find the files.

   In the environment with a Linux Cell Manager, the wildcard character `?` will not produce the desired results if you want to find a multi-byte character with it. You need to specify multiple wildcard characters `?`. For example, if `3` bytes are used to represent the multi-byte character in the current encoding, add `???` to your string.

   If the directories are available, compare only the base name with patterns. If the directories are not available, compare the full path name with patterns.
5. Optionally, specify other parameters. Click **Next**.

6. Optionally, specify the desired time frame and modification time. Click **Next**.

   Data Protector will list all files and directories matching the specified criteria.

7. From the list of files matching the selection criteria, select the files that you want to restore. To specify further options, click the appropriate tab. To specify the **Report level**, **Network load**, and **Enable resumable restore** options, click **Next**. To start the restore, click **Finish**.

Select a Windows shared disk for restore

Data Protector allows you to restore to a shared disk, even if the data was not originally backed up from the shared disk.

Reasons to restore a UNIX or Windows filesystem to a Windows shared disk:

- If the system is not a part of the Data Protector cell and does not have the Data Protector Disk Agent installed.
- If you want to restore to platforms not directly supported by Data Protector, such as Windows for Workgroups or Windows 3.1 systems.
- If you want to make the data available from several systems.

When you restore your data to a different filesystem type to the one from which it was backed up (UNIX system to Windows system, for example), filesystem-specific attributes may be lost.

You must change the Data Protector Inet account on the Disk Agent client in order to have the right permissions to access the shared disk that you want to restore to. This account has to have the permission to access both the local client system and the remote shared disks. It must be a specific user account, not the system account

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type.
3. Expand the client system with the data you want to restore, and then click the object that has the data.
4. In the Source property page, expand the object, and then select what you want to restore.
5. Click the **Destination** tab.
6. In the **Target client** drop-down list, select the Windows client system with the Disk Agent that you will use for restore.

> **Tip** You can skip the remaining steps if you enter the network path manually by specifying the UNC share name of the remote disk (\\COMPUTER_NAME\SHARE_NAME , for example, \\TUZLA\TEMP) in the **Restore to new location** text box.
>
> You have to do this if you are using the GUI on a UNIX system, since it is not possible for the system to confirm the existence of a Windows shared drive, or to browse it. Therefore, you must confirm yourself that it is available and correctly specified, or the restore may fail.

7. Select the **Restore to new location** option and then click **Browse** to display the **Browse Drives** dialog box.
8. Expand **Microsoft Windows Network** and select the shared disk to which you want to restore the data.
9. Click **OK**.

Restore objects in parallel

A parallel restore allows you to restore data concurrently from multiple objects to multiple disks or filesystems while reading the media only once, thus improving the speed of the restore.

At backup time, the data from the different objects must have been sent to the same device using a concurrency of 2 or more.

The following limitation applies:

You cannot restore the same object in parallel. For example, if you select for the same restore an object under **Restore Objects** and then select the session that includes the same object under **Restore Sessions**, the object will be restored only once and a warning will be displayed.

Complete the following steps:

1. Select the data as you would for a single restore. You can also specify the restore destination, options, and so forth.
2. Go back to the Restore context in the Scoping Pane and repeat step 1 for data under other objects you want to restore.
3. In the **Actions** menu, click **Start Restore**. You are informed that you selected multiple objects.
4. Select the **All selected objects (parallel restore)** option and click **Next**.
5. In the Start session wizard review your selection. Click **Next**.
6. Specify the **Report level**, **Network load**, and **Enable resumable restore** options and click **Finish** to start the restore of objects in parallel.

Disk image restore

A disk image restore is a fast restore of a corresponding disk image backup. Data Protector restores the complete image of a disk, sector-by-sector instead of only restoring selected files or directories.

To restore a UNIX or Windows disk image, expand the **Disk Image** object under the Restore context and then use the standard restore procedure.

Following are the prerequisites:

- The backup to be restored has to be of disk image type.
- On UNIX systems, you need to dismount a disk before a disk image restore and mount it back after the restore using the pre- and post-exec commands (for example, pre-exec: `umount /dev/rdsk/disk1` , post-exec: `mount /dev/rdsk/disk1 /mount_dir`).
- If you want to restore a disk image on a disk other than the disk from which you backed it up, the new disk must be of the same size or larger.

Restore from media in a vault

Restoring from a medium that comes from a vault is very similar to restoring from any other medium. Depending on how the data and catalog protection policies are defined, however, you may need to do some additional steps:

- If you have a library, enter the medium and scan it.
- If the catalog protection for the medium is still valid, restore the data by selecting what you want to restore using the Data Protector user interface.
- If the catalog protection for the medium has expired, Data Protector does not have detailed information about the data backed up. Restore the data by manually specifying the files or directories that you want to restore.

Tip To re-read the detailed information about the files and directories from the medium after the catalog protection has expired, export the medium, import it back, and specify that you want to read the Detail Catalog data. After that, you will be able to browse the files and the directories in the Data Protector user interface.

Web server restore

To restore a web server, use the standard restore procedure for restoring files, directories, and clients. Additionally, you need to consider the following:

- All data should be restored to the original location.
- Configuration files and root directories should always be included.
- During restore, the web server should be down, however the operating system must be up and running. Restart the web server after the restore.

In case a database, such as Oracle or Informix Server, is included on the web server, use the restore procedure specific for the database.

Restore without browsing

When the catalog protection for the data has expired or when the backup was done using the No Log or Log Directories option, you can manually specify a file or a directory for restore.

In case you do not know a file or a directory name, you can restore the entire object and then extract the parts that you need or you can use the **Restore only** feature to restore only files which match a specific pattern and then extract the parts that you need from them.

Restore the entire object and extract the needed parts

When you are not able to browse for a file or directory you want to restore, you can restore the entire object and then extract only the parts you need.

To restore the entire object, you need a temporary storage area as large as the entire object.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore, and then click the object you want to restore.
4. Click the **Destination** tab. Select a temporary directory that is large enough to store the entire object.
5. Specify options in the other restore property pages, including the selection of the device to be used.
6. In the **Actions** menu, click **Preview Restore** if you want to preview it or **Start restore** to actually start the restore process.
7. In the Start session wizard, review your selection and specify the **Report level**, **Network load**, and **Enable resumable restore** options. The Restore Monitor shows the progress of the restore.
8. When the restore is finished, you can extract the needed parts of data from the restored object and copy them to the desired location. Note that you do this outside Data Protector.

Restore parts of the backed up object using restore-only pattern match

When you are not able to browse for a file or directory you want to restore, the directory (or a file or a higher level directory) can be hit using a pattern match that avoids the restore of most unwanted parts of the object. By using wildcard characters, you can specify the pattern to be used.

> **Note** This functionality is not supported with Data Protector NDMP server integration.

Following are the prerequisites:

- You need to use a fairly specific pattern definition for this feature to be beneficial.
- You need a temporary storage area for the restored parts. Its size depends on the size of the restored object parts, which is connected to the precision of the matching pattern used.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object you want to restore.
4. In the Source property page, right-click the object you want to restore from and then click **Properties**.
5. Click the **Restore Only** tab and in the text box specify the pattern to match the files to be restored (for example, "*order*40*.ppt ") and then click **Add**. You should add several such patterns to specify as precisely as possible the type of files to be restored.
6. Click **OK**.
7. Click the **Destination** tab. Select a temporary directory that is large enough to store the parts of the backed up object.
8. Specify options in the other restore property pages, including the selection of the device to be used.
9. In the **Actions** menu, click **Preview Restore** if you want to preview it or **Start restore** to actually start the restore process.
10. In the Start session wizard, review your selection and specify the Report level, Network load, and Enable resumable

restore options. The Restore Monitor shows the progress of the restore. If you selected a "Warning" report level, Data Protector issues a Warning message because the list of files and directories is not in the IDB catalog. This does not influence the restore.

11. When the restore is finished you can extract the needed parts of data from the restored object and copy them to the desired location. Note that you do this outside Data Protector.

Restore the file or directory manually

When you are not able to browse for a file or directory you want to restore, you can specify a file or a directory manually. This happens when the catalog protection for your data has expired, or when backup was done using the **No log** option.

To add a file or a directory manually, you need to know the exact path and the name of the file or the directory. The file and path names are case-sensitive.

Compelet the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore, right-click the object that has the file or directory that you want to restore manually, and then click **Properties**.
4. Click the **Restore Summary** tab and then enter the missing part of the path and the name of the file or directory you want to restore in the text box.
5. Click **Add** to confirm. The Version window appears.
6. From the Version drop-down list, select the backup version you want to restore and then click **OK**. The object name and version are displayed.
7. Specify options in the other restore property pages, including the selection of the device to be used.
8. In the **Actions** menu, click **Preview Restore** if you want to preview it or **Start restore** to actually start the restore process.
9. In the Start session wizard, review your selection and specify the **Report level**, **Network load**, and **Enable resumable restore** options.

The Restore Monitor shows the progress of the restore. If you selected a "Warning" report level, Data Protector issues the Warning message because the list of files and directories is not in the IDB catalog. This does not influence the restore.

Restore options

Data Protector offers a set of comprehensive restore options that allow fine-tuning of a restore. All these options have default values which are appropriate in most cases.

The following list of options is set on a per-object basis. The restore options are available according to the type of data being restored.

General restore options

- **Show full chain.** Displays all the files and directories in the restore chain. By default, this option is selected and the entire restore chain is restored.
- **Show this session only.** Displays only the files and directories backed up in this session. This enables you to restore files and directories from an incremental backup session without restoring the entire restore chain. By default, this option is disabled.
- **Target client**. By default, you restore to the same client system from which the data was backed up. You can select another system in your cell from the drop-down list. The Disk Agent is started on the selected client system and the data is restored there.

  You need to have the **Restore to other clients** user right to be able to restore to another client system.
- **Omit deleted files**. For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

  If this option is selected, Data Protector recreates the state of the backed up directory tree at the time of the last incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are restored and later deleted at folder restore during subsequent incremental restore.

  If this option is not selected, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

  When using the **Restore As** or **Restore Into** functionality with this option enabled, carefully choose the restore location to prevent accidental removal of existing files.

  Default: not selected.
- **Move busy files**. This option is relevant if a file on the disk is being used by an application when a restore wants to replace this file. It only applies to the files that are locked by an operating system when they are used by the application or other process. The option is used with the **Keep most recent** or **Overwrite** options.

  By default, this option is disabled.

  On UNIX systems, Data Protector moves the busy file `filename` to `#filename` (adds a hash in front of the filename). The application will keep using the busy file until it closes the file. Subsequently, the restored file is used.

  On Linux systems, this option is not supported.

  On Windows systems, the file is restored as `filename.001`. All applications keep using the old file. When the system is rebooted, the old file is replaced with the restored file.
- **List restored data.** Displays the names of the files and directories in the monitor window as the objects are being restored. By default, this option is disabled.
- **Display statistical information.** Reports statistical information (such as size and performance) for each object that is backed up or restored. You can view the information in the monitor window. By default, this option is disabled.
- **Omit unrequired object versions**. This option applies if you select directories for restore and the backup was performed with the logging level **Log All** or **Log Files**.

  If this option is selected, Data Protector checks in the IDB for each backup in the restore chain if there are any files to restore. Backups with no object versions to restore are skipped. Note that this check may take some time.

  If this option is not selected, each backup in the restore chain is read, even if there was no change since the previous backup.

  To restore empty directories, clear this option.

  Default: selected.
- **Restore sparse files**. Restores sparse files in their original compressed form. This is important because sparse files can consume additional disk space unless they are restored in their original form. By default, this option is disabled.

  This option applies to UNIX sparse files only. Windows sparse files are always restored as sparse.
- **Lock files during restore.** Denies access to files during the restore. By default, this option is disabled.
- **Restore time attributes.** Preserves the time attribute values of each restored file. When this option is disabled,Data Protector sets the time attributes of the restored objects to the current date and time. By default, this option is enabled.

- **Restore protection attributes**. Preserves the original protection attributes of each restored file. If this option is disabled, Data Protector applies the protection attributes of the current restore session. By default, this option is enabled.

  On Windows systems, this option applies to file attributes only. Security information is always restored, even when this option is disabled.

- **Restore share info for directories.** Specifies that share information for directories will be restored. By default, this option is selected.

  When restoring a directory that was shared on the network when it was backed up, the directory will also be shared after restore if this option is selected, provided that the backup was made with the **Backup share information for directories** option selected.

Pre- and post-exec commands

- **Pre-exec.** Allows you to enter a command (or script) to be executed before the restore of each object is initiated. This command (or script) must return success for Data Protector to proceed with the restore.

  The pre-exec command (or script) is executed on the client system where the Disk Agent is running. On a Windows system, the scripts must be located in the `Data_Protector_home\bin` directory or its sub-directory. On Unix systems, the scripts must be located in `/opt/omni/lbin` directory, or its sub-directories.

  Note that only `.bat`, `.exe`, and `.cmd` are supported extensions for pre-exec scripts on Windows systems. To run a pre-exec script with an unsupported extension (for example, `.vbs`), create a batch file (`.bat`) that starts the script. Then configure Data Protector to run the batch file as a pre-exec command which then starts the script with the unsupported extension.

- **Post-exec**. Allows you to enter a command (or script) to be executed after the restore of each object is completed. The post-exec command (or script) is executed on the client system where the Disk Agent is running.

Device selection

- **Automatic device selection.** Applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup.

  By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option `AutomaticDeviceSelectionOrder`.

  For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup.

  Default: selected.

- **Original device selection**. Applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available.

  This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration.

  Default: not selected.

Manage file conflicts

- **Keep most recent.** If this option is selected, the most recent versions of files are kept. If a file on the disk is newer than the backed up version, the file is not restored. If a file on the disk is older than the backed up version, the file is overwritten with the newer version from the backup. By default, this option is enabled.
- **No overwrite.** If this option is selected, files that exist on the disk are preserved. This means that they are not overwritten by other versions of these files from the backup. Only non-existing files are restored from the backup. By default, this option is disabled.
- **Overwrite.** If this option is selected, existing files on the disk are replaced with files from the backup. By default, this option is disabled.

Active directory specific options

Replication mode

- **Authoritative.** This is a Windows Server specific option dealing with active directory restore. The Active Directory database is not updated after the restore and the restored data overwrites the existing data in the target destination. An

authoritative restore can only be performed by running ntdsutil.exe from the command prompt after the restore session has finished.
- **Nonauthoritative.** The Active Directory database is updated after the restore using standard replication techniques. The **Nonauthoritative** replication mode is the default option.
- **Primary.** The Primary replication mode allows you to keep the NT directory Service online and is used when you restore FileReplicationService along with the Active Directory service. This option must be used when all replication partners for a replicated share have been lost. With regard to the Certificate Server and the Active Directory Server, **Primary** is the same as **Authoritative**.

Setting restore options

After selecting the data that you want to restore, you can set the restore options. Restore options have default values that are appropriate in most cases. They are available according to the type of data being restored. For example, all restore options available for a filesystem restore are not available for a disk image restore.

Perform the following steps:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, under Restore Objects, expand the appropriate data type (for example, **Filesystem**).
3. Expand the client system with the data you want to restore and then click the object (mountpoint on UNIX systems, drive on Windows systems) that has the data.
4. In the Source property page, select the data to restore.
5. Click the **Options** tab to open the Options property page. Select or deselect an option by clicking the box next to it.

Windows systems restore

When restoring a Windows filesystem, Data Protector restores the data within the files and directories, as well as Windows-specific information about the files and directories.

The following Windows-specific information is restored:

- Full Unicode file names
- FAT16, FAT32, VFAT

  NTFS attributes
- Sets of alternate data streams.
- Share information

  If a directory is shared on a network during backup, the share information is stored on the backup medium. The directory will be shared on the network after the restore by default (unless a shared directory with the same share name already exists). To prevent restoring share information for directories that are being restored, deselect the Restore share information for directories option.

  File Conflict Handling options apply also for the restore of the directory share information. For example, if the No overwrite restore option is used for the restore, the directory share information for directories that exist on the disk, is preserved.
- NTFS alternate data streams
- NTFS security data

NTFS 3.1 filesystem features

- The NTFS 3.1 filesystem supports reparse points

  The volume mount points, Single Instance Storage (SIS), and directory junctions are based on the reparse point concept. These reparse points are selected as any other filesystem object.
- The NTFS 3.1 filesystem supports symbolic links.

  Data Protector handles symbolic links in the same way as NTFS reparse points.
- The NTFS 3.1 filesystem supports sparse files as an efficient way of reducing the amount of allocated disk space.

  These files are backed up sparse to save tape space. Sparse files are backed up and restored as sparse to the NTFS 3.1 filesystem only.
- Some of the NTFS 3.1-specific features are controlled by system services that maintain their own data records. These data structures are backed up as a part of CONFIGURATION.
- Encrypted files

  The Microsoft-encrypted NTFS 3.1 files are backed up and restored encrypted, but their contents can only be properly viewed when they are decrypted.
- Compressed files are backed up and restored compressed.

Consider the filesystem restore limitations when restoring to a different filesystem type than where the backup was performed.

Restore objects backed as shared disks

Objects that were backed up as shared disks are associated with the Disk Agent client that was used to back them up. If the environment has not changed, you can restore the shared disk as you would a local Windows filesystem. By default, the same Disk Agent client that was used to back up the shared disk is used to restore the data to the original location.

Windows filesystem restore limitations

You can restore your data to a different filesystem type than the one the backup was performed on.

From	To				
FAT32	FAT16	CDFS	UDF	NTFS 3.1	
FAT32	FC	FC	N/A	N/A	FC
FAT16	FC	FC	N/A	N/A	FC
CDFS	FC	FC	N/A	N/A	FC

UDF	FC	FC	N/A	N/A	FC
NTFS 3.1	*	*	N/A	N/A	FC

Legend	
FC	Full Compatibility. The file attributes are entirely preserved.
*	Reparse points, sparse files and encrypted files are not restored. Files are restored without security information and alternate data streams.

The table shows that NTFS 3.1 filesystem objects can only be adequately restored to the NTFS 3.1 filesystem. The filesystem-specific attributes and alternate data streams are lost when restoring into a different filesystem version.

- A Windows reparse point, such as a directory junction or a volume mountpoint, can be restored to an NTFS 3.1 filesystem only. UNIX reparse points cannot be restored to a NTFS 3.1 filesystem.
- When you restore an NTFS 3.1 filesystem that contains SIS reparse points, a full disk condition may occur. This happens if the original file is restored into multiple target files that can take up more space than available.
- Sparse files are restored as sparse to the NTFS 3.1 filesystem only.
- User Disk Quotas cannot be restored using Data Protector.
- If a user attempts to restore a sparse file to a non-NTFS 3.1 filesystem,Data Protector will issue a warning. A sparse file restored to a filesystem other than NTFS 3.1 will not include zero sections.
- The Microsoft encrypted NTFS 3.1 files can be restored to the NTFS 3.1 filesystem only, because other filesystem drivers cannot decrypt them.

Configuration restore

To restore the Windows CONFIGURATION, select the CONFIGURATION object or parts of it and follow the standard restore procedure.

The CONFIGURATION consists of data structures that influence system operation. Therefore, the system must be prepared for such a restore. The prerequisites depend on the contents of the CONFIGURATION item and the Windows operating system version.

The following limitations apply:

- Active Directory Service and SysVol should be restored in pair.
- User Disk Quotas cannot be restored using Data Protector. The backed up information can be restored manually, using Microsoft utilities.
- Although Data Protector allows you to restore single configuration objects, it is **not recommended** to do so. It is highly recommended that you perform a full configuration restore as part of the **Disaster Recovery** procedure.

Windows configuration objects

- Active Directory Service
- Certificate Server
- COM+ Class Registration Database (ComPlusDatabase)
- DFS
- DHCP
- DNS Server
- Event Logs
- File Replication Service
- Internet Information Server (IIS)
- User Profiles (Documents and Settings)
- Windows Registry
- Removable Storage Management Database
- SystemRecoveryData
- SysVol
- Terminal Services Database
- User Disk Quotas (QuotaInformation)
- WINS server

Restart the system after the restore of the whole CONFIGURATION object is finished in order for the restored data to become effective.

Some objects require special considerations and tasks.

Active Directory

To restore the Active Directory service, you have to restart the system using the Directory Services Restore Mode start-up option. When the system is started in the Directory Services Restore Mode, the domain user accounts cannot be used. You have to configure the Data Protector Inet and the crs service (for a Cell Manager) to log on using the local system account and then restart the services. When restoring the Active Directory, the File Replication Service (FRS) and Distributed File System (DFS) are also restored.

You can restore the Active Directory in one of three replication modes (Windows specific options):

- nonauthoritative
- authoritative
- primary

Note To perform an **Authoritative** restore, you also need to run ntdsutil.exe after the restore session has finished. For example, to perform a typical authoritative restore, at a command prompt enter ntdsutil, then authoritative restore, then restore database. Restart the server and wait for replication to take place.

Tip You can also create a post-exec command to perform the additional action needed for the Active Directory authoritative restore. For example, to perform an authoritative restore of an entire directory, use the following line:

```
ntdsutil "popups off" "authoritative restore" "restore database" quit quit
```

DFS

Data Protector restores Windows Distributed File System (DFS) as part of one of the following:

- Windows Registry, if the DFS is configured in a standalone mode
- Windows Active Directory, if the DFS is configured in a domain mode

Profiles

- A user profile cannot be restored successfully if the respective user is logged on, either interactively or as a service. If the user is logged on at the time of the restore, Data Protector will fail to restore the file NTUSER.DAT which contains the user's registry hive.

  You have to log off the system and stop all the services that are running under the user account whose profiles you want to restore. The restore session can be started from another system or by logging on the restore target system as a different user.

- To restore all user profiles at once, you must stop any services that do not run under the local system account, and log off from the system. Then start the restore session remotely, using Data Protector GUI on another client.

- A user profile can only be restored when its location is already defined on the system. Individual files of existing user profiles or deleted profiles can be still restored as long as they exist among the system's profiles. If a user profile was deleted from the Control Panel, or the user profile no longer exists on the system for some other reason, the restore fails with the following error:

  ```
  [84:208] Configuration object not recognized by the system => not restored.
  ```

  To restore such user profile, you must first recreate it by logging on as that user. The system assigns a directory for the user's profile and creates a default profile. To keep the restored files unmerged, you can delete the files in the newly created profile before running a restore session. Then log off and start the restore session by logging on as a different user or by using another system. The system may assign a different name to the user. In this case, use the **Restore As** option to restore the files to the newly assigned location.

- When user profiles are restored, files are always overwritten, regardless of the File Conflict Handling options in the restore specification. Also, the **Omit deleted files** option is not available. Files that exist on the disk, but were not present at the time of the backup, will remain in the user profile after the restore.

- User profiles can also be restored using the **Restore As** option. You can specify a temporary location for the files and then manually copy the desired files to the user's profile directory. Or, you can restore directly over the user's profile directory, possibly making use of the **Move busy files** option, which allows you to restore a user profile even if it is in use by a logged on user. However, note that in this case the files that are in use will only be replaced after the system is rebooted.

Registry

If you select the whole Windows Registry for a restore, some of the Registry keys are not restored and some are treated in a special way during a restore. This is because these keys are used by the operating system. You can find them under the following Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore
```

Removable storage manager database

The RSM service must be running on all systems with connected removable storage devices (except for CD-ROMs).

Server configuration objects

The target system must have the respective server installed and running. For all servers, except Certificate Server, the data is restored online.

Certificate Server data is restored offline. Stop the Certificate Server Services before starting a restore. You can restore the Certificate Server only using the authoritative mode.

SysVol

You can perform restore of SysVol directory in one of three modes:

- nonauthoritative

  If at least one domain controller in the domain is available and working, files are restored to their original location. The restored data is not propagated to other domain controllers.

- authoritative

  Perform authoritative restore if critical SysVol data is deleted from the local domain controller and the deletion is propagated to other domain controllers.

- primary

  If all domain controllers in the domain are lost and you want to rebuild domain controller from backup, the FRS is informed that you are restoring primary files and files are restored to their original location.

Windows TCP/IP services

On a Windows system that runs a Microsoft TCP/IP protocol and is configured as a WINS Server, a DHCP Server, or a DNS Server, you can restore the services that manage network communication.

To restore Windows TCP/IP services, expand the CONFIGURATION item and select WNS, DHCP, or DNSServerDatabase.

Each of these services is automatically stopped before the restore.

When the restore has finished, restart the system.

System state data restore

If you use Active Directory, which is always a part of the System State, you have to start the system in the Directory Services Restore Mode.

From the Data Protector point of view, the System State consists of some specific filesystem objects and CONFIGURATION objects. The System State also includes data belonging to additional server roles or services that may be installed. As opposed to selecting objects in the Backup wizard, different objects for restore are selected in separate Restore wizards.

In the Source property page, select:

- the System State objects that belong to CONFIGURATION:
  - ActiveDirectoryService
  - CertificateServer
  - Cluster Service information
  - IIS Metadirectory
  - RemoteStorageService
  - RemovableStorageManagementDatabase
  - SystemFileProtection
  - SYSVOL directory
  - TerminalServiceDatabase
- SystemVolumeInformation (including System File Protection service)
- boot files (they are located on the system drive)
- volumes on which data belonging to particular server roles or services resides or even the entire client system

When the restore is finished, restart the system.

Remote storage service

Remote Storage Service (RSS) is used to automatically move infrequently accessed files from local to remote storage. Remote files are recalled automatically when the file is opened.

Although the RSS databases are part of System State data, you restore them manually. The RSS database must be restored offline. You can provide pre- and post-exec scripts to stop and restart the service, or you can stop and restart it manually before and after the restore, respectively.

Select the following directories for restore:

%SystemRoot%\system32\RemoteStorage

%SystemRoot%\system32\NtmsData

System file protection

System File Protection service scans and verifies the versions of all protected system files after you restart your computer. If the System File Protection service discovers that a protected file has been overwritten, it retrieves the correct version of the file and then replaces the incorrect file. Data Protector enables you to back up and then restore protected files without being overwritten.

UNIX systems restore

When restoring files to the original location from which the backup was performed,Data Protector restores the files, including file attributes.

System specific data, such as Access Control List (ACL) on UNIX systems, is restored only on the same filesystem type and operating system from which the backup was made.

UNIX systems specific information

When restoring VxFS data, use the **Restore As** option and restore it to the desired location.

OpenVMS file system restore

Use the standard restore procedure to restore HP OpenVMS filesystems.

The following limitations apply:

- **Omit_deleted_files** and **Resume_restore** options are not supported.
- For files and directories saved on any other operating system platform not all file attributes are restored and no ACL is restored in this case.
- Directories that are created during a restore but have not been included in a save will get the attributes of the first file restored in the directory unless disabled by the -no_protection option.
- Any file specifications that are entered into the GUI or passed to the CLI must be in UNIX style syntax: /disk/directory1/directory2/filename.ext.n
  - The string should begin with a slash, followed by the disk, directories, and filename, separated by slashes.
  - Do not place a colon after the disk name.
  - A period should be used before the version number instead of a semi-colon.
  - File specifications for OpenVMS files are case insensitive.
    For example: an OpenVMS file specification 1DGA100:[USERS.DOE]LOGIN.COM';1 must be specified in the following format:

    /1DGA100/Users/Doe/Login.Com.1
- There is no implicit version number. You always have to specify a version number. Only file versions selected for the restore will be restored. If you wish to include all versions of the file, select them all in the GUI window, or, using the CLI, include the file specifications under the **Only** (-only) option, including wildcard characters for the version number, as follows:

  /DKA1/dir1/filename.txt.*
- If you restore to a location other that the original location, only the disk device and starting directory are changed. The original directory path is added to the destination path to form the new restore location.
- If the **Restore Time Attributes** (-notouch) option is disabled during a restore, the last accessed date will be updated with the current date and time on ODS-5 disks. On ODS-2 disks, the original dates will be set on the files.
- A file saved as a soft link will be restored using the equivalent of a DCL SET FILE/ENTER command. No data will be restored in this case. The soft link entered points to the primary path/filename for this file from the time the file was saved. If the primary path/filename does not exist or was not restored, the creation of the soft link will fail.

  To make a restored copy of an OpenVMS system disk bootable, the OpenVMS WRITEBOOT utility has to be used to write a boot block after the disk has been restored.
- The **Move Busy Files** (-move) and **Restore Sparse Files** (-sparse) options are not available on OpenVMS.
- Files backed up from an ODS-5 disk on an OpenVMS system that have extended filesystem names (that is, upper and lower case letters, Unicode characters, and so on) may not be restored to an ODS-2 disk.
- Files being restored are always locked regardless of whether the **Lock Files during Restore** (-lock) option is enabled or disabled.
- The default device and directory for pre- and post-exec command procedures is /omni$root/bin . To place the command procedure anywhere else the file specification must contain the device and directory path in UNIX style format. For example:

  /SYS$MANAGER/DP_SAVE1.COM
- If the **Restore Protection Attributes** (-no_protection) option is disabled, the files are created with the default owner, protection, and ACL.
- When specifying wildcard characters for **Skip** (-skip) or **Only** (-only) filters use '*' for multiple characters and '?' for single characters.
- On OpenVMS systems, Data Protector does not support disk quotas on volumes and volume sets.

  To perform restore of data located on a volume with disk quota enabled, configure the post-exec script so that it disables disk quota on the involved volume before restore starts, and configure the pre-exec script so that it enables the disk quota after restore completes.

Filesystem information restored

The directory structure and the files are restored, together with the following filesystem information:

- File and directory attributes
- ACL (Access Control List) if available (see Limitations)
- Secondary file entries

  During an OpenVMS filesystem backup, files with multiple directory entries are backed up once using the primary path name. Secondary path entries are saved as soft links.

For example, system specific roots on an OpenVMS system disk will have the SYSCOMMON.DIR;1 path stored as a soft link. The data for this path will be saved under [VMS$COMMON...].

During a filesystem restore, these extra path entries are restored.

Files can be restored to mounted FILES-11, ODS-2, or ODS-5 volumes only.

Set up ZDB and IR

This section provides a basic overview of zero downtime backup (ZDB) and instant recovery (IR). Conventional methods of backing up data are not well suited to applications operating on large volumes of data; for example database applications. Either the application has to be taken offline or, if the application supports it, put into “hot-backup” mode while data in it is streamed to tape. The first can cause major disruption to the application’s operation. The second can produce large transaction log files, putting extra load on the application system.

In today's storage environment, the requirements for data availability are constantly growing. For the information resources to be highly available, Data Protector zero downtime backup (ZDB) solution helps you meet your business needs, eliminating the application downtime and making mission-critical data available 24x7.

Zero downtime backup is a backup approach in which replication techniques are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first, and all subsequent backup operations are performed on the replicated data rather than the original data.

As a backup occurs in the background while the application remains online and available for use, the impact on your environment during a backup is minimal. The recovery window is reduced as well by using the instant recovery functionality, which enables recovery of vast amount of data in minutes rather than hours. This makes ZDB and IR capabilities suitable for high-availability systems and mission-critical applications.

Data Protector ZDB and IR techniques utilize mirror and snapshot technologies of disk-based arrays. The following are the basic principles behind ZDB and IR:

- Create, at high speed, a copy of the data to be backed up and then perform backup operations on the copy, rather than on the original data.
- Restore a backup copy of data, held on the array, to its original location on the array to facilitate high-speed recovery.

Zero downtime backup (ZDB) and instant recovery (IR) have two great advantages over conventional backup and restore techniques:

- Minimal downtime or impact on the application system during the session
- Shorter restore times

Configure P4000 SAN Solutions

This feature is available in the Premium Edition

This topic describes how to configure the Data Protector P4000 SAN Solutions integration.

The following prerequisites apply:

- Obtain or install:

  P4000 SAN Solutions licenses and components:

  - P4000 SAN/iQ software.
  - P4000 Virtual SAN Appliance Software / P4000 Centralized Management Console.
  - P4000 SAN Solutions DSM (Device Specific Module) for MPIO.

  Data Protector licenses and components:

  - Appropriate zero downtime backup extension and instant recovery extension licenses-to-use (LTU).
  - P4000 Agent on the application system and the backup system.
- Make sure the same operating system version is installed on the application system and the backup system.
- If the application system and the backup system reside in a Data Protector cell with secured clients, ensure that access between both systems is allowed in both directions.
- Source volumes must be created and presented to the application system and the backup system.

The following limitations apply:

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- In a Microsoft server cluster environment, all volumes which are selected for zero downtime backup session must belong to the same cluster.
- Backup preview is not supported.
- Object copying and object mirroring are not supported for ZDB to disk.
- Although you can create replica sets, replica set rotation is not supported.
- A replica cannot be used for instant recovery under any of the following conditions:
  - A target volume of the replica has been automatically removed during an instant recovery session based on another ZDB backup specification.
  - Other entities exist on the disk array which depend on the source volume that was used to create a target volume of the replica:
    - A newer target volume exists, and a smartclone is attached to it.
    - A newer snapshot exists, and the snapshot was not created by Data Protector.
- The Data Protector `omnidbp4000` command that you should use for configuring access to the CIMOM provider of the P4000 SAN Solutions is available only on Windows systems.

For information on either of the following items, see the Release notes:

- General Data Protector and integration-specific limitations
- Supported platforms and integrations
- Supported backup and connectivity topologies

To be able to use the Data ProtectorP4000 SAN Solutions integration with a storage system of the P4000 SAN Solutions family, you must perform the mandatory configuration step. In this step, you need to provide the Data Protector P4000 Agent the data which the ZDB agent will use to establish connection to a Common Information Model Object Manager (CIMOM) provider of your choice.

Configure CIMOM provider connection

In order to be able to connect to a CIMOM provider, the Data Protector P4000 Agent needs the following information:

- Fully qualified domain name or IP address of the system where the CIMOM service is running

  In case the system has multiple IP addresses configured, the address by which the system can be accessed by the Data Protector ZDB agent should be used.
- Whether the connection uses Secure Sockets Layer (SSL)
- Port number of the port on which the CIMOM service is accepting requests
- Username and password

  This data must belong to a user account which has administrative privileges on theP4000 SAN Solutions storage system.

This information should be provided for each CIMOM provider that the Data Protector P4000 Agent should connect to. Once added, the connection configuration data for a particular CIMOM provider is stored in a separate configuration file located on the Cell Manager in the directory:

Windows systems: Data_Protector_program_data\server\db80\smisdb\p4000\login

UNIX systems: /var/opt/omni/server/db80/smisdb/p4000/login

To add the connection configuration data, use the Data Protector `omnidbp4000` command. With `omnidbp4000`, you can also update or remove the configuration data, list the contents of the configuration files, and check if the connection to a particular CIMOM provider can be established. For these purposes, the `omnidbp4000` command provides the basic options `--add`, `--remove`, `--list`, and `--check`.

Backup

Zero downtime backup sessions that involve a storage system of the P4000 SAN Solutions family can only be initiated through the Data Protector Microsoft Volume Shadow Copy Service integration.

Restore

Instant recovery sessions that involve a storage system of the P4000 SAN Solutions family can only be initiated through the Data Protector Microsoft Volume Shadow Copy Service integration.

Troubleshoot

This section lists general checks and verifications that you may need to perform when you encounter problems with the P4000 SAN Solutions integration.

- Ensure that the latest official Data Protector patches are installed.
- Checks and verifications
  - On the application and backup systems, examine system errors logged into the `debug.log` file residing in the Data Protector log files directory.

Configure P9000 XP Disk Array family

This feature is available in the Premium Edition

This topic describes how to configure the Data Protector P9000 XP Disk Array Family integration, how to perform zero downtime backup and instant recovery using the P9000 XP Disk Array Family integration, and how to resolve the integration-specific Data Protector problems.

The following prerequisites apply:

- Obtain or install:

  P9000 XP Array components:

  - RAID Manager Library on the application system and the backup system.

    RAID Manager Library is disk array firmware-dependent. For installation instructions, see the RAID Manager Library documentation.

    Note that snapshots are supported only by the disk array microcode 50-04-20 and newer versions, and only by RAID Manager Library 01.15.00 and newer versions.

    To enable Data Protector to use a disk array through a command device which is operating in the user authentication mode (available only with specific disk array models), you must use a specific RAID Manager Library version.

  - Continuous Access (CA) P9000 XP and/or Business Copy (BC) P9000 XP license and microcode.

  - An appropriate multi-path device management software.

    The software must be installed on the application system and the backup system.

    HP-UX systems: Secure Path (HP-UX)

    On HP-UX 11.31 systems, the multi-path device management software is not required since the operating system has native device multi-pathing capability.

    Linux systems: Device Mapper Multipath Enablement Kit for Disk Arrays 4.2.0 or newer version

    To configure the installed multi-path device management software:

    1. Start the multipath daemon.
    2. Execute the following command to configure the daemon so that it gets started during system startup:

       Red Hat Enterprise Linux: chkconfig multipathd on

       SUSE Linux Enterprise Server: chkconfig boot.multipath on

    Windows systems: MPIO Full Featured DSM (Device Specific Module) for P9000 XP Disk Array Family

  Data Protector licenses and components:

  - Appropriate zero downtime backup extension and instant recovery extension licenses-to-use (LTU).
  - P9000 XP Agent on the application system and the backup system.

- Make sure that the same operating system version is installed on the application system and the backup system.
- If the application system and the backup system reside in a Data Protector cell with secured clients, ensure that access between both systems is allowed in both directions.
- Make sure the SAN environment and the P9000 XP Array storage systems are properly configured:
  - Primary volumes (P-VOLs) are available to the application system.
  - Secondary volumes (S-VOLs) of the desired type (mirror, snapshot storage volume) are available to the backup system.
  - A pair relationship is defined between both sets of volumes (LDEVs) with P9000 XP Remote Web Console (formerly known as Command View XP).
  - LUNs are assigned to the respective ports.
- On HP-UX 11.31 systems, if you use VxVM disk groups, enable the legacy Device Special Files format.

Prerequisites for Linux systems

- For each configured S-VOL, follow the steps:
  1. Put the corresponding LDEV pair into the SUSPENDED state, that is, suspend the pair relationships between the S-VOL and its P-VOL.
  2. If multiple S-VOLs are in a pair relationship with its P-VOL, change the UUID of the S-VOL by executing the command

pvchange -u PVName on the backup system, where PVName is the LVM physical volume name of the S-VOL.

Prerequisites for HP-UX

From Data Protector 9.05 onwards, only for SSEA backups, it is required to have LVM on HP-UX updated to the latest OS patch where “lvmadm” command is present. Hence, HPUX must be “HP-UX 11iv3 March 2008” or newer.

Prerequisites for Windows systems

- On Windows Server 2008 systems, disable the operating system option **Automatic mounting of new volumes**. In the Command Prompt window, execute the command mountvol /N.
- Do not manually mount target volumes that were created by Data Protector.

The following limitations apply:

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- Zero downtime backup using snapshots is only supported in Business Copy (BC) P9000 XP and Continuous Access + Business Copy (CA+BC) P9000 XP configurations.
- Instant recovery is only supported in Business Copy (BC) P9000 XP configurations.
- Using split mirror restore, you can only restore filesystems and disk images backed up in Business Copy (BC) P9000 XP configurations, including their single-host (BC1) implementations. Other Data Protector backup object types are not supported.
- Asynchronous Continuous Access P9000 XP configuration is not supported.
- The single-host (BC1) configuration based on Linux platform is not supported. In such a configuration, a single Linux system acts as the application system and the backup system.
- With the single-host (BC1) configuration, only filesystem and disk image backup are supported.
- Split-mirror restore (restore of data from the backup medium to a secondary volume and restore of data from the secondary volume to a primary volume afterwards) is supported for the filesystems and disk images in the Business Copy P9000 XP configuration. Database (application) split-mirror restore is not supported.
- In case Microsoft Exchange Server is installed on the backup system, its Information Store (MDB) and Directory Store have to be installed on the P9000 XP Disk Array Family LDEVs that are different than the mirrored LDEVs used for the integration. The drive letters assigned to these LDEVs have to be different from those assigned to the LDEVs that are used for the integration.
- Backup preview is not supported.
- Object copying and object mirroring are not supported for ZDB to disk.
- Instant recovery from a ZDB-to-disk+tape session cannot be performed using the Data Protector GUI after exporting or overwriting the media used in the backup session. The backup media must not be exported or overwritten even after an object copy session. If the backup media have been exported or overwritten, perform instant recovery using the Data Protector CLI.
- When restoring filesystems in an instant recovery session, no object other than those selected for instant recovery should share the disks that are used by objects selected for the session.
- Routine maintenance tasks, including (but not limited to) hot-swapping any field replaceable components like, disk array controllers, FC switches, and online firmware upgrade during backup are not supported. Backup is a high-IO activity and should not be done at the same time as routine maintenance.
- The maximum number of secondary volumes (mirrors, volumes to be used for snapshot storage) that can be created for a specific primary volume is limited by the P9000 XP Disk Array Family model used and its installed firmware revision. Note that the limitation for mirrors and the limitation for volumes to be used for snapshot storage differ.

For information on any of the following items, see Release notes:

- General Data Protector and integration-specific limitations
- Supported platforms and integrations
- Supported backup and connectivity topologies

ZDB database – XPDB

ZDB database for the Data Protector P9000 XP Disk Array Family integration is referred to as **XPDB**. It keeps information about:

- LDEV pairs that are split (put into the SUSPENDED state). This information includes:
  - ID of the ZDB session that involved handling the LDEV pair.
  - LDEV, volume group, and filesystem configuration.
  - CRC information calculated during the session.
  - IR flag (indicating that the target volume can be used for instant recovery)
- Filesystem and volume management system information.

The information is written to the XPDB when a LDEV pair is put into the SUSPENDED state, and is deleted from the XPDB when a LDEV pair is resynchronized (is put into the PAIR state). During resynchronization, prior version of data is overwritten.

Volume group configuration and the CRC information stored in XPDB is compared to the volume group configuration and the CRC information obtained during an instant recovery session. If these items do not match, the session fails.

Objects and their configuration during backup and restore sessions are kept in the XPDB for replica set rotation and instant recovery. Only the LDEV pairs tracked in the XPDB can be used for instant recovery.

XPDB resides on the Cell Manager in:

Windows systems: Data_Protector_program_data\server\db80\xpdb

UNIX systems: /var/opt/omni/server/db80/xpdb

Configure the integration

Before you start with the configuration, make sure the prerequisites listed in Data Protector P9000 XP Disk Array Family integration:

Solaris systems: Run the Sun format utility to label and format the paired LDEVs (on both the application system and the backup systems).

BC P9000 XP configurations: Connect the application system and the backup system to the same disk array unit.

When using first-level mirrors or snapshot volumes, primary LDEVs (P-VOLs) must be connected to the application system and the paired secondary LDEVs (S-VOLs) must be connected to the backup system.

CA P9000 XP configurations: Connect the application system to the Main Control Unit (MCU), and the backup system to the Remote Control Unit (RCU). ESCON links provide communication links between the P9000 XP Array MCU and RCU.

Main LDEVs (P-VOLs) must be connected to the application system and have paired disks (S-VOLs) assigned. Paired LDEVs (S-VOLs) in the remote disk array must be connected to the backup system.

Combined (CA+BC P9000 XP) configurations: Connect the application system to the MCU, and the backup system to the RCU.

Main LDEVs (P-VOLs) must be paired to remote volumes in the RCU (S-VOLs). S-VOLs also function as BC P9000 XP primary volumes (P-VOLs) and must be paired to local copies (BC P9000 XP S-VOLs):

- *Windows systems:* Connect only BC P9000 XP S-VOLs to the backup system.
- *HP-UX systems:* Connect only BC P9000 XP S-VOLs to the backup system. If CA P9000 XPS-VOLs are connected as well, special care must be taken if `/etc/lvmtab` is lost in this configuration: use `vgscan` to recreate the volume groups and `vgreduce` to delete potentially added `pvlinks` to the S-VOLs. Re-import or re-create the volume groups to ensure the configuration is correct.
- *Linux systems:* Connect only BC P9000 XP S-VOLs to the backup system.

HP-UX LVM mirroring: Use the physical volume groups mirroring of LDEVs to ensure that each logical volume is mirrored to an LDEV on a different I/O bus. This arrangement is called **PVG-strict mirroring**. Disk hardware must be already configured, so that each secondary LDEV is connected to the system on a different bus (not the bus used for the primary LDEV).

1. Create the volume group with the LDEVs that have S-VOLs assigned using `vgcreate`. LVM mirror primary volumes must be the LDEVs that have their S-VOLs.
2. Extend the volume group with LDEVs that have no S-VOLs assigned using `vgextend`. LVM mirror secondary volumes must be the LDEVs that have no S-VOLs.

> When using LVM mirroring with the SSEA integration, the devices in the logical volume can also be non-XP devices, such as IBM.

To configure the integration:

- Set the P9000 XP Array command devices.
- If needed, set the P9000 XP LDEV exclude file.
- To enable zero downtime backup and instant recovery sessions that involve a disk array which is operating in the user authentication mode, configure the user authentication data.

Command device handling

P9000 XP Disk Array Family **command devices** are dedicated volumes in the disk arrays which act as the interface between management applications and the storage systems. They cannot be used for data storage and only accept requests for operations that are then executed by the disk arrays. A command device is needed and used by any process requiring access to a P9000 XP Array. Data about all command devices detected by Data Protector is stored in the XPDB for the purpose of avoiding concurrent overallocation of each particular command device.

Whenever a ZDB session is started, the Data ProtectorP9000 XP Agent queries the XPDB for a list of command devices, and updates it if needed. When the first ZDB session is started, the P9000 XP Agent generates a list of command devices

connected to every application and backup system in the cell. All subsequent sessions automatically update the list if the configuration of command devices has changed.

Every command device is assigned an instance number (starting from 301) and the system name (hostname) having access to it. If a command device can be accessed from more than one system, the P9000 XP Agent recognizes that the command device is assigned to another system; such a command device-hostname combination gets the next available instance number.

Thus, every P9000 XP Array storage system attached to the application and backup systems has a list of command devices and systems having access to them (together with an instance number).

Below is an example of command device entries in the XPDB:

```
Serial#CU:Ldev(LDEV)InstSystem ======================================================
3537100:67(103)301application.system1.com 3537100:67(103)302backup.system.com 3537200:68(104)301application.system2.com
3537300:69(105)301application.system3.com
```

To be able to control which command device and instance number should be used on a specific system, you can disable the automatic update of the command device list in the XPDB. To disable the automatic update:

1. Set the `SSEA_QUERY_STORED_CMDDEVS` `omnirc` option to `1`.
2. Use the `omnidbxp` command to manually add, list, remove, and update the command devices.

If you decide to disable the automatic update, the initial list of command devices is still created in the XPDB during the first ZDB session. For subsequent backup sessions, the Data ProtectorP9000 XP Agent behavior is as follows:

- Whenever an application system or a backup system needs access to theP9000 XP Array storage system during a session, it uses the first assigned command device with the instance number from the list.
- If the command device fails, the next device from the list is used.
- If all devices fail, the session fails.
- If successful, the command device is used by the system until the end of the session, and the list of command devices is used for all consecutive sessions.

Configuring the user authentication data

Specific disk array models of the P9000 XP Disk Array Family provide increased security with authorization verification that involves user and resource groups, roles, and user authenticity verification. Authorization verification is enabled by a special operating mode called **user authentication mode**. When an application, for example the Data ProtectorP9000 XP Agent, communicates with a disk array which is operating in this mode, the application must supply appropriate user credentials in order for queries and modifications of the disk array configuration or its resources to succeed. On the disk arrays on which the conventional operating mode is still available for compatibility reasons, the user authentication mode is disabled by default.

Authorization system of a disk array on which the user authentication mode is available defines a fixed set of roles that belong to different task groups: security-related, storage-related, and maintenance-related tasks. It assigns a particular subset of roles and a particular set of resource groups to each user group. While there are several preconfigured user groups, which can be used immediately, you can easily create additional ones. Each disk array user account can belong to multiple user groups. Similarly, each user group can have multiple resource groups assigned, and each resource group can belong to multiple user groups. Each time an application attempts to start a specific operation on a specific resource of the disk array, the authorization system first determines the user account based on the supplied user credentials. It then checks if any user group the user account belongs to is allowed to perform the operation on the resource. If user credentials are not supplied, the disk array always rejects to execute the operation.

Important The operating mode setting is actually a command device property. For example, if a particular backward compatible disk array has two command devices configured, one can operate in the conventional mode and the other in the user authentication mode. It therefore depends on the configuration of the command device used whether the application should supply user credentials to successfully start the requested operation.

User authentication data and the XPDB

To enable the P9000 XP Agent to perform zero downtime backup (ZDB) and instant recovery (IR) sessions using a command device for which the user authentication mode is enabled, you must add appropriate user credentials to the ZDB database (XPDB) in advance. The credentials must belong to a disk array user account which has the *Local Copy*, the *Remote Copy*, or both roles assigned, depending on the P9000 XP Disk Array Family configuration. The P9000 XP Agent then reads the credentials from the XPDB each time such a ZDB or IR session is started. User credentials are bound to a specific disk array serial number. For each particular serial number, you can add user credentials of a single disk array user account. To add and manage user credentials in the XPDB, use the Data Protector `omnidbxp` command.

Configuration procedure

To properly add the required user credentials for a specific disk array that will be involved in the ZDB and IR sessions, follow the steps:

1. Identify the serial number of the disk array.

2. Identify which disk array volumes (LDEVs) will be involved in the ZDB and IR sessions.
3. Identify which disk array user group has been granted adequate access to all volumes that you identified in the previous step
4. Choose a disk array user account that belongs to the disk array user group from the previous step. Identify and write down its user name and password that you will need in the next step.
5. Using the `omnidbxp -user -add` command, add the user name and password that you acquired in the previous step to the XPDB, providing the disk array serial number you identified in step 1 of this procedure.
6. Using the `omnidbxp -user -check` command, verify that the P9000 XP Agent can connect to the disk array using the configured user authentication data.

P9000 XP LDEV exclude file

You can reserve certain LDEVs for purposes other than Data Protector backup and restore. A session is aborted if the participating replica contains an excluded LDEV.

Disabled secondary LDEVs (S-VOLs) are listed in the P9000 XPLDEV exclude file on the Cell Manager:

Windows systems: Data_Protector_program_data\server\db80\xpdb\exclude\XPexclude

UNIX systems: /var/opt/omni/server/db80/xpdb/exclude/XPexclude

Secondary LDEVs (S-VOLs) listed in this file must be the backup system LDEVs identified by the backup system LDEV#.

Use the `omnidbxp` command to:

- set and change the exclude file
- identify excluded LDEVs
- reset the exclude file
- delete the content of the exclude file

The file syntax and the example are as follows.

Syntax

```
# # Data Protector A.10.30 # P9000 XP Disk Array Family LDEV Exclude File # # [<XP1>] # <LDEV> # <LDEV1>, <LDEV2>, <LDEV3> # <LDEV1>-<LDEV2> # [<XP2>] # ... # # <XP> - disk array serial/sequence number # <LDEV> - CU#:LDEV number in decimal format # # End of file
```

Example

```
# # Data ProtectorA.10.30 # P9000 XP Disk Array Family LDEV Exclude File # [35241] 3603, 3610, 3620-3625 # Some excluded LDEVs 2577 # 2864-3527 # # # End of file
```

Automatic configuration of the backup system

When you start a ZDB session, Data Protector performs necessary configuration steps, such as configuring volume groups and filesystems on the backup system. Based on the volume group, filesystem, and mount point configuration on the application system, Data Protector creates the same volume group and filesystem structure on the backup system and mounts these filesystems during a ZDB-to-tape or ZDB-to-disk+tape session.

Maintain the integration

Maintenance tasks include querying the information kept in XPDB, in particular:

- available zero downtime backup sessions
- backup system LDEVs involved in a particular session
- backup system LDEVs stored in the XPDB
- XPDB information about particular LDEV pairs

You can retrieve the information stored in the XPDB using the `omnidbxp` command.

Backup

This section describes configuring filesystem and disk image ZDB using the Data Protector GUI.

You should be familiar with the P9000 XP Disk Array Family concepts and procedures and basic Data Protector ZDB and instant recovery functionality.

ZDB types

Using the P9000 XP Array integration, you can perform:

- ZDB to disk

  The replica produced is kept on a disk array until reused. This replica becomes part of the replica set and can be used for instant recovery.

  ZDB to disk is performed if the option **Track the replica for instant recovery** is selected in a ZDB backup specification, and **To disk** is selected when running/scheduling a backup.

  ZDB to disk is only possible using the BC P9000 XP configuration.

- ZDB to tape

  The replica produced is streamed to backup media, typically tape, according to the tape backup type you have selected (Full, Incr, Incr1-9).

  This replica is deleted after backup if the option **Keep the replica after the backup** is *not* selected in a ZDB backup specification. If this option is selected, the replica remains on a disk array until reused and becomes part of the replica set. However, it cannot be used for instant recovery.

- ZDB to disk+tape

  The replica produced is kept on a disk array until reused and is also streamed to backup media according to the tape backup type you have selected (Full, Incr, Incr1-9). This replica becomes part of the replica set and can be used for instant recovery.

  ZDB to disk+tape is performed when the option **Track the replica for instant recovery** is selected in a ZDB backup specification, and **To disk+tape** is selected when running/scheduling a backup.

  ZDB to disk+tape is only possible using the BC P9000 XP configuration.

Replica types

Using the P9000 XP Array integration, you can create the following replica types:

- split mirror

  This replica type is supported by all disk array models of the P9000 XP Disk Array Family that are officially supported by Data Protector.

- snapshot

  This replica type is supported by specific P9000 XP disk array microcode versions and specific RAID Manager Library versions only.

You cannot directly select a replica type when configuring a Data Protector ZDB backup specification. You must chose the replica type in advance when creating secondary LDEVs (S-VOLs) with P9000 XP Remote Web Console (formerly known as Command View XP). During ZDB sessions, the Data ProtectorP9000 XP Agent always uses the S-VOLs (the target volumes specified in the ZDB backup specification) in the same way, regardless of their type – mirror or snapshot storage volume. Thus, you can even create replica sets of which specific replicas are mirror copies and others are snapshots.

In general, both replica types are available for all ZDB types, for instant recovery, and for split mirror restore. However, a specific limitation applies to the Continuous Access (CA) P9000 XP configurations.

Backup concepts

P9000 XP Array zero downtime backup consists of two phases:

1. The data from P-VOLs presented to the application system is synchronized with the S-VOLs presented to the backup system.

   During this phase, the synchronization is performed on the level of participating volume groups (UNIX systems) or disks (Windows systems). Therefore, if multiple filesystems/disk images are configured in the same volume group or on the same disk, the *entire* volume group or disk (all filesystems or disk images in the group or on the disk) is synchronized to the backup system regardless of the objects selected for backup.

2. Synchronized backup system data is backed up to a backup device.

   During this phase, only the objects selected for backup are backed up.

> **Note** With ZDB to disk, the second phase does not occur. Backed up data can only be restored using instant recovery.

This concept enables a restore of selected objects for a split mirror restore and restore from backup media on LAN, but not for instant recovery.

With instant recovery, the links from the application to backup system are *not* synchronized before the restore, whereas with a split mirror restore they *are*, thus enabling the restore of selected objects by establishing the current state of the application system data on the backup system, and then restoring selected objects to the backup system and resynchronizing the backup system to the application system.

Create backup specifications

To create a ZDB backup specification for a disk array of the P9000 XP Disk Array Family using the Data Protector GUI (**Data Protector Manager**), follow the steps:

1. In the Context List, select **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**. Right-click **Filesystem** (for both object types: filesystem and disk image) and click **Add Backup**.

   The Create New Backup dialog box appears.

   In the Filesystem pane, select the **Blank Filesystem Backup** template or some other template which you might have created.

   Select **Snapshot or split mirror backup** as **Backup type** and **P9000 XP** as **Sub type**. For descriptions of options, press **F1**.

   Click **OK**.
3. Under Client systems, select **Application system** and **Backup system**. If the application system is part of a server cluster, select the virtual server.
4. Under Mirror type, select the P9000 XP Array configuration, and specify a value for **MU number(s)**. The maximum number of replicas that can be created for the same source volumes is different for mirror copies and snapshots. Both limitations are imposed by the P9000 XP Array storage system.
5. Under Replica management options, select the desired options.

   ZDB to disk, ZDB to disk+tape:

   Select the option **Track the replica for instant recovery** to enable instant recovery.

   > **Note** You can choose a ZDB-to-disk session or a ZDB-to-disk+tape session by selecting an appropriate value for the **Split mirror/snapshot backup** option when running or scheduling a ZDB session based on this ZDB backup specification.

   ZDB to tape:

   Leave the option **Track the replica for instant recovery** cleared.

   To preserve the replica on the disk array after the ZDB session, leave the option **Keep the replica after the backup** selected. To remove the replica after the session, clear this option.
6. Under At the start of the session and At the end of the session, specify how states of the source volumes and the corresponding target volumes are handled during zero downtime backup sessions.
7. Specify other zero downtime backup options as desired.
8. Select the desired backup objects.

   Filesystem backup: Expand the application system and select the objects to be backed up. Note that all drive letters or mount points that reside on the system are displayed. You must select only the objects that reside on the disk array, otherwise the ZDB session will fail.

   > **Important** To ensure that instant recovery succeeds and the environment is consistent after instant recovery, select all volumes on a disk (Windows systems) or all logical volumes of a volume group (UNIX systems) to be backed up. Even if you do not select an entire disk or volume group, the backup will succeed, but instant recovery may experience issues during configuration check of the environment. The configuration check can be disabled by clearing the option **Check the data configuration consistency** in the GUI or not specifying the option `-check_config` in the CLI when preparing for an instant recovery session. If this option is cleared (GUI) or not specified (CLI), the entire disk or volume group will be overwritten during instant recovery.

   Click **Next**.

   Disk image backup: Click **Next**.
9. Select devices. Click **Properties** to set device concurrency, media pool, and preallocation policy. For information on these

options, click **Help**.

To create additional copies (mirrors) of backup, specify the desired number of mirrors by clicking **Add mirror** or **Remove mirror**. Select separate devices for the backup image and each mirror.

> **Note** Object mirroring and object copying are not supported for ZDB to disk.

Click **Next**.

10. In the Backup Specification Options group box, click **Advanced** and then the **P9000 XP** tab to open the P9000 XP Array backup options pane.

    You can specify Application system options and modify all other options, except **Application system** and **Backup system** (note that you can change them after you save the ZDB backup specification).

    In the Filesystem Options group box, click **Advanced** and specify filesystem options as desired. For information, press **F1**.

    Windows systems: To configure a ZDB backup specification for incremental ZDB sessions, select the **Do not use archive attribute** filesystem option in the WinFS Options pane to enhance the incremental ZDB behavior.

    Click **Next**.

11. In the Backup Object Summary page, specify additional options.

    Filesystem backup: You can modify options for the listed objects by right-clicking an object and then clicking **Properties**. For information on the object properties, press **F1**.

    Disk image backup: Follow the steps:

    a. Click **Manual add** to add disk image objects.

    b. Select **Disk image object** and click **Next**.

    c. Select the client system. Optionally, enter the description for your object. Click **Next**.

    d. Specify General Object Options and Advanced Object Options. For information on these options, press **F1**.

    e. In the Disk Image Object Options window, specify disk image sections.

       Windows systems:

       Use the format

       `\\.\PHYSICALDRIVE#`

       where `#` is the current number of the disk to be backed up.

       HP-UX and Solaris systems:

       Specify a disk image section:

       `/dev/rdsk/filename` , for example: `/dev/rdsk/c2t0d0`

       On HP-UX 11.31 systems, the new naming system can be used:

       `/dev/rdisk/disk#` , for example `/dev/rdisk/disk2`

       Specify a raw logical volume section:

       `/dev/vgnumber/rlvolNumber` , for example: `/dev/vg01/rlvol1`

       Linux systems:

       Specify a disk image section:

       `/dev/Filename` , for example: `/dev/dm-10`

       > **Important** To ensure that instant recovery succeeds and the environment is consistent after instant recovery, select all volumes on a disk (Windows systems) or all logical volumes of a volume group (UNIX systems) to be backed up. Even if you do not select an entire disk or volume group, the backup will succeed, but instant recovery may experience issues during configuration check of the environment. The configuration check can be disabled by clearing the option **Check the data configuration consistency** in the GUI or not specifying the option `-check_config` in the CLI when preparing for an instant recovery session. If this option is cleared (GUI) or not specified (CLI), the entire disk or volume group will be overwritten during instant recovery.

    f. Click **Finish**.

Click **Next**.

12. Click **Save As** to save your ZDB backup specification. Optionally, you can click **Save and Schedule** to save, and then schedule the backup specification.

Note Backup preview is not supported.

Backup options

The following tables describe the P9000 XP Array and ZDB related backup options.

Client systems

Application system	The system on which the application runs. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).
Backup system	The system to which your data will be replicated (backed up). In ZDB-to-disk+tape and ZDB-to-tape sessions, the backup data is copied from this system to a backup device.

Mirror type

Business Copy P9000 XP	Select this option to configure a ZDB backup specification for the P9000 XP Disk Array Family configuration Business Copy P9000 XP. Default: selected.
Continuous Access P9000 XP	Select this option to configure a ZDB backup specification for the P9000 XP Disk Array Family configuration Continuous Access P9000 XP. Default: not selected.
Combined (Continuous Access P9000 XP + Business Copy P9000 XP)	Select this option to configure a ZDB backup specification for the P9000 XP Disk Array Family combined configuration Continuous Access P9000 XP + Business Copy P9000 XP. Default: not selected.

MU number(s)	This option is only available if the P9000 XP Disk Array Family configuration Business Copy P9000 XP is selected.
	
	This option defines the mirror unit (MU) number(s) of a replica or a replica set from which the Data ProtectorP9000 XP Agent, according to the replica set rotation, selects the replica to be used in the zero downtime backup session. The replica selection rule is described in the Data Protector Concepts Guide. The maximum number of replicas that can be created for the same source volumes is different for mirror copies and snapshots. Both limitations are imposed by the P9000 XP Disk Array Family storage system.
	
	You can specify one or more non-negative integer numbers, one or more ascending ranges of such numbers, or any combination of both. Use a comma as the separator character. Examples:
	
	`5`
	
	`7-9`
	
	`4,0,2-3`
	
	When a sequence is specified, it does not define the order in which the replicas are used.
	
	Default: `0` (nothing is specified).

Replica management options

Keep the replica after the backup	If configuring a ZDB to tape, select this option to keep the replica on the disk array after the zero downtime backup session. The replica becomes part of a replica set (specify a value for the option **MU number(s)**). Unless the additional option **Track the replica for instant recovery** is selected, the replica is *not* available for instant recovery. If this option is not selected, the replica is removed at the end of the session. If the option **Track the replica for instant recovery** is selected, this option is automatically selected and cannot be changed. Default: selected.
Track the replica for instant recovery	This option is only available if the P9000 XP Disk Array Family configuration **Business Copy P9000 XP** is selected. Select this option to perform a ZDB-to-disk or ZDB-to-disk+tape session and leave the replica on the disk array to enable instant recovery. If this option is not selected, you cannot perform instant recovery using the replica created or reused in this session. ⚠ **Caution** If you select this option, do not manually resynchronize the affected mirrors and do not empty the volumes used for snapshot storage. Otherwise, instant recovery will not be possible. Default: not selected.

At the start of the session

Synchronize the disks if not already synchronized	On the P9000 XP Array, primary volumes (source volumes) and their corresponding secondary volumes (target volumes) must be in the PAIR state to enable Data Protector zero downtime backup: mirrors must be synchronized and volumes to be used for snapshot storage must be empty. This option is automatically selected and cannot be changed if the option **Prepare the next mirror disk for backup (resynchronize)** is cleared. If this option is selected, all volumes of the replica to be used in the current ZDB session are put into the PAIR state with the corresponding source volumes at the start of the session: mirrors are resynchronized and volumes to be used for snapshot storage are made empty. Default: selected.
Abort the session if the mirror disks are not already synchronized	Available only if the option **Prepare the next mirror disk for backup (resynchronize)** is selected. The option is only applicable if at least one volume of the replica to be used in the current ZDB session is a mirror (or mirror copy). In the opposite case, Data Protector treats as if the option **Synchronize the disks if not already synchronized** is selected instead. If this option is selected and at least one volume of the replica to be used in the current ZDB session is not in the PAIR state with the corresponding source volume, the session fails. Default: not selected.

At the end of the session

Prepare the next mirror disk for backup (resynchronize)	This option is only applicable if at least one volume of the replica to be used in the next ZDB session is a mirror (or mirror copy). In the opposite case, Data Protector behaves as if the option is not selected. If this option is selected, all volumes of the replica to be used in the next ZDB session are put into the PAIR state with the corresponding source volumes at the end of the current ZDB session: mirrors are resynchronized and volumes to be used for snapshot storage are made empty. If this option is not selected, the volumes of the replica to be used in the next ZDB session are left intact at the end of the current ZDB session. If this option is not selected, the **Synchronize the disks if not already synchronized** option is automatically selected, and the **Abort the session if the mirror disks are not already synchronized** option is not available. Default: selected.

Application system options

Dismount the filesystems on the application system	Select this option to dismount the filesystems on the application system before replica creation and remount them afterwards. Additionally, when entire physical drives (on Windows systems) or entire disks or logical volumes (on UNIX systems) are selected as backup objects in a disk image backup specification, selecting this option will dismount and later remount all filesystems on these objects. If any of these filesystems cannot be dismounted, the backup session fails. If an integrated application (for example, Oracle Server) exclusively controls the data I/O on each physical drive, disk, or logical volume that will be backed up, the dismount operation is not needed. In such a case, you can leave this option cleared. Default: not selected.
Stop/quiesce the application command line	If a command is specified in this option, it is invoked on the application system immediately before replica creation. An example is to stop applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option. If the command fails, the command specified in the option **Restart the application command line** is not invoked. Thus, you may need to implement a cleanup procedure in the command specified in **Stop/quiesce the application command line**. If the `omnirc` option `ZDB_ALWAYS_POST_SCRIPT` is set to `1`, the command specified in the option **Restart the application command line** is always invoked.
Restart the application command line	If a command is specified in this option, it is invoked on the application system immediately after replica creation. An example is to resume operation of applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option.

Backup system options

Use the same mountpoints as on the application system	This option is not available if the application system is also the backup system (a single-host configuration). If this option is selected, the paths to mount points used for mounting the filesystems of the replica on the backup system are the same as paths to mount points where source volume filesystems were mounted on the application system. If the mount points are already in use, the session fails. For such circumstances, you must select the option **Automatically dismount the filesystems at destination mountpoints** in order for the session to succeed. **Windows systems:** The drive letters must be available, otherwise the session fails. Default: not selected.

Root of the mount path on the backup system	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. Specifies the root directory under which the filesystems of the replica are mounted. Where exactly the filesystems are mounted depends on how you define the option **Add directories to the mount path**. **Note** For the SAP R/3 integration, the option is not applicable (the mount points created are always the same as on the application system). Defaults: **Windows systems:** c:\mnt **UNIX systems:** /mnt

Add directories to the mount path	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. This option enables control over the created mount points. It defines which subdirectories will be created in the directory defined with the **Root of the mount path on the backup system** option. When Session ID is used in path composition, this guarantees unique mount points. Example for **Windows systems**: Root directory: C:\mnt Application system: applsys.company.com Backup session ID: 2008–02–22–4 Mount path on the application system: E:\disk1 If **Hostname** is selected: C:\mnt\applsys.company.com\E\disk1 If **Hostname and session ID** is selected: C:\mnt\applsys.company.com\2008–02–22–4\E\disk1 If **Session ID** is selected: C:\mnt\2008–02–22–4\E\disk1 If **Session ID and hostname** is selected: C:\mnt\2008–02–22–4\applsys.company.com\E\disk1 **Note** For the SAP R/3 integration, the option is not applicable (the mount points created are always the same as on the application system). Default: Hostname and session ID.
Automatically dismount the filesystems at destination mountpoints	If the mount points are in use (for example, volumes involved in the previous session may still be mounted) and this option is selected, Data Protector attempts to dismount the mounted filesystems. If the option is not selected and the mount points are in use, or if the option is selected and the dismount operation fails, the session fails. Default: not selected.

Leave the backup system enabled	This option is only available if the option **Keep the replica after the backup** is selected. If this option is selected, the filesystems remain mounted, the volume groups remain imported and active (UNIX systems), and the target volumes remain presented after the session. In this case, you can use the backup system for data warehousing purposes, but *not* for instant recovery. If the replica has to be reused later on (deleted, rotated out, or used for instant recovery), Data Protector automatically connects to the backup system, dismounts the filesystems, unpresents the target volumes, and clears the related logical structures on the backup system. At that point in time, if the filesystems are not mounted to the current backup system, Data Protector cannot perform a proper cleanup, and aborts the operation or the instant recovery session. If this option is not selected, Data Protector dismounts filesystems, exports volume groups (UNIX systems), and unpresents the target volumes on the backup system at the end of the ZDB session. Default: not selected.
Enable the backup system in read/write mode	This option is applicable to and can only be changed for UNIX systems only. On Windows systems, filesystems cannot be mounted in the read-only mode. Select this option to enable write access to volume groups and filesystems on the backup system. For backup purposes, it is sufficient to activate the backup system volume groups and mount the filesystems in the read-only mode. For other tasks, the read/write mode may be needed. Note that when this option is selected, the replica is open to modifications while the backup system is online. Consequently, data restored from such a replica includes all potential modifications. Defaults: **Windows systems:** selected. **UNIX systems:** not selected.

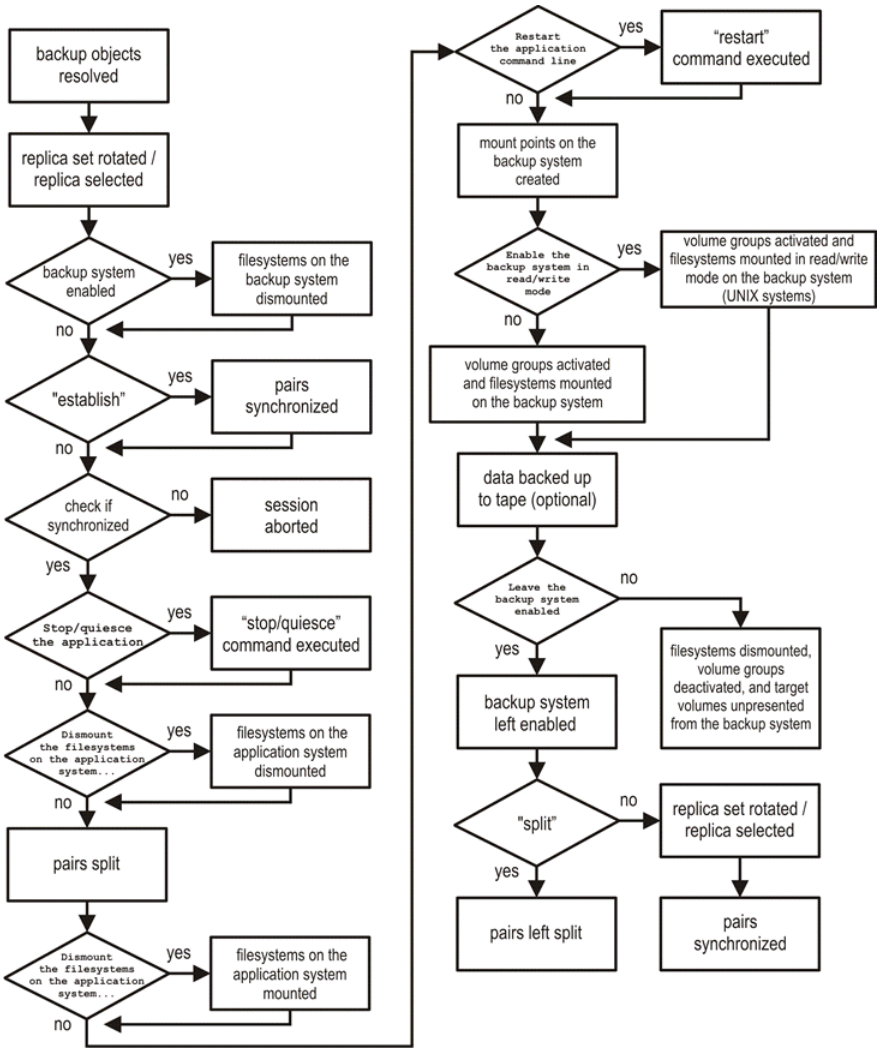
Note In a particular ZDB session, the mount point paths to which filesystems of the replica are mounted on the backup system correspond the mount point paths to which source volumes were mounted on the application system if at least one of the following conditions is met:

- The GUI option **Use the same mountpoints as on the application system** is selected.
- The omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 1.

If the option **Use the same mountpoints as on the application system** is not selected, and the omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 0, the mount point paths are determined by the GUI options **Root of the mount path on the backup system** and **Add directories to the mount path**, and the omnirc options ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH are ignored.

The chart and table below provide detailed backup flow according to the backup options selected.

ZDB session flow for filesystem backup objects



The “establish” and “split” checks depend on the P9000 XP Array zero downtime backup options listed in the table Relation between particular zero downtime backup options and the “establish” and “split” checks .

Relation between particular zero downtime backup options and the “establish” and “split” checks

The option **Synchronize the disks if not already synchronized** is selected.	"establish" = yes
The option **Abort the session if the mirror disks are not already synchronized** is selected.	"establish" = no
The option **Prepare the next mirror disk for backup (resynchronize)** is selected.	"split" = no
The option **Prepare the next mirror disk for backup (resynchronize)** is cleared.	"split" = yes
No value or a single number is specified for the option**MU number(s)** or the option **Keep the replica after the backup** is selected.	"split" = yes

Restore

This section describes configuring and running a filesystem or disk image restore of the data backed up using theP9000 XP Array integration. The sections describe restore procedures using the Data Protector GUI and CLI.

The data backed up in a ZDB session can be stored on a disk array (ZDB to disk, ZDB to disk+tape) or on backup media (ZDB to tape, ZDB to disk+tape).

Available restore types are:

- Restore from backup media on LAN (standard restore).
- Split mirror restore.

- Instant recovery.

Restore types

	Standard restore	Split mirror restore	Instant recovery
ZDB to disk	N/A	N/A	Yes
ZDB to disk+tape	Yes	Yes	Yes
ZDB to tape	Yes	Yes	N/A

Standard restore

Data backed up in ZDB-to-tape and ZDB-to-disk+tape sessions can be restored from the backup media to the application system through a LAN.

Tip You can improve the data transfer rate by connecting a backup device to the application system.

The procedure below is a general description of restoring the objects backed up in a ZDB session.

1. In the Context List, select **Restore**.
2. Select the objects for restore and click them to display their properties.

   In the Scoping Pane, select the application system as **Target client** under the **Destination** tab.

   For information on restore options, press **F1**.
3. Click **Restore**. The **Start Restore Session** dialog box appears.
4. Click **Next** to specify the report level and network load. Click **Next**.
5. In the **Start Restore Session** window, select **Disabled** as **Mirror mode**. This sets a direct restore to the application system.
6. Click **Finish** to start the restore.

Split mirror restore

Split mirror restore can be run with both replica types: split mirror and snapshot. The same split mirror restore procedure applies in both cases.

You can start a split mirror restore session only after the preceding session using the same internal disks on the application system finishes with the disk pairs synchronization (the transition of the LDEV pairs into the PAIR state).

Split mirror restore process

Data is restored from backup media on LAN to the secondary LDEVs (S-VOLs), and then copied to the primary LDEVs (P-VOLs). The process consists of the following automated steps:

1. Applying replica set rotation (if a replica set is defined) to the specified replica set to select the replica for restore.
2. Preparing the application system and the backup system.
3. Restoring data from the backup media on LAN to the backup system and copying this data to the application system.

Split mirror restore procedure

Perform the following steps:

1. In the Context List, select **Restore**.
2. Select the objects for restore and click them to display their properties.

Note Select the application system as **Target client** under the **Destination** tab. If the backup system is selected, standard restore to the backup system is performed.

3. Click **Restore**. The **Start Restore Session** dialog box appears.
4. Click **Next**.
5. Specify the report level and network load. Click **Next**.
6. Specify the split mirror restore options.
7. Click **Finish** to start the split mirror restore.

Note If LVM mirroring is used, a warning appears during the session, since the volume group LDEVs in the physical volume group on the application system do not have BC P9000 XP pairs assigned. This warning should be ignored.

Split mirror restore options

The following table explains the split mirror restore options.

Split mirror restore options

Data Protector GUI	Function
Mirror mode	Selects a P9000 XP Array configuration. Only the Business Copy P9000 XP configuration is supported.

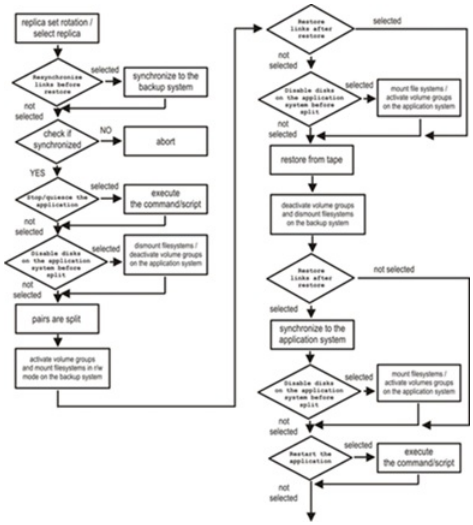
MU Number(s)	This option defines the mirror unit (MU) number(s) of a replica or a replica set from which the Data ProtectorP9000 XP Agent, according to the replica set rotation, selects the replica to be used in the restore session. The replica selection rule is described in the Data Protector Concepts Guide.
	
	You can specify one or more non-negative integer numbers, one or more ascending ranges of such numbers, or any combination of both. Use a comma as the separator character. Examples:
	
	`5`
	
	`7-9`
	
	`4,0,2-3`
	
	When a sequence is specified, it does not define the order in which the replicas are used.
	
	Default: `0` (nothing is specified).

Application system	Specifies the system to which your data will be restored. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).
Backup system	Specifies the system to which your data will be restored from the backup media on LAN.

Stop/quiesce the application	Optionally specifies the command/script to be run before the LDEV pairs are split (put into the SUSPENDED state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for stopping the application, dismounting the file systems that are not to be restored in the active session, but belong to the same volume group or disk, or preparing the volume group for deactivation. If this command/script fails, the command/script specified with the option **Restart the application** is not executed. Therefore, you need to implement a cleanup procedure in this command/script. Note that if the omnirc option `ZDB_ALWAYS_POST_SCRIPT` is set to `1`, the command/script specified with the option **Restart the application** is always executed.
Restart the application	Specifies the command/script to be run immediately after the LDEV pairs are resynchronized (put into the PAIR state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for restarting the application or mounting the filesystems.
Resynchronize links before restore	Directs the Data Protector disk array agent to synchronize the LDEV pairs, that is, to copy the application data to the disks which store backup data. This is necessary to prepare the disks for restore and to enable consistent data restore. If the paired LDEVs have been split (put into the SUSPENDED state) before the restore, and only some files need to be restored, then this option updates the backup system. This will ensure that the correct data is resynchronized to the application system. If this option is not selected, the synchronization is not performed. Default: not selected.
Disable disks on the application system before split	Directs the Data Protector disk array agent to disable disks on the application system, that is, dismount the filesystems and deactivate the volume groups. This is performed before the LDEV pairs are split. The disks are enabled after the links are restored. Note that only filesystems selected for restore are dismounted. If other filesystems exist in the volume group or on the disk, appropriate commands/scripts must be used to dismount these filesystems (specified with the options **Stop/quiesce the application** and **Restart the application**). You must always select this option for restore when you want to copy data from the backup system to the application system, that is, to incrementally restore links. The application system disks have to be disabled to provide data integrity after the links are restored, that is, data is copied. Default: selected.
Restore links after restore	Directs the Data Protector disk array agent to incrementally restore the links for the LDEVs that Data Protector has successfully restored to the backup system. The P9000 XP Agent also incrementally re-establishes links for the LDEVs for which the Data Protector restore failed. Default: selected.

The chart below provides detailed split mirror restore flow depending on the options selected.

Filesystem split mirror restore flow



Split mirror restore in a cluster

Split mirror restore in configurations with the application system in Serviceguard or a Microsoft server cluster requires additional steps.

Serviceguard procedure

1. Stop the filesystem cluster package:

   cmhaltpkg ApplicationPackageName

   This stops filesystem services and dismounts the mirrored volume group filesystem.
2. Deactivate the mirrored volume group from cluster mode and activate it in normal mode:

   vgchange -c n /dev/mirror_vg_name

   vgchange -q n -a y /dev/mirror_vg_name
3. Mount the mirrored volume group filesystem:

   mount /dev/mirror_vg_name /lv_name /mountpoint
4. Start split mirror restore.

   > **Important** When specifying the application system, specify the hostname of the application system *node* on which the mirrored volume group was activated in the normal mode (Deactivate the mirrored volume group from cluster mode and activate it in normal mode: of this procedure).

5. After the restore, dismount the mirrored volume group filesystem:

   umount /mountpoint
6. Deactivate the mirrored volume group in normal mode and activate it in cluster mode:

   vgchange -a n /dev/mirror_vg_name

   vgchange -c y /dev/mirror_vg_name
7. Start the filesystem cluster package:

   cmrunpkg ApplicationPackageName

Instant recovery

Instant recovery restores data directly from a replica to the source volumes, without involving a backup device. All data (entire volume group on UNIX systems or entire disk on Windows systems) in the replica is restored.

You can perform instant recovery using the Data Protector GUI or CLI .

Considerations

- Only first-level mirrors or snapshot volumes can be used for instant recovery. Second-level (cascading) mirrors and snapshot volumes are not supported.

- Instant recovery can be run with both replica types: split mirror and snapshot. The same instant recovery procedure applies in both cases.
- When instant recovery starts, Data Protector disables the application system. This includes dismounting filesystems and exporting volume groups (on UNIX systems only). Before this is done, filesystems' and volume groups' status is checked, and only mounted filesystems and imported volume groups are dismounted and exported. At the end of the session, dismounted filesystems are mounted and exported volume groups are imported to the same mount points as were used during backup.
- You cannot start several instant recovery sessions using the same disk on the application system at once. A session can be started only after the preceding session using the same source volume on the application system finishes synchronization.

Important After instant recovery, restored filesystems are mounted to the same mount points/drive letters as they were at the backup time. If these mount points/drive letters have other filesystems mounted, these filesystems are automatically dismounted before instant recovery, and the restored filesystems are mounted afterwards.

Important Instant recovery does not recover databases or applications. It only synchronizes the primary LDEVs on the application system with the secondary LDEVs on the backup system. To recover a database or application data, you need to perform additional steps.

Prior to instant recovery, Data Protector:

- checks the volume group configuration (on UNIX systems only)
- verifies the replica

These steps assure that data in the replica has been left intact after the replica was created. If either of these steps fails, the instant recovery session fails.

Once the replica is restored, it can be left unchanged or resynchronized, depending on the selected instant recovery options.

Instant recovery procedure

Before performing a disk image instant recovery, manually dismount the disks before the instant recovery, and re-mount them afterwards.

Instant recovery using the GUI

Perform the following steps:

1. In the Context List, select **Instant Recovery**.
2. Select the backup session whose replica you want to use for instant recovery. This can be done by selecting:
   - a zero downtime backup session ID and the corresponding ZDB backup specification name:

     In the Scoping Pane, expand **Restore Sessions** and select the session from a list of ZDB-to-disk and ZDB-to-disk+tape sessions.
   - a backup object type, a ZDB backup specification name, and a ZDB session ID:
     a. In the Scoping Pane, expand **Restore Objects**.

        Backup object types are displayed. Examples of backup object types are filesystem, disk Image, SAP R/3, and Microsoft SQL Server.

     b. Expand the backup object type for which you want to perform instant recovery.

        Available backup specifications used in ZDB-to-disk or ZDB-to-disk+tape sessions for the selected backup object type are displayed.

     c. Expand the ZDB backup specification containing the required objects. Available ZDB sessions are displayed.

   In the Scoping Pane, click the desired ZDB session.

   The application system and its mount points/drive letters backed up during the selected session are displayed.
3. Select the application system and specify the instant recovery options.
4. Click **Restore** to start the instant recovery, or **Preview** to preview it.
5. Select **Start Restore Session** to start instant recovery, or **Start Preview Session** to start the preview. Click **OK**.

Note You cannot use the CLI to perform instant recovery from ZDB to disk+tape after exporting or overwriting the media used in the session. Use the GUI instead. Note that backup media must not be exported or overwritten even after an object copy session.

Instant recovery using the CLI

Complete the following steps:

1. all available ZDB-to-disk and ZDB-to-disk+tape sessions, identified by the session ID:

   ```
   omnidbxp -ir -session -list
   ```

   From the output, select the backup session whose replica you want to use for instant recovery.

2. Execute:

   ```
   omnir -host ClientName -session SessionID -instant_restore [INSTANT_RECOVERY_OPTIONS]
   ```

   where the meaning of the options is as follows:

ClientName	The application system name.
SessionID	The backup session ID

For INSTANT_RECOVERY_OPTIONS , see Instant recovery options .

Instant recovery options

Instant recovery options are listed below:

Data Protector GUI/CLI	Function
Check the data configuration consistency/ -check_config	If this option is selected in the GUI or specified in the CLI, the current configuration of the participating volume groups is compared with the volume group configuration as it was during the ZDB session and which is stored in the XPDB. If the configuration has changed since the ZDB session, the instant recovery session aborts. Additionally, the CRC information for the selected LDEV pairs stored in the XPDB is compared to the current CRC information. If the items compared do not match, the instant recovery session aborts. A RAID Manager Library flag, which is set whenever the selected secondary LDEV is accessed/changed by any process (including non-Data Protector processes) is checked. If the flag is set, the session fails with an appropriate warning. **Serviceguard clusters:** When instant recovery is performed to some other node than the one from where the volumes were backed up, the current volume group configuration on the target node is different from the volume group configuration kept in the XPDB. In such a case, the XPDB volume group configuration data is replaced by the current volume group configuration data on the target node, and the session does not abort. When performing instant recovery to some other node than the one that was backed up, select (GUI) or specify (CLI) this option. Default (GUI): selected.

Keep the replica after the restore/ -keep_version	If this option is selected in the GUI or specified in the CLI, the LDEV pairs involved in the current instant recovery session are split and left in the SUSPENDED state after the restore of data is complete. In the opposite case, the LDEV pairs are left in the PAIR state. Even if the instant recovery is successful, it is recommended to keep the replica until the next ZDB session. **Linux systems:** This option must be selected (GUI) or specified (CLI) if the replica set consists of more than a single replica. Default (GUI): selected.

Instant recovery and LVM mirroring

If you use an LVM mirroring configuration, perform the following instant recovery steps:

1. Reduce all logical volumes which have LVM mirrors, specifically, reduce or remove the mirrors that reside on primary LDEVs that are not paired with secondary LDEVs on the P9000 XP Array. This ensures that restored data cannot be accidentally overwritten by a synchronization of the LVM mirror.

   Rebuild the LVM mirroring environment to the previous configuration.
2. Start the instant recovery session.
3. Extend the logical volume containing LVM mirroring disks (using the `lvextend -m` command) with the LVM mirror disk that was previously excluded from the logical volume.

Instant recovery in a cluster

For information about and instructions for instant recovery in configurations with the application system in Serviceguard or a Microsoft server cluster, see Instant recovery in a cluster.

Troubleshoot

This section lists general checks and verifications plus problems you may encounter when using the P9000 XP Array integration.

- Ensure that the latest official Data Protector patches are installed.

Checks and verifications

- On the application and backup systems, examine system errors logged into the `debug.log` file residing in the default Data Protector log files directory.
- Ensure that RAID Manager Library is correctly installed on the application system and the backup system and is accessible by the P9000 XP Agent, that is, listed in the library path.

General problems

Problem

A process stops responding when attempting to read data from a secondary LDEV (SVOL) in the PAIR state

When a secondary LDEV (S-VOL) is presented to the backup system, the LDEV pair it belongs to is in the PAIR state, and a process attempts to read the data from the secondary LDEV, the process stops responding. If such a problem occurs, all other processes attempting to read the data from such a secondary LDEV, for example the `pvscan` command, are affected, too.

Action

Unpresent the secondary LDEV from the backup system or unzone them.

> ⚠ **Caution** Under the described circumstances, you should not try to restart the backup system before resolving the issue. Doing so may result in a data loss due to corruption of the involved file system. If the file system is corrupt, the backup system may even not be able to start up.

Problem

SSEA continuous access (CA) ZDB backups stop working if the target CA ports are changed.

Action

Recreate the CA port pairs in order to have a working SSEA CA ZDB backup.

Backup problems

Problem

You cannot select the P9000 XP mode in the Data Protector user interface when creating a ZDB backup specification

Action

Check that the P9000 XP Agent integration module is installed on the application and backup systems. To do that, open the cell_info file located on the Cell Manager in the following directory:

Windows systems: Data_Protector_program_data\Config\server\cell\cell_info

UNIX systems: /etc/opt/omni/server/cell/cell_info

File contents should look similar to:

```
-host "sap001.company.com" -os "HPs800 hp-ux-11.10" -cc A.10.30 -da A.10.30 -ssea A.10.30

-host "sap002.company.com" -os "HPs800 hp-ux-11.10" -cc A.10.30 -da A.10.30 -ma A.10.30 -ssea A.10.30
```

Problem

On the application system, dismounting of a filesystem fails

Action

In the Stop/quiesce the application command line or Stop/quiesce the application script, stop all processes using the filesystem.

Use appropriate operating system tools or utilities to get a list of processes that are using the filesystem in order to identify any processes that lock the filesystem. For example, lsof on HP-UX.

Problem

On the backup system, mounting of a filesystem fails

Action

Check that the mountpoint directory exists on the backup system and that it is writable. On Windows Server 2008 systems, if the option **Automatically dismount the file systems on the application system** is selected, check if any processes are locking the filesystem.

Problem

Pair synchronization fails (the split fails)

To successfully split the pair, the P9000 XP Agent first checks its status. Pairs can only be split (in PSUS/SSUS status) after they are synchronized (in PAIR status). P9000 XP Agent checks the status of links after every 2 seconds and retries 10 times.

Action

Increase the time frame for synchronization by setting SSEA_SYNC_RETRY and SSEA_SYNC_SLEEP_TIME options.

Problem

P-VOL has no paired S-VOL

Action

Check the P9000 XP Array configuration as follows:

BC P9000 XP: All P-VOLs on the application system must have associated BC P9000 XP S-VOLs on the backup system.

CA P9000 XP: All P-VOLs on the application system must have associated CA P9000 XP S-VOLs on the backup system.

CA+BC P9000 XP: All P-VOLs on the application system must have associated CA P9000 XP S-VOLs on the backup system and all S/P-VOLs must have BC P9000 XPS-VOLs.

Problem

Invalid pair state of LDEVs

Action

Check the link state. If the link is split, use the **Prepare/resync the mirror disks at the start of the backup** option.

Configure and start RAID Manager P9000 XP instances manually. You can get a list of LDEVs from the backup session report. Alternatively, with newer models of the P9000 XP Disk Array Family, you can use also P9000 XP Remote Web Console (formerly known as Command View XP).

Problem

Missing details for a specific LDEV/MU# are reported

```
[Warning] From: SSEA@machine_app.company.com "" Time: 17.10.2008. 10:41:27 Failed to get a BC pair for LDEV 55, MU# 1 in RAID 35371. (Details unknown.) [Normal] From: SSEA@machine_app.company.com "" Time: 17.10.2008. 10:41:27 Resolving of backup objects on the application system completed. [Normal] From: SSEA@machine_bu.company.com "" Time: 17.10.2008. 10:41:27 Resolving backup objects on the backup system. [Critical] From: SSEA@machine_bu.company.com "" Time: 17.10.2008. 10:41:29 Resolving of backup objects on the backup system failed.
```

Action

1. In the backup specification, specify an existing and configured LDEV/MU# on the backup system, or ensure that LDEV/MU# stated in the output is not set in the P9000 XP LDEV exclude file.
2. Restart the session.

Problem

Filesystems not resolved on the backup system

On Windows systems, in some initial configurations filesystems may not be resolved on the backup system. The filesystems do not show up at all, even after a manual pair or split operation is performed on the disk array.

Action

Using the device manager, remove the problematic disks from the disk array and rescan the backup system.

Problem

During a zero downtime backup session, when a second replica is selected from the replica set specified by the ZDB backup specification option MU number(s), the session fails

If more than one replica is specified in the ZDB backup specification option **MU number(s)**, and a ZDB session is run which, according to the replica selection rule, selects the second or any subsequent replica, the session fails.

Action

The problem may be related to the duplicate disk signatures assigned to the target volumes by the Windows operating system.

Perform the following:

1. Unpresent all involved target volumes from the backup system.

2. On the backup system, clean the Registry.

   Windows Server 2008: Run the DiskPart utility by invoking the `diskpart` command. Inside the DiskPart shell, execute the command `automount scrub`.

3. Put all involved P-VOL - S-VOL pairs into the SUSPENDED state.
4. Present the target volumes to the backup system.
5. Start the ZDB session once again.

Problem

A warning message is displayed in the Windows event logs when using the P9000 XP Array with two or more MU number(s).

If two or more **MU number(s)** are used with P9000 XP Array, a warning message is displayed in the Windows event logs.

Action

No action is required as this warning does not have a negative impact on the backup. The warning message appears when more than one mirror of the same disk is present on a Windows system.

Split mirror restore problems

Problem

Session fails with the following message:

```
[Major] From: SSEA@machine.company.com "" Time: 17.10.2008. 11:06:46 Filesystem /dev/bc_nested/hfs could not be dismounted from
```

```
/BC/fs/HFS/usr/sbin/vgchange -a n /dev/bc_nested [Major] From: SSEA@machine.company.com "" Time: 17.10.2008. 11:06:47 [224:8]Volume group /dev/bc_nested could not be deactivated.
```

Action

Ensure that the filesystem/volume group is not in use (you are positioned in the filesystem mountpoint directory), and then restart the session.

Problem

LDEV pair is in “STAT_COPY” state when split mirror restore starts, and the session fails with:

```
[Critical] From: SSEA@machine.company.com "" Time: 16.10.2008. 17:25:00 The following BC pairs have an invalid status for the requested operation: SEQ# LDEV Port TID LUN MU# Status SEQ# LDEV ---------- 35371 00A8h ( 168) CL1-D 1 3 0 STAT_COPY 35371 01A5h ( 421) 35371 00A8h ( 168) CL1-D 1 3 0 STAT_COPY 35371 01A6h ( 422) ---------- [Critical] From: SSEA@machine.company.com "" Time: 16.10.2008. 17:25:00 Failed to resolve objects for Instant Recovery.
```

Action

Wait until the LDEV pair is in “PAIR” or “PSUS/SSUS” status, and then restart the session.

Instant recovery problems

Problem

LDEV pair is in “STAT_COPY” state when split mirror restore starts, and the session fails with:

```
[Critical] From: SSEA@machine.company.com "" Time: 16.10.2008. 17:25:00 The following BC pairs have an invalid status for the requested operation: SEQ# LDEV Port TID LUN MU# Status SEQ# LDEV ---------- 35371 00A8h ( 168) CL1-D 1 3 0 STAT_COPY 35371 01A5h ( 421) 35371 00A8h ( 168) CL1-D 1 3 0 STAT_COPY 35371 01A6h ( 422) ---------- [Critical] From: SSEA@machine.company.com "" Time: 16.10.2008. 17:25:00 Failed to resolve objects for Instant Recovery.
```

Action

Wait until the LDEV pair is in “PAIR” or “PSUS/SSUS” status, and then restart the session.

Configure 3PAR StoreServ Storage

This topic describes how to configure the Data Protector 3PAR StoreServ Storage integration, and how to perform zero downtime backup and instant recovery using the 3PAR StoreServ Storage integration through native storage system support built-in in the Data Protector P6000 / 3PAR SMI-S Agent.

The following prerequisites apply:

- Obtain or install:

  Data Protector licenses and components:

  - Appropriate zero downtime backup extension and instant recovery extension licenses-to-use (LTU).
  - Backup and Application hostname should match the name of the host on 3PAR as seen from 3PAR Management console or by running 3PAR CLI command showhost. The hostname is case-sensitive.
  - P6000 / 3PAR SMI-S Agent installed on both the application system and the backup system.
  - An appropriate multi-path device management software.

    The software must be installed on the application system and the backup system.

    HP-UX systems: Secure Path

    On HP-UX 11.31 systems, the multi-path device management software is not required since the operating system has native device multi-pathing capability.

    Linux systems: Device Mapper Multipath Enablement Kit for Disk Arrays 4.2.0 or newer version.

    To configure the installed multi-path device management software:

    1. Start the multipath daemon and run the following command to configure the daemon so that it gets started during system startup:

       Red Hat Enterprise Linux: `chkconfig multipathd on`

       SUSE Linux Enterprise Server: `chkconfig boot.multipath on`

    2. Prevent the multipath device management software from queuing for unavailable disk volumes by modifying its configuration file.

       Add the following line into the `defaults` section of the file `/etc/multipath.conf`:

       ```
       no_path_retry        fail
       ```

       Ensure that this `no_path_retry` parameter value is not overridden by analogous entries in the `device` sections of the same file in which the corresponding 3PAR storage systems are configured.

    3. Ensure that the correct preferred names are used for pathnames that are referencing the same device for physical volumes as they are used in device-mapper multipathing.

       Open the `lvm.conf` file, residing in the `/etc/lvm/` directory, and set the following variable:

       ```
       preferred_names = [ "^/dev/mpath/", "^/dev/mapper/mpath", "^/dev/[hs]d" ]
       ```

- Make sure the same operating system version is installed on both the application system and the backup system.
- If the application system and the backup system reside in a Data Protector cell with secured clients, ensure that access between both systems is allowed in both directions.
- Connect a storage system of the 3PAR StoreServ Storage family to the application and backup systems through the SAN. The backup system must be connected to the same SAN as the storage system of the 3PAR StoreServ Storage family.
- Source volumes must have *snapshot space* (*copy space*) in a storage system's Common Provisioning Group (CPG) associated with.
- You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk. In case of ZDB, you must use the second way:
  - \\.\DriveLetter:, for example: \\.\E:

    > When a drive letter is specified for the volume name, the volume is not being locked during the backup. A volume that is not mounted or mounted as an NTFS folder cannot be used for disk image backup.

  - \\.\PHYSICALDRIVE#, where # is the current number of the disk you want to back up. For example: \\.\PHYSICALDRIVE3
- **[Linux systems:]** Make sure you make logical volumes and volume groups inside multipath devices. Use the following commands:

```
fdisk /dev/mapper/mpathb
```

```
n
```

```
p
```

```
w
```

```
pvcreate /dev/mapper/mpathb_part1 -ff
```

```
vgcreate vg_mpathb /dev/mapper/mpathb_part1
```

```
vcreate vg_mpathb -L 19.8G -n lvm_mpathb
```

```
mkfs.ext3 /dev/vg_mpathb/lvm_mpathb
```

```
mount /dev/vg_mpathb/lvm_mpathb /sap3par/SAPDATA
```

Add the disk to `/etc/fstab` directory.

Note ZDB backup is not supported for volumes that were migrated from another 3PAR array.

The following limitations apply:

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- If replica is tracked for instant recovery, the volumes that are made active by applying either the "Host set" or the "Port presents" VLUN template types, cannot be used as source volumes.

For information on either of the following items, see Release Notes:

- General Data Protector and integration-specific limitations
- Supported platforms and integrations
- Supported backup and connectivity topologies

Configure the integration

Before you start with the configuration, make sure the prerequisites listed in above (for P6000 / 3PAR SMI-S Agent) or in Microsoft Volume Shadow Copy Service (for 3PAR VSS Agent) are fulfilled.

To prepare the Data Protector 3PAR StoreServ Storage integration for use with a storage system of the 3PAR StoreServ Storage family, you must perform the mandatory configuration step. In this step, you need to provide a Data Protector 3PAR StoreServ Storage integration agent the data which the agent will use to establish connection to a Common Information Model Object Manager (CIMOM) provider of your choice. To integrate with this storage system family, Data Protector can use 3PAR VSS Agent and P6000 / 3PAR SMI-S Agent (hereafter both referred to as **Data Protector 3PAR StoreServ Storage integration agent**).

CIMOM provider connection configuration

The connection configuration data includes user credentials that you must add to the ZDB database (the 3PAR StoreServ part of SMISDB) in advance, before running Data Protector instant recovery (IR) sessions. The credentials are bound to a specific application system in the Data Protector cell. The Data Protector 3PAR StoreServ Storage integration agent then reads the credentials from the ZDB database each time a zero downtime backup or instant recovery session for data residing on a 3PAR StoreServ system is started.

Connection configuration data

To be able to connect to a CIMOM provider and perform zero downtime backup or instant recovery sessions, the Data Protector 3PAR StoreServ Storage integration agent needs the following information:

- Fully qualified domain name or IP address of the system where the CIMOM service is running

  In case the system has multiple IP addresses configured, the address by which the system can be accessed by the Data

Protector ZDB agent should be used.

- Whether the connection uses Secure Sockets Layer (SSL)
- Port number of the port on which the CIMOM service is accepting requests
- Username and password

  These credentials must belong to a 3PAR StoreServ system user account with the *Edit* privilege level in the following 3PAR StoreServ system virtual domains, depending on the effective disk array configuration:

  - Domain of the application system and the source volumes-When the source volumes and the application system belong to a specific domain
  - All domains of a domain set-When the application system and the source volumes belong to this domain set
  - All existing domains-When the application system and the source volumes do not belong to any domain

The above information should be provided in advance for each CIMOM provider that the Data Protector 3PAR StoreServ Storage integration agent should connect to. It is stored in the 3PAR StoreServ Storage part of the SMISDB.

Configuration procedure

To add the required user credentials for an application system where the CIMOM service is running, use the Data Protector `omnidbzdb` command. Follow the steps:

1. Identify the source volumes that will be involved in the ZDB-to-disk or ZDB-to-disk+tape sessions.
2. Identify the 3PAR StoreServ system virtual domains or domain set to which the application system and the source volumes belong.
3. Choose a disk array user account that has a proper privilege level on the corresponding domains. Identify and write down its username and password that you will need in the next step.
4. Using the `omnidbzdb --diskarray 3PAR --ompasswd --add` command , add the username and password that you acquired in the previous step to the ZDB database, providing the name of the application system you identified in Identify the source volumes that will be involved in the ZDB-to-disk or ZDB-to-disk+tape sessions. of this procedure.
5. Using the `omnidbzdb --diskarray P10000 --ompasswd --check` command (for 3PAR VSS Agent) or the `omnidbzdb --diskarray 3PAR --ompasswd --check` command (for 3PAR VSS Agent or P6000 / 3PAR SMI-S Agent), verify that the Data Protector 3PAR StoreServ Storage integration agent can connect to the disk array using the configured user authentication data.

Tip For each application system, you can add user credentials of multiple disk array user accounts. When several are configured for the same system, the Data Protector 3PAR StoreServ Storage integration agent checks user accounts in alphabetical order and uses the first account with *Edit* privilege level on the application system and the source volumes.

Backup

Zero downtime backup sessions that involve a storage system of the 3PAR StoreServ Storage family can be initiated:

- Through the Data Protector Microsoft Volume Shadow Copy Service integration - if the application and backup systems are running on a Windows operating system, and have the Data Protector P6000 / 3PAR SMI-S Agent installed
- Natively - if the application and backup systems are running on Windows or UNIX operating system and have the Data Protector P6000 / 3PAR SMI-S Agent installed

ZDB types

Using the 3PAR StoreServ Storage integration through the Data Protector P6000 / 3PAR SMI-S Agent, you can perform all zero downtime backup types:

- **ZDB to disk**

  The replica produced is kept on a disk array until reused. This replica becomes part of the replica set and can be used for instant recovery.

  ZDB to disk is performed if the option **Track the replica for instant recovery** is selected in a ZDB backup specification, and **To disk** is selected when running/scheduling a backup.

- **ZDB to tape**

  The replica produced is streamed to backup media, typically tape, according to the tape backup type you have selected (Full, Incr, Incr1-9).

  This replica is deleted after backup if the option **Keep the replica after the backup** is cleared for the backup

specification. If this option is selected, the replica remains on a disk array until reused and becomes part of the replica set. However, it cannot be used for instant recovery.

- **ZDB to disk+tape**

  The replica produced is kept on a disk array until reused and is also streamed to backup media according to the tape backup type you have selected (Full, Incr, Incr1-9). This replica becomes part of the replica set and can be used for instant recovery.

  ZDB to disk+tape is performed if the option **Track the replica for instant recovery** is selected in a ZDB backup specification, and **To disk+tape** is selected when running/scheduling a backup.

ZDB for 3PAR Remote Copy environments

3PAR Remote Copy Software provides enterprise and cloud data centers with autonomic replication and disaster recovery technology that allows the protection and sharing of data from any application simply, efficiently, and affordably.

In the Remote Copy environments, the 3PAR storage system containing source volumes is known as a **local (primary) disk array**, while the 3PAR storage system on which the replicas are created is a**remote (secondary) disk array**. The mirrored source and target volumes constitute a **copy set**. Remote copy configurations are based on the relationship between a pair of storage systems, known as the remote copy pair. Within a remote copy pair, the primary storage system is the system that holds the volumes that are copied to the backup storage system.

Data Protector allows you to perform zero downtime backups of the 3PAR Remote Copy replica. The data backed up in 3PAR remote copy configurations can be restored using either instant recovery or the standard Data Protector restore from tape procedure.

Supported 3PAR Remote Copy configurations

3PAR Remote Copy Configuration	Supported by Data Protector
1-to-1	Yes
N-to-1	No
1-to-N	No

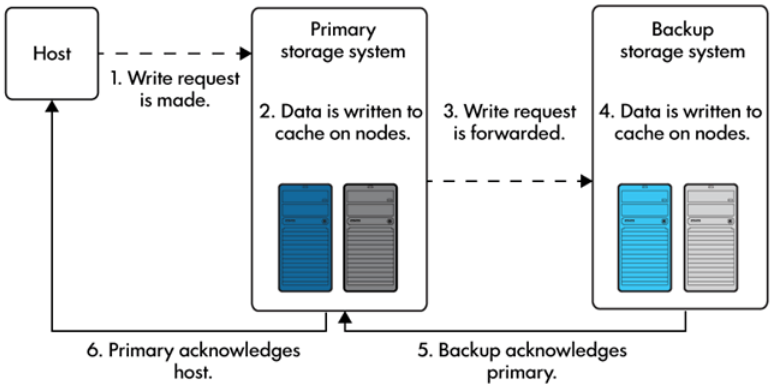
Data Protector supports the 1-to-1 configuration only. A 1-to-1 remote copy configuration consists of a single remote copy pair. Both unidirectional and bidirectional 1-to-1 configurations.

3PAR remote copy modes

Data Protector supports Synchronous and Periodic modes. The modes supported are briefly explained below.

Synchronous Mode

When remote-copy volume groups operate in synchronous mode, a host write must be committed to both the primary and the backup storage systems before the primary array acknowledges the host write. Remote copy in synchronous mode is illustrated below.

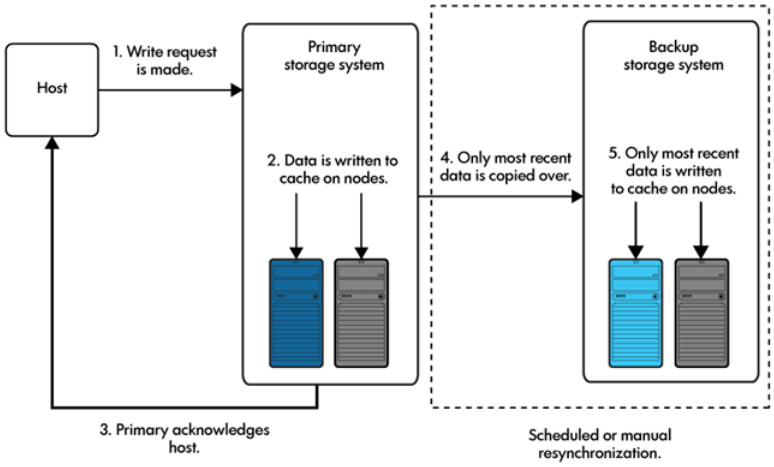


Periodic Mode

When remote-copy volume groups operate in periodic mode, the host sends a write request to the primary system. As soon as the data is written into cache on the primary system, 3PAR Remote Copy acknowledges the host write. Remote copy in period mode is illustrated below. The data will be synchronized to the backup system during the scheduled periodic time interval, or during the manual sync operation.

In the periodic mode, before creating the replica, the sync operation is triggered to sync the data between the primary and

secondary storage volumes. If the sync operation is not complete within specified duration of time, backup of the volume is ignored.

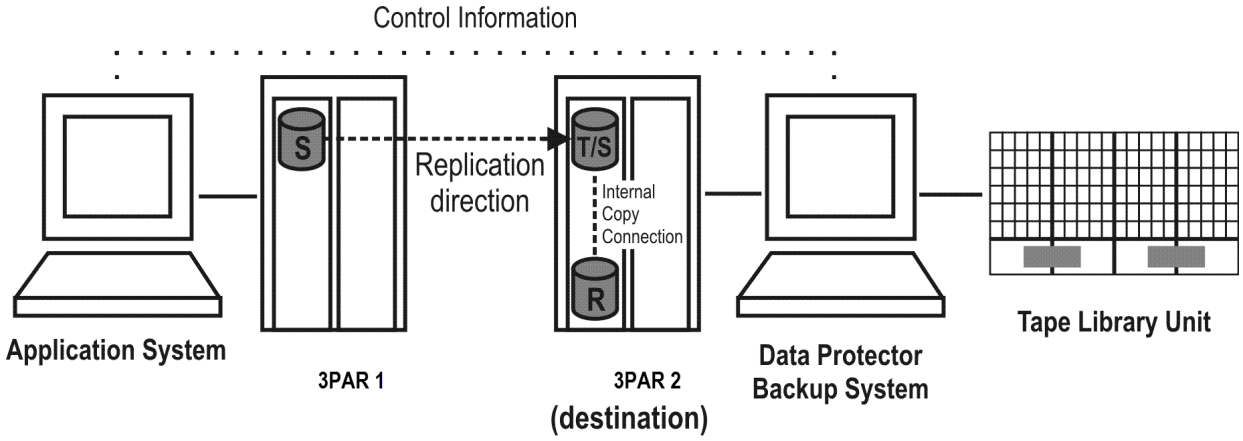


ZDB 3PAR Remote Copy scenarios

3PAR Remote Copy enables the following backup scenarios:

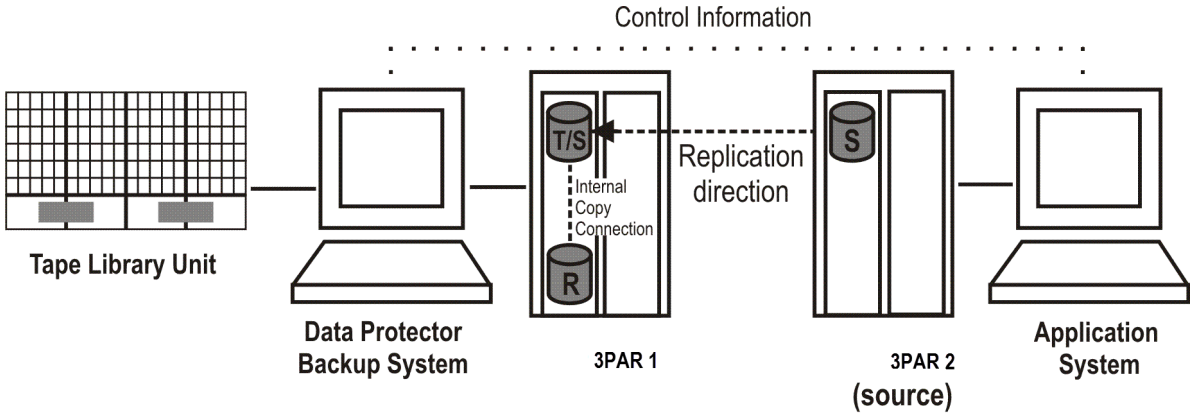
- Ideal, or non-failover scenarios, where replicas are always created on the array remote to *primary*.

  A non-failover scenario



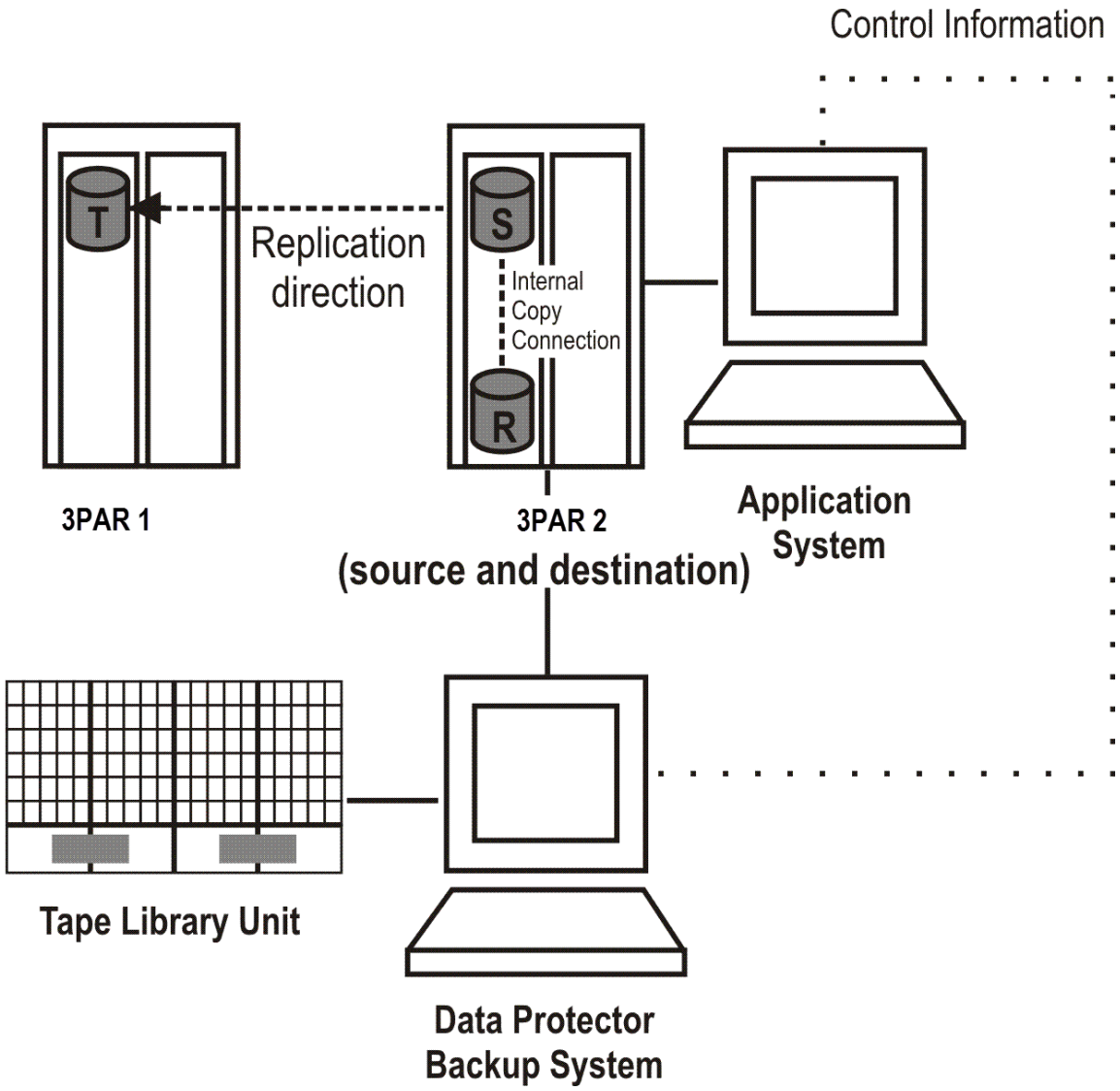
- Failover scenarios, where the roles of original source and destination are reversed after a failover. Replicas in such scenarios can be created:
  - On the disk array remote to the current source (**Follow direction of replication** backup option selected in the backup specification). It means that after a failover, the replication direction is reversed and the replicas are created on the array that was originally a source 3PAR array. Failover scenario 1 depicts an environment where the location of replica creation was switched after a failover.

    Failover scenario 1



- On the array remote to primary (**Maintain replica location** backup option is selected in the backup specification). It means that after a failover, replica location is maintained and replicas continue on the destination array that has now become a source array. Note that for the time of replica creation, the source array performance may be affected.

  Failover scenario 2



Consider the following:

- If you intend to always follow the replication direction, make sure the backup system has access to both local and remote 3PAR array storage systems. Otherwise, after a failover, ZDB session fails because the replication direction switches and the backup system is no longer visible to the array where the replicas are created.

Replica set rotation

In the 3PAR Remote Copy non-failover scenarios, replicas are always created on the array remote to primary. If the existing replica count (on the array where new replicas are) exceeds the specified number of replicas rotated, the oldest replica is deleted and the new one is created in its place (ensuring the maximum number of replicas is always within the defined rotation set).

In the 3PAR Remote Copy failover scenarios, replicas are created either on:

- The array remote to current source (or on the primary disk array)
- The array remote to primary

In the first case, the number of replicas in a rotation set is only checked on the current destination array. The replicas created on the current source, which was a destination before a failover, are ignored. Therefore, there are situations when two replica sets are created on both the source and destination arrays.

In the second case, replica set rotation verification happens in a normal way.

Note Replica rotation set is only created if you select the option **Keep the replica after the backup** and specify **Number of replicas rotated**. Without these options specified, the replica is deleted from the array after the backup to tape is completed.

The following limitations apply:

- Consider all the limitations that apply to the Data Protector 3PAR StoreServ Storage integration.
- The selected volumes are backed up only if the remote copy group is in the *Start* state.
- If a switchover operation is performed on the 3PAR remote copy groups, the roles of primary and secondary array are reversed. Data Protector does not consider this as a remote copy group failover, and continues to create the replica on the secondary array even after the switchover operation.

ZDB in HP-UX LVM mirroring environments

Create the backup specification

This section guides you through the process of configuring a ZDB backup specification for backing up data that resides on a storage system of the 3PAR StoreServ Storage family.

Data Protector 3PAR Remote Copy Omnirc Variables

Data Protector performs a periodic sync operation before the backup is executed. This periodic sync may take more time if your arrays span across different data centers. Therefore, you can use the below omnirc variables to set the wait time, and retry count for the periodic sync operations. Note that if the sync is not completed, the backup session may be aborted.

- ZDB_WAIT_FOR_PERIODIC_SYNC_TO_COMPLETE
  - This variable sets the time period for the remote copy group periodic sync to complete.
  - Default value: 300 seconds, for Windows and Linux.
- ZDB_WAIT_FOR_PERIODIC_SYNC_RETRY_COUNT
  - This variable sets the number of retries to check the status of the remote copy periodic sync completion.
  - Default value: 1

Complete the following steps:

1. In the Context List, select **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**. Right-click **Filesystem** (for both object types: filesystem and disk image) and click **Add Backup**.

   The Create New Backup dialog box appears.

   In the Filesystem pane, select the **Blank Filesystem Backup** template or some other template which you might have created.

   Select **Snapshot or split mirror backup** as **Backup type** and **3PAR** as **Sub type**. For description of options, press **F1**.

   Click **OK**.
3. Under Client systems, select **Application system** and **Backup system**. If the application system is part of a server cluster, select the virtual server.

   Under Replication mode, select **3PAR Local Copy** or **3PAR Remote Copy**, based on your requirements. If you select 3PAR Remote Copy, specify the choice for replica handling during failover scenarios.

   Under Snapshot management options, **Virtual copy** is preselected for the snapshot type and cannot be changed.
4. Under Replica management options, specify if you want to keep the replica after backup, the number of rotated replicas, and whether to track the replica for instant recovery. For more information, press **F1**.
5. Under Application system options and Backup system options, specify other zero downtime backup options as desired.

   Click **Next**.
6. Select the desired backup objects.

   Filesystem backup: Expand the application system and select the objects to be backed up. Note that all drive letters or mount points that reside on the system are displayed. You must select only the objects that reside on the disk array, otherwise the ZDB session fails.

   In remote copy backups, if local volumes are selected, the ZDB session falls back to the local copy for the selected local volumes. A warning will be displayed for the same.

   Click **Next**.

Disk image backup: Click **Next**.

7. Select the devices to be used in the backup session.

   To create additional copies (mirrors) of the backup image, specify the desired number of mirrors by clicking **Add mirror** or **Remove mirror**. Select separate devices for the backup image and each mirror.

   Click **Next**.

8. In the Backup Specification Options group box, click **Advanced** and then the **3PAR** tab to open the options pane with 3PAR StoreServ Storage specific backup options.

   You can specify Application system options and modify all other options, except **Application system** and **Backup system** (note that you can change them after you save the ZDB backup specification).

   Click **Next**.

9. In the **Backup Object Summary** page, specify additional options.

   Filesystem backup: You can modify options for the listed objects by right-clicking an object and then clicking **Properties**. For information on the object properties, press **F1**.

   Disk image backup: Follow the steps:

   a. Click **Manual add** to add disk image objects.

   b. Select **Disk image object** and click **Next**.

   c. Select the client system. Optionally, enter the description for your object. Click **Next**.

   d. Specify General Object Options and Advanced Object Options. For information on these options, press **F1**.

   e. In the Disk Image Object Options window, specify disk image or raw logical volume sections.

   f. Click **Finish**.

   Click **Next**.

10. Click **Save As** to save your ZDB backup specification. Optionally, you can click **Save and Schedule** to save, and then schedule the backup specification.

Backup options

The following tables describe the ZDB-related backup options that you can modify when configuring ZDB backup specifications that include storage systems of the 3PAR StoreServ Storage family.

Client systems

Application system	The system on which the application runs. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).
Backup system	The system to which your data will be replicated (backed up), and from which the backup data is copied to a backup device.

Replica management options

Keep the replica after the backup	If configuring a ZDB to tape, select this option to keep the replica on the disk array after the zero downtime session. The replica becomes part of a replica set (specify a value for the option **Number of replicas rotated**). Unless the additional option **Track the replica for instant recovery** is selected, the replica is *not* available for instant recovery. If this option is not selected, the replica is removed at the end of the session. If the option **Track the replica for instant recovery** is selected, this option is automatically selected and cannot be changed.

Number of replicas rotated	This option is only available if the option **Keep the replica after the backup** is selected. During ZDB sessions, Data Protector creates a new replica and leaves it on the disk array until the value specified for the option **Number of replicas rotated** is reached. After that, the oldest replica is deleted and a new one created. The number of standard snapshots or vsnaps is limited by the 3PAR StoreServ Storage system. Data Protector does not limit the number of replicas rotated, but the session fails if the limit is exceeded. Default: 1.
Track the replica for instant recovery	This option is only available if the option **Keep the replica after the backup** is selected. Select this option to perform a ZDB-to-disk or ZDB-to-disk+tape session and leave the replica on the disk array to enable instant recovery. Specify also a value for the option **Number of replicas rotated**. If this option is not selected, you cannot perform instant recovery using the replica created or reused in this session.

Replication mode

3PAR Local Copy	Select this option to configure a ZDB backup specification for 3PAR storage systems, which are not part of the remote copy group. If a volume that is part of the 3PAR Remote Copy group is selected for the backup, this volume will not be considered as part of the Remote Copy group, and backup continues to create the replica on the primary array.
3PAR Remote Copy	Select this option to configure a ZDB backup specification for 3PAR storage systems, which are part of the remote copy group. If a volume that is not part of the 3PAR Remote Copy group is selected for backup, this volume will be considered as part of the Remote Copy group, and backup continues to create the replica on the primary array.
Follow direction of replication	This option is only available if **3PAR Remote Copy** option is selected. Select to follow the replication direction and create replicas on the disk array remote to the current source. After a failover, the replication direction is reversed and the replicas are created on the disk array that was originally a source 3PAR storage system.
Maintain replica location	This option is only available if **3PAR Remote Copy** option is selected. Select to maintain replica location and create replicas on the disk array remote to primary array. After a failover, replicas will continue on the destination disk array that became the primary 3PAR storage system during the failover.

Application system options

Dismount the filesystems on the application system before replica generation	Select this option to dismount the filesystems on the application system before replica creation and remount them afterwards. Additionally, when entire physical drives entire disks or logical volumes (on UNIX systems) are selected as backup objects in a disk image backup specification, selecting this option will dismount and later remount all filesystems on these objects. If any of these filesystems cannot be dismounted, the backup session fails. If an integrated application (for example, Oracle Server) exclusively controls data I/O on each physical drive, disk, or logical volume that will be backed up, the dismount operation is not needed. In such a case, you can leave this option cleared. Default: not selected.
Stop/quiesce the application command line	If a command is specified in this option, it is invoked on the application system immediately before replica creation. An example is to stop applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option. If the command fails, the command specified in the option **Restart the application command line** is not invoked. Thus, you may need to implement a cleanup procedure in the command specified in **Stop/quiesce the application command line**. If the `omnirc` option `ZDB_ALWAYS_POST_SCRIPT` is set to `1`, the command specified in the option **Restart the application command line** is always invoked.
Restart the application command line	If a command is specified in this option, it is invoked on the application system immediately after replica creation. An example is to resume operation of applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option.

Backup system options

Use the same mountpoints as on the application system	This option is not available if the application system is also the backup system (a single-host configuration). If this option is selected, the paths to mount points used for mounting the filesystems of the replica on the backup system are the same as paths to mount points where source volume filesystems were mounted on the application system. If the mount points are already in use, the session fails. For such circumstances, you must select the option **Automatically dismount the filesystems at destination mountpoints** in order for the session to succeed. Default: not selected.

Root of the mount path on the backup system	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. Specifies the root directory under which the filesystems of the replica are mounted. Where exactly the filesystems are mounted depends on how you define the option **Add directories to the mount path**. **Note** For the SAP R/3 integration, the option is not applicable (the mount points created are always the same as on the application system). Defaults: **UNIX systems:** /mnt
Add directories to the mount path	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. This option enables control over the created mount points. It defines which subdirectories will be created in the directory defined with the **Root of the mount path on the backup system** option. When Session ID is used in path composition, this guarantees unique mount points.
Automatically dismount the filesystems at destination mountpoints	If the mount points are in use (for example, volumes involved in the previous session may still be mounted) and this option is selected, Data Protector attempts to dismount the mounted filesystems. If the option is not selected and the mount points are in use, or if the option is selected and the dismount operation fails, the session fails. Default: not selected.
Leave the backup system enabled	This option is only available if the option **Keep the replica after the backup** is selected. If this option is selected, the filesystems remain mounted, the volume groups remain imported and active (UNIX systems), and the target volumes remain presented after the session. In this case, you can use the backup system for data warehousing purposes, but *not* for instant recovery. If the replica has to be reused later on (deleted, rotated out, or used for instant recovery), Data Protector automatically connects to the backup system, dismounts the filesystems, unpresents the target volumes, and clears the related logical structures on the backup system. At that point in time, if the filesystems are not mounted to the current backup system, Data Protector cannot perform a proper cleanup, and aborts the operation or the instant recovery session. If this option is not selected, Data Protector dismounts filesystems, exports volume groups (UNIX systems), and unpresents the target volumes on the backup system at the end of the ZDB session.

Enable the backup system in read/write mode	This option is applicable to and can only be changed for UNIX systems only. Select this option to enable write access to volume groups and filesystems on the backup system. For backup purposes, it is sufficient to activate the backup system volume groups and mount the filesystems in the read-only mode. For other tasks, the read/write mode may be needed. Note that when this option is selected, the replica is open to modifications while the backup system is online. Consequently, data restored from such a replica includes all potential modifications. Defaults: **UNIX systems:** not selected.

Note In a particular ZDB session, the mount point paths to which filesystems of the replica are mounted on the backup system correspond the mount point paths to which source volumes were mounted on the application system if at least one of the following conditions is met:

- The GUI option **Use the same mountpoints as on the application system** is selected.
- The omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 1.

If the option **Use the same mountpoints as on the application system** is not selected, and the omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 0, the mount point paths are determined by the GUI options **Root of the mount path on the backup system** and **Add directories to the mount path**, and the omnirc options ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH are ignored.

Restore

Instant recovery sessions that involve a 3PAR StoreServ Storage system can be initiated natively using the 3PAR StoreServ Storage integration, or through the Data Protector Microsoft Volume Shadow Copy Service integration using the 3PAR VSS Agent, provided that the corresponding zero downtime backup sessions were also initiated through this integration.

Instant recovery

Instant recovery restores data directly from a replica to source volumes, without involving a backup device. All data in the replica is restored, including filesystems or other objects which were not explicitly selected for backup.

You can perform instant recovery using:

- The Data Protector GUI
- The Data Protector CLI

The number of replicas available for instant recovery is limited by the value of the option **Number of replicas rotated**, which determines the size of the replica set. You can view these replicas in the GUI in the Instant Recovery context by expanding Restore Sessions. Replicas are identified by the backup specification name and the session ID. Other information, such as time when the replica was created, is also provided. Alternately, you can use the Data Protector command omnidbzdb to list sessions.

When instant recovery starts, Data Protector disables the application system. This includes dismounting filesystems and deactivating or exporting volume groups (UNIX). Before this is done, filesystems' and volume groups' status is checked, and only mounted filesystems are dismounted and active volume groups are deactivated or exported. At the end of the session, volume groups are reactivated and dismounted filesystems are mounted to the same mount points as were used during backup.

The following limitations apply:

- Instant recovery fails in the following situations:
  - The source volumes do not exist on the disk array any more.
  - The source volumes are not presented to the application system.
  - If the current configuration of the participating volumes (on Windows systems) or volume groups (on UNIX systems) is different from the volume/volume group configuration that existed at the time of the ZDB session and which was recorded in the SMISDB.
  - After instant recovery, restored filesystems are mounted to the same mount points or drive letters on the application system as they were at the backup time, but these mount points or drive letters have other filesystems mounted.

- While an instant recovery session is in progress, you cannot perform a zero downtime backup session that involves the source volumes to which the data is being restored.

Instant recovery methods

With 3PAR StoreServ Storage, instant recovery can be performed using the "copy-back" method, which copies replica data without retaining the source volumes.

With this instant recovery method, the source volumes are directly overwritten with data from the replica. 3PAR does not allow to continue before restore is completed. The restore process runs until finished or aborted. The source volumes are not retained and if the instant recovery session fails, the original application data residing on the source volumes is lost.

The following prerequisites apply:

- Target volumes used in an instant recovery session should not be presented to any system. You can make Data Protector automatically remove any disallowed target volume presentations by selecting the option **Force the removal of all replica presentations** in the GUI or by specifying the omnir option -force_prp_replica in the CLI.
- If a disk image backup with filesystems mounted on the selected disks was performed, manually dismount the filesystems on the disks to be restored before disk image instant recovery. If the option **Check the data configuration consistency** is cleared in the GUI or the omnir option -check_config is not specified in the CLI, the disks are dismounted automatically. In any case, re-mount the filesystems back after instant recovery.

Instant recovery using the GUI

Follow the steps:

1. In the Context List, select **Instant Recovery**.
2. In the Results Area, select the backup session (replica) from which you want to perform the recovery. This can be done by selecting:
   - Backup session ID and name (in the Scoping Pane, expand **Restore Sessions** and select a session from the list of ZDB-to-disk and ZDB-to-disk+tape sessions)
   - Backup object type (Filesystem, SAP R/3, ...) and backup session name and ID:
     a. In the Scoping Pane, expand **Restore Objects**.

        Backed up object types are displayed.

     b. Expand the object type you want to restore.

        All available backup specification used in ZDB-to-disk or ZDB-to-disk+tape sessions for the selected object type are displayed.

     c. Expand the backup specification containing the replica set. Available sessions IDs (replicas) are displayed.
3. In the Scoping Pane, click the backup session (replica) you want to restore.
4. Check the selection box next to the application system to select the session for restore.
5. Specify other instant recovery options as desired.
6. Click **Restore** to start the instant recovery session or **Preview** to start the instant recovery preview.

> **Important** You cannot use the Data Protector GUI to perform instant recovery using backup data crated in a ZDB-to-disk+tape session after the media used in the session has been exported or overwritten. In such circumstances, use the Data Protector CLI instead. Note that the backup media must not be exported or overwritten even after an object copy session.

Instant recovery using the CLI

1. List all available ZDB-to-disk or ZDB-to-disk+tape sessions (identified by the session ID):

   ```
   omnidbzdb --list --session --ir
   ```

   From the output, select the backup session you want to restore.
2. Run the following command:

   ```
   omnir -host ClientName -session SessionID -instant_restore [INSTANT_RECOVERY_OPTIONS]
   ```

   where the meaning of the options is as follows:

ClientName

SessionID

For INSTANT_RECOVERY_OPTIONS , see Instant recovery options .

Instant recovery options Instant recovery options are listed below:

Data ProtectorGUI/CLI	Function
Copy replica data to the source location / -copyback	This is the only available method with 3PAR StoreServ Storage. It copies the replica data of the specified ZDB session to the original storage. **Caution** If the instant recovery session fails, a data loss on the source volumes may occur. After the instant recovery session, the replica is not deleted from the replica set, and the information about it is not deleted from the SMISDB. Therefore, the replica is available for another instant recovery session until it is rotated out from the replica set or deleted manually. This instant recovery method takes about as much time as the replica creation did, but the storage redundancy level is preserved and the source volumes remain in their disk group.
Wait for the replica to complete / -wait_clonecopy	This option always enabled as 3PAR StoreServ Storage does not allow creating presentations while copying data to the source location. Instant recovery session cannot continue before copy-back has finished and presentations cannot be created while restore is in progress.
Check the data configuration consistency / -check_config | -no_check_config	If this option is selected in the GUI or the -check_config option is specified in the CLI, Data Protector performs a sanity check and a comparison of current volume group configuration of the volume groups participating in the instant recovery session and the volume group configuration information kept in the SMISDB after the corresponding zero downtime backup session. If the sanity check fails or the volume group configuration has changed since the zero downtime backup session, the instant recovery session aborts. **MC/ServiceGuard clusters:** When performing instant recovery to some other node than the one from which data was backed up, you must select this option in the GUI or specify the -check_config option in the CLI. In such circumstances, the current volume group configuration on the node to which data is to be restored differs from the volume group configuration kept in the SMISDB. Consequently, the SMISDB volume group configuration data is replaced by the current volume group configuration data on the node to which data is to be restored, and the instant recovery session succeeds.
Force the removal of all replica presentations / -force_prp_replica	If this option is selected in the GUI or specified in the CLI, and a target volume containing data to be restored is presented to a system, the P6000 / 3PAR SMI-S Agent removes such presentation. If the option is not selected in the GUI or not specified in the CLI, the instant recovery session fails in such circumstances.
Force restore of 3PAR volume set / -force_restore_volset	If this option is selected in the GUI or specified in the CLI, and a source volume (a member of the volume set) is exported to the application host using volume set, the P6000 / 3PAR SMI-S Agent removes all volumes that are part of the volume set presentation during instant recovery and adds them back after the restore completes. If the option is not selected in the GUI or not specified in the CLI, the instant recovery session fails in such circumstances. Note that if this option is selected during remove presentation, none of the volumes part of the volume set can be accessed.

Instant recovery for 3PAR Remote Copy environments

This section describes the steps to be followed for executing the instant recovery procedure in 3PAR Remote Copy environments of the 3PAR storage systems using Data Protector.

Instant recovery restores data directly from a replica to source volumes, without involving a backup device.

The following sections outline different 3PAR remote copy configurations, and the steps you need to follow for a successful instant recovery.

Supported remote copy configurations for instant recovery

The manual steps needed to prepare the environment for instant recovery differ depending on th 3PAR remote copy configurations.

Identifying the setup depends on the following environment information:

- The current site for the source side of any remote copy groups that include the source storage volumes
- Whether the remote copy or target storage volumes are on the same array as the source storage volumes (*primary*), or on the remote side of the DR group (*secondary*)

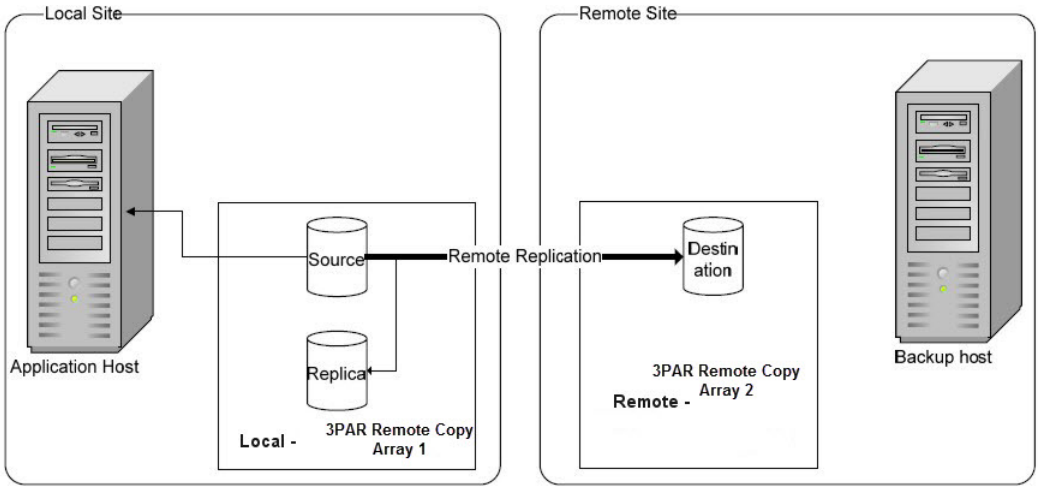
From this information, there are two possible configurations:

- Configuration I – 3PAR remote copy replica is on the local side of the remote copy group
- Configuration II – 3PAR remote copy replica is on the remote side of the remote copy group

Configuration I – local 3PAR Remote Copy Replica

In this configuration, at the time of instant recovery, the source and replica storage volumes reside on the current local site.

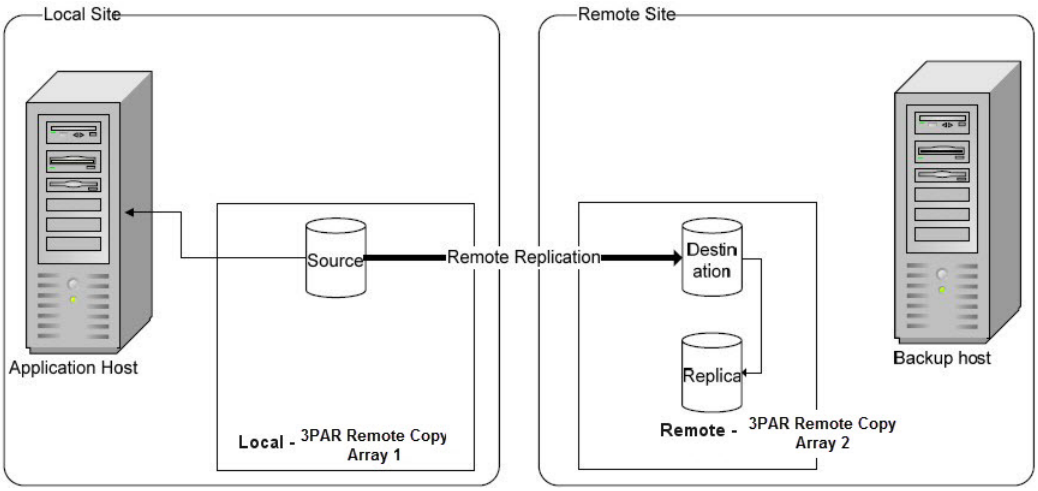
Replicas on the local site:



Note The source storage volume (“Source” in the diagram) acts as both the source of the replica storage volume and the source for the remotely replicated storage volume (“Destination” in the diagram).

Configuration II – remote 3PAR Remote Copy Replica

Replicas on the remote site



In this configuration, at the time of instant recovery, the ZDB environment has the source virtual disk residing on the local site. The remote replica (the replica of the source virtual disk replicated using 3PAR remote copy) and its local replica are both on the remote site.

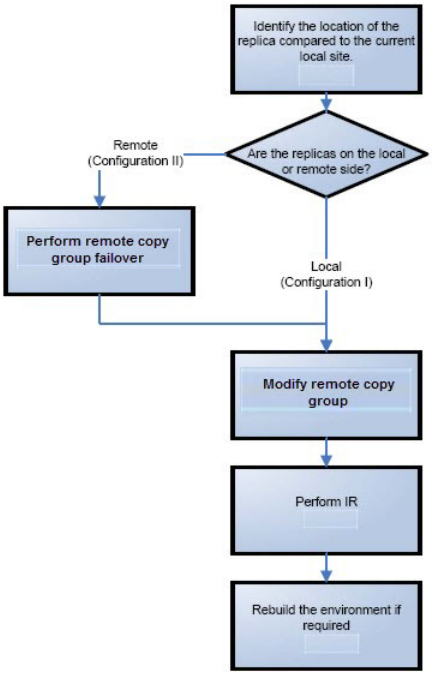
Note The storage volume marked “Destination” in the diagram is both the *destination* of the remote copy group and the *source* of the replica storage volume.

Instant recovery in 3PAR Remote Copy environments

The steps for an instant recovery procedure is as follows:

1. Identify the current configuration
2. Perform a remote copy group failover, if the replica is on the remote side
3. Modify or remove the remote copy group
4. Perform instant recovery
5. Rebuild the remote copy group, if the replica is on the remote side

The following flow chart summarizes this general process.



Identify the current configuration

The following steps help identify the location of the source and target volumes:

1. Select the session for which instant recovery will be performed.

   List the sessions available for instant recovery using the Data Protector GUI (the **Instant Recovery** context) or the Data Protector CLI (the `omnidbzdb` command)

   ```
   # omnidbzdb --diskarray 3par -list -session -ir
   ```

   ```
   Found 2 3PAR SMI-S session(s) in the internal database: Session ID IR Type Excluded Backup Specification
   ========== 2015/06/02-1 Yes VSnap No DP-Dev-3par-backup 2015/06/02-2 Yes VSnap No DP-Dev-3par-backup
   ```

   ```
   #
   ```

2. Identify the source objects and the remote copy information.

   Query the objects of the specific session using the `omnidbzdb` command. The following example is for a session with ID 2015/06/02-2.

   ```
   #omnidbzdb --diskarray 3par -show -session 2015/06/02-2 Info on session "2015/06/02 0002":
   ```

   ```
   Target volume virtual disk name : DP-2015.06.02-2-XXXE267X Target volume virtual disk ID : 5000-XXXX-YYYY-ZZZZ Target volume virtual disk WWN : 5000-XXXX-YYYY-ZZZZ Array Family name : 3PAR Array Family ID : 130XXXX Target volume snapshot type : VSnap Source volume virtual disk ID : 5000-XXXX-YYYY-ZZZZ Session ID : 2015/06/02-2 Creation Date : Tue Jun 02 14:56:00 2015 IR flag : 1 Excluded : 0 Source disk version : 0 Backup specification : DP-Dev-3par-backup Application System : computer1.company.com Backup System : computer2.company.com
   ```

   ```
   #
   ```

   From this output, you can find the following information:

   - The target/replica virtual disk WWN, and the name:
     - *WWN:* 5000-XXXX-YYYY-ZZZZ¸
     - *Name:* DP-2015.06.02-2-XXXE267X
   - The 3PAR array name and the WWN where the matched primary and secondary volumes exist:
     - *Name:* 3PAR

3. Use this information to locate the source storage volume and the 3PAR replica where it resides. You can also locate the target storage volume or the target virtual disk to verify that it still exists:

   a. Connect to the 3PAR Management Console.

   b. Navigate through the 3PAR Array, and get the virtual volume name from the Provisioning tab. Look for the virtual disk with a matching WWN.

   c. The following information should be gathered from this panel:

      - Remote Copy status group name
      - Remote Copy group

      The remote copy status is used to identify the configuration of the current environment

      - If the remote copy status is “Primary”, the current environment is Configuration I. In this case, proceed to Step 3: Modifying or removing the Remote Copy group.
      - If the remote copy status is “Secondary”, the current configuration is Configuration II. In this case, proceed to Step 2: Performing failover.

      > **Note** Complex environments may include a mixture of Configuration I and Configuration II. In this scenario, remote copies exist that are both local and remote in relation to the source storage volumes. To handle this, perform the actions stated in Step 2: Performing Failover only to the remote copy groups with the “Secondary” status.

Perform failover

Use the information you have gathered regarding remote copy groups to perform failover as appropriate for the environment.

For more complex environments, including clusters or other high-availability solutions, see the appropriate documentation for that solution before performing any failover actions.

After performing the failover, proceed to modify or remove the remote copy group.

Modify or remove the Remote Copy group

> **Note** Before taking any action, record the information relating to the remote copy groups. This includes such things as the virtual disks participating in the remote copy group, which the 3PAR storage systems are being replicated to, the mode of operation, and other specific details.

Modify the environment so that the source virtual disks no longer participate in a remote copy group.

When this is completed, proceed to step 4 to perform the instant recovery.

Perform instant recovery

Using the Data Protector GUI or CLI, perform instant recovery with the selected session. This should complete successfully with the appropriately reconfigured environment.

When this has been completed, optionally proceed to rebuilding the remote copy group.

Rebuild the Remote Copy group

If the replica is on the remote side (Configuration II), return the new source virtual disks to the specific remote copy groups. Using the information you recorded in step 3 regarding the environment and specific remote copy groups, either rebuild or recreate the remote copy groups.

> **Note** Ensure that you use the newly-recovered storage volumes for this rebuild of the 3PAR remote copy groups. These storage volumes should have the same names and the WWNs as the storage volumes used previously. However, as these are different virtual disks, the UUIDs will be different from those used by the application system before for the virtual disks.

You may also need to perform additional steps to bring the environment to the same initial state, including failing over the 3PAR remote copy groups, to return operation to the correct 3PAR storage systems and application servers.

Troubleshoot

This section lists general checks and verifications that you may need to perform when you encounter problems with the 3PAR StoreServ Storage integration.

- Ensure that the latest official Data Protector patches are installed.

Checks and verifications

- On the application and backup systems, examine system errors logged into the `debug.log` file residing in the default Data Protector log files directory.

Backup problems

Problem

You cannot select the 3PAR sub type in the Data Protector user interface when creating a ZDB backup specification

Action

Check that the `P6000 / 3PAR SMI-S Agent` integration module is installed on the application system and the backup system. To do that, open the `cell_info` file located on the Cell Manager in the following directory:

Windows systems: Data_Protector_program_data\Config\server\cell\cell_info

UNIX systems: /etc/opt/omni/server/cell/cell_info

File contents should look similar to the following:

```
-host "sap002.company.com" -os "HPs800 hp-ux-11.00" -cc A.10.04 -da A.10.04 -ma A.10.04 -SMISA A.10.04
```

Problem

The P6000 / 3PAR SMI-S Agent fails to connect to the Cell Manager and retrieve configuration data

```
[Major] Cannot connect to the Cell Server. (Insufficient permissions. Access denied.)
```

The P6000 / 3PAR SMI-S Agent is always started as an administrator's process on the application and backup systems. Therefore, the user who starts it must be the member of **admin** or **operator** user groups.

Action

Using the GUI, check if the user is a member of **admin** or **operator** user groups. If not, add the user to one of these groups. In addition, ensure that administrators from both the application and backup systems belong to Data Protector**admin** or **operator**.

Problem

On an HP-UX system, the P6000 / 3PAR SMI-S Agent fails to communicate with the array provider using SSL

```
[Warning] The SSL connection to the SMI-S provider has failed. The error description returned is: SSL Exception: Random seed file required
```

On HP-UX systems, Pegasus libraries require the random number generator pseudo device for its SSL-based communication with the SMI-S provider. If the pseudo device is not present, the warning appears.

Action

1. Install the pseudo device in `/dev/random` on the HP-UX backup system.
2. Re-run the session.

Problem

No SMI-S CIMOM login entries are configured within SMISDB

Action

Add an SMI-S CIMOM login information to SMISDB:

```
omnidbzdb --diskarray 3PAR --ompasswd --add ClientName [--ssl] [--port PortNumber] [--user Username] [--passwd Password]
```

Problem

On a UNIX system, ZDB sessions stop responding for a long time during the resolving of the backup objects on the application system

When resolving the backup objects on the application system, Data Protector sends SCSI inquiries to identify the vendor-specific details of the virtual disk to be replicated. If this virtual disk belongs to a DR group that is in the "failsafe-locked" mode, SCSI inquiries do not return at all. As a result, the session stops responding.

Action

1. Abort the session and stop the ZDB agent processes that stopped responding on the application system.
2. Identify the root cause for the "failsafe-locked" mode of the DR group and fix it by bringing the DR group back into normal operational mode.

Problem

On the application system, dismounting a filesystem fails

Action

Ensure that no other processes use the filesystem to be dismounted. If `Stop/quiesce the application command line` was specified, check that it stops all processes using the filesystem.

Problem

On a Windows system, replica cannot be mounted to the target location on the backup system

```
[Major] Filesystem \\.\Volume{9640da9a-6f36-11d7-bd7a-000347add7ba} could not be mounted to C:\mnt. ([145] The directory is not empty.).
```

When a backup with nested mountpoint objects is run, replica cannot be mounted to the target mountpoint location on the backup system if cleaning of the target mountpoint location fails.

Action

On the backup system, manually empty the directory where filesystems are to be mounted or select the backup option **Automatically dismount the filesystems at destination mountpoints**. If you choose manual action, and leave the default root mount path `c:\mnt` in the ZDB backup specification, you should empty the `mnt` directory.

Problem

Data Protector fails to delete a replica from the replica set in a cluster environment

A ZDB session reports the following major error and message:

```
[Major]
```

```
Resolving of storage volume TargetVolumeID has failed. ...[Normal] Some disks are still in use. They will be moved in purge bucket.
```

This error may occur in a cluster environment with the backup system which is a cluster virtual server. In such circumstances, after a failover, new backup sessions cannot rotate out the replicas on the active node because the presentations match the passive node. The replicas to be removed are marked with the purge flag in the SMISDB, and you are advised to delete such replicas.

Action

To delete the replicas with the purge flag from the disk array and the SMISDB, perform one of the following actions:

- Manually delete all storage volumes that are marked for purging by running:

  `omnidbzdb --diskarray 3PAR --purge [--force] --host ClientName`

  where *ClientName* is the name of the node on which you want to perform the purge operation.

  Use the `-force` option to remove the volumes marked for purging even if they are presented to a system.

- Perform manual failover and run another ZDB session. The session will delete all the volumes marked for purging on the new active node.

Problem

On an HP-UX system, backup session freezes during either preparation or resuming of the backup system

One of the following messages appears:

```
[Normal] Starting drive discovery routine.
```

```
[Normal] Resuming the backup system.
```

During the backup system preparation, Data Protector adds new devices to the Secure Path control and runs device scanning. When resuming the backup system, Data Protector removes devices from the Secure Path control and runs device scanning.

If some other process runs Secure Path commands or device scanning at the same time (during either preparation or resumption), the session may freeze. To identify this problem, run the `ps -ef` command several times on the backup system and check if any `ioscan` or `spmgr` processes persist in the output.

Action

Abort the backup session and stop the hanging `ioscan` and `spmgr` processes.

If processes cannot be stopped, restart the backup system and clean it up manually:

1. On the backup system, run `spmgr display` to display the target volumes (created in the failed session) left under the Secure Path control.
2. Remove such target volumes from the Secure Path control using `spmgr delete` .
3. Run `spmgr update` , and then follow reported instructions to make changes persistent across system restart processes.
4. Using the 3PAR Management Console, delete all presentations attached to removed target volumes.

Problem

On Linux systems, a backup to LVM volumes fails.

The option **Leave the backup system enabled** was selected for the backup. The following error message is displayed:

[Major] From: SMISA@company.com "SMISA" Time: 12/06/2013 1:06:26 PM

It is possible that duplicated LVM UUIDs and/or names will appear on the backup system.

Session will abort.

Action

Set the `lvm.conf` file parameters properly.

Problem

The 3PAR ZDB remote copy periodic backup fails.

The 3PAR remote copy periodic backup of some of the storage volumes fails with the following error message:

[Major] From: SMISA@hostname "SMISA" Time: Date Time

Skipping the backup of storage volume as Remote Copy group sync operation in progress.

Group name : 3PAR remote-copy-group name

Storage volume : 3PAR remote-copy-group storage volume name

Action

- If a manual sync operation is still in progress when the backup is started, then wait for the manual sync operation to complete, and then start the ZDB backup.
- If the sync operation initiated by Data Protector does not complete in the specified time period, increase the wait-time for the sync operation in the `ZDB_WAIT_FOR_PERIODIC_SYNC_TO_COMPLETE` and the `ZDB_WAIT_FOR_PERIODIC_SYNC_RETRY_COUNT` variables.

Problem

The 3PAR ZDB remote copy backup fails.

The 3PAR remote copy backup of some of the storage volumes fails with the following error message:

[Major] From: SMISA@hostname "SMISA" Time: Date Time>

Skipping the backup of storage volume as remote copy group is in stopped state.

Group name : 3PAR remote-copy-group name

Storage volume : 3PAR remote-copy-group storage volume name

Action

The 3PAR remote copy group is in the *Stopped* state. *Start* the remote copy group and run the backup.

Restore problems

Problem

On the Unix or Linux operating system, after the successful ZDB raw disk image restore, the data is not visible.

Action

Re-mount the volumes, and check again for the data.

Example: umount/<disk mountpoint name> and mount/<disk mountpoint name>

Instant recovery problems

Problem

Instant recovery fails

The problem may occur if the option **Force the removal of all replica presentations** is not selected and a target volume from the selected replica is presented to some system other than the backup system or the target volume cannot be dismounted.

Action

Select the option **Force the removal of all replica presentations** and restart the instant recovery session.

Problem

On a Windows system, instant recovery to a different cluster node fails

```
[Major] Filesystem volume_name could not be dismounted from drive_letter ([2] The system cannot find the file specified.). [Critical] Failed to disable the application system. [Critical] Failed to resolve objects for Instant Recovery.
```

On Windows systems, the automatic preparation of the application system cannot match clustered volumes from one cluster node to the volumes on another node.

Action

Disable the automatic preparation of the application system:

1. On the application system, enable the ZDB_IR_MANUAL_AS_PREPARATION options and manually dismount the volumes to be restored.
2. Start instant recovery.
3. After instant recovery, manually mount restored volumes.

Problem

The 3PAR ZDB remote copy group instant recovery fails

3PAR ZDB remote copy group instant recovery fails with the following error message:

[Minor] From: SMISA@hostname "SMISA" Time: Date Time

A SMI-S call to the array did not behave as expected.

Failed volume: DP-201X.XX.01-1-0XXXCDXXX

Returned message: Error calling provider to present volume 5XXX2ACXXXXXXXBX: Invalid parameter for promote snapshot volume: RW parent (3PAR remote copy group storage volume name) is involved in a remote copy group

Action

Remove the storage volume that is part of the 3PAR remote copy group, and start the instant recovery.

Problem

The 3PAR ZDB local instant recovery fails

The 3PAR ZDB local instant recovery fails with the following error message:

[Minor] From: SMISA@hostname "SMISA" Time: Date Time

A SMI-S call to the array did not behave as expected.

Failed volume: DP-201X.XX.01-1-0XXXCDXXX

Returned message: Error calling provider to present volume 5XXX2ACXXXXXXXBX: Invalid parameter for promote snapshot volume: RW parent (3PAR remote copy group storage volume name) is involved in a remote copy group

Action

Remove the storage volume that is part of the 3PAR remote copy group, and start the local 3PAR ZDB instant recovery.

Configure NetApp Storage

This topic describes how to configure the Data Protector NetApp Storage integration, how to perform zero downtime backup and instant recovery (IR) using the NetApp storage system, and how to resolve the integration-specific Data Protector problems.

It also provides information on the Data Protector ZDB database and lists prerequisites and limitations.

Prerequisites

- Make sure the same operating system version is installed on both the application system and the backup system.
- If the application system and the backup system reside in a Data Protector cell with secured clients, ensure that access between both systems is allowed in both directions.
- Connect a NetApp storage system to the application and backup systems through the SAN.
- Source volumes must have enough space for snapshots and clones
- Before starting instant recovery, you must manually break the relationship between SnapMirrored volumes. And complete the following manual steps:
  1. Remove presentation of source LUN(s) from source array to application host
  2. Perform reverse sync to bring data back to source volume(s)
  3. Re-present the remote volume(s) to application host(s). Note: Remote volume(s) must be presented and not the volume(s) from volume clone which has “DP_Clone” in its volume name.

NetApp Storage licenses and components

- Obtain FC/FCoE license for accessing LUNs on the NetApp storage system.
- Obtain iSCSI license for accessing LUNs on the NetApp storage system.
- Obtain SANworks Snapshot licenses.
- Obtain FlexClone license.
- Obtain NetApp SnapMirror license.
- Enable the httpd admin access or SSL encrypted admin connection, or both by running the following commands on the NetApp console:

  ```
  netapp1> options httpd.admin.enable on
  netapp1> httpd.admin.ssl.enable on
  ```

- Make sure that the names of Initiator Groups on the NetApp storage system are the same as the fully-qualified domain names of the systems they represent.
- Make sure that an appropriate multi-path device management is installed on the application system and the backup system.

  Linux systems: Device Mapper Multipath Enablement Kit for Disk Arrays 4.2.0 or newer version.

  To configure the installed multi-path device management software:

  1. Start the multipath daemon and run the following command to configure the daemon so that it gets started during system startup:

     Red Hat Enterprise Linux: `chkconfig multipathd on`

     SUSE Linux Enterprise Server: `chkconfig boot.multipath on`

  2. Prevent the multipath device management software from queuing for unavailable disk volumes by modifying its configuration file. In the `defaults` section of the file `/etc/multipath.conf` file, add the following line:

     ```
     no_path_retry        fail
     ```

     Ensure that this `no_path_retry` parameter value is not overridden by equivalent entries in the `device` sections of the same file in which the corresponding NetApp storage systems are configured.

  3. Ensure that the correct preferred names are used for pathnames that are referencing the same device for physical volumes as they are used in device-mapper multipathing.

     Open the `lvm.conf` file, residing in the `/etc/lvm/` directory, and set the following variable:

     ```
     preferred_names = [ "^/dev/mpath/", "^/dev/mapper/mpath", "^/dev/[hs]d" ]
     ```

Data Protector licenses and components

- An appropriate zero downtime backup extension for non–HPE Storage Arrays licenses-to-use (LTU).
- The NetApp Storage Management Initiative Specification (SMI-S) Provider installed on both the application system and the backup system.

Limitations

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- Instant Recovery of Exchange Database is not supported. This is due to a limitation of the ONTAP VSS Hardware Provider.

- Volume spanning and RAID is not supported on windows platform.
- As both the replica and the volume snapshot are going to be available, if you mount the replica and make changes, the changes will not get reflected in the volume snapshot copy due to which the restored copy will not contain the changes made in replica.
- 7-mode is not supported.
- Atomic operations and group replica are not supported.

ZDB database - SMISDB

ZDB database for the Data Protector NetApp storage integration is referred to as SMISDB. It keeps information about NetApp storage systems. For each system, the following is stored:

- Hostname as recognized in the IP network.
- User name and encoded password for the NetApp Storage Provider SMISDB resides on the Cell Manager in:
  - Linux: /var/opt/omni/server/db80/smisdb
  - Windows: data_protector_program_data\server\db80\smisdb

Configure the integration

To integrate with the NetApp storage system, Data Protector uses the NetApp SMI-S Provider. This plug-in enables NetAPP storage support within the Data Protector ZDB (SMI-S) agent. To configure the Data Protector NetApp Storage integration, provide the data that the Data Protector ZDB agent will use to establish connection to a NetApp storage system of your choice.

The connection related configuration data includes user credentials that you must add to the ZDB database (the NetApp part of SMI-S database). The credentials are bound to a specific application system in the Data Protector cell. The Data Protector ZDB agent then reads the credentials from the ZDB database each time a zero downtime backup for data residing on a NetApp storage system is started. The Data Protector ZDB NetApp agent uses SMI-S Provider to manage the NetApp array. You need to install the NetApp SMI-S Provider available at https://library.netapp.com/ecmdocs/ECMLP2608866/html/index.html. See the instructions in the NetApp SMI-S Provider documentation for configuring the SMI-S Provider. After configuring, add an administrative SMI-S user and the NetApp array from which backup is to be performed to the NetApp SMIS server.

For SnapMirror, the Data Protector NetApp agent uses NetApp SMI-S server as well as direct connectivity with NetApp array. Hence, both the NetApp SMI-S server details as well as the source and destination array details of SnapMirror volume are required to be entered in the SMI-S database. In case of non-SnapMirror backup, do not specify any NetApp array details in SMI-S database.

Connection configuration data

To be able to connect to a NetApp storage system and perform zero downtime backup sessions, the Data Protector ZDB agent needs the following information:

- If the system has multiple IP addresses, use the address by which the Data Protector ZDB agent can access the system.
- Whether the connection uses Secure Sockets Layer (SSL).
- Username and password. For C-mode, use SVM username (typically `vsadmin` user) and for 7-mode, use Vserver username (typically root user).

  These credentials must belong to the NetApp storage system administrator account.
- Fully qualified domain name or IP address of the NetApp SMIS server.
- Username and password of NetApp SMIS user.

These are stored in the NetApp part of the SMISDB.

Configure NetApp storage

To establish connection to the NetApp storage system, use the Data Protector`omnidbzdb` command. Follow the steps:

1. Select the NetApp storage system user account that has a proper privilege level on the corresponding domains. Identify and write down its username and password, which you will need in the next step.
2. Add NetApp storage system to the NetApp SMIS server using the `smis add` command. For more details, see the NetApp SMI-S Provider documentation available at https://library.netapp.com/ecmdocs/ECMLP2608866/html/index.html.
3. Use the `omnidbzdb` command to establish connection to the NetApp storage system and to add the username and password that you acquired in the previous step to the ZDB database. Run the following command:

   ```
   omnidbzdb --diskarray ArrayFamily --ompasswd --add ClientName --user UserName --passwd password
   ```

   where:

   - *ArrayFamily* is NetApp, specified as **netapp**.
   - *ClientName* is fully qualified domain name of the NetApp SMIS Provider.
   - *UserName* and *password* is NetApp SMIS Provider user credentials.

> **Note** If you add NetApp storage system residing in the cluster environment, run this command for every destination array in the cluster.

For example:

```
omnidbzdb --diskarray netapp --ompasswd --add netappstorage.company.com --user Administrator --passwd pwd
```

4. Using the `omnidbzdb --diskarray netapp --ompasswd --check` command, verify that the Data Protector NetApp Storage Provider can connect to the NetApp storage system using the configured user authentication data.

Tip For each application system, you can add user credentials of multiple NetApp Storage user accounts in the NetApp SMIS server. Then add them to SMISDB using the `omnidbzdb`.

Note In case of mixed C-mode and 7-mode NetApp configuration, make sure that they reside on a separate NetApp SMI-S Providers.

Configure NetApp SnapMirror

NetApp SnapMirror is supported only on ONTAP 9.3 C-mode array.

To configure NetApp SnapMirror, use the Data Protector`omnidbzdb` command. Follow the steps:

1. Add the NetApp SnapMirror source and destination array details in the NetApp SMI-S Provider.
2. Add the SMI-S Provider details in the SMI-S database using the `omnidbzdb` command:

   ```
   omnidbzdb --diskarray netapp --ompasswd --add <sourcearray> --user <username> --passwd <password>
   ```

   ```
   omnidbzdb --diskarray netapp --ompasswd --add <destinationarray> --user <username> --passwd <password>
   ```

   Where *username* and *password* are of the NetApp array SVM.

   Example:

   ```
   omnidbzdb --diskarray netapp --ompasswd --add sourcenetappstorage.company.com --user vsadmin --passwd netapppwd
   ```

   ```
   omnidbzdb --diskarray netapp --ompasswd --add destinationnetappstorage.company.com --user vsadmin --passwd netapppwd
   ```

3. Add the NetApp source and destination array in SMI-S database. This agent uses both the SMI-S and direct connectivity to manage the array.
4. Use the `omnidbzdb --diskarray netapp --ompasswd --check` command to verify that the Data Protector NetApp storage provider is connected to the NetApp SMI-S server.

Backup

This section describes configuration of a filesystem or disk image ZDB and IR backup using the Data Protector GUI.

With the NetApp Storage Provider integration, you can perform the zero downtime backup of the ZDB to tape type only.

Create backup specification

The following limitations apply when creating back specification:

- Only one snapshot type for target volumes can be created during a ZDB session.
- When cloning process for a source volume is in progress, another snapshot (any type) of that source volume cannot be created.
- You cannot back up replicas (target volumes from existing and currently recorded backup sessions).
- If there is not enough space for a fully allocated replica creation, the session fails.

To create a ZDB backup specification for a NetApp storage using the Data Protector GUI (Data Protector Manager), follow the steps:

1. In the Context List, select **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**. Right-click **Filesystem** (for both object types: filesystem and disk image) and click **Add Backup**.

   The Create New Backup dialog box appears.

   In the Filesystem pane, select the **Blank Filesystem Backup** template or some other available template.

   Select **Snapshot or split mirror backup** as Backup type and **Storage Provider** as Sub type. For description of options, press **F1**.

Click **OK**.

3. Under Client systems, select **Application system** and **Backup system**. If the application system is part of a server cluster, select the virtual server.
4. Under Add Storage Provider, select **NetApp Storage Provider** from the Storage provider drop-down list and then click **Add**. The NetApp Storage Options dialog opens. Select either Snapshot or SnapMirror. Select a **Thin provisioned** or **Fully allocated** replica provision type and click **OK**. NetApp Storage is added to the list. You can later change its options by clicking **Edit** or remove it from the list by clicking **Remove**.
5. Under Application system options and Backup system options, specify other zero downtime backup options as required.

   For instant recovery backup, select **Replica Management options**, and then, select the **Keep the replica after the backup** and **Track the replica for instant recovery** check boxes for NetApp Storage Provider. Click **Next**.
6. Select the objects for backup.
   - **Filesystem backup:** Expand the application system and select the objects to back up. Note that all drive letters or mount points that reside on the system are displayed. You must select only the objects that reside on the NetApp storage system, otherwise the ZDB session fails. Click **Next**.
   - **Disk image backup:** Click **Next**.
7. Select the devices to use in the backup session.

   To create additional copies (mirrors) of the backup image, specify the number of mirrors by clicking **Add mirror** or **Remove mirror**. Select separate devices for the backup image and each mirror.

   Click **Next**.
8. In the Backup Specification Options group box, click **Advanced** and then the **Storage Provider** tab to open the options pane with NetApp storage specific backup options.

   You can specify Application system options and modify all other options, except **Application system** and **Backup system** (note that you can change them after you save the ZDB backup specification).

   Click **Next**.
9. In the Backup Object Summary page, specify additional options.
   - **Filesystem backup:** To modify options for the listed objects, right-click an object and then click **Properties**. For information on the object properties, press **F1**.
   - **Disk image backup:** Follow the steps:
     a. Click **Manual add** to add disk image objects.
     b. Select **Disk image object** and click **Next**.
     c. Select the client system. Optionally, enter the description for your object. Click **Next**.
     d. Specify General Object Options and Advanced Object Options. For information on these options, press **F1**.
     e. In the Disk Image Object Options window, specify disk image or raw logical volume sections.

        Specify a disk image section:

        /dev/rdsk/Filename , for example: /dev/rdsk/c2t0d0

        Specify a raw logical volume section:

        /dev/vgnumber/rlvolNumber , for example: /dev/vg01/rlvol1

     f. Click **Finish**.

   Click **Next**.
10. Click **Save As** to save your ZDB backup specification. Optionally, you can click **Save and Schedule** to save, and then schedule the backup specification.

Backup options

The following tables describe the ZDB-related backup options that you can modify when configuring ZDB backup specifications that include storage systems of the NetApp Storage family.

Client systems

Application system	The system on which the application runs. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).
Backup system	The system to which your data will be replicated (backed up), and from which the backup data is copied to a backup device.

NetApp storage replica provision options

Thin provisioned	Select this replica provision type to provision more storage on a LUN than is currently available on the volume, thus increasing the capacity utilization of that volume. It allows free space sharing between LUNs and enables LUNs to consume only the space they actually use. With thin provisioning, you can present more storage space to the backup system connected to the NetApp storage than is actually available to provide the storage you need at any given time.
Fully allocated	Select this replica provision type to enable space-reserved LUNs and snapshot copies have pre-allocated space that can be continually overwritten. This guaranteed space is not available to any other LUNs or snapshot copies within the volume.

Application system options

Dismount the filesystems on the application system before replica generation	Select this option to dismount the filesystems on the application system before replica creation and remount them afterwards. Additionally, when entire physical drives (on Windows systems) or entire disks or logical volumes (on Linux systems) are selected as backup objects in a disk image backup specification, selecting this option will dismount and later remount all filesystems on these objects. If any of these filesystems cannot be dismounted, the backup session fails. If an integrated application exclusively controls data I/O on each physical drive, disk, or logical volume that will be backed up, the dismount operation is not needed. In such a case, you can leave this option cleared. Default: not selected.
Stop/quiesce the application command line	If a command is specified in this option, it is invoked on the application system immediately before replica creation. An example is to stop applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option. If the command fails, the command specified in the option **Restart the application command line** is not invoked. Thus, you may need to implement a cleanup procedure in the command specified in **Stop/quiesce the application command line**. If the omnirc option ZDB_ALWAYS_POST_SCRIPT is set to 1, the command specified in the option **Restart the application command line** is always invoked.
Restart the application command line	If a command is specified in this option, it is invoked on the application system immediately after replica creation. An example is to resume operation of applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option.

Backup system options

Use the same mountpoints as on the application system	This option is not available if the application system is also the backup system (a single-host configuration). If this option is selected, the paths to mount points used for mounting the filesystems of the replica on the backup system are the same as paths to mount points where source volume filesystems were mounted on the application system. If the mount points are already in use, the session fails. For such circumstances, you must select the option **Automatically dismount the filesystems at destination mountpoints** in order for the session to succeed. **Windows systems:** The drive letters must be available, otherwise the session fails. Default: not selected.
Root of the mount path on the backup system	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. Specifies the root directory under which the filesystems of the replica are mounted. Where exactly the filesystems are mounted depends on how you define the option **Add directories to the mount path**. Defaults: **Windows systems:** c:\mnt **Linux systems:** /mnt

Add directories to the mount path	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. This option enables control over the created mount points. It defines which subdirectories will be created in the directory defined with the **Root of the mount path on the backup system** option. When Session ID is used in path composition, this guarantees unique mount points. Example for **Windows systems**: Root directory: C:\mnt Application system: applsys.company.com Backup session ID: 2008–02–22–4 Mount path on the application system: E:\disk1 If **Hostname** is selected: C:\mnt\applsys.company.com\E\disk1 If **Hostname and session ID** is selected: C:\mnt\applsys.company.com\2008–02–22–4\E\disk1 If **Session ID** is selected: C:\mnt\2008–02–22–4\E\disk1 If **Session ID and hostname** is selected: C:\mnt\2008–02–22–4\applsys.company.com\E\disk1 Default: Hostname and session ID.
Automatically dismount the filesystems at destination mountpoints	If the mount points are in use (for example, volumes involved in the previous session may still be mounted) and this option is selected, Data Protector attempts to dismount the mounted filesystems. If the option is not selected and the mount points are in use, or if the option is selected and the dismount operation fails, the session fails. Default: not selected.
Leave the backup system enabled	This option is only available if the option **Keep the replica after the backup** is selected. If this option is selected, the filesystems remain mounted, the volume groups remain imported and active (Linux systems), and the target volumes remain presented after the session. In this case, you can use the backup system for data warehousing purposes. If the replica has to be reused later on (deleted or rotated out), Data Protector automatically connects to the backup system, dismounts the filesystems, unpresents the target volumes, and clears the related logical structures on the backup system. At that point in time, if the filesystems are not mounted to the current backup system, Data Protector cannot perform a proper cleanup, and aborts the operation). If this option is not selected, Data Protector dismounts filesystems, exports volume groups (Linux systems), and unpresents the target volumes on the backup system at the end of the ZDB session.

Enable the backup system in read/write mode	This option is applicable to Linux systems only. On Windows systems, filesystems cannot be mounted in the read-only mode. Select this option to enable write access to volume groups and filesystems on the backup system. For backup purposes, it is sufficient to activate the backup system volume groups and mount the filesystems in the read-only mode. For other tasks, the read/write mode may be needed. Note that when this option is selected, the replica is open to modifications while the backup system is online. Consequently, data restored from such a replica includes all potential modifications. Defaults: **Windows systems:** selected. **Linux systems:** not selected.

Note In a ZDB session, the mount points to which filesystems of the replica are mounted on the backup system are the same as the mount points to which source volumes were mounted on the application system, if at least one of the following conditions is met:

- The GUI option **Use the same mountpoints as on the application system** is selected.
- The omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 1.

If the option **Use the same mountpoints as on the application system** is not selected, and the omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 0, the mount points are determined by the GUI options **Root of the mount path on the backup system** and **Add directories to the mount path**, while the omnirc options ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH are ignored.

Restore

This section describes configuring and running a filesystem or disk image restore of the data backed up using the Data Protector NetApp Storage integration.

The data backed up in a ZDB session using NetApp Storage can be stored on backup media only (ZDB to tape).

Data backed up in ZDB-to-tape sessions can be restored from the backup media to the application system.

Tip You can improve the data transfer rate by connecting a backup device directly to the application system.

Instant Recovery

This section describes instant recovery of the data backed up using the Data Protector NetApp Storage integration.

There are three types of backup options in NetApp:

- Tape (Writes to a tape device only, no instant recovery, only recovery from tape)
- Disk + Tape (Supports instant recovery from disk, no instant recovery, only recovery from tape)
- Disk (Supports instant recovery from disk, no instant recovery, only recovery from tape)

Disk backup creates a volume snapshot of the source volume and a replica (LUN clone) of the source LUN. The volume snapshot is used for performing actual recovery. The replica is used for VMware restore.

- Snapshot backup/instant recovery (local): In case of Local Instant recovery, the LUN replica and the volume snapshot reside on the same local array. During instant recovery, the local copy is used for performing restore.
- SnapMirror backup/ instant recovery (remote): For performing SnapMirror backup/restore, the volume snapshot is present on both the source as well as (remote) destination array and the volume clone and the replica are present on remote side. For SnapMirror type restore, you can select to restore either to Local or Remote array.

Instant recovery using GUI

Complete the following steps to perform instant recovery from Data Protector GUI.

1. Select **Instant Recovery** from context panel.
2. Expand **Filesystem**. IR backup specifications is listed.
3. Expand the required specification and double click on the session id. Instant recovery panel opens.
4. Click **Restore**.

Restore to SnapMirror destination

You can restore to SnapMirror destination that is on local or remote array.

Select the “Perform Restore from Remote Destination” checkbox in the Instant Recovery panel.

It is valid only if “SnapMirror” is selected at the time of backup and not valid for “Snapshot” type of backup.

Note: If you don’t select the **Perform Restore from Remote Destination** checkbox, instant recovery is performed on the source LUN.

Troubleshoot

This section lists general checks and verifications that you may need to perform when you encounter problems with the Data Protector NetApp Storage integration.

- Ensure that the latest Data Protector patches are installed.

Checks and verifications

- On the application and backup systems, examine system errors logged into the `debug.log` file residing in the Data Protector log files directory.

Problem

"checkconfiguration" of NetApp fails.

The `–check` of omnidbzdb fails or checkconfiguration of backup fails.

Action

Check the following:

- The SVM/Vserver username, password and array IP address added correctly in NetApp SMI-S Provider.
- Ensure that the entry made in SMISDB through the `omnidbzdb` command is of NetApp SMI-S Provider and not that of SVM/Vserver.

Problem

The VMware backup fails during presentation.

Action

Any active port which is not correctly zoned with array may cause presentation to fail on ESX host. Ensure that the active ESX FC ports are properly zoned with the array or disable/inactivate the unused ESX FC ports.

Problem

The backup fails during presentation with iSCSI.

Action

Make sure that the backup host is logged in to iSCSI target on the array.

Problem

Check configuration of NetApp fails for SnapMirror.

The `–check` option of `omnidbzdb` fails or check configuration of backup fails.

Action

Check the following:

- The SVM/Vserver username, password, and array IP address are added correctly in NetApp SMI-S Provider.
- Ensure that the entry made in the SMI-S database through the `omnidbzdb` command is of NetApp SMI-S Provider.
- Ensure that correct username, password, and IP address of source/destination array are used. If adding an array, ensure that the username and password is of SVM user (for example, vsadmin user) with admin rights.

Problem

NetApp SnapMirror gets converted to a Snapshot backup.

Action

If there is no SnapMirror relation between the two volumes, Data protector NetApp agent converts it to Snapshot backup. If the relation is SnapMirror, ensure that the source and destination array details are entered in the SMI-S database, and also both the arrays are also added in SMI-S server.

Problem

NetApp SnapMirror backup fails.

Action

Ensure that there is enough space available in the destination array volume’s aggregate.

Problem

Backup fails after presentation is completed for the volume. It fails to discover the presented volume even after a drive scan.

This issue occurs when there are multiple initiator ports registered with the NetApp array but not all the ports have connectivity between array and backup host. In case of FC, if the registered host port is not correctly zoned with array, it will cause the presentation to fail. Data protector selects appropriate initiator host (FC/iSCSI) for presentation during backup because the array connectivity to backup host can be configured on either FC or iSCSI.

Action

To fix this issue, ensure that the registered host ports have proper connectivity/zoning between array and backup host. If the host port is not correctly configured, it should not be registered as a valid initiator host port with the array.

Problem

MSSQL backup with NetApp Snapmirror fails with timeout error.

Action

There may be a delay of up to 5 minutes for the the Netapp replica information to appear in the SMI-S server, due to which NetApp agent reports timeout error. To avoid the timeout issue and to ensure that the backup is completed successfully, increase the timeout value of global option SmWaitForFirstBackupClient in the global file. See Customize the global options to update the global option.

Problem

Instant Recovery fails for snapshot IR backup if the **Perform Restore from Remote Destination** is selected.

Action

Unselect the GUI checkbox **Perform Restore from Remote Destination**.

Configure NetApp SMI-S

This topic describes how to configure the Data Protector NetApp Storage Management Initiative Specification (SMI-S) Provider.

Overview

NetApp SMI-S Provider (formerly Data ONTAP SMI-S Agent) enables you to manage and monitor storage systems and to manage LUNs and volumes of storage systems, CIMOM configuration settings, and CIM server users. NetApp SMI-S Provider is a command-based interface that detects and manages platforms that run ONTAP software. SMI-S Provider uses Web-Based Enterprise Management (WBEM) protocols, which enable you to manage, monitor, and report on storage elements. For more information on NetApp SMI-S Provider, see https://library.netapp.com/ecmdocs/ECMLP2608866/html/GUID-EE384353-6024-4CEA-AD57-6BB590E6791C.html.

To integrate with the NetApp storage system, Data Protector uses the NetApp SMI-S Provider. This plug-in enables NetApp storage support within the Data Protector ZDB (SMI-S) agent. To configure the Data Protector NetApp storage integration, provide the data that the Data Protector ZDB agent will use to establish connection to a NetApp storage system of your choice. The connection related configuration data includes user credentials that you must add to the ZDB database (the NetApp part of SMISDB). The credentials are bound to a specific application system in the Data Protector cell. The Data Protector ZDB agent then reads the credentials from the ZDB database each time a zero downtime backup for data residing on a NetApp storage system is started. The Data Protector ZDB NetApp agent uses SMI-S Provider to manage the NetApp array.

The following NetApp SMI-S Provider versions are supported:

NetApp SMI-S Provider version	Supported platform
5.2.3	Windows 2012
5.2.4	Windows 2016 and Linux

For more information on the supported operation systems, see the "Data Protector Zero Downtime Backup Support Matrix for NetApp storage" available at the Support Matrix page.

Integrating NetApp SMI-S Provider includes the following tasks:

1. Download NetApp SMI-S Provider.
2. Install NetApp SMI-S Provider on Windows or Install NetApp SMI-S Provider on Linux.
3. Configure NetApp SMI-S Provider.

Download NetApp SMI-S Provider

Perform the below steps to download the NetApp SMI-S Provider from the NetApp website. This requires a NetApp support account.

1. Go to Support site.
2. Browse to **Downloads** > **Software** page and locate NetApp SMI-S Provider.
3. Select the operating system and click **Go!**.
4. Select the version number and click **View & Download**.
5. In the Software download section, click **CONTINUE**.
6. Read and accept the End User License Agreement.
7. Select the software package file and save it to a local path.

Install NetApp SMI-S Provider on Windows

To install NetApp SMI-S Provider on Windows server, perform the following steps:

1. Meet the following prerequisites:
   - Access to login credentials for the Windows administrator account.
   - Access to the downloaded NetApp SMI-S Provider software package.
2. Login to the desired host machine.
3. Remove the directory `C:\Program Files (x86)\NetApp\smis` if it already exists.
4. Navigate to the directory that contains the NetApp SMI-S Provider software package (smisprovider-*version_number*.msi) and double-click the package file to begin installation.
5. Complete the steps in the wizard. The NetApp SMI-S Provider service starts automatically after the installation is complete. If the service does not start, restart the SMI-S provider system.
   For advance installation options, see NetApp SMI-S Provider documentation at https://library.netapp.com/ecmdocs/ECMLP2608866/html/GUID-C62332FC-1C20-44B5-9B4D-96D5A4FE1E64.html.

Install NetApp SMI-S Provider on Linux

To install NetApp SMI-S Provider on Linux server, complete the following steps:

1. Meet the following prerequisites:
   - Access to login credentials of the root user.
   - Access to the downloaded NetApp SMI-S Provider software package.
2. Log in as root on the host server where you want to install the NetApp SMI-S Provider.
3. Remove the `/usr/netapp/smis/Pegasus` directory, if it already exists.
4. Navigate to the directory that contains the NetApp SMI-S Provider software package and perform the following:

1. Extract the smisprovider-*version_number.*tar file into a temporary directory and delete all temporary files, including the install script (install_smisprovider).
   Example: $ tar -xvf smisprovider-version_number.tar.
2. Change the file permission on the install script to read, write and execute. Example: chmod 755 install_smisprovider.

5. Install the NetApp SMI-S Provider using the command **$./install_smisprovider**. The NetApp SMI-S Provider service starts automatically after the installation is complete. If the service does not start, restart the SMI-S provider system.
   For advance installation options, see NetApp SMI-S Provider documentation at https://library.netapp.com/ecmdocs/ECMLP2608866/html/GUID-C62332FC-1C20-44B5-9B4D-96D5A4FE1E64.html.

Uninstall NetApp SMI-S Provider in Windows

To uninstall NetApp SMI-S Provider from Windows server, complete the following steps:

1. Click the **Start** in your Windows server.
2. Browse to Control Panel and select **Add Remove/Programs**.
3. Select **NetApp SMI-S Provider** from the list of installed programs and click **Uninstall**.
4. Delete the directory `C:\Program Files (x86)\NetApp\smis` using Windows Explorer.

Uninstall NetApp SMI-S Provider in Linux

To uninstall NetApp SMI-S Provider on Linux server, complete the following:

1. Log in as a root user in the Linux server where NetApp SMI-S Provider is installed.
2. Navigate to the `/usr/netapp/smis/pegasus/bin` directory, and uninstall the NetApp SMI-S Provider from the Linux host using the command: **$./uninstall_smisprovider**.

Configure NetApp SMI-S Provider

This section describes configuration of NetApp SMI-S Provider ZDB using Data Protector.

1. Meet the following prerequisites:
   - At least one NetApp array is available.
   - The NetApp array should be reachable from the NetApp SMI-S Provider.
2. Add an user with administrator access in the NetApp SMI-S Provider. The user being added must be available in the system.
   - Windows: Go to the `C:\Program Files (x86)\NetApp\smis\pegasus\bin` folder and run the command `cimuser -a -u <user name>`. Enter the password when prompted.
     Example: cimuser -a -u Administrator.
   - Linux: Go to the `/usr/netapp/smis/pegasus/bin` folder and run the command `cimuser -a -u <user name>`. Enter the password when prompted.
     Example: cimuser -a -u Administrator.
3. Add an array. Use the command `smis add <storage_sys> <storage_sys_user>` (non secure) or `smis addsecure <storage_sys> <storage_sys_user>` (secure). Enter password when prompted.
   Example: `smis addsecure 1.1.1.10 Administrator`.
4. Verify if the array is added correctly.
   - To list the arrays, use the `smis list` command.
   - To list all LUNs of the SVM, use the `smis luns` command.

   Example:

   ```
   smis list ONTAP_FilerData.hostName="1.1.1.10",port=443.
   ```

5. Add the NetApp SMI-S Provider to SMISDB using the `omnidbzdb` command: `omnidbzdb --diskarray ArrayFamily --ompasswd --add NetApp_SMIS_Provider_address --user SMIS_Provider_username --passwd SMI-S_Provider_user_password`.

   where:

   - *ArrayFamily* is NetApp, specified as **netapp**.
   - *NetApp_SMIS_Provider_address* is IP address/fully qualified domain name of the system where the NetApp SMI-S Provider is installed.
   - *SMIS_Provider_username* and *SMIS_Provider_user_password* is credentials of the user with admin access in the NetApp SMIS Provider.

   Example: `omnidbzdb --diskarray netapp --ompasswd --add 1.1.1.10 --user Administrator --passwd admin`.

   For more information on the options and usage of the `omnidbzdb` command, see omnidbzdb.

6. Verify if the SMI-S Provider is connected to NetApp array. Run the command: `omnidbzdb --diskarray ArrayFamily --ompasswd --check [--host NetApp_SMIS_Provider_address]`

   Sample output:

   ```
   omnidbzdb --diskarray netapp --ompasswd --check --host 1.1.1.10 Starting configuration check on host 1.1.1.10. [Normal] From: SMISA@1.1.1.10.test (SMISA%401.1.1.10.agent.test) "SMISA" Time: 02/20/2019 09:28:07 PM Checking the NetApp provider using this connection data: Host: 1.1.1.10 User: Administrator Namespace: root/ontap Port: 5989 SSL mode: TRUE [Normal] From: SMISA@1.1.1.10.test (SMISA%401.1.1.10.agent.test) "SMISA" Time: 02/20/2019 09:28:07 PM This NetApp provider has access to the following unit: Name: NetApp Release 9.3: Thu Jan 04 10:56:26 UTC 2018 WWN: DPNetApp7-SVM01 Description: NetApp Release 9.3: Thu Jan 04 10:56:26 UTC 2018 Configuration check finished.
   ```

Troubleshoot

Problem

The backup fails after upgrading to Data Protector 2019.02.

The following error messages are displayed:

- There are no valid objects left.
- Some or all storage volumes cannot be backed up. Session will abort.

Action

Check if the NetApp SMI-S Provider is installed and configured correctly. See the sections *Install NetApp SMI-S Provider on Windows* or *Install NetApp SMI-S Provider on Linux* and *Configure NetApp SMI-S Provider* in this page.

Problem

The SMI-S Provider service is not up.

After installing, the NetApp SMI-S Provider service may not be up. **Action**

To get the NetApp SMI-S Provider service in "up" state, complete the following:

1. Check if the NetApp SMI-S Provider installation is complete without any errors.
2. Restart the system where the NetApp SMI-S Provider system is installed.

Configure Dell EMC Unity Storage

This topic describes how to configure the Data Protector and Dell EMC Unity storage integration, how to perform backup and Instant Recovery (IR) using the Dell EMC Unity storage system, and how to resolve the integration-specific problems. It also provides information on the Data Protector ZDB database and lists prerequisites and limitations.

Prerequisites

- Ensure that the same operating system version is installed on both the application system and the backup system.
- If the application system and the backup system reside in a Data Protector cell with secured clients, ensure that access between both systems is allowed in both directions.
- In case of Linux backup host, it should have a LUN with host LUN ID (HLU) 0 already mounted on it for backup to work properly.
- Application host and Backup host must be in array zone with SAN.
- Ensure that enough disk space is available for snapshot operations on Dell EMC Unity array. Only iSCSI interface is supported.
- Ensure that an appropriate multipath device management is installed on the application system and the backup system. Download the Device Mapper Multipath Enablement Kit for Disk Arrays 4.2.0 or later version from https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c01762511.

To configure the installed multi-path device management software:

1. Start the multipath daemon and run the following command to configure the daemon so that it gets started during system startup:
   - Red Hat Enterprise Linux: `chkconfig multipathd`
   - SUSE Linux Enterprise Server: `chkconfig boot.multipath`
2. Prevent the multipath device management software from queuing for unavailable disk volumes by modifying its configuration file. In the defaults section of the file `/etc/multipath.conf`, add the following line: `no_path_retry fail`

Ensure that this `no_path_retry` parameter value is not overridden by equivalent entries in the device sections of the same file in which the corresponding Dell EMC Unity storage systems are configured.

1. Ensure that the correct preferred names are used for pathnames that are referencing the same device for physical volumes as they are used in device-mapper multipathing.

Open the `/etc/lvm/lvm.conf` file and set the variable: `preferred_names = [ "^/dev/mpath/", "^/dev/mapper/mpath", "^/dev/[hs]d" ]`

Prerequisites for instant recovery

- You must configure LUNs in the same consistency group. If you want to restore them individually, configure them in multiple consistency groups.
- For remote replication, manually prepare the environment (quiesce application, unmount volumes) and follow steps for failover operation.

Data Protector licenses and components

- An appropriate zero downtime backup extension for Dell EMC Unity storage arrays licenses-to-use (LTU).
- The Dell EMC Unity storage installed on both the application system and the backup system.

Limitations

- In Windows Cluster setup on Virtual Machines, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- In case of VMware backup, hostname of ESX server added in the Dell EMC Unity array should be exactly same as the ESX server name.
- Fiber Channel is not supported. Only iSCSI interface is supported.
- Unity Array does not allow any change in the configuration for the consistency group, if there are snapshots available.
- All LUNs of the consistency group are restored during an instant recovery operation even if a single LUN is selected.
- If there is any change in the consistency group at the array side backup, the previously taken instant recovery restore session will not be applicable as there is a configuration change. In this case, perform the backup again with the new configuration.

ZDB database - SMISDB

ZDB database for the Data Protector Dell EMC Unity storage provider integration is referred to as SMISDB. It keeps information about Dell EMC Unity storage systems. For each system, the following is stored:

- Hostname as recognized in the IP network.
- Dell EMC Unity storage array credentials resides on the Cell Manager in:
  - Linux: `/var/opt/omni/server/db80/smisdb/ DellEmcUnity/login`
  - Windows: `\program_data\OmniBack\server\db80\smisdb\DellEmcUnity\login`

Instant Recovery Database

Instant Recovery database (IRDB) for the Data Protector Dell EMC Unity storage provider maintains information about Dell EMC Unity storage volume, snapID, and arrays.

IRDB stores the following information in IRDB/SMISDB:

IRDB file path –

Linux: /var/opt/omni/server/db80/smisdb/ DellEmcUnity/replica

Windows: \ProgramData\OmniBack\server\db80\smisdb\dellemcunity\replica

Configure the integration

To integrate with the Dell EMC Unity storage system, Data Protector uses the REST server. This enables Dell EMC Unity storage support within the Data Protector ZDB (SMI-S) agent. To configure the Data Protector Dell EMC Unity Storage integration, provide the data that the Data Protector ZDB agent will use to establish connection to a Dell EMC Unity storage system of your choice.

The connection related configuration data includes user credentials that you must add to the ZDB database (the Unity part of SMI-S database). The credentials are bound to a specific application system in the Data Protector cell. The Data Protector ZDB agent then reads the credentials from the ZDB database each time a zero downtime backup for data residing on a Unity storage system is started. The Data Protector ZDB Dell EMC Unity component uses REST to manage the Unity array.

Connection configuration data

To be able to connect to a Dell EMC Unity storage provider system and perform zero downtime backup sessions, the Data Protector ZDB agent needs the following information:

- If the system has multiple IP addresses, use the address by which the Data Protector ZDB agent can access the system.
- Whether the connection uses Secure Sockets Layer (SSL).
- Fully qualified domain name or IP address of the Dell EMC Unity Storage Array.
- Username and password of Dell EMC Unity Array user.

These are stored in the Unity part of the SMISDB.

Configure Dell EMC Unity storage

To establish connection to the Dell EMC Unity storage provider system, use the Data Protector `omnidbzdb` command. Follow the steps:

1. Select the Dell EMC Unity storage system user account that has a proper privilege level on the corresponding domains. Identify and make a note of its username and password.
2. Use the `omnidbzdb` command to establish connection to the Dell EMC Unity storage system and to add the username and password to the ZDB database. Run the following command: `omnidbzdb --diskarray <ArrayFamily> --ompasswd --add <ClientName> --user <UserName> --passwd <password>` where:
   - ArrayFamily is Unity, specified as **dellemcunity**.
   - ClientName is fully qualified domain name of the Dell EMC Unity Array.
   - UserName and password is Dell EMC Unity Array user credentials.

   If you add Unity storage system residing in the cluster environment, run this command for every destination array in the cluster. For example: `omnidbzdb --diskarray dellemcunity --ompasswd --add unitystorage.company.com --user admin --passwd pwd`
3. Use the `omnidbzdb --diskarray Unity--ompasswd --check` command to verify that the Data Protector Unity Storage Provider can connect to the Unity storage system using the configured user authentication data.

> **Tip** For each application system, you can add user credentials of multiple Unity Array user accounts in the Unity REST server. Then add them to SMISDB using the `omnidbzdb` command.

Backup

This section describes configuration of a file system or disk image ZDB using the Data Protector GUI.

With the Dell EMC Unity Storage Provider integration, you can perform the zero downtime backup to tape type only.

Create backup specification

The following limitations apply when creating backup specification:

- Only one snapshot type for target volumes can be created during a ZDB session.
- You cannot back up replicas (target volumes from existing and currently recorded backup sessions).
- If there is not enough space for replica creation on Dell EMC Unity Array, the replica creation fails which eventually fails backup session.

To create a ZDB backup specification/IR backup specification for a Dell EMC Unity storage using the Data Protector GUI, follow the steps:

1. In the Context list, select **Backup**.
2. In the **Scoping Pane**, expand **Backup Specifications**. Right-click **Filesystem** (for both object types: filesystem and disk image) and click **Add Backup**. The Create New Backup dialog box appears.
   In the Filesystem pane, select the **Blank Filesystem Backup** template or some other available template.
   Select **Snapshot** as Backup type and **Storage Provider(s) Plugin** as Sub type. Click **OK**.
3. Under Client systems, select **Application system** and **Backup system**. If the application system is part of a server cluster, select the virtual server.
4. Under Add Storage Provider, select **Dell EMC Unity Storage Provider** from the Storage provider drop-down list and then click **Add**. The Unity Storage provider Options dialog opens. Select **Snapshot** and click **OK**. Dell EMC Unity Storage

Provider is added to the list. You can later change its options by clicking **Edit** or remove it from the list by clicking **Remove**. For IR backup, select **Replica Management options**, and then, select the **Keep the replica after the backup** and **Track the replica for instant recovery** check boxes for Dell EMC Unity Storage Provider.

5. Under Application system options and Backup system options, specify other zero downtime backup options as required. Click **Next**.
6. Select the objects for backup.
   - Filesystem backup: Expand the application system and select the objects to back up. Note that all drive letters or mount points that reside on the system are displayed. You must select only the objects that reside on the Dell EMC Unity storage system, otherwise the ZDB session fails. Click Next.
7. Select the devices to use in the backup session.
8. In the Backup Specification Options group box, click **Advanced** and then the **Storage Provider** tab to open the options pane with Dell EMC Unity storage specific backup options.
   You can specify application system options and modify all other options, except Application system and Backup system (you can change these after you save the ZDB backup specification). Click **Next**.
9. In the Backup Object Summary page, specify additional options.
   - Filesystem backup: To modify options for the listed objects, right-click an object and then click **Properties**.
10. Click **Save As** to save your ZDB backup specification. Optionally, you can click **Save and Schedule** to save, and then schedule the backup specification.

Backup options

The following tables describe the ZDB-related backup options that you can modify when configuring ZDB backup specifications that include storage systems of the Dell EMC Unity Storage family.

Client systems

Application system	The system on which the application runs. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).
Backup system	The system to which your data will be replicated (backed up), and from which the backup data is copied to a backup device.

Application system options

Dismount the filesystems on the application system before replica generation	Select this option to dismount the file systems on the application system before replica creation and remount them afterwards. Additionally, when entire physical drives (on Windows systems) or entire disks or logical volumes (on Linux systems) are selected as backup objects in a disk image backup specification, selecting this option will dismount and later remount all file systems on these objects. If any of these file systems cannot be dismounted, the backup session fails. If an integrated application exclusively controls data I/O on each physical drive, disk, or logical volume that will be backed up, the dismount operation is not needed. In such a case, you can leave this option cleared. Default: not selected.
Stop/quiesce the application command line	If a command is specified in this option, it is invoked on the application system immediately before replica creation. An example is to stop applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option. If the command fails, the command specified in the option Restart the application command line is not invoked. Thus, you may need to implement a cleanup procedure in the command specified in Stop/quiesce the application command line. If the omnirc option ZDB_ALWAYS_POST_SCRIPT is set to 1, the command specified in the option Restart the application command line is always invoked.
Restart the application command line	If a command is specified in this option, it is invoked on the application system immediately after replica creation. An example is to resume operation of applications not integrated with Data Protector. The command must reside on the application system in the default Data Protector administrative commands directory. Do not specify the path to the command in this option.

Backup system options

Use the same mount points as on the application system	This option is not available if the application system is also the backup system (a single-host configuration). If this option is selected, the paths to mount points used for mounting the filesystems of the replica on the backup system are the same as paths to mount points where source volume filesystems were mounted on the application system. If the mount points are already in use, the session fails. For such circumstances, you must select the option **Automatically dismount the filesystems at destination mountpoints** in order for the session to succeed. **Windows systems**: The drive letters must be available, the session fails if the drive letters are not available. Default: not selected.

Root of the mount path on the backup system	This option is only available if the option **Use the same mountpoints as on the application system** is not selected. Specifies the root directory under which the filesystems of the replica are mounted. Where exactly the filesystems are mounted depends on how you define the option Add directories to the mount path. Defaults: **Windows systems**: C:\mnt **Linux systems**: /mnt
Add directories to the mount path	This option is only available if the option Use the same mountpoints as on the application system is not selected. This option enables control over the created mount points. It defines which subdirectories will be created in the directory defined with the Root of the mount path on the backup system option. When Session ID is used in path composition, this guarantees unique mount points. Example for Windows systems: Root directory: C:\mnt Application system: applsys.company.com Backup session ID: 2019–08–22–4 Mount path on the application system: E:\disk1 If Hostname is selected: C:\mnt\applsys.company.com\E\disk1 If Hostname and session ID is selected: C:\mnt\applsys.company.com\2019–08–22–4\E\disk1 If Session ID is selected: C:\mnt\2019–08–22–4\E\disk1 If Session ID and hostname is selected: C:\mnt\2019–08–22–4\applsys.company.com\E\disk1 Default: Hostname and session ID.
Automatically dismount the filesystems at destination mount points	If the mount points are in use (for example, volumes involved in the previous session may still be mounted) and this option is selected, Data Protector attempts to dismount the mounted filesystems. If the option is not selected and the mount points are in use, or if the option is selected and the dismount operation fails, the session fails. Default: not selected.
Leave the backup system enabled	This option is only available if the option Keep the replica after the backup is selected. If this option is selected, the filesystems remain mounted, the volume groups remain imported and active (Linux systems), and the target volumes remain presented after the session. In this case, you can use the backup system for data warehousing purposes. If the replica has to be reused later on (deleted or rotated out), Data Protector automatically connects to the backup system, dismounts the filesystems, unpresents the target volumes, and clears the related logical structures on the backup system. At that point in time, if the filesystems are not mounted to the current backup system, Data Protector cannot perform a proper cleanup, and aborts the operation). If this option is not selected, Data Protector dismounts filesystems, exports volume groups (Linux systems), and unpresents the target volumes on the backup system at the end of the ZDB session. Default: not selected.

Enable the backup system in read/write mode	This option is applicable to UNIX systems only. On Windows systems, filesystems cannot be mounted in the read-only mode. Select this option to enable write access to volume groups and filesystems on the backup system. For backup purposes, it is sufficient to activate the backup system volume groups and mount the filesystems in the read-only mode. For other tasks, the read/write mode may be needed. Note that when this option is selected, the replica is open to modifications while the backup system is online. Consequently, data restored from such a replica includes all potential modifications. Defaults: **Windows systems**: not selected. **Linux systems**: not selected.

Note In a ZDB session, the mount points to which filesystems of the replica are mounted on the backup system are the same as the mount points to which source volumes were mounted on the application system, if at least one of the following conditions is met:

- The GUI option Use the same mountpoints as on the application system is selected.
- The omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 1.

If the option Use the same mountpoints as on the application system is not selected, and the omnirc option ZDB_PRESERVE_MOUNTPOINTS is set to 0, the mount points are determined by the GUI options Root of the mount path on the backup system and Add directories to the mount path, while the omnirc options ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH are ignored.

Restore

This section describes configuring and running a filesystem or disk image restore of the data backed up using the Data Protector Dell EMC Unity Storage integration.

The data backed up in a ZDB session using Dell EMC Unity Storage can be stored on backup media only (ZDB to tape).

Data backed up in ZDB-to-tape sessions can be restored from the backup media to the application system.

Tip You can improve the data transfer rate by connecting a backup device directly to the application system.

Instant Recovery

This section describes instant recovery of the data backed up using the Data Protector Dell EMC Unity Storage integration.

Three types of backup options available in Dell EMC Unity are:

- Tape (Writes to a tape device only, no instant recovery, only recovery from tape)
- Disk + Tape (Supports instant recovery from disk, no instant recovery, only recovery from tape)
- Disk (Supports instant recovery from disk, no instant recovery, only recovery from tape)

Two types of backup are supported:

- Snapshot backup/restore (Local): In case of Local Instant recovery, the LUN replica and the volume snapshot reside on the same local array. During instant recovery, the local copy will be used for performing restore.
- During local replication, both the original volume and its remote volume along with its LUN replica resides on the same site.

Remote replication

For performing remote replication, the LUN replica must be on the remote site. This is achieved by performing synchronization. During instant recovery, the remote copy will be used for performing restore to remote volume.

Data Protector offers Dell EMC Unity instant recovery for agents within a VMware Virtual Machine (VM). This is supported only for physical Raw device mapping (RDM).

Prerequisite for remote replication instant recovery

1. Manually prepare the application host for IR (Freeze the application, remove the mountpoint from the application host).
2. Perform the following steps for fail over to destination. Refer *Remote Replication failover and failback* topic. It makes the destination volume read-write, and the role is reversed at this stage. **Note:** As a prerequisite, administrator must complete the steps manually on Data Protector. - Select Instant Recovery context from Data Protector GUI drop-down list. - Select the file system drive to restore. - Select restore session and click **Restore**. This will restore data at remote destination.
3. New Destination (original source) volume would be automatically synced with destination volume (original destination).

4. At this point, if you want to do a fail back, you must do it manually. Refer *Remote Replication failover and failback* topic. Post-IR, perform the post-configuration operations manually, including mounting the mount-point and unfreezing.

Prerequisite for remote replication Oracle instant recovery

To perform an instant recovery on Linux and Windows:

1. Shut down the Oracle database instance using sqlplus. In case of RAC, shut down all instances. For example: /sqlplus /nolog connect sys/oracle@APPN as sysdba sql> shutdown immediate sql> exit
2. For Linux: Unmount the volume before the IR session - umount /dev/Unity_ESX2/lvol0
   - For Windows: Make the disks offline before the IR session.
3. Prepare Application Host to remove volume (export, deactivate, and backup Volume Group).
4. Remove hard disks from Application host on vCenter server.
5. Rescan volumes on VM, and confirm that the disk is not available any more on the Application Host.
6. Execute instant recovery. **Note**: If you are using the Oracle integration for instant recovery, ensure that you deselect the Recovery checkbox.
7. Add the hard disks back to the application host from the vCenter server.
8. Rescan Application Host for new volume.
9. Add the exported Volume Group.
10. For Linux: Mount the volume after the IR session. For Windows: Make the disks online after the IR session.
11. Follow the steps as mentioned in the Oracle database recovery after the instant recovery section.

Instant recovery using GUI

Complete the following steps to perform instant recovery from Data Protector GUI:

1. Select **Instant Recovery** from context panel.
2. Expand **Filesystem**. IR backup specifications are listed.
3. Expand the desired specification. Double click the session id. Instant recovery panel opens.
4. Click **Restore**.

Remote Replication failover and failback

1. Go to the LUN properties and click on **Replication** tab.
2. Click **Yes** in Failover Session window.
3. Perform resume operation on destination side. It makes the destination volume read-write, and reverses the roll as well.
4. Click **Yes** to resume the session.
5. Optionally, you can do a fail back by clicking on failback button.

Troubleshoot

This section lists general checks and verification that you may need to perform when you encounter problems with the Data Protector Dell EMC Unity Storage provider integration.

- ◦
  -
    -
      -

Problem symptoms	Workaround/Solution
The VMware backup fails during presentation.	1. Remove the http proxy from .bashrc file present in /root/.bashrc of Linux Cell Manager. 2. Disable firewall and restart the Cell Manager.
Check configuration of Dell EMC Unity fails. The -check opion of omnidbzdb command fails or check configuration of backup fails.	Ensure that the entry made in SMISDB through the omnidbzdb command is of Dell EMC Unity storage provider.
The backup fails during presentation with iSCSI.	Make sure that the backup host is logged in to iSCSI target on the array.
Restored data is not visible after successful completion of Instant Recovery session.	To make data visible, move the restored disk to offline state and bring it back to online state.

Schedule ZDB sessions

This feature is available in the Premium Edition

To schedule a filesystem or disk image ZDB, create a new backup specification or modify an existing backup specification.

Start interactive ZDB sessions

This feature is available in the Premium Edition

In a Microsoft Cluster Service configuration, if a cluster resource disk is to be backed up, it should not be in a maintenance mode before the backup.

Note When running concurrent ZDB sessions using one or several application systems, consider the limitations described in the Data Protector Concepts Guide.

Using the GUI

Complete the steps below:

1. In the **Context List**, select **Backup**.
2. In the Scoping Pane, expand **Backup**, **Backup Specification**, and **Filesystem**. Right-click the required backup specification, and select **Start Backup**.
3. The **Start Backup** dialog box appears.

   For ZDB to tape and ZDB to disk+tape, specify **Backup Type**.

   To run ZDB to disk or ZDB to disk+tape (**Track the replica for instant recovery** selected), select **To disk** or **To disk+tape** in the **Split mirror/snapshot backup** drop-down list.

   For information on options, press **F1**.
4. Click **OK**.

Using the CLI

Execute:

ZDB to tape, ZDB to disk+tape: omnib -datalist Name

ZDB to disk: omnib -datalist Name -disk_only

where Name is the backup specification name.

Alternate paths support

For systems with multiple host adapters and connections to a disk array, the multi-path device management solution performs dynamic load balancing and monitors each path to ensure that the I/O subsystem completes its transactions. If a path between a disk array and a server fails, alternate path software automatically switches to an alternate path, removing the failed path from I/O rotation without data loss. Failover is transparent to applications, so they continue unaffected.

Note On HP-UX 11.31 systems, the multi-path device management software is not supported since the operating system has native device multi-pathing capability.

With the P9000 XP Disk Array Family, you can control AutoPath load balancing using the OB2AUTOPATH_BALANCING_POLICY omnirc option (by default, AutoPath Round Robin load balancing policy is used).

When using AutoPath, consider the following:

- During a ZDB-to-tape session, if a failover to an alternate path occurs and the AutoPath Shortest Queue Length load balancing is set, the session completes with errors.
- If a failover to an alternate path occurs during disk image backup without using raw logical volumes (rlvols), the session completes with errors. If rlvols are used, the session completes successfully.

Cluster configurations

Data Protector ZDB agents support:

- Serviceguard (on HP-UX systems) with all disk array models supported by Data Protector
- Veritas Cluster (on Solaris systems) with disk arrays of the P9000 XP Disk Array Family
- Microsoft Cluster Server (on Windows systems) with disk arrays of the P9000 XP Disk Array Family

If the application system is in a server cluster, the backup system must be outside this cluster: it may run in a different cluster or may not be part of a cluster at all.

Important If the backup system is running in a server cluster, target volumes on this system must not be configured as cluster resources.

Important If a failover to the remote site happens, the disk array configuration changes from the combined CA+BC P9000 XP (P9000 XP Disk Array Family) to BC P9000 XP (P9000 XP Disk Array Family). This means that the next ZDB session can no longer start automatically, so the ZDB backup specification must be updated to reflect the configuration change.

Sections below discuss supported ZDB cluster configurations.

Client on the application system in a cluster through EMC GeoSpan for Microsoft Cluster Service illustrate Data Protector *application* backup disk array configurations and scenarios. For *filesystem and disk image* backup, only a Data Protector ZDB agent is needed; an application database and binaries are not installed as presented in the figures. On Windows systems, to perform zero downtime backup and instant recovery using Microsoft Volume Shadow Copy Service, the Data Protector component MS Volume Shadow Copy Integration must be installed.

Note For applications in a cluster, use a floating IP address rather than a static one. This allows a successful backup to start even after a local failover.

Client on the application system in a cluster, Cell Manager in a cluster

Cell Manager is installed in a cluster on any system that is not a backup or application system.

Scenarios

- Application failover during backup: session fails and must be restarted manually.
- Application failover before backup: session completes successfully.
- Cell Manager failover during backup: failed session is automatically restarted, provided the option **Restart backup of all objects** is selected.
- Cell Manager failover before backup: session completes successfully.

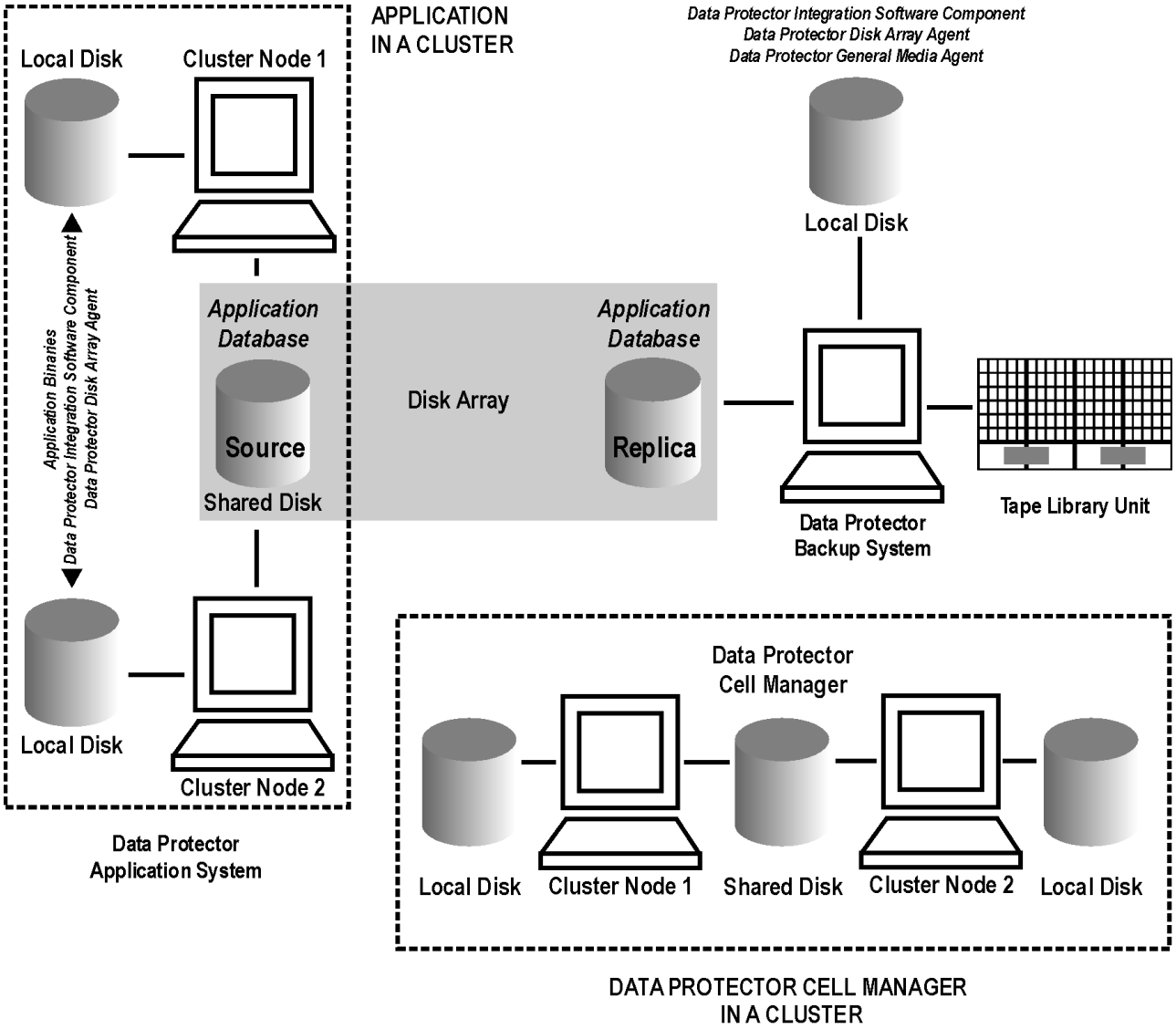
Limitations

- Not supported in Veritas Cluster.

Install:

- On the application system on all cluster nodes on local disks: application binaries, Data Protector integration software component, Data Protector ZDB agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be on a disk array.
- On any system cluster shared disk: Cell Manager.
- On the backup system on local disks: Data Protector integration software component, Data Protector ZDB agent, Data Protector General Media Agent.

Client on the application system in a cluster, Cell Manager in a cluster



Cell Manager on the backup system in a cluster

Scenarios

- Cell Manager failover during backup: session is automatically restarted, provided the option **Restart backup of all objects** is selected.
- Cell Manager failover in between backups: session completes successfully.

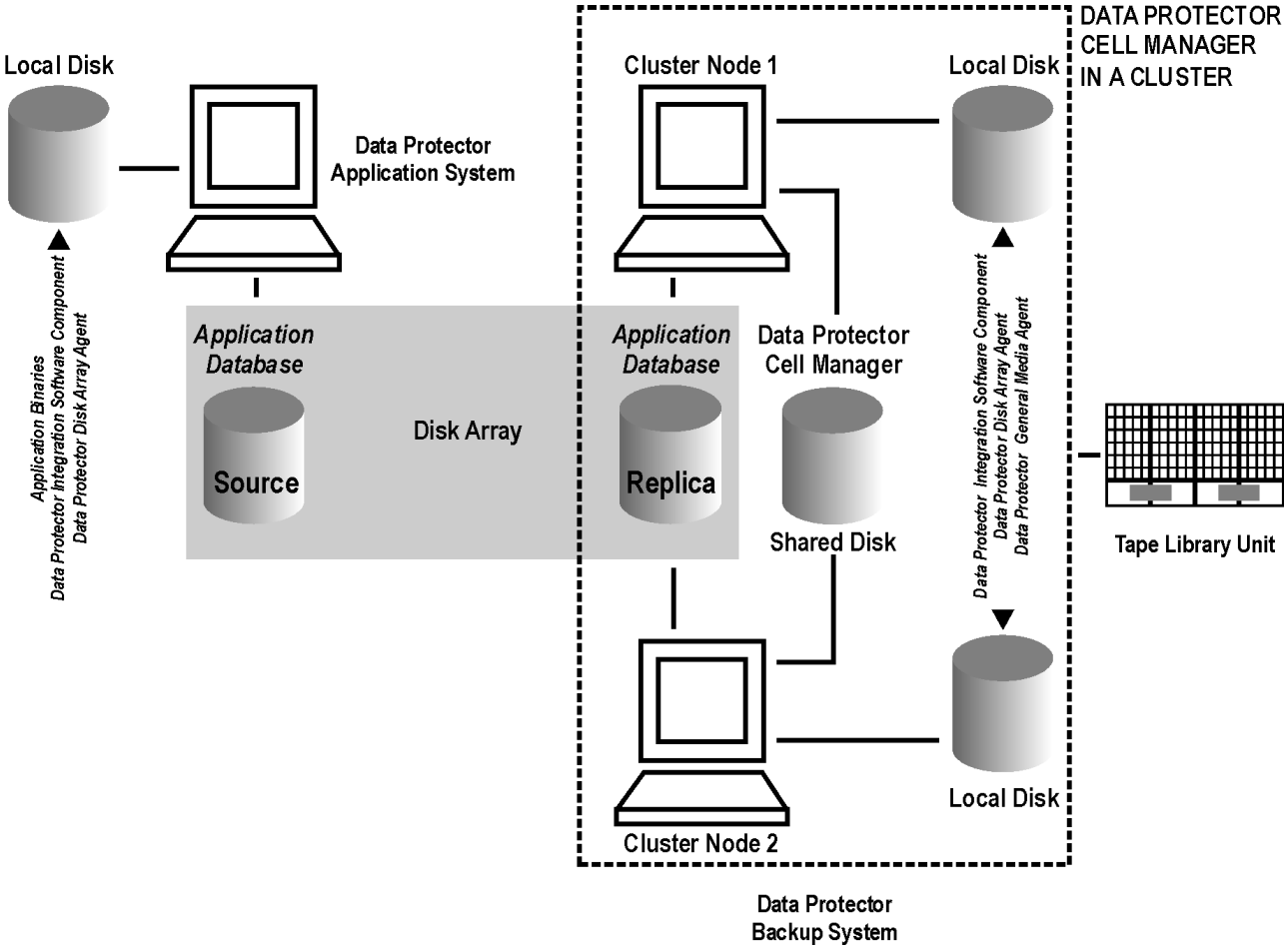
Limitations

- Not supported in Veritas Cluster.

Install:

- On the application system: application binaries, Data Protector integration software component, Data Protector ZDB agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be a disk array replicated disk.
- On the backup system cluster shared disk: Cell Manager. Note that this shared disk must be a disk array replicated disk.
- On the backup system on all cluster nodes on local disks: Data Protector integration software component, Data Protector ZDB agent, Data Protector General Media Agent.

Cell Manager on the backup system in a cluster



Cell Manager and client on the application system in a cluster

Scenarios

- Application or Data Protector failover during backup: session is restarted automatically.
- Application or Data Protector failover in between backups: session completes successfully.

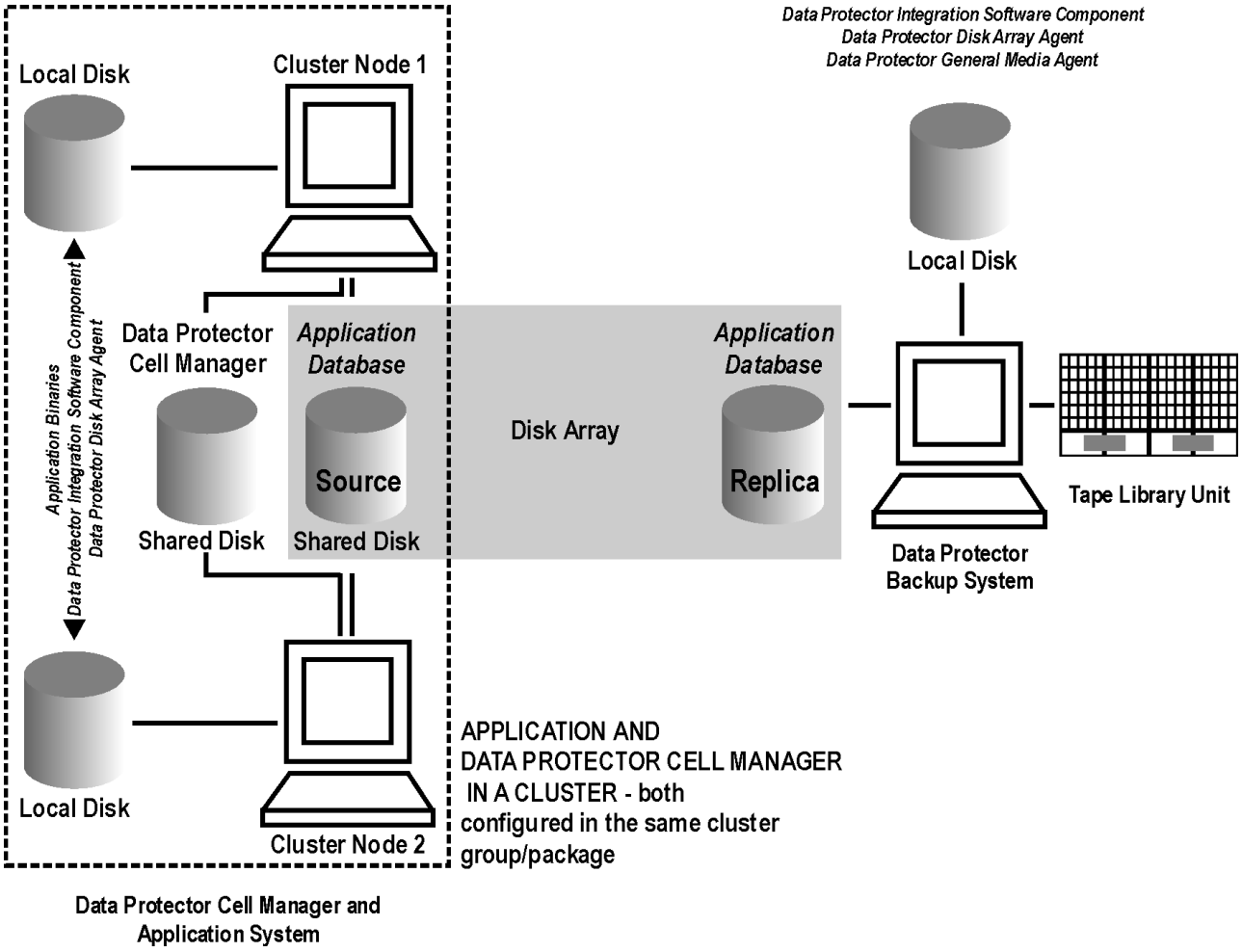
Limitations

- Not supported in Veritas Cluster.
- Split mirror restore is not possible (P9000 XP Disk Array Family).

Install:

- On the application system on all cluster nodes on local disks: application binaries, Data Protector integration software component, Data Protector ZDB agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be a disk array replicated disk.
- On the application system cluster shared disk: Cell Manager.
- On the backup system on local disks: Data Protector integration software component, Data Protector ZDB agent, Data Protector General Media Agent.
- Configure Cell Manager cluster’s critical resources in the same cluster group/package as those for the application being backed up.

Cell Manager and client on the application system in a cluster



Client on the application system in a cluster, Cell Manager not in a cluster

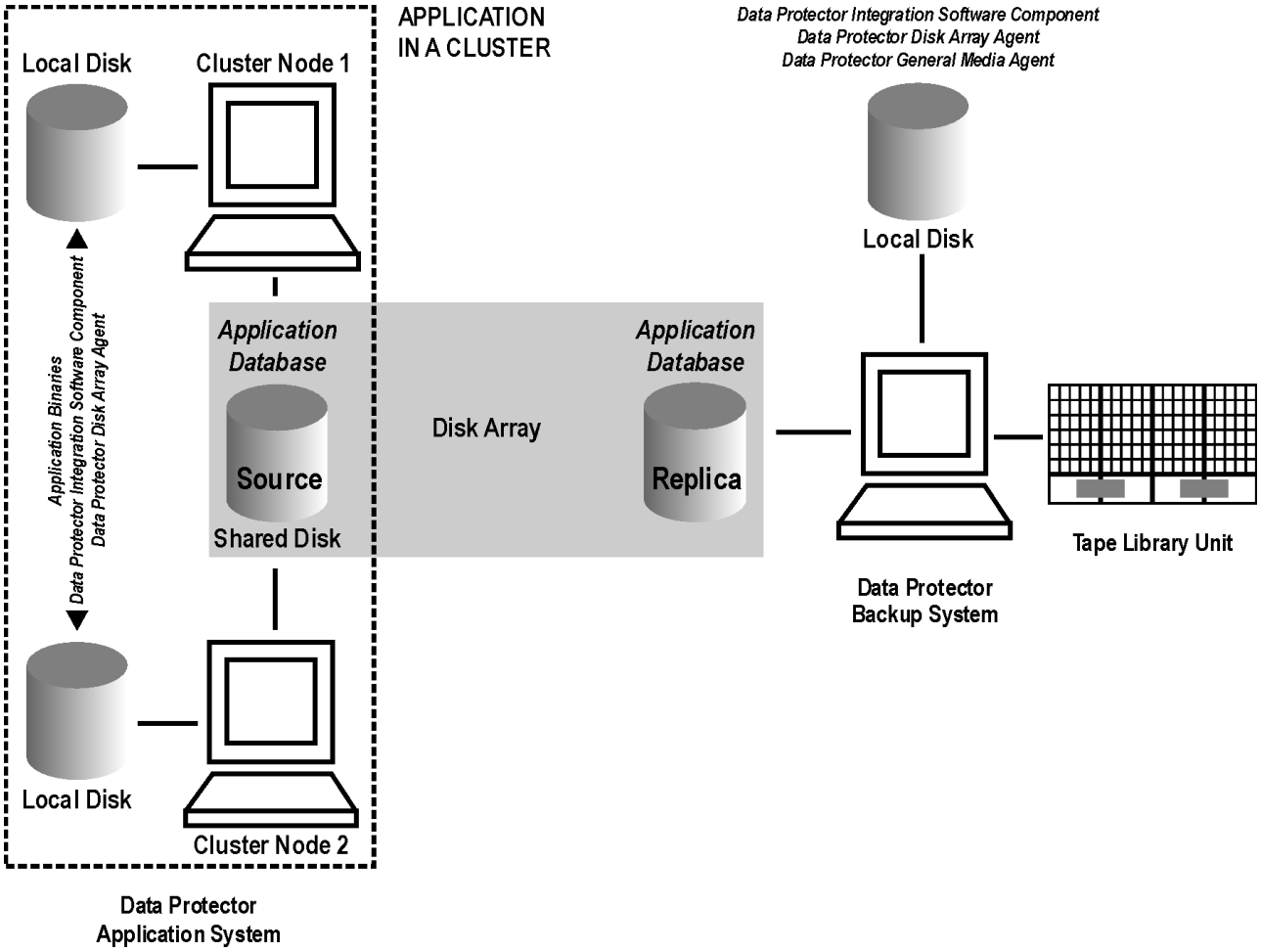
Scenarios

- Application failover during backup: session fails and must be restarted manually.
- Application failover in between backups: session completes successfully.

Install:

- On the application system on all cluster nodes on local disks: application binaries, Data Protector integration software component, Data Protector ZDB agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be on a disk array.
- On the backup system on local disks: Data Protector integration software component, Data Protector ZDB agent, Data Protector General Media Agent.

Client on the application system in a cluster



Client on the application system in a cluster, Cell Manager on the backup system in a cluster

Scenarios

- Application failover during backup: session fails and must be restarted manually.
- Application failover before backup: session completes successfully.
- Cell Manager failover during backup: failed session is automatically restarted, provided the option **Restart backup of all objects** is selected.
- Cell Manager failover before backup: session completes successfully.

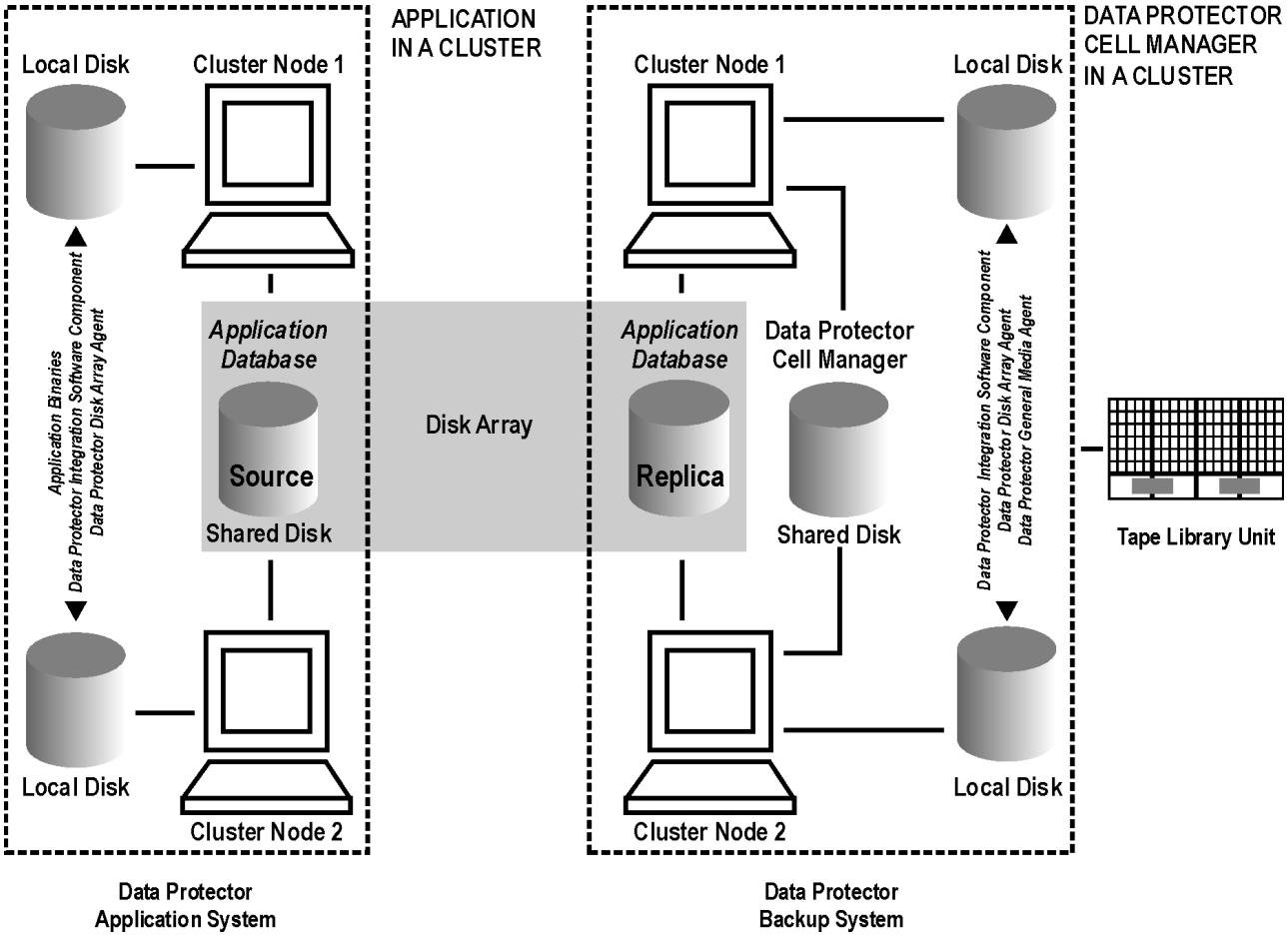
Limitations

- Not supported in Veritas Cluster.

Install:

- On the application system on all cluster nodes on local disks: application binaries, Data Protector integration software component, Data Protector ZDB agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be a disk array replicated disk.
- On the backup system cluster shared disk: Cell Manager.
- On the backup system on all cluster nodes on local disks: Data Protector integration software component, Data Protector ZDB agent, Data Protector General Media Agent.

Client on the application system in a cluster, Cell Manager on the backup system in a cluster



EMC GeoSpan for Microsoft Cluster Service

Cell Manager is not in a cluster; application client is in a cluster on the application system.

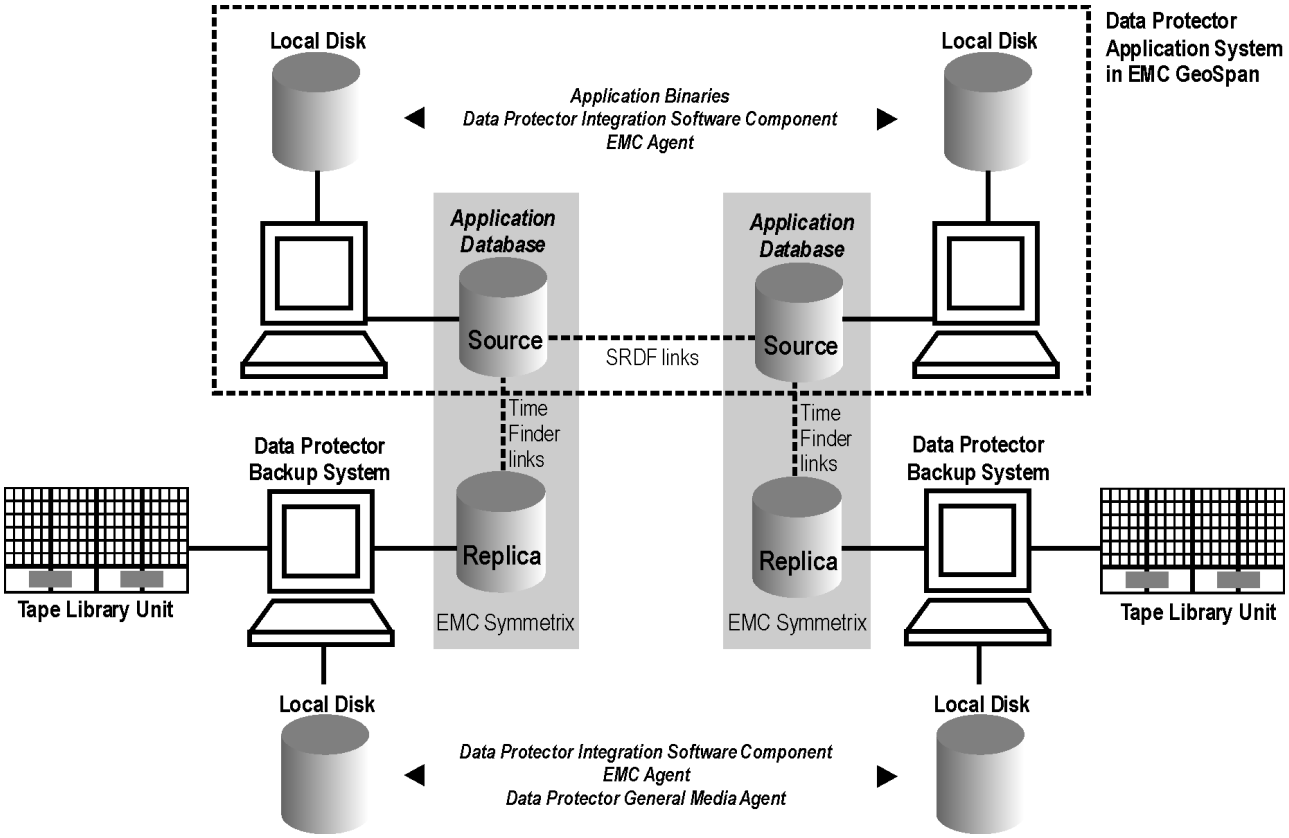
Scenarios

- Application/hardware failover during backup: session fails and must be restarted manually. The backup system in the backup specification must be set as the backup system for the active node.
- Application failover before backup: session completes successfully if the backup system is set as the backup system for the active node.

Install:

- On the application system on all cluster nodes on local disks: application binaries, Data Protector integration software component, EMC Agent.
- On the application system cluster shared disk: application database. Note that this shared disk must be a disk array replicated disk.
- On the backup system on local disks: Data Protector integration software component, Data Protector EMC Agent, Data Protector General Media Agent.

EMC GeoSpan for Microsoft Cluster Service


Local Disk
Application Binaries
Data Protector Integration Software Component
EMC Agent
Local Disk
Data Protector
Application System
in EMC GeoSpan
Application
Database
Source
SRDF links
Source
Application
Database
Time
Finder
links
Time
Finder
links
Data Protector
Backup System
Replica
Replica
Data Protector
Backup System
Tape Library Unit
EMC Symmetrix
EMC Symmetrix
Tape Library Unit
Local Disk
Data Protector Integration Software Component
EMC Agent
Data Protector General Media Agent
Local Disk

Instant recovery in a cluster

With an application or filesystem running on Serviceguard or Microsoft Cluster Server on the application system, instant recovery requires some *additional* steps. Additionally, there are limitations regarding instant recovery on Microsoft Cluster Server.

Important If HP-UX LVM mirroring is used, see also Instant recovery and LVM mirroring under Configure P9000 XP Disk Array family.

Vertias Cluster Volume Manager

Prerequisites

Before performing the instant recovery in Veritas Cluster, ensure the following:

- SMISA Agent must run on the master node during instant recovery.
- The File System must be dismounted on all other hosts, except the master node before instant recovery.
- The `/etc/default/vxdg` file must be created with the following content in the master node:

  ```
  enable_activation=true
  ```

Note Restart the `deamon` file using the following command:

```
vxconfigd -k
```

Serviceguard

Complete the following steps:

1. Stop the application cluster package:

   ```
   cmhaltpkg ApplicationPackageName
   ```

2. In the *shell script for starting, shutting down and monitoring the database*, comment the lines that monitor application processes (by putting # at the beginning of the line).

   Oracle example

   ```
   #set -A MONITOR_PROCESSES ora_pmon_${SID_NAME} ora_dbw0_${SID_NAME} ora_ckpt_${SID_NAME} ora_smon_${SID_NAME} ora_lgwr_${SID_NAME} ora_reco_${SID_NAME} ora_arc0_${SID_NAME}
   ```

   This shuts down the application (database) running in the cluster without causing a failover.

3. Restart the application cluster package:

   ```
   cmrunpkg ApplicationPackageName
   ```

4. Shut down the application (database).
5. Start instant recovery.

   Important When performing instant recovery to the node other than that backed up, select the**Check the data configuration consistency** instant recovery option.

6. When the session finished, stop the application cluster package:

   ```
   cmhaltpkg ApplicationPackageName
   ```

7. Uncomment the lines (delete #) that you previously commented to re-enable an application failover.
8. Restart the application cluster package:

   ```
   cmrunpkg ApplicationPackageName
   ```

9. After instant recovery, recover the database.

Note After resynchronization with the application system finishes, enable replicated volume groups on the application system in the exclusive mode by setting the `ZDB_IR_VGCHANGE_A` omnirc option on the application system to `vgchange -a e`.

Microsoft Cluster Server

Limitations

- Instant recovery of a cluster quorum disk is not supported because the cluster service must never lose the connection with the quorum disk, which happens during instant recovery (when disks are unpresented).
- In the configuration where a local disk is mounted to a cluster resource disk, instant recovery of a such disk is not supported.
- Any target cluster disk resource must be owned by the currently active node. Instant recovery is not supported if the disk resource is owned by the non-active node.
- Instant recovery of combination of cluster and non-cluster disks is not supported.

Considerations

- In a Microsoft Cluster Server environment, disks are distinguished by their disk signature. Because two disks cannot have the same signature, the operating system dynamically changes the signature once it detects the replica on the backup system. During the instant recovery procedure, Data Protector restores the disk signature to ensure that the recovered disk will have the same signature as the original disk on the application system. Data Protector will display notifications, informing you about the changed signature.

Complete the following steps:

1. Using the Cluster Administrator utility or Cluster CLI, take the application cluster resource offline.
2. Shut down the application (database).
3. Start instant recovery.
4. Restart the application (database).
5. Recover the database.
6. Using the Cluster Administrator utility or CLI, put the application cluster resource online.

ZDB omnirc options

This feature is available in the Premium Edition

To customize operation of the ZDB agents, you can set the omnirc options on the application system and the backup system. Changes to the options in the omnirc file on a particular system do not affect the agents that are already running on the system at the moment the changes are made.

Common ZDB options

This section explains omnirc options that can be set for all ZDB agents.

ZDB_PRESERVE_MOUNTPOINTS: Determines, together with ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH, the mount point creation on the backup system.

If ZDB_PRESERVE_MOUNTPOINTS is set to 0 (default value), the mount point for a backed up filesystem is created as follows:

- When ZDB_MULTI_MOUNT is set to 1:
  - *P9000 XP Array:*

    BU_MOUNT_PATH/Application_System_Name/Mount_Point_Name_on_Application_System_LDEV_MU#
- When ZDB_MULTI_MOUNT is set to 0 or not set:

  BU_MOUNT_PATH/Application_System_Name/Mount_Point_Name_on_Application_System

where BU_MOUNT_PATH corresponds to one of the following locations on a Data Protector client:

- With ZDB_MOUNT_PATH set: ZDB_MOUNT_PATH
- With ZDB_MOUNT_PATH not set:
  - Windows system: Data_Protector_home\tmp
  - UNIX systems: /var/opt/omni/tmp

If ZDB_PRESERVE_MOUNTPOINTS is set to 1, the mount point for a backed up filesystem is created on the backup system at:

- *Windows systems:* \Mount_Point_Name_on_Application_System or Drive_Letter_on_Application_System:\
- *UNIX systems:* /Mount_Point_Name_on_Application_System

Important For zero downtime backup of disk images, Oracle 8/9/10 databases, SAP R/3 databases, and Microsoft SQL Server 2000 databases, Data Protector adopts that ZDB_PRESERVE_MOUNTPOINTS is set to 1, and ignores its override and the options ZDB_MULTI_MOUNT and ZDB_MOUNT_PATH.

ZDB_MULTI_MOUNT: Determines, together with ZDB_PRESERVE_MOUNTPOINTS and ZDB_MOUNT_PATH, the mount point creation on the backup system.

ZDB_MULTI_MOUNT is ignored if ZDB_PRESERVE_MOUNTPOINTS is set to 1.

If ZDB_MULTI_MOUNT is set to 1 (default value), LDEV MU# (P9000 XP Array) is appended at the end of the mount point path, thus enabling every group of mount points for one replica in the replica set to be mounted to their own mount points.

If ZDB_MULTI_MOUNT is set to 0, the selected group of mount points for one replica in the replica set is mounted to the same mount points.

ZDB_MOUNT_PATH: Determines, together with ZDB_PRESERVE_MOUNTPOINTS and ZDB_MULTI_MOUNT, the mount point creation on the backup system.

ZDB_MOUNT_PATH is ignored if ZDB_PRESERVE_MOUNTPOINTS is set to 1.

By default, this option is not set. In this case, the first part of the mount point path is defined as:

Windows systems: Data_Protector_home\tmp

UNIX systems: /var/opt/omni/tmp

To set this option, specify the first part of the mount point path.

> **Note** If the option **Use the same mountpoints as on the application system** is not selected in the GUI, the option ZDB_MOUNT_PATH is ignored and values of the ZDB options **Root of the mount path on the backup system** and **Add directories to the mount path** specified in the Data Protector GUI are used for mount point creation in the ZDB session instead.

ZDB_ALWAYS_POST_SCRIPT: By default, the command specified in the option **Restart the application command line** is not executed if the command specified in the option **Stop/quiesce the application command line** fails.

If this option is set to 1, the command specified in the option **Restart the application command line** is always executed.

Default: 0.

ZDB_IR_VGCHANGE: On HP-UX platform, determines the mode in which replicated volume groups on the application system are activated after restore. The option can be set on the application system only.

> **Note** This option is not supported on EMC.

Select from the following modes:

- *Exclusive*: ZDB_IR_VGCHANGE_A=vgchange -a e
- *Shared*: ZDB_IR_VGCHANGE_A=vgchange -a s
- *Normal (default)*: ZDB_IR_VGCHANGE_A=vgchange -q n -a y

> **Important** Use exclusive mode to enable instant recovery if an application/filesystem runs in the Serviceguard cluster on the application system.

ZDB_IR_MANUAL_AS_PREPARATION: To manually prepare the application system for instant recovery (dismounting filesystems and disabling volume groups), set this option to 1. After instant recovery, manually enable volume groups and mount filesystems again.

Use this option also if automatic preparation of the application system fails because the application data configuration changed after backup. For example, if a failover to a secondary cluster node occurred between backup and instant recovery, Data Protector may have difficulty matching the secondary node resources to resources that existed on the primary node during backup.

Default: 0.

3PAR StoreServ Storage specific options

This section explains 3PAR StoreServ Storage specific omnirc options.

> **Important** Besides the 3PAR_MSGWAITING_INTERVAL and 3PAR_COPYBACKSTS_QUERY_INTERVAL, the following options apply to the 3PAR StoreServ Storage: ZDB_VOLUMESCAN_RETRIES, ZDB POST_RESCAN_INIT_DELAY, ZDB_LVM_PREFERRED_PVG, SMISA_MSGWAITING_INTERVAL, SMISA_FORCE_DISMOUNT, ZDB_DONOT_PRESENT_DISKS, ZDB_SKIP_LOCK_AT_DISMOUNT, ZDB_SMISA_LVM_MIRRORING_DISABLED, SMISA_CHECKFORABORT_DELAY.

3PAR_MSGWAITING_INTERVAL:

Determines the time interval between messages reporting the snapclone creation progress (monitored during ZDB-to-tape and

ZDB-to-disk+tape sessions immediately after the backup system preparation). The backup option Delay the tape backup by a maximum of n minutes if the snapclones are not fully created must be selected.

Default: 10 minutes.

3PAR_COPYBACKSTS_QUERY_INTERVAL: Determines the time interval between status checks.

ZDB_VOLUMESCAN_RETRIES: During the backup system preparation, the system is scanned for new filesystem volumes. This option determines the number of scans required to identify the new volumes.

The option is only applicable on Windows.

Default: 5 retries. If scanning takes longer increase the default setting.

ZDB_POST_RESCAN_INIT_DELAY: During the backup system preparation, the system is scanned for new filesystem volumes. This option sets the time period to wait before initiating next scan of new filesystem volumes.

The option is only applicable on Windows.

Default: 30 seconds.

SMISA_BACKUPPREPARE_RETRY: Determines the number of the 3PAR SMI-S Agent queries checking for completion of container allocation or creation and setting the write cache policy on the source volumes to the write-through mode during zero downtime backup sessions. If the operations do not complete by the time the last query is made, the 3PAR SMI-S Agent aborts the currently running session.

Default: 10 queries.

SMISA_BACKUPPREPARE_DELAY: Determines the interval (specified in seconds) between the 3PAR SMI-S Agent queries checking for completion of container allocation or creation and setting write cache policy on the source volumes to the write-through mode during zero downtime backup sessions.

Default: 120 seconds.

SMISA_CONTAINERCREATION_RETRY: Determines the number of the 3PAR SMI-S Agent queries checking for completion of container allocation or creation during instant recovery sessions. If the operation does not complete by the time the last query is made, the 3PAR SMI-S Agent aborts the currently running session.

Default: 10 queries.

SMISA_CONTAINERCREATION_DELAY: Determines the interval (specified in seconds) between the 3PAR SMI-S Agent queries checking for completion of container allocation or creation during instant recovery sessions.

Default: 120 seconds.

SMISA_MSGWAITING_INTERVAL: Determines the interval (specified in seconds) between session messages reporting the progress of container allocation or creation during zero downtime backup and instant recovery sessions, between session messages reporting the progress of setting the write cache policy on the source volumes to the write-through mode during zero downtime backup sessions, and between session messages reporting the progress of deleting storage volumes from the disk array.

Default: 300 seconds.

SMISA_CHECKFORABORT_DELAY: Many operations that the 3PAR SMI-S Agent triggers are long-lasting. During the wait for their completion, the agent periodically checks whether an abort request was issued. This option determines the interval (specified in seconds) between each pair of checks for the abort request.

Default: 2 seconds.

SMISA_FORCE_DISMOUNT: Determines whether the Data Protector 3PAR SMI-S Agent performs forced dismount of the volumes which are locked by the Windows system processes and cannot be dismounted using the ordinary dismount operation. You can enable forced dismount operation by setting this option to `1`.

Default: `0` (disabled). Possible: `0` | `1`.

ZDB_DONOT_PRESENT_DISKS: During ZDB-to-disk sessions, if this option is set to `1`, the 3PAR SMI-S Agent does not present volumes to the backup system. ZDB-to-disk+tape and ZDB-to-tape sessions are not affected by the option.

Default: `0` (disabled). Possible: `0` | `1`.

ZDB_SKIP_LOCK_AT_DISMOUNT: On Windows systems, the 3PAR SMI-S Agent locks the volumes on the application system prior to dismounting them. If this option is set to `1`, the volumes do not get locked. Other operating systems are not affected by the option.

Default: `0` (disabled). Possible: `0` | `1`.

EVA_CIMOM_CONNECTION_TIMEOUT: Determines the interval (specified in seconds) for which the 3PAR SMI-S Agent waits for a response to an outstanding request from the CIMOM.

Default: 900 seconds.

EVA_CIMOM_QUERY_RETRIES: CIMOM operations include communication over the network and may fail unexpectedly. This option determines the maximum number of retried attempts the 3PAR SMI-S Agent performs if the CIMOM returns an unexpected response.

Default: 10 attempts.

EVA_CIMOM_QUERY_INTERVAL: Determines the interval (specified in seconds) between each pair of attempts, whose maximum number is defined by `EVA_CIMOM_QUERY_RETRIES`.

Default: 10 seconds.

SMISA_ENFORCE_MULTISNAP: Determines how Data Protector behaves if disk array limitation on the number of source disks that can be involved in multisnapping is exceeded

If multisnapping is enforced by `SMISA_ENFORCE_MULTISNAP`, the zero downtime backup session is aborted.

If multisnapping is not enforced, Data Protector creates target volumes sequentially (in the first case) or attempts to create target volumes with several multisnapping operations instead of only one (in the other two cases).

Note that `SMISA_ENFORCE_MULTISNAP` should not be used to enforce multisnapping in zero downtime backup sessions for backing up the Oracle Server data in ASM configurations, since the 3PAR SMI-S Agent detects such sessions automatically.

Default: `0` (multisnapping not enforced). Possible: `0` | `1`.

SMISA_WAIT_MIRRORCLONE_PENDING_TIMEOUT: Determines the time period (specified in minutes) for which the 3PAR SMI-S Agent waits for the mirrorclone link to transition from some other state into the synchronized state. If the time period expires before the mirrorclone link gets into the synchronized state, the 3PAR SMI-S Agent aborts the session. The option affects only the zero downtime backup sessions for which the selected snapshot source is mirrorclone.

Default: 60 minutes.

SMISA_WAIT_MIRRORCLONE_PENDING_RETRY: Determines the interval (specified in seconds) between each pair of checks of the mirrorclone link state when waiting for the link to transition into the synchronized state. The option affects only the zero downtime backup sessions for which the selected snapshot source is mirrorclone.

Default: 30 seconds.

P9000 XP Array specific options

This section explains P9000 XP Array-specific `omnirc` options.

ZDB_BACKUP_VG_EXIST: On HP-UX platform, for systems configured with multiple HBAs and connections to a disk array, the alternate paths solution performs dynamic load balancing. By default, during preparation for backup and restore, Data Protector creates a volume group with the disk on the first HBA as the primary path.

To disable volume group autoconfiguration on the backup host and load balance the data across multiple paths manually, set this option to `1`. The existing backup volume group will be used in the next backup or restore session.

Note If this option is set, volume groups are not removed from /etc/lvmtab on the backup system after each backup.

Default: 0.

OB2AUTOPATH_BALANCING_POLICY: Determines the AutoPath load balancing policy used.

AutoPath provides enhanced data availability for systems configured with multiple host adapters and connections to a disk array. When several alternate paths are available, AutoPath dynamically balances data load between the alternate paths to achieve optimum performance.

Possible values are:

- 0 [none] – No policy
- 1 [RR] – Round Robin policy (default)
- 2 [SQL] – Shortest Queue Length policy

  Important During a ZDB-to-tape session, if the AutoPath Shortest Queue Length load balance policy is set and failover to an alternate path occurs, the session is aborted.

- 3 [SST] – Shortest Service Time policy

SSEA_SPLIT_REPORT_RATE: During the split, the P9000 XP Agent checks the status of mirrored disks within an interval determined by SSEA_SPLIT_SLEEP_TIME for the number of times determined by SSEA_SPLIT_RETRY.

SSEA_SPLIT_REPORT_RATE determines the frequency of displaying the mirrored disks' status to the Data Protector Monitor. For example, if SSEA_SPLIT_SLEEP_TIME is 2 seconds and SSEA_SPLIT_REPORT_RATE is 5, the status is displayed for every fifth check (every 10 seconds).

Default: 5.

SSEA_SPLIT_RETRY: During the split, the P9000 XP Agent checks the mirrored disks' status within an interval determined by SSEA_SPLIT_SLEEP_TIME. SSEA_SPLIT_RETRY determines the number of retries for the checks. If there is no progress after that, the split is aborted.

Default: 120 retries.

SSEA_SPLIT_SLEEP_TIME: During the split, the P9000 XP Agent checks the mirrored disks status for the number of times determined by SSEA_SPLIT_RETRY. SSEA_SPLIT_SLEEP_TIME determines the time interval between the status checks.

Default: 2 seconds.

SSEA_SYNC_REPORT_RATE: During the disks' resynchronization, the P9000 XP Agent checks the mirrored disks' status within an interval determined by SSEA_SYNC_SLEEP_TIME for the number of times determined by SSEA_SYNC_RETRY.

SSEA_SYNC_REPORT_RATE determines the rate of displaying the mirrored disks status. For example, if SSEA_SYNC_SLEEP_TIME is 5 seconds and SSEA_SPLIT_REPORT_RATE is 2, the status is displayed for every second check (every 10 seconds).

Default: 2.

SSEA_SYNC_RETRY: During the disks' resynchronization, the P9000 XP Agent checks the mirrored disks' status within an interval specified by SSEA_SYNC_SLEEP_TIME. SSEA_SYNC_RETRY determines the number of retries for these checks. If there is no progress after that, the resynchronization is aborted.

Default: 10 retries.

SSEA_SYNC_SLEEP_TIME: During the disks' resynchronization, the P9000 XPAgent checks the mirrored disks' status for the number of times determined by SSEA_SYNC_RETRY. SSEA_SYNC_SLEEP_TIME determines the time interval between the status

checks.

Default: 5 seconds.

SSEA_WAIT_PAIRS_PROPER_STATUS: All disk pairs must be in proper status (either STAT_PSUS/SSUS or STAT_PAIR) before a process continues. This option determines the maximum waiting period for disk pairs to change to proper status.

SMB_SCAN_RDSK_TIMEOUT: On Windows, during backup system preparation, the system is scanned for new devices. When new devices are detected, they appear on the backup system as new physical drives. This option sets the maximum time (in seconds) for which a ZDB Agent on the backup system waits for a new physical drive to appear.

Default: 30 seconds. Usually, it is sufficient, unless there are configuration problems on the backup system.

SMB_SCAN_FOR_VOLUME_TIMEOUT: On Windows, sets the maximum time (in seconds) for which a ZDB Agent on the backup system waits for new volumes to appear on the backup system. This happens after a physical drive is detected during backup system preparation.

Default: 300 seconds. Usually, it is sufficient, unless there are configuration problems on the backup system.

Default: 120 minutes.

SSEA_FORCE_DISMOUNT: Determines whether the P9000 XP Agent will perform forced dismount of the volumes which are locked by the Windows system processes and cannot be dismounted using the ordinary dismount operation. You can enable forced dismount operation by setting this option to 1.

Default: 0 (disabled). Possible: 0 | 1.

MAXIMUM_HOST_LOCKING_RETRY: The P9000 XP Agent will lock the backup system during the backup system preparation. The lock operation may fail due to concurrent ZDB sessions or similar actions. This option determines the maximum number of attempts by the P9000 XP Agent at locking the backup system.

Default: 60 attempts.

SSEA_ATTACH_RETRY: Prior to manipulating volumes on a disk array, the P9000 XP Agent must connect to an appropriate command device. In case of a problem with the SAN connectivity, establishing such a connection may fail. This option determines the number of attempts made by the P9000 XP Agent at connecting to the command device.

Default: 5 attempts.

SSEA_ATTACH_SLEEP_TIME: Determines the interval (specified in seconds) between each pair of attempts of P9000 XP Agent at connecting to the command device.

Default: 10 seconds.

EMC specific options

This section explains EMC-specific omnirc options.

SYMA_SYNC_RETRY, **SYMA_SLEEP_FOR_SYNC**: To successfully split the disks, EMC Agent first checks the links' status (links can be split only after all devices are synchronized).

Default: 15 retries, 30 seconds sleep time.

These two options are also used for incremental restore of device groups. EMC Agent starts the incremental restore only when there are no write pending tracks to devices in the restore device group.

Default: 15 retries; checking the number of write pending track - every 30 seconds.

SYMA_REC_FILE_LIMIT: Invalid records are automatically deleted when the EMC Agent recovery file exceeds a certain size.

Default: 102400 bytes.

SYMA_MOUNT_R2_READWRITE:

Determines the mode in which volume groups and filesystems are activated and mounted:

- 0: read-only mode (default)
- 1: read/write mode

For backup, it is sufficient to activate volume groups and filesystems in read-only mode. If you use the mirror for DSS or other tasks after backup, this may not be sufficient.

SYMA_UMOUNT_BEFORE_SPLIT:

Determines whether filesystems on the application system are dismounted before the split:

- 0: not dismounted (default)
- 1: dismounted before the split, remounted after (to ensure filesystem data is consistent)

A filesystem does not have a stop I/O to flush data from the filesystem cache to disk and stop I/O during the split. The only way to back up filesystems in split mirror mode is to dismount the mount point on the application system. If applications run on the filesystem, they control I/O to the disk. In this case, it is not necessary to dismount the filesystem before the split.

User scenarios - examples of ZDB options

This feature is available in the Premium Edition

This section gives examples of backup policies with appropriate ZDB options.

P9000 XP Array integration

Example 1

A replica set is configured, with all replicas available for instant recovery. The next replica must be prepared according to replica set rotation after zero downtime backup and forcibly synchronized before the next zero downtime backup.

To implement such policy, select the following options:

- Track the replica for instant recovery
- Synchronize the disks if not already synchronized
- Prepare the next mirror disks for the backup (resynchronize)

The following option is selected automatically:

- Keep the replica after the backup

Example 2

A replica set is configured, with all replicas available for offline data processing after the ZDB session. The next replica must be prepared according to replica set rotation after the zero downtime backup, and the next ZDB session must be aborted if data processing is not finished.

Note This example assumes that offline data processing involves splitting links before data processing and resynchronizing links afterwards.

To implement such policy, select the following options:

- Keep the replica after the backup
- Abort the session if the mirror disks are not synchronized
- Prepare the next mirror disks for the backup (resynchronize)
- Leave the backup system enabled

Example 3

A replica set is configured, with versions on replicas available for on-demand offline data processing (links are split on demand and the backup system is prepared for offline data processing manually), but not for instant recovery. The replica must be prepared at the start of a ZDB session.

To implement such policy:

- Select **Synchronize the disks if not already synchronized**.
- Clear **Keep the replica after the backup**.

Example 4

A single replica is configured, with the version on the replica available for offline data processing. The replica must be prepared at the start of a ZDB session.

To implement such policy, select the following options:

- Keep the replica after the backup
- Synchronize the disks if not already synchronized
- Leave the backup system enabled

Conflicting Options

If a single replica is configured and the following options are selected, the second option is ignored, since the replica to be kept is at the same time the replica to be prepared for the next zero downtime backup:

- Keep the replica after the backup
- Prepare the next mirror disks for the backup (resynchronize)

Note A conflict may also occur when a replica set is configured, depending on the replica set selection and the P9000 XP LDEV exclude file.

EMC integration

Example 1

After zero downtime backup, the replica must be discarded and prepared for the next zero downtime backup at the end of the ZDB session.

To implement such backup policy:

- Select **Re-establish links after backup**.
- Do not select **Re-establish links before backup**.

Example 2

After zero downtime backup, the replica must be used for offline data processing and prepared at the start of the next ZDB session.

To implement such backup policy:

- Select **Re-establish links before backup**.
- Do not select **Re-establish links after backup**.

Backup system mount point creation

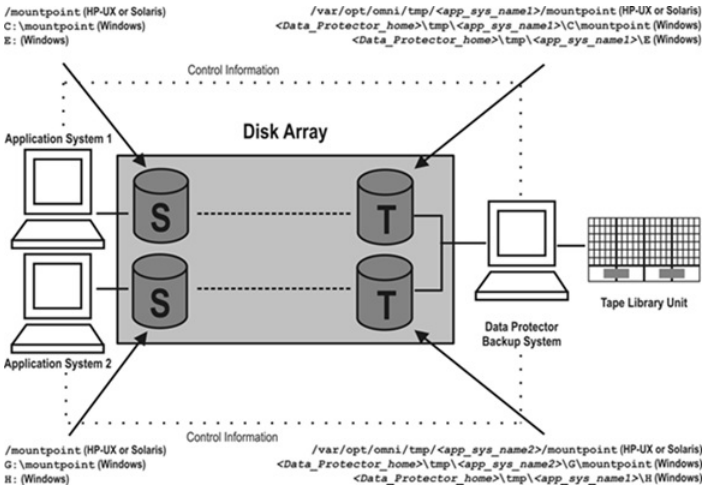
Data Protector disk array integrations support configurations where multiple application systems are connected to a disk array and one system (the backup system) is responsible for backing up these applications. Local, remote, or remote plus local replication configuration (if supported on a particular array) can be used for ZDB in such a configuration.

Each application system uses its own original storage, from which replicas are created; in case of ZDB to tape and ZDB to disk+tape, filesystems are mounted on the backup system.

Filesystem and Microsoft Exchange Server backup

To perform a concurrent backup of multiple application systems, the mount points assigned to the filesystems in the original storage *do not need to be* different for each application system. The backup of the Microsoft Exchange Server application is performed as *filesystem* backup. With filesystem backup, Data Protector, during a ZDB session, creates or reuses unique mount points on the backup system. Data Protector then mounts filesystems to these mount points.

Backup system mount point creation: filesystem and Microsoft Exchange Server backup



Note The above example depicts the default Data Protector behavior. You can change the backup system mount point pathname creation by setting the ZDB_PRESERVE_MOUNTPOINTS, ZDB_MOUNT_PATH and ZDB_MULTI_MOUNT omnirc options in the .omnirc file.

Application and disk image backup

The information in this section applies only for the backup of the following:

- Disk images
- Oracle
- SAP R/3
- Microsoft SQL Server

Applications on filesystems

To perform a concurrent backup of multiple application systems, the mount points or drive letters assigned to the original storage *must be* different for each application system. Data Protector, during a ZDB session, creates mount points or drive letters with the same names as on the application system. Data Protector then mounts filesystems in a replica to these mount points.

If the mount points or drive letters are the same for different application systems, concurrent backup of such systems is not

possible; backup of objects that belong to these mount points or drive letters must be run sequentially.

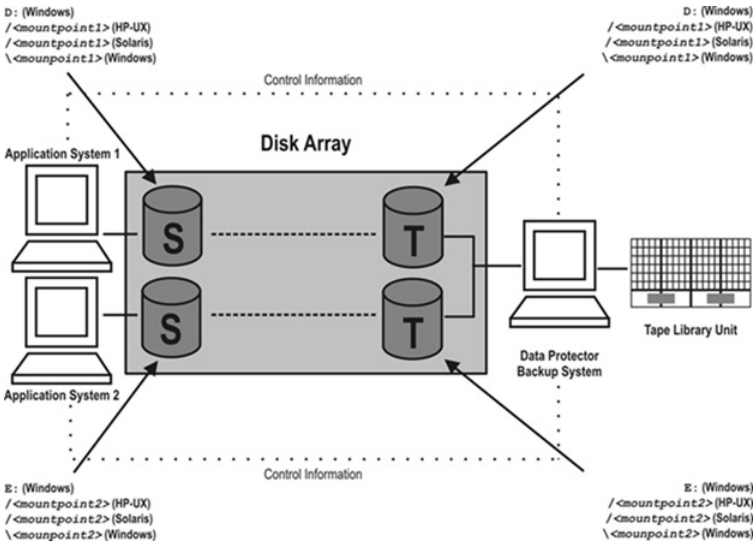
Applications on disk images + disk image backup

If your application uses disk images as the data source, or if you are performing a disk image backup without an application, the following applies: Data Protector, during a ZDB session, finds and uses raw device files (UNIX systems) or physical drive numbers (Windows systems) for the replica created from the original storage raw device files (UNIX systems) or physical drive numbers (Windows systems) on the backup system. Therefore, make sure the device file names and physical drive numbers are the same on the application and the backup systems.

Note that due to the limitation described above, snapshot integrations are not suitable for such backups (with snapshot integrations, Data Protector cannot guarantee that after presentation to the backup system replicas are assigned the same raw device files or physical drive numbers as on the application system).

Note With the P9000 XP Disk Array Family, if the Business Copy (BC) P9000 XP first-level mirrors or snapshot volumes are configured, the integration always mounts the selected first-level mirror or snapshot volume to the same mount point.

Backup system mount point creation: application or disk image backup



Troubleshoot

To identify physical devices belonging to a particular volume group in HP-UX, execute:

On the application system:

- strings /etc/lvmtab

  All volume groups and devices belonging to volume groups are displayed.

- vgdisplay -v /dev/VG_name

  Logical volumes and devices for a specified volume group are displayed.

On the backup system:

- /usr/symcli/bin/symdg list

  Device group names and additional information about devices is displayed.

- /usr/symcli/bin/symdg show DgName

  Detailed information about devices and associated BCVs is displayed.

Monitor Data Protector

This section provides information on Monitoring, Reporting, Notifications, and Data Protector Event Log. The following topics are included:

Monitor Sessions

Data Protector monitoring allows you to manage running sessions and to respond to mount requests. You can view the status of sessions, their type, owner, and session ID; the start time of the sessions as well as the names of the corresponding backup specifications.

When you run an interactive backup, restore, object copy, object consolidation, object verification, or media management session, a monitor window opens, showing the objects, backup devices, and messages generated during the session. Even if the user interface is closed, the session continues.

You can change the level of reported messages during a backup or restore session by changing the **Report level** option during configuration of a backup specification or during startup of a restore session.

You can monitor several cells at the same time using the Manager-of-Managers functionality.

View currently running sessions

You can view currently running sessions in the Monitor context.

Note A currently running session is displayed in the Monitor context after the pre-exec script has finished.

At refresh intervals (by default 5 seconds), the list of currently running sessions is automatically updated with new sessions. To change the default refresh interval, in the File menu, click **Preferences**, and then click the Monitor tab. You can specify the refresh interval in seconds for the Cell Manager and for the MoM.

You either have to be added to the Admin user group or granted the Monitor user rights.

Complete the following steps:

1. In the Context List, click **Monitor**.

   In the Results Area, the status of current sessions is displayed.

   Tip You can sort the sessions (by status, type, owner, and so on) by clicking the corresponding column header. For VMware integration, you can sort the sessions by VM name and item name as well. Here, VM name refers to the name of the virtual machine in vCenter and item name refers to the name of the disk object or configuration associated with the virtual machine.

2. Double click the running session you want to view.

Tip To remove all completed or aborted sessions from the Results Area of the Monitor context, in the Scoping Pane, click **Current Sessions** and then select **Clear Sessions** from the Action menu. To remove a particular finished or aborted session from the current sessions list, right-click the session and select **Remove From List**. All completed or aborted sessions are automatically removed from the Results Area of the Monitor context if you restart the Data Protector GUI.

View finished sessions

You can view completed or aborted sessions in the Internal Database context.

You either have to be added to the Admin user group or granted Monitor user rights.

Complete the following steps:

1. In the Context List, click **Internal Database**.

   If you are running Manager-of-Managers, select **Monitor** in the Context List and then select a Cell Manager of your choice. From the Tools menu, select **Database Administration** to open a new Data Protector GUI with the Internal Database context selected.
2. In the Scoping Pane, expand **Sessions** to display all the sessions stored in the IDB. The sessions are sorted by date. Each session is identified by a session ID consisting of a date in a YY/MM/DD format and a unique number.
3. Right-click the session and select **Properties** to view details on a specific session.
4. Click the **General**, **Messages**, or **Media** tab to display general information on the session, session messages, or information on media used for this session, respectively.

Abort running sessions

You abort a session if you want to stop a backup, restore, or media management operation. A backup copy or restored data only exist for data that was backed up or restored before you aborted the session.

You either have to be added in the admin user group or granted the Monitor user rights.

Complete the following steps:

1. In the Context List, click **Monitor**. The progress and status of current sessions appear in the Results Area.

   If you are running a Manager-of-Managers, expand the **Enterprise Monitor** in the Scoping Pane and then select the Cell Manager you want to monitor. The progress and status of current sessions appear in the Results Area.
2. Click the column headings to sort the sessions.
3. Right-click the session and select **Abort**.

If you abort a backup session while it is still determining the sizes of the disks that you have selected for the backup, it does not abort immediately. The backup is aborted once the size determination (treewalk) is completed.

Tip If you started a backup, restore, or media management session interactively, you can also abort the session in the Data Protector Backup, Restore, or Devices & Media context respectively.

Related tasks

- Respond to mount requests
- Restart Failed Backups
- Restart failed object copy sessions

- Resume failed sessions

- Abort running sessions

Notifications

Data Protector allows you to send notifications from the Cell Manager when specific events occur. For example, when a backup, object copy, object consolidation, or object verification session is completed, you can send an e-mail with the status of the session.

You can set up a notification so that it triggers a report.

You can configure notifications using the Data Protector GUI or any Web browser with Java support.

Input parameters let you customize notifications. Some input parameters allow multiple selections. All other input parameters depend on the type of the notification. Depending on the send method, the recipient can be any of the following:

- a system
- an e-mail address
- an SNMP trap
- a script
- a file
- a configured report group
- the Data Protector Event Log

By default, notifications are configured with default values and are sent to the Data Protector Event Log. To send additional notification using some other sending method and/or other input parameters values, the configuration values must be changed.

To access the Data Protector notification functionality. You either have to be added in the `admin` user group or granted the **Reporting and notifications** user rights.

Notification types - events that trigger notifications

There are two main types of notifications.

- Notifications that are triggered when an event occurs
- Notifications that are scheduled and started by the Data Protector checking and maintenance mechanism

Notifications that are triggered when an event occurs

- Alarm
- Expired Certificates
- Check UNIX Media Agent
- Csa Start Session Failed
- Device Error
- End of Session
- IDB Corrupted
- File Library Disk Usage
- Mail Slots Full
- Mount Request
- Session Error
- Start of Session
- Too Many Sessions

Notifications that are scheduled and started by the Data Protector checking and maintenance mechanism

- Health Check Failed
- IDB Backup Needed
- IDB Limits
- IDB Reorganization Needed
- IDB Space Low
- License Warning
- License Will Expire
- Not Enough Free Media
- Unexpected Events
- User Check Failed

Alarm

Event/notification name:	Alarm
What triggers the notification:	Data Protector Internal critical conditions, such as Automated Media Copy upgrade, Upgrade Core Part End, Upgrade Detail Part End, Purge End, abort of session, Disk Agents upgrade during UCP, and so on.
Default message level:	Warning
Message displayed:	Alarm: Alarm_message

Expired certificates

Event/notification name:	ExpiredCertificates
What triggers the notification:	The certificate stored on Cell Manager certificate directory is expired or not yet valid. The Cell Manager certificate directory stores all client certificates for Secure Control Communication.
Default message level:	Warning
Message displayed:	Certificate *certificate_name* expired or not yet valid.

Csa start session failed

Event/notification name:	CsaStartSessionFailed
What triggers the notification:	The backup session that ends with the error message: Could not start a new backup session.
Default message level:	Major
Message displayed:	CsaStartSession failed for datalist *datalist_name*.

Device error

Event/notification name:	DeviceError
What triggers the notification:	An error on the device **Device** (default: <Any>).
Default message level:	Critical
Message displayed:	Error on device Device occurred.

End of session

Event/notification name:	EndofSession
What triggers the notification:	A backup, copy, consolidation, or object verification session specified in the session specification **Session Specification** (default: <Any>) that ends with the message **Session Status** (default: Completed with errors).
Default message level:	Warning
Messages displayed:	Backup session session_ID of session specification backup_specification, backup specification group group completed with overall status session_overall_status; session_type session session_ID of session specification session_spec , completed with overall status session_status .

File library disk usage

Event/notification name:	FileLibraryDiskUsage
What triggers the notification:	A lack of free disk space for the file library **Name of the File Library** (default: All).
Default message level:	Warning

Message displayed:	The File Library Device is low in disk space in the File Library Path directory.

Health check failed

Event/notification name:	HealthCheckFailed
What triggers the notification:	A non-zero value returned by the omnihealthcheck command. The command returns zero if the following is true: • The Data Protector services (CRS, MMD, hpdp-idb, hpdp-idb-cp, hpdp-as, KMS , omnitrig, and omniinet) are active. • The Data Protector Media Management Database (MMDB) is consistent. • At least one backup of the IDB exists. By default, Data Protector starts the Health Check (which runs the omnihealthcheck command) once a day.
Default message level:	Critical
Message displayed:	Health check message: healthcheck_command failed.

IDB backup needed

Event/notification name:	IDBBackupNeeded
What triggers the notification:	Too many successive incremental IDB backups or insufficiently frequent full IDB backup.
Default message level:	Warning
Message displayed:	There are *n* successive incremental IDB backups. The last backup of the Data Protector Internal Database was done on *MM/DD/YY hh:mm:ss* .

IDB corrupted

Event/notification name:	IDBCorrupted
What triggers the notification:	Corruption of a part of the IDB.
Default message level:	Critical
Message displayed:	Corruption in the IDB_part part of the Data Protector Internal Database has been detected (error_message). Values for error messages are: • Verification of datafile(s) failed. • KeyStore is corrupted. • Media and Media in position tables are not consistent. • Database is not in consistent state. • Database schema is not consistent .

IDB limits

Event/notification name:	IDBLimits
What triggers the notification:	Reaching the limit of any of the MMDB or CDB parts.
Default message level:	Major
Message displayed:	The IDB_part part of the Data Protector Internal Database has reached its limit.

IDB reorganization needed

Event/notification name:	IDBReorganizationNeeded

What triggers the notification:	One or more IDB entities need to be reorganized due to fragmentation or wasted space.
Default message level:	Warning
Message displayed:	Bloat on table *name_ of_table* detected. Fragmentation of table name_of_table on column *uuid* detected. Fragmentation of index *name_ of_index* detected.

IDB space low

Event/notification name:	IDBSpaceLow
What triggers the notification:	One of the following events: • The maximum free disk size is below the **IDB Disk Free Threshold [MB]** (default: 300 MB) value. • The difference between the maximum and current size of all DC directories falls below the **DCBF Size Limit Threshold [MB]** (default: 500 MB) value. • The maximum free disk size is below the **WAL Disk Free Threshold [MB]** (default: 300 MB) value. By default, Data Protector checks the IDB Space Low condition once a day.
Default message level:	Major
Message displayed:	Data Protector Internal Database is running out of space.

License warning

Event/notification name:	LicenseWarning
What triggers the notification:	A need for purchased licenses.
Default message level:	Warning
Message displayed:	n licenses need to be purchased for category name of the license. Run omnicc -check_licenses -detail for more info.

License will expire

Event/notification name:	LicenseWillExpire
What triggers the notification:	The forthcoming expiration date of the Data Protector license. The license will expire in number of days specified in **License expires in days** (default: 10).
Default message level:	Warning
Message displayed:	The first license will expire in License expires in days days.

Mail slots full

Event/notification name:	MailSlotsFull
What triggers the notification:	Full mail slots of the device **Device** (default: <Any>).
Default message level:	Warning
Message displayed:	All mail slots of library Device are full. Remove them immediately.

Mount request

Event/notification name:	MountRequest

What triggers the notification:	A mount request for the device **Device** (default: <Any>).
Default message level:	Warning
Message displayed:	Mount request on device Device.

Not enough free media

Event/notification name:	NotEnoughFreeMedia
What triggers the notification:	A lack of free media in the **Media Pool**. Notice, that if a **Media Pool** is configured to use a **Free Pool**, the **Number of Free Media** from the **Free Pool** is also considered.
Default message level:	Warning
Message displayed:	Media pool Media Pool contains only number_of_media free media.

Session error

Event/notification name:	SessionError
What triggers the notification:	A backup, copy, consolidation, or object verification session with a message of the level Single Message Level (default: Major) or higher, displayed in the Monitor window.
Default message level:	Major
Messages displayed:	Backup session session_ID of session specification backup_specification , backup specification group group has errors: number_of_errors . session_type session session_ID of session specification session_spec has errors: number_of_errors .

Start of session

Event/notification name:	StartofSession
What triggers the notification:	A start of a backup, copy, consolidation, or object verification session specified in the session specification **Session Specification** (default: <Any>).
Default message level:	Normal
Messages displayed:	Backup session session_ID started for session specification backup_specification backup specification group group . session_type session session_ID started for session specification session_spec .

Too many sessions

Event/notification name:	TooManySessions
What triggers the notification:	Start of a session when 1000 sessions are already running concurrently.
Default message level:	Warning
Message displayed:	Session cannot start because the maximum number of concurrently running sessions has been reached.

Unexpected events

Event/notification name:	UnexpectedEvents

What triggers the notification:	An unusually high number of new events in the Data Protector Event Log since the last time the check was made. The number exceeds **Number of events** (default: 20). By default, Data Protector checks the condition once a day.
Default message level:	Warning
Message displayed:	Data Protector Event Log increased for number_of events_in_last_day unexpected events in the last day.

Check UNIX media agent

Event/notification name:	UnixMediaAgentWarning
What triggers the notification:	The mrgcfg -check_ma command triggers this notification when client devices are using rewind device files instead of no-rewind device files.
Default message level:	Warning
Message displayed:	Media Agents, clients devices may have been configured using rewind device files instead of no-rewind device files. This may lead to problems in SAN environments.

User check failed

Event/notification name:	UserCheckFailed
What triggers the notification:	A non-zero value returned by the user-created script/command with the name **Command Path** located in the default Data Protector administrative commands directory. By default, Data Protector starts the User Check (which runs the script) once a day (default: None).
Default message level:	Major
Message displayed:	User check failed with exit code error_code : error_description .

Notifications Send Methods

You can choose among various send methods when configuring a notification. By default, all notifications are configured to be sent to the Data Protector Event Log. To send a notification using another sending method, also, you must configure an additional notification. The available notification send methods are:

- Broadcast message send method
- E-mail send method
- E-mail (SMTP) send method
- External send method
- Log to file send method
- Data Protector Event Log send method
- SNMP send method
- Use report group send method

Broadcast Message send method

The broadcast message send method allows you to send a broadcast message with the output of the notification to specified systems after a specified event occurs.

Broadcast messages can be sent to Windows systems only by specifying the target system. Broadcast messages are limited to 1000 characters, so a short format is preferred.

E-mail send method

You can send an e-mail with the output of a notification to specified recipients. Make sure you provide the full e-mail address of the recipient.

Important Due to security features of Microsoft Outlook, using the e-mail send method may cause the CRS service to stop responding. Therefore, the recommended method for sending e-mail notifications is SMTP.

On Windows systems

To send an e-mail notification from a Windows system, you need to have a mail profile. You can either use an existing mail profile or create a new one, named OmniBack.

To use an existing mail profile, add the following line to the Data Protector omnirc file:

```
OB2_MAPIPROFILE=existing_MAPI_profile_name
```

On UNIX systems

The e-mail subsystem has to be configured and running on a UNIX system.

Due to the operating system limitations, international characters in localized e-mail notifications can be displayed incorrectly on UNIX systems, if they are passed between systems using a different locale.

E-mail (SMTP) send method

You can send an e-mail with the output of a notification to specified recipients. Make sure you provide the full e-mail address of the recipient.

This is the recommended e-mail send method.

By default, the address of the SMTP server used for sending the notifications is set to the Cell Manager IP address. To change the address, edit the SMTPServer global option. The SMTP server must be accessible from the Cell Manager system, but does not need to be part of the Data Protector cell.

External send method

The external script send method allows you to process the output of the notification in your own script. The script receives the output as standard input (STDIN).

The script, which is located on the Cell Manager system, must reside in the default Data Protector administrative commands directory. Provide only the name of the script, no path.

Note that only .bat, .exe, and .cmd are supported extensions for external scripts on Windows systems. To run a script with an unsupported extension (for example, .vbs), create a batch file that starts the script. Then configure Data Protector to run the batch file as an external script, which then starts the script with the unsupported extension.

You can also use this delivery method to perform a scheduled eject of the specified media.

Log to file send method

The log to file send method lets you post a file with the output of the notification when a specified event occurs.

The file is posted to the Cell Manager system. You have to specify the name of the file to which you want to post the notification. The file will be overwritten if it exists.

Data Protector Event Log send method

By default, all notifications are sent to the Data Protector Event Log. The Data Protector Event Log is accessible only for Data Protector users in the admin user group and to Data Protector users that are granted the Reporting and notifications user rights. You can view or delete all events in the Data Protector Event Log.

SNMP send method

SNMP send method allows you to send an SNMP trap with the output of the notification when a specified event occurs. The SNMP trap can be further processed by applications using SNMP traps.

On Windows systems

On a Windows Cell Manager, SNMP traps are sent to the systems configured in the Windows SNMP traps configuration. You need to configure Windows SNMP traps to use the SNMP send method on Windows systems.

On Linux systems

On a Linux Cell Manager, SNMP traps are sent to the systems configured in the notification.

Use report group send method

Use report group send method allows you to run a report group when a specified event occurs.

Configure Notifications

To configure a notification you need to provide a name for the notification, a type of notification, message level, send method, and recipient. All other input parameters depend on the type of the notification.

You either have to be added in the admin user group or granted the Reporting and notifications user rights.

Complete the following steps:

1. In the Context List, select **Reporting**.
2. Right-click **Notifications** and click **Add Notification** to open the wizard.
3. The wizard options depend on the notification you selected. For example, all options available for the IDB Space Low notification are not available for the IDB Limits notification. Click **Next** as many times as needed to reach the last page of the wizard.
4. Click **Finish** to exit the wizard.

The notification will be sent using the specified send method when the specified event occurs.

Tip To trigger a report group by a notification, configure a report group and then configure the notification to use the Use Report Group send method.

Related task

- Troubleshoot Reports and Notifications

Data Protector Event Log

The Data Protector Event Log represents a centralized event management mechanism, dealing with specific events that occurred during the Data Protector operation. The Data Protector event logging mechanism logs two types of events: process-triggered and user-triggered. The events are logged on the Cell Manager in the Ob2EventLog.txt file residing in the default Data Protector log files directory.

Viewing the Data Protector Event Log using the Event Log Viewer helps you troubleshoot possible problems.

The Data Protector GUI is automatically switched to the Reporting context.

The following may provide additional information:

- You have to be either a member of the admin user group or granted the Reporting and notifications user rights.
- The Data Protector Event Log is not refreshed automatically. To view the new messages, refresh it manually by pressing **F5**.

Process-triggered events

An event is logged by the notifications functionality.

User-triggered events

An event is logged when a user performs a certain GUI operation or a set of GUI operations. This set of operations includes modifications of backup, object copy and consolidation specifications, operations on users and user groups, creation and modifications of devices and media related configuration, and remote installation operations.

Logging of user-triggered events is disabled by default. To enable it, you must set the global option EventLogAudit to 1.

In a MoM environment, if the global option is set to 1, the events are logged only on the local Cell Manager system.

Access event log viewer

You can browse the recorded events by accessing the Data Protector Event Log Viewer.

You have to be either a member of the admin user group or granted the Reporting and notifications user rights.

Complete the following steps:

1. In the Context List, select **Reporting**.
2. In the Scoping Pane, expand **Reporting**.
3. Select **Event Log** to display it.

Delete event log viewer contents

You either have to be a member of the Admin user group or granted the Reporting and notifications user rights.

Note Deleting the Event Log Viewer contents does not delete the contents of the Ob2EventLog.txt file.

Complete the following steps:

1. In the Context List, select **Reporting**.
2. In the Scoping Pane, expand **Reporting**.
3. Right-click **Event Log** and select **Empty Event Log** to delete all entries in the Event Log Viewer.

Auditing

Data Protector provides backup, restore, copy, and consolidation session auditing, which stores non-tamperable and non-overwritable information about all backup, restore, copy, and consolidation tasks that were performed over user-defined periods for the whole Data Protector cell. The auditing information is retrievable on demand in an integral and printable fashion for auditing or administrative purposes.

You can enable or disable audit logs and set the retention period for audit log files during Cell Manager installation. For more information, see the *Related Topics* section. You can also enable or disable audit logs and set the retention period later by using the omnicc -auditlog <*Value*> [-retention_months <*retentionValue*>] command.

Generate an audit report

To generate an audit report, follow the steps below.

> **Note** In a MoM environment, you have to generate audit reports for each Cell Manager separately.

1. In the Context List, click **Internal Database**.
2. In the Scoping Pane, click the **Auditing** item to open the Auditing page.
3. From the Search interval drop-down list, select one of the values (for example, Last week).
4. Click the **Update** button to display a list of all backup, restore, copy and consolidation sessions performed during the selected period.
5. Select a specific session from the session list to display detailed information about used media and objects in the middle and bottom part of the Auditing property page.

Related Topics

- For more information about enabling audit logs during Cell Manager installation, see Install Cell Manager in non-cluster mode and Install Cell Manager in cluster mode.
- For more information about enabling audit logs using command-line interface, see omnicc command-line interface.

Check if Data Protector functions properly

Checks Performed by Data Protector

Data Protector provides its own checking and maintenance mechanism, which performs maintenance tasks and checks on a daily basis. The daily maintenance executes a series of commands that purge obsolete data from many sections of the Data Protector Internal Database.

By default, daily maintenance takes place at noon each day. It does not purge all parts of the IDB, just the parts that can be done without exclusive access to the IDB.

Maintenance tasks

Every day at 12:00 P.M. by default, Data Protector:

- Deletes obsolete DC binary files, sessions, and related messages by executing the following omnidbutil -purge commands:
  - -dcbf
  - -sessions
  - -messages
- The daily maintenance -sessions option is dependent on the setting of the KeepObsoleteSessions global option and the -messages option on the KeepMessages global option.
- Finds any free (unprotected) media in media pools in which the **Use free pool** and **Move free media to free pool** options are set and deallocates the free media to a free pool by executing the omnidbutil -free_pool_update command.
- Checks the protection for the media and deletes media and the corresponding media locations. If the media is exported from the IDB, the location is no longer known to the IDB and thus Data Protector can not free the storage for such media. The media must be manually removed from the storage and media locations (slots) should also be manually deleted from the device context.

Checks

Every day at 12:30 P.M. by default, Data Protector starts checks for the following notifications:

- IDB Space Low
- IDB Limits
- IDB Backup Needed
- Not Enough Free Media
- Health Check Failed
- User Check Failed (if configured)
- Unexpected Events
- License Warning
- License Will Expire

Every Monday at 12:30 P.M. by default, Data Protector starts check for the following notification:

- IDB Reorganization Needed

By default, any triggered notification is sent to the Data Protector Event Log.

> **Tip** You can change the default schedule values for maintenance tasks and checks. Use the DailyMaintenanceTime and DailyCheckTime global options respectively with twenty-four hour clock notation.

What checks should I perform

Besides the checks that Data Protector performs by default, it is recommended that you perform some regular checks. This way you ensure that Data Protector is functioning properly and identify potential problems before they arise.

> **Tip** You can automate these checks by developing scripts and using the User Check Failed notification.

Some of the checks (for example, the omnihealthcheck and omnitrig -run_checks commands) are already performed as part of the Data Protector checking and maintenance mechanism.

What check to perform?	What is checked and how?
Check the Data Protector Cell Manager	The following checks complete successfully if the exit code of the command is `0` (OK). Exit values other than 0 indicate that the check failed. 1. Run the `omnihealthcheck` command to check if: ◦ the Data Protector services (CRS, MMD, hpdb-idb, hpdp-idb-cp, hpdp-as, omnitrig, KMS, and Inet) are active ◦ the Data Protector Media Management Database is consistent ◦ at least one backup image of the IDB exists The exit code of the command is `0` (OK) only if all three checks completed successfully (exit code for every check was `0`). 2. Run the `omnidbcheck -quick` command to check the IDB.
Check if backups are configured properly	1. Run the backup preview for crucial backup specifications. Successfully completed previews prove that: ◦ All clients in the backup specification are accessible from the Cell Manager. ◦ All files are accessible. ◦ The amount of data to be backed up is determined. ◦ All backup devices are configured properly. Note that preview is not supported for some integrations and for ZDB. 2. Run the `omnirpt -report dl_sched` command to check whether the backup specifications are scheduled in compliance with your backup policy. The command lists all backup specifications and their schedule.
Verify the Data Protector installation	Verify the installation using the Data Protector GUI, Clients context, to check if the Data Protector software components are up and running on the Cell Manager or the client systems.
Check the Data Protector log files	Inspect the following Data Protector log files and identify possible problems: • event.log • debug.log • purge.log
Run the notifications check	By default, Data Protector starts a check for the following notifications once a day. Any triggered notification is sent to the Data Protector Event Log. You can also run the `omnitrig -run_checks` command to start checks for the notifications: • IDB Space Low • Not Enough Free Media • Unexpected Events • Health Check Failed • IDB Limits • IDB Backup Needed • IDB Reorganization Needed • License Will Expire • License Warning • User Check Failed (if configured)
Check other system resources	Inspect the following operating system log files and identify possible problems: **Windows systems:** the Windows Event Viewer and its Security, System, and Application logs **UNIX systems:** /var/adm/syslog/syslog.log
Check the IDB recovery file	Check the IDB recovery file, `obrindex.dat`, to make sure that the IDB and configuration files needed for successful recovery of a Cell Manager system are created regularly.

How to automate checks

You can automate checks by using a script and configuring the User Check Failed notification.

The User Check Failed notification executes the command or script specified as an input parameter in this notification and

triggers the notification if the return value of any the executed commands in the script is not `0`. You are notified via the selected send method.

The command/script must reside on the application system in the default Data Protector administrative commands directory.

The configured User Check Failed notification is started every day in the course of the Data Protector daily checks and is, if triggered, sent to the Data Protector Event Log.

Related task

- Verify the installation

CLI reference

This topic includes the following:

Introduction to CLI

omniintro - introduction to the Data Protector commands and command-line utilities

DESCRIPTION

Data Protector is an enterprise backup solution that provides reliable data protection and high accessibility for business data. Data Protector provides extensive media management, unattended backups, post-backup data management, integrations with various databases and supports various backup and other backup-dedicated devices.

COMMANDS

USER COMMANDS (1):

omniabort

Aborts an active session.

This command is available on systems with the Data Protector User Interface component installed.

omniamo

Starts an automated media operation session.

This command is available on the Data Protector Cell Manager.

omnib

Backs up filesystems, disk images, the Data Protector Internal Database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server 2010/2013, Microsoft SQL Server, Microsoft SharePoint Server 2010/2013, SAP R/3, SAP MaxDB, Oracle, MySQL, PostgreSQL, Informix Server, VMware vSphere, Microsoft Hyper-V, Sybase, Lotus, IBM DB2 UDB, and NDMP objects.

This command is available on systems with the Data Protector User Interface component installed.

omnicc

Handles the Data Protector licensing, reports the number of configured and available Data Protector licenses, installs the licenses, imports and exports Data Protector clients, manages access to secured clients, and creates a template for the user_restrictions file.

This command is available on systems with any Data Protector component installed.

omnicellinfo

Displays configuration information about the Data Protector cell.

This command is available on systems with the Data Protector User Interface component installed.

omniclus

Manages load balancing in a cluster environment in the event of an application (Data Protector or other) failover.

This command is available on systems with the Data Protector MS Cluster Support component installed (Windows systems) and on the Data Protector Cell Manager (Linux systems).

omnicreatedl

Creates a filesystem backup specification file (datalist); or an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB backup specification file (datalist).

This command is available on systems with the Data Protector User Interface component installed.

omnidb

Queries the Data Protector Internal Database (IDB).

This command is available on systems with the Data Protector User Interface component installed.

omnidbp4000

Manages the configuration data which the Data Protector P4000 VSS Agent uses to connect to the CIMOM providers.

This command is available on Windows systems with the Data Protector User Interface component installed.

omnidbsmis

Executes administrative tasks on the ZDB database (SMISDB).

This command is available on systems with the Data Protector User Interface component installed.

omnidbvss

Queries the VSS database; manages, browses, and lists the items of the VSS database.

This command is available on systems with the Data Protector User Interface component installed.

omnidbxp

Queries the ZDB database (XPDB), manipulates the P9000 XP LDEV exclude file, configures the P9000 XP Disk Array Family command devices usage, and manages the user authentication data which the Data Protector P9000 XP Agent uses to connect to specific disk arrays.

This command is available on systems with the Data Protector User Interface component installed.

omnidbzdb

Executes administrative tasks on 3PAR StoreServ Storage and NetApp Storage, as well as manages the configuration data, which the integration agents use to connect to the CIMOM providers and storage systems.

This command is available on systems with the Data Protector User Interface component installed.

omnidownload

Downloads information about a backup device and a library from the Data Protector Internal Database (IDB).

This command is available on systems with the Data Protector User Interface component installed.

omniiso

Primarily serves as a pre-exec script to prepare the ISO image file for One Button Disaster Recovery (OBDR); can also be used as a standalone command to automate your backup and disaster recovery process.

This command is available on systems with the Data Protector Automatic Disaster Recovery component installed.

omnimcopy

Makes a copy of a Data Protector medium using Data Protector backup devices as the source and destination.

This command is available on systems with the Data Protector User Interface component installed.

omniminit

Initializes a Data Protector medium.

This command is available on systems with the Data Protector User Interface component installed.

omnimlist

Lists the contents of a Data Protector medium.

This command is available on systems with the Data Protector User Interface component installed.

omnimm

Provides media management for Data Protector.

This command is available on systems with the Data Protector User Interface component installed.

omnimnt

Responds to a Data Protector mount request for a medium.

This command is available on systems with the Data Protector User Interface component installed.

omnimver

Verifies data on a medium.

This command is available on systems with the Data Protector User Interface component installed.

omniobjconsolidate

Consolidates Data Protector backup objects into synthetic full backups.

This command is available on systems with the Data Protector User Interface component installed.

omniobjcopy

Creates additional copies of objects backed up with Data Protector on a different media set.

This command is available on systems with the Data Protector User Interface component installed.

omniobjverify

Verifies Data Protector backup objects, either interactively or using pre-configured post-backup, or scheduled verification specifications.

This command is available on systems with the Data Protector User Interface component installed.

omnir

Restores filesystems, disk images, the Data Protector Internal Database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Server, MySQL, PostgreSQL, SAP R/3, SAP MaxDB, Informix Server, VMware vSphere, Microsoft Hyper-V, Lotus, IBM DB2 UDB, and NDMP objects backed up with Data Protector. The command is also used to start the instant recovery process. To restore a Sybase database, see the syb_tool man page.

This command is available on systems with the Data Protector User Interface component installed.

omnirpt

Generates various reports about the Data Protector environment, for example, about backup, object copy, object consolidation, and object verification sessions in a specific time frame, session specifications, media, Data Protector configuration, and single sessions.

This command is available on systems with the Data Protector User Interface component installed.

omnistat

Displays the status of active Data Protector backup and restore sessions.

This command is available on systems with the Data Protector User Interface component installed.

omniupload

Uploads information about a backup device from an ASCII file to the Data Protector Internal Database (IDB).

This command is available on systems with the Data Protector User Interface component installed.

omniusb

Writes the DR ISO image to a USB drive, and makes the drive bootable

This command is available on systems with the Data Protector Automatic Disaster Recovery component installed.

omniusers

Adds or removes Data Protector users to or from an existing Data Protector user group, or lists the configured Data Protector users.

This command is available on non-Windows systems with the Data Protector User Interface component installed.

SharePoint_VSS_backup.ps1

Creates backup specifications and starts backup sessions for Microsoft SharePoint Server.

This command is available on Windows systems with the Data Protector MS Volume Shadow Copy Integration component installed.

syb_tool

A utility used to get ISQL command needed to restore a Sybase database that was backed up by Data Protector.

This command is available on systems with the Data Protector Sybase Integration component installed.

ADMINISTRATIVE COMMANDS (1M):

ob2install

Runs installation, removal, upgrade, or installation check of the specified Data Protector components to/from/on a remote Linux and Windows systems using the specified an appropriate Installation Server.

This command is available on the Data Protector Installation Server.

omnib2dinfo

Displays information about ObjectStore and StoreOnceSoftware stores.

This command is available on systems with the Data Protector User Interface component installed.

omnicheck

Performs a DNS connections check within a Data Protector cell and lists Data Protector patches installed on Data Protector clients.

This command is available on systems with any Data Protector component installed.

omnidbcheck

Checks the consistency of the Data Protector Internal Database (IDB).

This command is available on the Data Protector Cell Manager.

omnidbinit

Initializes the Data Protector Internal Database (IDB).

This command is available on the Data Protector Cell Manager.

omnidbutil

Handles various Data Protector Internal Database (IDB) maintenance tasks.

This command is available on the Data Protector Cell Manager.

omnidlc

Gathers or deletes Data Protector debug, log, and getinfo files from the Data Protector cell or from a MoM environment.

This command is available on the Data Protector Cell Manager

omnidr

A general purpose Data Protector disaster recovery command. Based on its input, it decides on what type of restore to perform (online restore using omnir or offline restore using omnioffl r), as well as how to perform the restore (whether or not to use live operating system features).

This command is available on systems with the Data Protector User Interface component installed.

omnihealthcheck

Checks the status of Data Protector services, the consistency of the Data Protector Internal Database (IDB), and if at least one backup of the IDB exists.

This command is available on the Data Protector Cell Manager.

omniinetpasswd

Manages the local Data Protector Inet configuration on Windows systems where the Inet process must be run under a specific user account, and sets a user account to be used by the Installation Server during remote installation.

This command is available on systems with any Data Protector component installed.

omniintconfig.pl

Configures, updates configuration parameters, and checks the configuration of one or multiple Oracle databases.

This command is available on systems with the Data Protector User Interface component installed.

omnikeytool

Manages keys used to encrypt backup data.

This command is available on the Data Protector Cell Manager.

omnimigrate.pl

Migrates the Data Protector Internal Database (IDB) from the format used in earlier versions to the format used in the latest Data Protector version.

This command is available on the Data Protector Cell Manager.

omniofflr

Enables restore of any type of Data Protector backup objects in the absence of operable Data Protector Internal Database (IDB), including the IDB itself.

This command is available on systems with any Data Protector component installed.

omniresolve

Resolves a filesystem object or a list of filesystem objects and writes the results to the standard output or to a Unicode file.

This command is available on systems with any Data Protector integration component installed.

omnirsh

Returns the hostnames of the physical and virtual nodes for the specified cluster hostname, or returns the cell information stored in the cell_info file on the specified cluster.

This command is available on the Data Protector Cell Manager.

omnisetup.sh

Installs or upgrades a Data Protector Linux Cell Managers, Linux Installation Servers, and UNIX client systems locally; installs and removes patch bundles.

This command is available on the Data Protector installation DVD-ROMs for Linux systems or is provided together with a patch bundle.

omnisrdupdate

Updates the System Recovery Data (SRD) file.

This command is available on systems with the Data Protector User Interface component installed.

omnisv

Starts or stops the Data Protector services or daemons, displays their status, or turns the maintenance mode on or off.

This command is available on the Data Protector Cell Manager

omnitrig

Triggers Data Protector scheduled backups.

This command is available on the Data Protector Cell Manager.

sanconf

Auto-configures a library, modifies an existing library or drive configuration, or removes drives from a library configuration, within a SAN environment.

This command is available on systems with the Data Protector User Interface component installed.

util_cmd

Sets, retrieves or lists the parameters stored in the Data Protector Oracle, MySQL, SAP R/3, Microsoft Exchange Server 2010/2013, Informix, and Sybase configuration files.

This command is available on systems with any Data Protector component installed.

util_oracle8.pl

Configures an Oracle database and prepares the environment for backup, and checks the configuration of an Oracle database.

This command is available on systems with the Data Protector Oracle Integration component installed.

vepa_util.exe

Configures a VMware ESX(i) Server system, VMware vCenter Server system, Microsoft Hyper-V system, checks the configuration, configures virtual machines, browses and lists VMware datacenters.

This command is available on systems with the Data Protector Virtual Environment Integration component installed.

COMMAND-LINE UTILITIES (1M):

cjutil

Starts, stops, and queries the Windows Change Journal.

This command is available on systems with the Data Protector Disk Agent component installed.

omnicjutil

Remotely controls and administers the Windows Change Journal on Windows clients.

This command is available on the Data Protector Cell Manager.

uma

Controls the robotics of SCSI compliant autochangers.

This command is available on systems with the Data Protector General Media Agent or NDMP Media Agent component installed.

RETURN VALUES:

Possible return values of commands are:

0 - Program completed successfully.

1 - Program failed, command syntax error.

2 - Program failed, invalid argument.

3 - Program failed, internal error.

4 - Program failed, reason unknown.

Some commands may return additional error messages. These are described in individual reference pages.

COMMANDS FOR LAUNCHING THE Data Protector GUI

manager

Launches the Data Protector GUI with all Data Protector contexts activated or, when additional options are specified, with the specified contexts activated.

This command is available on systems with the Data Protector User Interface component installed.

mom

Launches the Data Protector Manager-of-Managers GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts) or, when additional context options are specified, with the specified contexts activated.

This command is available on systems with the Data Protector Manager-of-Managers User Interface component installed.

COMMAND LOCATIONS

WINDOWS SYSTEMS:

- user commands (1), administrative commands (1M), command-line utilities (1M):

  Data_Protector_home\bin

- commands that launch the Data Protector GUI (5):

  Data_Protector_home\bin

SOLARIS AND LINUX SYSTEMS:

- user commands (1):

  /opt/omni/bin

- administrative commands (1M), command-line utilities (1M):

  /opt/omni/lbin

  /opt/omni/sbin

OTHER UNIX SYSTEMS:

- user commands (1), administrative commands (1M), command-line utilities (1M):

  /usr/omni/bin

recommends that you enable invocations of the Data Protector commands from any directory by extending the value of the appropriate environment variable in your operating system configuration with the above paths. Procedures in the Data Protector documentation assume the value has been extended.

DIRECTORY STRUCTURE ON WINDOWS CELL MANAGERS

Data_Protector_home

- Data Protector home directory

Data_Protector_home\bin

- Directory containing Data Protector commands, Disk Agent, Media Agent files, message catalogs, and commands for Cell Manager maintenance

Data_Protector_home\docs

- Provides access to Data Protector documentation.

Data_Protector_home\help

- The Data Protector Help

Data_Protector_program_data

- Data Protector program data directory

Data_Protector_program_data\Config\client

- Directory containing the client configuration directories and files

Data_Protector_program_data\Config\Server

- Directory containing the following configuration directories:

  barlists - database backup specifications

  cell - the cell configuration

  datalists - backup specifications

  devices - templates for devices

  options - default options

  sessions - data about sessions

  snmp - the OpenView/SNMP trap sending configuration

  users - the user configuration

Data_Protector_program_data\Config\Server\dr

- Directory containing the following disaster recovery directories:

  asr - ASR archive files

  p1s - P1S files for Enhanced Automated Disaster Recovery

  srd - SRD files

Data_Protector_program_data\Config\Server\export\keys and Data_Protector_program_data\Config\Server\import\keys

- Directories containing encryption keys

Data_Protector_program_data\server\db80

- The Data Protector Internal Database (IDB)

Data_Protector_program_data\server\db80\idb

- The IDB tablespaces

Data_Protector_program_data\server\db80\dcbf

- The Detail Catalog Binary Files (DCBF) part of the IDB

Data_Protector_program_data \server\db80\keystore

- The encryption keystore database

Data_Protector_program_data \server\db80\keystore\catalog

- The keyid catalog

Data_Protector_program_data \server\db80\logfiles

- The IDB archived log files and the IDB recovery file (obdrindex.dat)

Data_Protector_program_data \server\db80\msg

- The Data Protector session messages

Data_Protector_program_data \server\db80\smisdb

- The ZDB database (SMISDB)

Data_Protector_program_data \server\db80\smisdb\p4000\login

- The data which the Data Protector P4000 VSS Agent uses to connect to the configured CIMOM providers

Data_Protector_program_data \server\db80\smisdb\p10000\login

- The data which the Data Protector 3PAR VSS Agent and the Data Protector P6000 / 3PAR SMI-S Agent use to connect to the configured CIMOM providers for the 3PAR StoreServ Storage disk arrays

Data_Protector_program_data \server\db80\smisdb\netapp\login

- the data which the Data Protector NetApp Storage Provider uses to connect to the NetApp Storage system

Data_Protector_program_data \server\db80\vssdb

- The VSS database (VSSDB)

Data_Protector_program_data \server\db80\xpdb

- The ZDB database (XPDB)

Data_Protector_program_data \log and Data_Protector_program_data \log\server

- Log files

Data_Protector_program_data \log\server\auditing

- Audit logs

Data_Protector_program_data \tmp

- Temporary and debug log files

DIRECTORY STRUCTURE ON LINUX CELL MANAGERS

/etc/opt/omni/client

- Directory containing the client configuration directories and files

/etc/opt/omni/IS

- Directory, containing the Installation Server configuration directories and files.

/etc/opt/omni/server

- Directory containing the following configuration directories:

barlists

- database backup specifications

cell

- the cell configuration

datalists

- backup specifications

devices

- templates for devices

options

- default options

sessions

- data about sessions

sg

- scripts for Service Guard support

snmp

- the OpenView/SNMP trap sending configuration

users

- the user configuration

/etc/opt/omni/server/dr

- Directory containing the following disaster recovery directories:

asr

- ASR archive file

p1s

- P1S files for Enhanced Automated Disaster Recovery

srd

- SRD files

/opt/omni

- Data Protector home directory. It contains the following Data Protector executable directories:

bin

- Data Protector user commands

lbin

- Disk Agent and Media Agent files and some administrative commands

sbin

- Cell Manager and Data Protector Internal Database (IDB) administrative commands

/opt/omni/doc

- Provides access to Data Protector documentation.

/opt/omni/help

- The Data Protector Help

/opt/omni/lib

- Directory containing the following directories:

/opt/omni/lib/man

- Data Protector man pages

/opt/omni/lib/nls

- message catalogs

/var/opt/omni

- Directory containing the following directories:

/var/opt/omni/log and /var/opt/omni/server/log

- log files

/var/opt/omni/server/export/keys and /var/opt/omni/server/import/keys

- encryption keys

/var/opt/omni/server/log/auditing

- audit logs

/var/opt/omni/server/sessions

- data about sessions

/var/opt/omni/tmp

- temporary files

/var/opt/omni/server/db80

- Directory containing the following Data Protector Internal Database (IDB) directories:

/var/opt/omni/server/db80/idb

- the IDB tablespaces

/var/opt/omni/server/db80/dcbf

- the Detail Catalog Binary Files (DCBF) part of the IDB

/var/opt/omni/server/db80/keystore

- the encryption keystore database

/var/opt/omni/server/db80/keystore/catalog

- the key ID catalog

/var/opt/omni/server/db80/logfiles

- the IDB archived log files and the IDB recovery file (obdrindex.dat)

/var/opt/omni/server/db80/msg

- the Data Protector session messages

/var/opt/omni/server/db80/smisdb

- the ZDB database (SMISDB)

/var/opt/omni/server/db80/smisdb/p4000/login

- the data which the Data Protector P4000 VSS Agent uses to connect to the configured CIMOM providers for the 3PAR StoreServ Storage disk arrays

/var/opt/omni/server/db80/smisdb/p10000/login

- the data which the Data Protector 3PAR VSS Agent and the Data Protector P6000 / 3PAR SMI-S Agent use to connect to the configured CIMOM providers for the 3PAR StoreServ Storage disk arrays

/var/opt/omni/server/db80/smisdb/netapp/login

- the data which the Data Protector NetApp Storage Provider uses to connect to the NetApp Storage system

/var/opt/omni/server/db80/xpdb

- the ZDB database (XPDB)

Section 1: User commands

This section includes the following topics:

omniabort

omniabort - aborts an active session
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniabort -version | -help

omniabort -session *SessionID*

DESCRIPTION

This command aborts an active session, identifying it by the *SessionID*. A list of all active sessions and their session IDs is available using the omnistat command.

OPTIONS

-version

Displays the version of the omniabort command.

-help

Displays the usage synopsis for the omniabort command.

-session *SessionID*

Specifies the *SessionID* of the session to be aborted. Use the omnistat command to get the *SessionID* of the session.

NOTES

When using this command to abort the check for unrequired incrementals, manually terminate the omniabort utility afterwards.

EXAMPLES

1. To abort a session with the SessionID "R-2013/05/13-12", execute:

   omniabort -session R-2013/05/13-12

   omniabort -sess 12

SEE ALSO

omnistat(1)

omniamo

omniamo - starts an automated media operation session
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omniamo -version | -help

omniamo -amc *ConfigurationName* { -post_backup | -scheduled }

DESCRIPTION

This command starts an automated media operation session for the specified post-backup or scheduled configuration. Before starting a post-backup operation, you must export the session ID of the backup session that used the media you want to copy.

Windows systems: set SESSIONID= *SessionID*

UNIX systems: export SESSIONID= *SessionID*

Use this command if you want to immediately start an automated media operation. Also, if an automated media operation has failed, you can use this command to start the operation again.

OPTIONS

-version

Displays the version of the omniamo command.

-help

Displays the usage synopsis for the omniamo command.

-amc *ConfigurationName* { -post_backup | -scheduled }

Starts the post-backup or scheduled automated media copy operation with the specified name.

EXAMPLES

1. To start the scheduled automated media copy operation with the configuration name "MediaCopy1", execute:

   omniamo -amc MediaCopy1 -scheduled

2. To start the post-backup automated media copy operation with the configuration name "MyFiles" and session ID 2011/09/13-0001 on Windows, execute:

   set SESSIONID=2011/09/13-0001

   omniamo -amc MyFiles -post_backup

3. To start the post-backup automated media copy operation with the configuration name "MyDocs" and session ID 2011/09/13-0002 on UNIX, if you are using an sh-like shell, execute:

   SESSIONID=2011/09/13-0002

   export SESSIONID

   omniamo -amc MyDocs -post_backup

4. To start the post-backup automated media copy operation with the configuration name "MyBackup" and session ID

2011/09/13-0003 on UNIX, if you are using a csh-like shell, execute:

```
export SESSIONID=2011/09/13-0003

omniamo -amc MyBackup -post_backup
```

SEE ALSO

omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnib

omnib - This command is available on systems with the Data Protector User Interface component installed. It is used to back up objects such as filesystem, disk image, block-based, the Data Protector Internal Database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Server, SAP R/3, SAP MaxDB, SAP HANA, Oracle, MySQL, PostgreSQL, Informix Server, VMware vSphere, H3C CAS, Microsoft Hyper-V, Sybase, Lotus, IBM DB2 UDB, and NDMP objects.

SYNOPSIS

omnib -version | -help

omnib {-filesystem | -vprotect} Client:MountPoint Label -device BackupDevice [MIRROR_OPTIONS...] [GENERAL_OPTIONS] [FILESYSTEM_OPTIONS] [-public]

omnib -filesystem *Client:MountPoint Label* -device *BackupDevice* -ndmp *NDMP_Server_Type* [*NDMP_OPTIONS*] [-public]

omnib -winfs *Client:MountPoint Label* -device *BackupDevice* [*MIRROR_OPTIONS* ...] [*GENERAL_OPTIONS*] [*FILESYSTEM_OPTIONS*] [*WINFS_OPTIONS*] [-public]

omnib -winfsblockbased *HostName Volume* -device *BackupDevice* [*MIRROR_OPTIONS* ...] [*GENERAL_OPTIONS*] [public]

omnib -host *Client:/ Label* -device *BackupDevice* [*MIRROR_OPTIONS* ...] [*GENERAL_OPTIONS*] [*FILESYSTEM_OPTIONS*] [-public [-storedrim]]

omnib -rawdisk *Client Label SectionList* -device *BackupDevice* [*MIRROR_OPTIONS* ...] [*GENERAL_OPTIONS*] [-public]

omnib -restart *SessionID*

omnib -datalist *Name* [*BACKUP_SPECIFICATION_OPTIONS*]

omnib -resume *SessionID* [-no_monitor]

omnib -sap_list *ListName* [-barmode *SapMode*] [*LIST_OPTIONS*]

omnib -hana_list *ListName* [-barmode *HanaMode*] [*LIST_OPTIONS*]

omnib -sapdb_list *ListName* [-barmode *SapdbMode*] [*LIST_OPTIONS*]

omnib -oracle8_list *ListName* [-barmode *Oracle8Mode*] [*LIST_OPTIONS*]

omnib -sybase_list *ListName* [-barmode *SybaseMode*] [*LIST_OPTIONS*]

omnib -informix_list *ListName* [-barmode *InformixMode*] [*LIST_OPTIONS*]

omnib -mssql_list *ListName* [-barmode *MSSQLMode*] [*LIST_OPTIONS*]

omnib -msese_list *ListName* [-barmode *MSExchangeMode*] [*LIST_OPTIONS*]

omnib -e2010_list *ListName* [-barmode *E2010Mode*] [*LIST_OPTIONS*]

omnib -lotus_list *ListName* [-barmode *LotusMode*] [*LIST_OPTIONS*]

omnib -msvssw_list *ListName* [-barmode *VSSMode*] [*LIST_OPTIONS*]

omnib -mbx_list *ListName* [-barmode *MSMailboxMode*] [*LIST_OPTIONS*]

omnib -db2_list *ListName* [-barmode *DB2Mode*] [*LIST_OPTIONS*]

omnib -mssps_list *ListName* [-barmode *MSSPSMode*] [*LIST_OPTIONS*]

omnib -mssharepoint_list *ListName* [-barmode *MSSharePointMode*] [*LIST_OPTIONS*]

omnib -idb_list *ListName* [-barmode *IDBMode*] [*LIST_OPTIONS*]

omnib -veagent_list *ListName* [-barmode *VirtualEnvironmentMode*] [*LIST_OPTIONS*]

omnib -integ MySQL ListName [-barmode MySQLMode]

omnib -integ PostgreSQL ListName [-barmode PostgreSQL]

MIRROR_OPTIONS

-mirror *BackupDevice* [-pool *MediaPool* -prealloc *MediaList*]

GENERAL_OPTIONS

-preview

-pool *MediaPool*

-prealloc *MediaList*

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

-report { warning | minor | major | critical }

-pre_exec *Pathname*

-post_exec *Pathname*

-compress

-encode [aes256]

-load { low | medium | high }

-crc

-no_monitor

-keepcatalog { weeks *n* | days *n* | until *Date* }

-variable *VariableName VariableValue*

FILESYSTEM_OPTIONS

-trees *TreeList*

-only *MatchPattern*

-exclude *TreeList*

-skip *MatchPattern*

-lock

-touch

-[no_] log | -log_dirs | -log_file

-mode { Full | Incremental| Incremental[1-9] }

-enh_incr

-clp

-[no_] hlink

-size *FromRange ToRange*

BLOCKBASED_OPTIONS

-trees *TreeList*

-only *MatchPattern*

-exclude *TreeList*

-skip *MatchPattern*

-lock

-touch

-mode { Full | Incremental }

WINFS_OPTIONS

-no_share[_info]

-[no_]nthlinks

-[no_]archatt

-[no_]vss [fallback]

-async

BACKUP_SPECIFICATION_OPTIONS

-select *SelectList*

-mode { Full | Incremental[1-9] }

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

-preview

-disk_only

-load { low | medium | high }

-crc

-no_monitor

-priority *NumValue*

LIST_OPTIONS

-barcmnd *Command*

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

-load { low | medium | high }

-crc

-no_monitor

-test_bar

-disk_only

NDMP_OPTIONS

-ndmp_user *UserName*

-ndmp_passwd *Password*

-ndmp_env *FileName*

-ndmp_bkptype { dump | nvb | SMTape }

-[no_]log -log_dirs -log_file

-mode { full | incremental1 }

-pool *MediaPool*

-prealloc *MediaList*

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

-report { warning | minor | major | critical }

-variable *VariableName VariableValue*

OTHER OPTIONS

NDMP_Server_Type = Generic | NetApp | Celerra | BlueArc | Hitachi | HPX9000

SapMode = full | incr

SapdbMode = full | diff | trans

HanaMode= full | incr

Oracle8Mode = full | incr1 | ... | incr4

SybaseMode = full | trans

InformixMode = full | inf_incr1 | inf_incr2

MSSQLMode = full | copy | diff | trans

MSSPSMode = full | diff | trans

MSExchangeMode = full | incr

E2010Mode = full | copy | incr | diff

LotusMode = full | incremental

VSSMode = full | copy | incr | diff

MSMailboxMode = full | incr | incr1

DB2Mode = full | incr | delta

MSSharePointMode = full | diff | incr

IDBMode = full | incr

VirtualEnvironmentMode = full | diff | incr

MySQLMode = full | incr | trans

PostgreSQLMode = full | incr

Date = [*YY*] *YY*/*MM*/*DD* (1969 < *YYYY* < 2038)

DESCRIPTION

The omnib command uses a backup specification (list of file or database objects) to back up data objects. The following Data Protector functionality is supported:

Session management: Controls the backup sessions. The Session Manager reads the backup specification or uses the command options to determine what to back up and how many copies of the backup objects to create (object mirroring), then initiates the Disk and Media Agents for disks and backup devices which will be used in the session. Once the session has completed, the Session Manager updates the MMDB with the session information.

Media management: Provides easy and efficient management of large sets of media by grouping media, tracking their status, implementing a media rotation policy, supporting the barcode recognition, vaulting the media, automating the library device operations, storing the media related information in a central place and sharing this information among several Data Protector cells.

Data compression: Writes data to media in a compressed format.

Data encryption: Writes data to media in an encrypted format using the Advanced Encryption Standard (AES) algorithm.

Backup monitoring: When the backup command is executed, it sends a request (specifying the backup objects) to the Session Manager. When the Session Manager (SM) accepts the request, it assigns a unique SessionID to the session. You can use this SessionID to monitor the progress of the session using the Monitor context of the Data Protector GUI or the omnistat command. You can also use the omniabort command to terminate a session.

Note During the Internal Database Backup (PostgreSQL) in Incr mode, the configuration files are backed up as full.

OPTIONS

-version

Displays the version of the omnib command

-help

Displays the usage synopsis for the omnib command

-filesystem *Client:MountPoint Label*

Specifies the client, mount point and label of the filesystem to be backed up.

-vprotect *Client:MountPoint Label*

Specifies the client, mount point and label of the vProtect node to be backed up.

-winfs *Client:MountPoint Label*

Specifies the client, mount point and label of the Windows filesystem to be backed up.

-winfsblockbased *HostName Volume*

Specifies the host name and volume details of the Windows block to be backed up.

-host *Client:/ Label*

Specifies the client to be backed up as a set of filesystems defined at backup time. The label is used as a prefix for each of these filesystem labels. Client backup is useful for systems with filesystem configuration that often changes.

-rawdisk *Client Label SectionList*

Specifies the client, sections (pathnames of disk image sections) and label of the node to be backed up.

-datalist *Name*

Specifies the name of the backup specification file for the backup. The backup specification contains the data objects (filesystems and disk image sections) to be backed up.

-restart *SessionID*

Tries to restart a failed session, specified by its sessionID.

-resume *SessionID*

Resumes a failed or aborted backup session. This option is applicable to a filesystem backup and Oracle Server integration backup. While resume of a filesystem backup creates an incremental backup of the failed session, the Oracle Server integration resumes the backup by creating a new session using the same backup specification as the failed session. In both cases, only the data that has not been backed up in the failed session is backed up.

-sap_list *ListName*

Specifies the name of the SAP R/3 backup specification file for the backup. The SAP R/3 backup specification contains the SAP R/3 objects to be backed up.

-barmode *SapMode*

For SAP R/3 objects, the possible modes are full and incr. The default value for this option is full.

-hana_list *ListName*

Specifies the name of the SAP HANA backup specification file for the backup. The SAP HANA backup specification contains the SAP HANA objects to be backed up.

-barmode *HanaMode*

For SAP HANA objects, the possible modes are full and incr. The full option triggers a full backup of the SAP HANA instance, and the incr option triggers an incremental backup. The default value for this option is full.

-sapdb_list *ListName*

Specifies the name of the SAP MaxDB backup specification file for the backup. The SAP MaxDB backup specification contains the SAP MaxDB objects to be backed up.

-barmode *SapdbMode*

For SAP MaxDB objects, the possible modes are full, diff, and trans. The full option triggers a full backup of the SAP MaxDB instance, the diff option triggers a differential backup, and the trans option triggers an archive logs backup. The default value for this option is full.

-oracle8_list *ListName*

Specifies the name of the Oracle backup specification file for the backup. The Oracle backup specification contains the Oracle objects to be backed up.

-barmode *Oracle8Mode*

For Oracle objects you can specify full for full backup or incr1 through incr4 for incremental backups.

-sybase_list *ListName*

Specifies the name of the Sybase backup specification file for the backup. The Sybase backup specification contains the Sybase objects to be backed up.

-barmode *SybaseMode*

For Sybase objects you can specify full for full database backup or trans for transaction backup. The default value for this option is full.

-informix_list *ListName*

Specifies the name of the Informix Server backup specification file for the backup. The Informix Server backup specification contains the Informix Server objects to be backed up.

-barmode *InformixMode*

For Informix Server objects you can specify the following modes:

full : full backup of dbspaces specified during the backup specification creation time,

inf_incr1 : first incremental backup,

inf_incr2 : second incremental backup.

The default value for this option is full .

-mssql_list *ListName*

Specifies the name of the Microsoft SQL Server backup specification file for the backup. The Microsoft SQL Server backup specification contains the Microsoft SQL Server objects to be backed up.

-barmode *MSSQLMode*

For Microsoft SQL Server objects you can specify full for a full database backup, copy for a copy-only full backup, diff for a differential database backup or trans for a transaction log backup. The default value for this option is full .

In Microsoft SQL Server log shipping configurations, transaction log backup cannot be performed. A differential database backup is started when a transaction log backup is requested.

In Microsoft SQL Server availability group configurations, when you trigger a full or a differential backup of a database belonging to an availability group secondary replica, the backup type is automatically changed to a copy-only full backup.

-integ PostgreSQL ListName

Specifies the name of the PostgreSQL backup specification file for the backup. The PostgreSQL backup specification contains a list with the PostgreSQL objects to be backed up.

-barmode PostgreSQL

For PostgreSQL objects, you can specify full for a full backup or incr for an incremental backup. Note, that an incremental backup cannot be run without a previously successful full backup.

If this option is not specified, Data Protector performs a full backup.

-e2010_list *ListName*

Specifies the name of the Microsoft Exchange Server backup specification file for the backup. The Microsoft Exchange Server backup specification contains the Microsoft Exchange Server 2010/2013 objects to be backed up.

-barmode *E2010Mode*

For Microsoft Exchange Server 2010/2013 objects, you can specify full for a full backup, copy for a copy backup, incr for an incremental backup, or diff for a differential backup.

Note that an incremental backup session cannot be followed by a differential backup session, nor the other way around. You must first run a full backup session.

If this option is not specified, a full backup is performed.

-lotus_list *ListName*

Specifies the name of the Lotus Notes/Domino Server backup specification file for the backup. The Lotus Notes/Domino Server backup specification contains the Lotus database objects to be backed up.

-barmode *LotusMode*

For Lotus Notes/Domino Server objects you can specify full for full database backup or incr for a full backup of selected Lotus Notes/Domino objects, if the amount of data changed from the last backup is bigger than the value specified for the backup specification option Amount of log changes (KB) in the Data Protector GUI. In case that transaction logging is enabled, the full backup of all archived transaction logs is also performed. The default value for this option is full.

-msvssw_list *ListName*

Specifies the name of the Microsoft VSS backup specification file for the backup. The Microsoft VSS backup specification contains the Microsoft VSS objects to be backed up.

-barmode *VSSMode*

Available backup types primarily depend on the VSS writer that is chosen to be backed up. While some VSS writers support several backup types (for example full, copy, incr, diff with Microsoft Exchange Server 2003 writer), others support only full. Even when supported with the selected VSS writer by Data Protector, not all types might be available at all times.

Data Protector aborts the backup session if an unsupported or unavailable backup type is specified.

-mbx_list *ListName*

Specifies the name of the Microsoft Exchange Server single mailbox backup specification file for the backup. The Microsoft Exchange Server single mailbox backup specification contains single mailboxes to be backed up.

-barmode *MSMailboxMode*

For Microsoft Exchange Server single mailboxes, you can specify full for a full mailbox backup, incr for an incremental mailbox backup, or incr1 for an incremental1 mailbox backup. The default value for this option is -full.

-db2_list *ListName*

Specifies the name of the IBM DB2 UDB backup specification file for the backup. The IBM DB2 UDB backup specification contains the IBM DB2 UDB objects to be backed up.

-barmode *DB2Mode*

For IBM DB2 UDB objects you can specify full for full database backup, incr for incremental database backup, or delta for delta database backup. The default value for this option is full.

-mssps_list *ListName*

Specifies the name of the Microsoft SharePoint Portal Server backup specification file for the backup. The Microsoft SharePoint Portal Server backup specification contains the Microsoft SharePoint Portal Server objects to be backed up.

-barmode *MSSPSMode*

For Microsoft SharePoint Portal Server objects you can specify the following modes:

full: full backup,

diff: differential database backup of Microsoft SQL Server databases and full backup of other Microsoft SharePoint Portal Server objects,

trans: transaction log backup of Microsoft SQL Server databases and full backup of other Microsoft SharePoint Portal Server objects.

The default value for this option is full.

-mssharepoint_list *ListName*

Specifies the name of the Microsoft SharePoint Server 2010/2013 backup specification file for the backup. The Microsoft SharePoint Server 2010/2013 backup specification contains the Microsoft SharePoint Server 2010/2013 objects to be backed up.

-barmode *MSSharePointMode*

For Microsoft SharePoint Server 2010/2013 objects you can specify the following modes:

full : full backup,

diff : a Microsoft SQL Server differential backup of the database, and backup of the index files that have been changed since the last full backup,

incr : a backup of transaction logs (.log) that have been created since the last transaction log backup of the Microsoft SQL Server database, and backup of the index files that have been changed or created since the last backup of any type.

If this option is not specified, a full backup is performed.

-idb_list *IDBList*

Specifies the name of the Internal Database backup specification file for the backup. The Internal Database backup specification contains a list with the Data Protector Internal Database and its related objects to be backed up.

-barmode *IDBMode*

For Internal Database objects, you can specify full for a full backup or incr for an incremental backup. Note that an incremental backup cannot be run without a previously successful full backup.

If this option is not specified, a full backup is performed.

-veagent_list *ListName*

Specifies the name of the virtual environment backup specification file for the backup. The backup specification contains the virtual environment objects to be backed up.

-barmode *VirtualEnvironmentMode*

For VMware vSphere and H3C CAS objects, the available modes are full , diff , and incr . The full option triggers a full backup, the diff option triggers a differential backup(For H3C CAS, CBT backup method does not support differential backup), and the incr option triggers an incremental backup.

For Microsoft Hyper-V objects, the available modes are full and incr . The full option triggers a full backup and the incr option triggers an incremental backup. Under specific circumstances, the incremental backup session falls back and Data Protector performs a full backup instead.

If this option is not specified, Data Protector attempts to start a full backup.

-integ MySQL *ListName*

Specifies the name of the MySQL backup specification file for the backup. The MySQL backup specification contains a list with the MySQL objects to be backed up.

-barmode *MySQLMode*

For MySQL objects, you can specify full for a full backup, incr for an incremental backup, or trans for transaction log backup. Note, that an incremental backup cannot be run without a previously successful full backup.

If this option is not specified, Data Protector performs a full backup.

-device *BackupDevice*

Specifies the backup device to be used for the backup.

-public

If you use this option, you allow other users to see and restore your data. By default for filesystem backups, only the Data Protector administrator and the user who created a backup can see and restore the data.

-storedrim

If this option is specified, a disaster recovery OS image is created and saved to theCell Manager's disk at the end of the backup session.

The image is stored in P1S files directory with the filename ClientName .img.

Note that you can obtain the image from a disk much faster than from a backup medium.

MIRROR_OPTIONS

-mirror *BackupDevice*

Specifies one or several backup devices to be used for object mirroring. Different backup devices should be specified for the backup and for each mirror.

-pool *MediaPool*

Instructs the Session Manager to use an alternate media pool for object mirroring. By default, the default media pool for the backup device is used.

-prealloc *MediaList*

Specifies a list of media to be used for object mirroring. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt is issued. NOTE: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

GENERAL_OPTIONS

-preview

Checks the backup objects, backup devices and options you selected, without performing the backup. The check includes: backup objects, status of the backup device, available media, and the approximate amount of data which will be backed up.

-pool *MediaPool*

Instructs the Session Manager to use an alternate media pool for the backup. By default, the default media pool for the backup device is used.

-prealloc *MediaList*

Specifies a list of media to be used for the backup. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt is issued. NOTE: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

Sets the level of protection for the backup session. The media containing this backup session cannot be overwritten until the protection expires. By default, the protection is permanent.

-report { warning | minor | major | critical }

Sets the level of error notification for the session. Errors are classified (in ascending order) as: warning , minor , major and critical . When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if major is selected, only major and critical errors are reported. By default, all errors are reported.

-pre_exec *Pathname*

Instructs the Session Manager to execute this command before starting the backup session. The complete *Pathname* of the command should be specified. The command is executed on the Session Manager system.

-post_exec *Pathname*

Instructs the Session Manager to execute this command after the backup session. The complete *Pathname* of the command should be specified. The command is executed on the Session Manager system.

-compress

Instructs the General Media Agent to write data to media in the compressed format.

-encode [aes256]

Instructs the General Disk Agent to write data to media in encoded format.

If the aes256 option is specified, data is written to media in encrypted format, using the Advanced Encryption Standard (AES) algorithm.

-load { low | medium | high }

Specifies the level of network traffic generated by a session during a time period. High level generates as much traffic as

allowed by the network, resulting in a faster backup. Low level has less impact on the network performance, but results in a slower backup. By default, this option is set to high.

-crc

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the omnimver command.

-no_monitor

By default, the command monitors the session and displays the status of the session during the session. If this option is used, the SessionKey is displayed and the command is disconnected from the session.

-keepcatalog { weeks *n* | days *n* | until *Date* }

This option specifies file catalog retention time. If you do not want to save the file catalog at all, use the -no_log option. By default, this option is set to the same value as specified by the protection option.

-variable *VariableName VariableValue*

This option lets you specify a variable name and its value for proper operation of some platforms and integrations. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

-priority *NumValue*

In case multiple running sessions request access to a specific device at the same time, this option determines the order in which the sessions will be queued. The *NumValue* can be any value from 1 (the highest priority) to 6000 (the lowest priority). In case the option is not specified, the default value of 3000 is set.

If a low priority session is running when a high priority session starts queuing, the currently running session is allowed to finish. When more sessions request access to a device with the same priority, any of these sessions might acquire access first.

FILESYSTEM_OPTIONS

-trees *TreeList*

Specifies the trees to be included in the backup. If this option is not used, the filesystem is backed up from the mount point level downwards. When specifying several trees, separate each *Tree* with a space. *Tree* must start with a /. Note that when specifying trees on UNIX systems, the complete tree must be specified including the mountpoint, whereas on Windows systems, trees must be specified without volumes (drives). For example: -tree /usr/temp (UNIX system) or -tree \temp (Windows system). This option is not supported with Data Protector NDMP server integration.

-only *MatchPattern*

Specifies that only files that match the *MatchPattern* will be backed up. This option is not supported with Data Protector NDMP server integration.

-exclude *TreeList*

Specifies trees not to be backed up. This option is not supported with Data Protector NDMP server integration.

-skip *MatchPattern*

Specifies that files matching the *MatchPattern* will not be backed up. This option is not supported with the Data Protector NDMP server integration.

-lock

Instructs the Disk Agent to lock each file before backing it up. If the file is in use (and cannot be locked), the session manager displays a warning that this file cannot be locked and backs up the file anyway. This warning is also logged to the catalog database. By default, files are not locked at backup.

-no_log

Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log

The default option. All detailed information about backed up files and directories (filenames, file versions, and attributes)

are logged to the Data Protector Internal Database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

-log_dirs

If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log_file

All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector Internal Database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape.

It also does not take much space since some information on file details (file attributes) is not logged to the database.

-mode { Full | Incremental[1-9] }

Specifies the type for the backup session. Full type backs up all specified files. Incremental[1-9] backs up only a subset of the specified files, based on whether or not the files were modified since the last Full or lower-level Incremental backup. Default is the Full type. The level of incremental backup is based on the level number which is specified.

For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 or lower backup.

-touch

Whenever a file is opened, read, or locked, which happens during backup, the file's access time attribute changes. By default, after backup, Data Protector resets the file's access time attribute to the value it had before backup. However, on UNIX, this resetting of the access time attribute modifies the file's change time.

If the -touch option is specified, Data Protector does not reset access time attributes. Then, on UNIX, Data Protector can also use the file's change time (inode modification time) as an incremental backup criterion. As a result, files with a changed name, location, or attributes are backed up in an incremental backup.

-no_hlink

If this option is specified, then hard link detection is disabled and hard links are backed up as normal files. This speeds up the first traversal of the filesystem.

-enh_incr

This option enables enhanced incremental backup. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up files with changes in name, location, and attributes. It is also a prerequisite for subsequent object consolidation (synthetic backup).

NOTE: After you select this option, incremental backup will run in the enhanced mode only after a full backup is performed.

-clp

This option enables using the Windows NTFS Change Log Provider with enhanced incremental backups and conventional incremental backups. A list of files to be backed up will be generated by querying the Windows Change Journal rather than performing a file tree walk.

-size *FromRange* *ToRange*

Limits backup to those files only, of which sizes are in the specified range. The sizes are set in kB. If you set *ToRange* to 0, all files larger then *FromRange* will be backed up.

WINFS_OPTIONS

-no_share[_info]

If this option is specified, share information for directories on Windows systems is *not* backed up. By default, if a directory was shared on the network when a backup was run, the share information for directory is backed up, unless the -no_share[_info] option is specified.

Backing up share information for shared directories enables you to automatically share such directories after restore.

-[no_]nthlinks

If this option is specified then NTFS hard link detection is disabled and NTFS hard links are backed up as normal files. This speeds up the first traversal of the filesystem.

-[no_]archatt

By default, Data Protector uses the archive attribute as an incremental backup criterion and also clears the file's archive attribute after the file is backed up. The archive attribute is automatically set by the system when the file's content, properties, name, or location changes.

If archive attributes cannot be cleared, an error is reported. This affects future incremental backups, so that the files are backed up, although they have not changed. This may happen when backing up removable media with write protection. In the case of ZDB, archive attributes are cleared on the replica and this is not reflected on the source volume. As a result, in the next incremental ZDB session, when a new replica is created, the archive attributes appear again and the corresponding files are backed up although they may not have changed. To enhance the incremental ZDB behavior, specify the -[no_]archatt option.

If the -[no_]archatt option is specified, Data Protector ignores archive attributes and detects changed files using other criteria, such as the file's modification time.

-[no_]vss [fallback]

If the -vss option is specified, the VSS filesystem backup is performed. If the shadow copy creation on the system where the VSS filesystem backup is running, fails, the backup also fails by default. However, you can avoid backup failure by specifying the fallback option. In this case, the backup will continue as the normal filesystem backup.

NOTE: VSS file system backup is used on Windows systems even if the -vss is not specified. To ensure that VSS is not used, specify -no_vss .

-async

If this option is specified, Disk Agent performs asynchronous reading from the disk without using Windows cache manager. Concurrent reads of the same file are started simultaneously. If this option is not specified, synchronous reading from the disk is performed.

BACKUP_SPECIFICATION_OPTIONS

-select *SelectList*

Specifies which objects (of those in the backup specification) to back up. The *SelectList* is the list of objects to be backed up.

-mode { Full | Incremental[1-9] }

Specifies the type for the backup session. Full type backs up all specified files. Incremental[1-9] backs up only a subset of the specified files, based on whether or not the files were modified since the last full or lower-level Incremental backup. Default is the Full type. The level of incremental backup is based on the level number which is specified. For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 (or lower) backup.

Use incremental level 1 to back up files that were changed since last full backup only. The Incremental without level will back up the files that changed since the last backup only (regardless whether it was full or incremental of any level).

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

See *GENERAL_OPTIONS* .

-preview

Checks the backup objects, backup devices and options you selected, without performing the backup. The check includes: objects due for backup, status of the backup device, available media, and approximate amount of data which will be backed up.

-disk_only

A ZDB related option. It instructs Data Protector to perform a ZDB-to-disk session rather than a ZDB-to-tape or ZDB-to-disk+tape session. With ZDB, if the option is not specified, a ZDB-to-tape or ZDB-to-disk+tape session is performed.

-load { low | medium | high }

See *GENERAL_OPTIONS* .

-crc

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the omnimver command.

-no_monitor

By default, the command monitors the session and displays the status of the session during the session. If this option is used only the SessionKey is displayed and the command is disconnected from the session.

LIST OPTIONS

-barcmnd *Command*

Specifies the command that will be used instead of the command specified with exec option in the backup specification. The command should reside in the default Data Protector administrative commands directory.

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

See *GENERAL_OPTIONS*.

-load { low | medium | high }

See *GENERAL_OPTIONS*.

-crc

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the omnimver command.

-no_monitor

By default, the command monitors the session and displays the status of the session during the session. If this option is used, only the SessionKey is displayed, and the command is disconnected from the session.

-test_bar

Enables backup preview mode. Backup preview is only available for backup sessions for Oracle Server, SAP R/3, SAP MaxDB, Microsoft Exchange Server single mailbox, Lotus Notes/Domino Server, IBM DB2 UDB, SAP HANA, Informix Server, and Sybase integrations. Zero downtime backup preview is not supported.

This option checks the backup objects, backup devices, and options you selected, without actually performing the backup. The check includes: objects due for backup, status of the backup device, available media, and the approximate amount of data which will be backed up.

-disk_only

This ZDB-related option is supported only for specific application integrations, and not for the Internal Database backup. It instructs Data Protector to perform a ZDB-to-disk session rather than a ZDB-to-tape or ZDB-to-disk+tape session.

With ZDB backup specifications, if the option is not specified, a ZDB-to-tape or ZDB-to-disk+tape session is performed.

NDMP_OPTIONS

-ndmp_user *UserName*
Sets the username that is used by Data Protector to establish the connection to the NDMP server.

-ndmp_passwd *Password*
Sets the password for the username that is used by Data Protector to establish the connection to the NDMP server.

-ndmp_env *FileName*
Specifies the filename of file with NDMP environment variables for specific NDMP implementations.

-ndmp_bkptype { Dump | NVB | SMTape }
Specifies the backup type for NDMP EMC Celerra backups. Dump is the default backup type, that backs up data at a file level. NDMP volume backup (NVB) is an EMC-specific NDMP backup type. NVB backs up data blocks at a volume level. SMTape backup is an NetApp-specific NDMP backup type. SMTape backs up data blocks at a volume level.

-no_log
Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log
The default option. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the Data Protector Internal Database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

-log_dirs
If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log_file
All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector Internal Database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape. It also does not take much space since some information on file details (file attributes) is not logged to the database.

-mode { Full | Incremental[1-9] }
Specifies the mode for the backup session. Full mode backs up all specified files. Incremental[1-9] backs up only a subset of the specified files, based on whether or not the files were modified since the last Full or lower-level Incremental backup. Default is the Full mode. The level of incremental backup is based on the level number which is specified. For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 or lower backup.

-pool *MediaPool*
Instructs the Session Manager to use an alternate media pool for the backup. By default, the default media pool for the backup device is used.

-prealloc *MediaList*
Specifies a list of media to be used for the backup. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt is issued. NOTE: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

-protect { none | weeks *n* | days *n* | until *Date* | permanent }
Sets the level of error notification for the session. Errors are classified (in ascending order) as: warning, minor, major and critical. When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if major is selected, only major and critical errors are reported. By default, all errors are reported.

-report { warning | minor | major | critical }
See *GENERAL_OPTIONS*.

-variable *VariableName VariableValue*
This option lets you specify a variable name and its value for proper operation of some platforms and integrations. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

RETURN VALUES

See the man page omniintro for return values. Additional return values of the omnib command are:

10 - There was an error while backing up some files. All agents completed successfully.

11 - One or more agents failed, or there was a database error.

12 - None of the agents completed the operation; session was aborted by Data Protector.

13 - Session was aborted by user.

EXAMPLES

The following examples illustrate how the omnib command works:

1. To do a backup of a tree "/usr" of filesystem "senna" with the label "work", using the compress option, to the backup device "DAT", execute:

   ```
   omnib -device DAT -filesystem senna:/ work -tree /usr -compress
   ```

2. To perform an incremental backup using the backup specification OMNIGROUP, and to make the devices available to this session with the highest priority in case of resource conficts, execute:

   ```
   omnib -datalist OMNIGROUP -mode Incremental -priority 1
   ```

3. To perform a backup of the tree "/Amt3" of the filesystem "Munich", skipping the files with the ".fin" extension, execute:

   ```
   omnib -filesystem Munich:/ -tree /Amt3 -skip "*.fin"
   ```

4. To execute a disk image backup of the section "/dev/rdsk/c201d1s0" on the client "xanadu" to the backup device "Exa" and protecting the session against overwrite for 4 weeks:

   ```
   omnib -rawdisk xanadu section /dev/rdsk/c201d1s0 -dev Exa -protect weeks 4
   ```

5. To execute a full Lotus backup using the "test2" backup specification with the high network load and permanent protection set:

   ```
   omnib -lotus_list test2 -barmode full -protect permanent -load high
   ```

6. To start a full backup using an IBM DB2 UDB backup specification named "TEST", and to set data protection to 10 weeks, execute:

   ```
   omnib -db2_list TEST -barmode full -protect weeks 10
   ```

7. To start a differential backup using an SAP MaxDB backup specification named "test", and write a CRC checksum at the end of every block on the medium, execute:

   ```
   omnib -sapdb_list test -barmode diff -crc
   ```

8. To start a differential backup of H3C CAS virtual machines using the backup specification named `bSpec1`, execute:

   ```
   omnib -veagent_list bSpec1 -barmode diff
   ```

9. To start a differential backup using a Microsoft Exchange Server backup specification named "bSpec1", execute:

   ```
   omnib -e2010_list bSpec1 -barmode diff
   ```

10. To perform an encrypted backup of a tree "/usr" of filesystem "alpha.hp.com" with the label "work", using the `encode aes256` option, to the backup device "ENC1", execute:

    ```
    omnib -filesystem alpha.hp.com:/work -device ENC1 -tree /usr -encode aes256 -mode full
    ```

11. To back up a volume "/vol/vol1" of the Celerra NDMP Server "alpha.hp.com" using the NVB backup type option, to the backup device "DAT", execute:

    ```
    omnib -filesystem alpha.hp.com:/vol/vol1 /vol/vol1 -device DAT -ndmp Celerra -ndmp_bkptype nvb
    ```

12. To start a full backup using a Microsoft SharePoint Server 2013 backup specification named "myBackup", execute:

    ```
    omnib -mssharepoint_list myBackup -barmode full
    ```

13. To perform a full backup of the Data Protector Internal Database (IDB) using the backup specification named "idb_weekly" and omit session monitoring in the command output, execute:

    ```
    omnib -idb_list idb_weekly -no_monitor
    ```

14. To perform a full block based backup of *Volume E* on host *hostname.company.com* and device *device_name* execute:

    ```
    omnib -winfsblockbased hostname.company.com E "E: [New Volume]" –device device_name
    ```

15. To perform an incremental backup of the Data Protector Internal Database (IDB) using the backup specification named "idb_daily", with as little impact on the network traffic during the session as possible, execute:

    ```
    omnib -idb_list idb_daily -barmode incr -load low
    ```

16. To start an incremental backup of Microsoft Hyper-V virtual machines using the backup specification named "hyperv_host_4" and disable session monitoring, execute:

    ```
    omnib -veagent_list hyperv_sys_4 -barmode incr -no_monitor
    ```

17. To start an incremental backup of H3C CAS virtual machines using the backup specification named `iSpec1`, execute:

    ```
    omnib -veagent_list iSpec1-barmode incr
    ```

18. To start a transaction log backup of your MySQL instance using the backup specification named "mysql_instance_core_sys", execute:

    ```
    omnib -integ MySQL mysql_instance_core_sys -barmode trans
    ```

SEE ALSO

omnikeytool(1M), omniobjconsolidate(1), omniobjcopy(1), omniobjverify(1), omnir(1)

omnicc

omnicc - handles the Data Protector licensing, reports the number of configured and available Data Protector licenses, installs the licenses, imports and exports Data Protector clients, manages access to secured clients, and creates a template for the user_restrictions file
(this command is available on systems with any Data Protector component installed)

> **Note:** The output for the omnicc -query, omnicc -check_license, omnicc -check_license -detail, and omnicc -password_info commands is displayed incorrectly due to the emergency license that is active even after applying a new license. To display the output correctly, remove the emergency license key and its annotation from the **lic.dat** file in the \programdata\config\server\cell\ (Windows) or /etc/opt/omni/server/cell/ (Linux) path.

SYNOPSIS

omnicc -version | -help

omnicc -redistribute

omnicc -import_host HostName [-virtual] [-accept_host]

omnicc -import_mac_host HostName [-virtual]

omnicc -import_openvms_host HostName [-virtual]

omnicc -import_ndmp HostName -type NdmpType -port Port -user UserName -passwd Password

omnicc -import_is HostName [-accept_host]

omnicc -export_is HostName

omnicc -update_host HostName [-accept_host]

omnicc -update_all [-force_cs] [-accept_host]

omnicc -update_port [Port] [-old_port OldPort]

omnicc -update_local_port InetPort

omnicc -export_host HostName

omnicc -install_license password

omnicc -password_info

omnicc -socket_info

omnicc -add_certificate CertificateName PathOfCertificateFile

omnicc -get_certificate CertificateName

omnicc -list_certificates

omnicc -confirm_mom_clients

omnicc -update_mom_server

omnicc -check_licenses [-detail[-online][-exact]]

omnicc -cbl_detail

omnicc -dp4cw[_data] [-detail]

omnicc [-query]

omnicc -create_userrestrictions_tmpl

omnicc -gre_license_info

omnicc -impersonation -add_user -user {User@Domain | Domain\User} {-host Hostname [-host Hostname...] | -all} {-passwd Password | -passwdfile PasswordFile}

omnicc -impersonation -modify_user -user {User@Domain | Domain\User} {-host Hostname [-host Hostname...] | -all} {-passwd Password | -passwdfile FileName} {-old_passwd OldPassword | -old_passwdfile OldFileName}

omnicc -impersonation -delete_user -user {User@Domain | Domain\User} {-host Hostname [-host Hostname...] | -all} {-passwd Password | -passwdfile FileName}

omnicc -secure_comm -remove_peer {Hostname1 [Hostname2 ...]}

omnicc -secure_comm -configure_peer {Hostname1 [Hostname2 ...]} [-accept_host]

omnicc -secure_comm -configure_peer_with_cert Hostname [-certfile <CertificateFilePath>]

omnicc -secure_comm -configure_for_dr Hostname [-overwrite]

omnicc -secure_comm -configure_for_cm Hostname [-overwrite]

omnicc -secure_comm -configure_for_is Hostname [-overwrite]

omnicc -secure_comm -configure_for_gui Hostname [-overwrite]

omnicc -secure_comm -configure_for_legacy_client Hostname [-overwrite]

omnicc -secure_comm -regenerate_cert [Hostname]

omnicc -secure_comm -renew_cert [NumberOfDays]

omnicc -secure_comm -reconfigure_peer HostName

omnicc -secure_comm -reconfigure_peer_all [InputFile]

omnicc -secure_comm -get_fingerprint

omnicc -import_esx HostName -port Port -user UserName -passwd Password -web_root WebRoot -integrated_sec { 0 | 1 }

omnicc -import_vcenter HostName -port Port -user UserName -passwd Password -web_root WebRoot -integrated_sec { 0 | 1 } -register_greplugin {0 | 1 }

omnicc -import_hyperv HostName -user UserName -passwd Password

omnicc -import_vcd HostName -user UserName -passwd Password

omnicc -import_h3ccas HostName -port Port -user UserName -passwd Password

omnicc -import_cs HostName [-accept_host]

omnicc -export_cs HostName

omnicc -add_socket –virtualhost <hostname> [-hypervisor <hypervisorname>]

omnicc –reclaim_socket –uuid <uuid>

omnicc -unregister_greplugin HostName

omnicc -upgrade_greplugin HostName

omnicc -migrate_devfilter [HostName] [-delete_old_devfilter]

omnicc -update_local_port InetPort

NdmpType = { Generic | NetApp | Celerra | BlueArc | Hitachi | HP-X9000}

omnicc -firewall { -host Hostname [Hostname] | -all } [-enable_dp|-disable_dp] [-enable_os|-disable_os]

omnicc -update_port [new_port] [-old_port old_port]

omnicc -update_omnirc variableName -value variableValue [inputFile]

omnicc -secure_data_comm <*Value*>

omnicc -auditlog <*Value*> [-retention_months <*retentionValue*>]

omnicc -chgblkdrvr_install [-force]

omnicc -chgblkdrvr_uninstall

omnicc -chgblkdrvr_status

omnicc -chgblkdrvr_remove_config <devName>

omnicc -import_dp4cw HostName -port Port -user UserName -passwd Password

omnicc -export_dp4cw HostName

DESCRIPTION

The omnicc command is used for licensing, importing and exporting clients, managing secured clients, and creating a template for the user_restrictions file.

OPTIONS

The following firewall commands are executed on the Cell Manager:

-version

Displays the version of the omnicc command.

-help

Displays the usage synopsis for the omnicc command.

-redistribute

Displays licensing information for multicell environments. The first part shows the number of allocated licenses and the second shows the number of licenses actually used per server.

-import_host *ClientName* [-virtual] [-encr_disable] [-encr_recreate_cert]

Imports the specified server into the cell. If the client has multiple names, import each additional name with the -virtual option

If –encr_disable is specified, encrypted communication is not enabled on the client.

If –encr_recreate_cert is specified, certificates are recreated and the existing ones are overwritten.

-import_host *ClientName* [-virtual]

Imports the specified client into a cell. This allows you to move a client between two cells without reinstalling the Data Protector modules.

When you import the next one among multiple network names (clusters, service guards), use the -virtual option. This way you keep Data Protector from assigning licenses to all the network names of the same system.

-import_ndmp *ClientName*

Imports the specified NDMP server into the cell.

-type *NdmpType*

Sets the NDMP data format when importing an NDMP server into a cell.

-port *Port*

Sets the TCP/IP port number of the NDMP server when importing an NDMP server into a cell.

-user *UserName*

Sets the username that is used by Data Protector to establish the connection to the NDMP server when importing an NDMP server into a cell.

-passwd *Password*

Sets the password for the username that is used by Data Protector to establish the connection to the NDMP server when importing an NDMP server into a cell.

-import_is *ClientName*

Imports an already installed Installation Server into the cell.

-export_is *ClientName*

Exports an already installed Installation Server from the cell.

-update_host *ClientName*

Updates the version information and installed components information in the Cell Manager configuration file for the specified client. You can use this option in circumstances when new remote installation packages for particular components exist on the client, but the component upgrade has failed.

-accept_host

This option is used to skip the finger print verification while specifying the client for verification by the user.

-update_all [-force_cs]

Updates the version information and installed components information in the Cell Manager configuration file for all clients in the cell. You can use this option in circumstances when new remote installation packages for particular components exist on some clients, but the component upgrade processes have failed.

If the -force_cs option is specified, it checks if any clients have been improperly added to the current cell. If such clients

exist, the command properly imports them into the cell before updating the information on the Cell Manager.

-export_host *ClientName*

Exports the specified client from the cell. This enables you to remove a client from the cell without uninstalling its Data Protector modules.

If the host is a vCenter system with the Advanced GRE Web Plug-in installed, then this command unregisters the Advanced GRE Web Plug-in from the vCenter and then exports the vCenter client from the cell server.

In case of Data Protector Express license, if the host is an imported client (vCenter, ESX or hyper-V), then the sockets associated with the hypervisor are reclaimed.

-list_authorities *ClientName*

Lists systems from which the specified client accepts requests on the Data Protector port (by default 5555/5565).

-secure_client *ClientName*

Specifies the client to be secured.

-authorities *ClientName* [*ClientName2* ...]

Specifies systems from which the specified client accepts requests on the Data Protector port (by default 5555/5565). Consequently, other computers will not be able to access this client. For tasks like backup and restore, starting pre- or post-execution scripts, or importing and exporting clients, the client checks whether the computer which triggers one of these tasks via the Data Protector port is allowed to do so. This security mechanism instructs the client to accept such actions only from the systems specified by this option.

-unsecure_client *ClientName*

Specifies the client from which you want to remove security. Such a client will enable access to all systems in the cell.

-install_license *password*

Installs an encrypted Data Protector license. The password must be formatted as a single line and must not contain any embedded carriage returns. The password must be in quotes. If the password includes also a description in quotes, the quotes in this description must be preceded with backslashes.

-password_info

Displays information about password for one installed license with aggregated capacity per category.

-socket_info

This option is applicable for Data Protector Express only. It provides details on the number of sockets used by the licensed hypervisor clients.

-add_certificate *CertificateName* *PathOfCertificateFile*

Adds a certificate to the Cell Manager.

-get_certificate *CertificateName*

Downloads the certificate from the Cell Manager and displays its content.

-list_certificates

Lists certificates uploaded to the Cell Manager.

-confirm_mom_clients

Collects the cell_info files from MoM clients (Data_Protector_program_data \Config\Server\cell\mom_info on Windows clients or /etc/opt/omni/server/cell/mom_info on UNIX clients) and stores them on the MoM Manager into the directory Data_Protector_program_data \Config\Server\mom\cell_info (Windows systems) or /etc/opt/omni/server/mom/cell_info (Linux systems) under client

Cell Manager name. Use this command when switching MoM clients to CMMDB mode. The omnicc command with this option specified has to be executed on the MoM Manager.

-update_mom_server

Pushes the mom_info file located in the directory Data_Protector_program_data\Config\Server\cell (Windows systems) or /etc/opt/omni/server/cell (Linux systems) to MoM and CMMDB server to MoM into the directory Data_Protector_program_data\Config\Server\mom\cell_info (Windows systems) or /etc/opt/omni/server/mom/cell_info (Linux systems) under client Cell Manager name. Use this command when switching to CMMDB mode. The omnicc command with this option specified has to be executed on the client Cell Manager.

-check_licenses [-detail[-online][-exact]]

Reports licensing related information from the cell.

If the -detail option is specified, a detailed report is produced.

If the -detail option is not specified, the command returns information on whether the Data Protector licensing is covered or not. The following information is returned: the time when the report was generated, the licensing mode, the license server and the total TB of data under protection.

You can use the -online option to see a list of hosts that are using the online licenses.
You can use the -exact option to calculate total protected data for full backups beyond last 90 days, if there is any incremental backup within the 90 days.

Traditional licensing model: The license checker returns the following information for every license in the cell: product edition, licensing mode, license server, license type and the duration left along with the summary. Product Edition can be any of the following:

- Premium (Term based or Permanent)
- Express
- Traditional
- Trial (term based only)

Note that in a traditional licensing model for drive extension licenses-to-use, the license checker also returns information about configured drives and recommended additional licenses. You need as many licenses as there are drives in use at any point in time. This is typically the total number of configured drives to allow all drives to be used simultaneously.

Capacity based licensing model: The license checker returns the following information: the license name and the capacity of installed licenses.

In a MoM environment with the CMMDB configured, when producing a license report for the items that are subject to libraries and devices related licenses, such as media (including advanced file device media), backup devices, drives and slots, the omnicc command must be executed on the Cell Manager with the CMMDB installed.

In a MoM environment, only the data specific to this Cell Manager is reported, not for all the cells in the MoM environment.

-cbl_detail

Displays a report which contains the backup type, object ID, backup name and object size of objects that are used to calculate the total protected data capacity.

-dp4cw[_data] [-detail]

Displays a report about protected Data Protector for Cloud Workload data.

- If the -detail option is specified, a detailed report categorized by object label displays.
- If the -detail option is not specified, the command returns the protected data size in TB.

-query

Displays information about the number of available licenses.

-create_userrestrictions_tmpl

Creates the user_restrictions_tmpl file which is a template for the user_restrictions file, populated by names of all systems of the Data Protector cell and names of all configured user groups other than *admin* and *operator*.

To put the template into use, change its contents as desired, and rename it to user_restrictions .

-gre_license_info

Reports Granular Recovery licensing related information from the cell. The following information is returned: the database

server name, the application type, the time when the license was used for restore, the time when the license will be released for the next restore from another database server, and the number of days remaining until the license release.

-impersonation -add_user -user { *User@Domain* | *Domain|User* } { -host *ClientName* [-host *ClientName...*] | -all }{ -passwd *Password* | -passwdfile *FileName* }

Sets up a user account for the Data Protector Inet service user impersonation on one or more specified clients, by specifying the user name and the password directly or by saving the user name and the password into the specified file.

To enable user impersonation on all clients in the cell, specify the -all option.

-impersonation -modify_user -user { *User@Domain* | *Domain|User* } { -host *ClientName* [-host *ClientName...*] | -all } { -passwd *Password* | -passwdfile *FileName* } { -old_passwd *OldPassword* | -old_passwdfile *OldFileName* }

Modifies a user account for the Data Protector Inet service user impersonation on one or more specified clients, by specifying the user name and the new password directly or by saving the user name and the new password into the specified file and by specifying the user's old password directly or in the specified file.

To modify user impersonation on all clients in the cell, specify the -all option.

-impersonation -delete_user -user { *User@Domain* | *Domain|User* } { -host *ClientName* [-host *ClientName...*] | -all } { -passwd *Password* | -passwdfile *FileName* }

Deletes a user account for the Data Protector Inet service user impersonation on one or more specified clients.

To remove user impersonation from all clients in the cell, specify the -all option.

-encr_param { *Hostname1* [*HostName2* ...] | -all } [-tls_min TLSvMin] [-tls_max TLSvMax]

This option specifies the minimum and/or maximum versions of TLS for host.

The values for TLSvMin and TLSvMax can be specified as:

TLSv1 , TLSv1.1 , TLSv1.2 , (or) 1 , 1.1 , 1.2

-import_esx *ClientName*

This is a VMware specific option.

Specifies the VMware ESX(i) client to import.

-import_vcenter *ClientName*

This is a VMware specific option.

Specifies the VMware vCenter client to import.

-import_hyperv *ClientName*

This is a Hyper-V specific option.

Specifies the Hyper-V client to import.

-import_cs *HostName*

-export_cs *HostName*

Imports or exports the remote Cell Manager.

-import_h3ccas *HostName*

This is a H3C CAS specific option.

Specifies the H3C CAS management server to import.

-migrate_devfilter [HostName] [-delete_old_devfilter]

This option is used to migrate existing OMNIRC based device filter tags from Data Protector clients to a centralized Cell Manager file in the Cell Manager.

- Linux: /etc/opt/omni/server/cell/hosttags
- Windows: <Data_Protector_home>\Config\server\cell\hosttags

If the HostName option is specified, the device filter tag from the hostname is printed to the console in the following format:

<HostName> <tag>

If the -delete_old_devfilter option is specified, the OMNIRC variable OB2DEVICEFILTER and its value are removed from the host(s).

If the hosttags file is already present and you run this option, the hosttags_tmp file is created in the same location as that of the hosttags file. You need to manually merge the hosttags_tmp file with the hosttags file.

-port *Port*

This is a VMware specific option.

Specifies the port to connect to (for example, 443).

-user *UserName*

Specifies an operating system user account for the connection.

-passwd *Password*

Specifies the user's password.

-web_root *WebRoot*

This is a VMware specific option.

Specifies the web service entry point URI (for example, /sdk).

-integrated_sec { 0 | 1 }

This is a VMware specific option.

Specifies the security mode.

If the 0 option is specified, you have to specify all login credentials manually (standard security).

If the 1 option is specified, Data Protector connects to the VMware vCenter Server system with the user account under which the Data Protector Inet service on the backup host is running (integrated security). Ensure this user account has appropriate rights to connect to the VMware vCenter Server system.

-register_greplugin { 0 | 1 }

This is a VMware specific option.

It registers the Advanced GRE Web Plug-in into the vCenter client.

If the 0 option is specified, Data Protector does not register the plug-in.

If the 1 option is specified, Data Protector registers the plug-in into the vCenter.

-remove_peer

This option is used to remove the trust configuration of the remote host so that the remote host is denied from communication.

-configure_peer

This option is used to add the trust configuration of a remote host so that the remote host can securely communicate.

-configure_peer_with_cert

This option is used to add the trust configuration of a remote host if the current certificate of the remote host is already available.

-configure_for_dr

For online disaster recovery, this option is used on the Cell Manager to allow Cell Manager host to communicate with the disaster recovery agent. For Offline disaster recovery, this option is used on the Media Agent host to allow Media Agent host to communicate with the disaster recovery agent.

-configure_for_cm

This option is used on Cell Manager host to allow the Data Protector GUI client older than DP 10.00 to communicate with the Cell Manager.

-configure_for_is

This option is used on the Cell Manager host to allow the Data Protector Installation Server older than DP 10.00 to communicate with the Cell Manager.

-configure_for_gui

This option is used on the Data Protector GUI client to allow the GUI to communicate with the Cell Manager which is older than DP 10.00.

-configure_for_legacy_client

This option is used on the Cell Manager host to allow the Cell Manager to communicate with the DP clients which are older than DP 10.00.

-regenerate_cert

This option is used to regenerate certificate.

-reconfigure_peer [client_host_name]

This option is used when the client certificate is regenerated. This option is used to redistribute and reconfigure client certificate on the Cell Manager.

-reconfigure_peer_all [input_file_path]

This option is used when the Cell Manager certificate is regenerated. This option is used to redistribute and reconfigure client certificate run on the Cell Manager. The parameter input_file_path is optional. This file should have the credentials for all the clients that are part of the cell.

-renew_cert [number_of_days]

This option is used to extend certificate validity. If number_of_days option is not specified, certificate will be extended for 3650 days by default. Extension of validity takes effect from the day the command is executed.

-firewall {-host Hostname1 [HostName2 ...] | -all} -enable_dp

This option is used to enable Data Protector firewall in the cell. When enabled, all Data Protector processes listen to the loopback interfaces only, therefore only local peers can connect. The exceptions are: OmniInet, Application Server port and Internal database.

-firewall {-host Hostname1 [HostName2 ...] | -all} -disable_dp

This option is used to disable Data Protector firewall in the cell.

-firewall {-host Hostname1 [HostName2 ...] | -all} -enable_os

This option enables all the Data Protector rules in Windows firewall. The exceptions are: OmniInet, Application Server port and Internal database.

-firewall {-host Hostname1 [HostName2 ...] | -all} -disable_os

This option disables all the Data Protector rules in Windows firewall.

-update_port

This option is used to update port number in the Installation server and all the clients that are part of the cell. If an

Installation Server is part of multiple Cell Managers, then the port number has to be updated in all the Cell Managers. The Cell Manager in which port number is not updated will not be able to communicate with the Installation Server. If any of the clients in the cell are in pre-10.01 version, then the port number cannot be updated. If you update the port on a Cell Manager, restart the Data Protector services using the command `omnisv -restart`.

new_port

INET listening port will be changed to new_port value in all clients and Installation Servers. Default value: 5565

-old_port

This option is used specify the old port on which the INET is listening.

old_port

This option is used specify the old port on which the INET is listening.

- If the `-old_port` option is specified, then the `new_port` value has to be specified.
- If the `-old_port` option is not specified, then the `new_port` is optional and default value 5565 will be used.

variableName

This option is used to specify the variable name to be added in `omnirc` file.

value

This option is used to specify the variable value.

inputFile

This is a optional input file containing client hosts. The hosts mentioned in input file should be part of the cell. If the input file is not provided, variable will be updated in all clients which are part of the cell.

-get_fingerprint

This option is used to get the fingerprint of local host.

-update_local_port

This option is used to change the Inet listening port number in local system. Inet port can be changed even when client is not part of the Cell Manager.

InetPort

Current Inet listening port is changed to `InetPort` value in the local system only.
If you update the Inet port on a Cell Manager, restart the Data Protector services using the command `omnisv -restart`.

-add_socket -virtualhost <hostname> [-hypervisor <hypervisor>]

This option is applicable only if the Data Protector Express license is used. It is used to license hypervisor(s) of the virtual client. If the hypervisor field is not specified, then all the hypervisors of that particular virtual client (vCenter, ESX, HyperV Cluster, HyperV node) are licensed. The `-hypervisor` option is not supported with H3C CAS virtualization.

-reclaim_socket –uuid <uuid>

This option is applicable only if the Data Protector Express license is used. It is used to reclaim the socket associated with the hypervisor uuid. This hypervisor uuid can be obtained using the `-socket_info` command option.

omnicc -secure_data_comm <*Value*>

This option enables secure data communication. The <*Value*> is either 0 or 1. Default is 1. The "Client configuration" and "Security admin" user rights have to be enabled to use this option.

- <*Value*> of 0 disables secure data communication and sets the global variable "EnableSecureDataCommunication" to 0.
- <*Value*> of 1 enables secure data communication and sets the global variable "EnableSecureDataCommunication" to 1.

omnicc -auditlog <*Value*> [-retention_months <*retentionValue*>]

This option enables audit log. The <*Value*> is either 0 or 1. Default is 1. The "Client configuration" and "Security admin" user rights have to be enabled to use this option.

You can also specify how long (number of months) audit log files are kept before being purged. Audit logs are purged on a monthly basis, meaning that the session information for an entire month is removed after the specified number of months. By default, the audit log is retained for 7.5 years (90 months). If the value is set to 0, audit log purging is

disabled. If the -retention_months option is not used, then a default value of 90 months is set.

- <*Value*> of 0 disables audit log and sets the global variable "AuditLogEnable" to 0.
- <*Value*> of 1 enables audit log and sets the global variable "AuditLogEnable" to 1.
- <*retentionValue*> specifies how long (number of months) audit log files are kept before being purged. Audit logs are purged on a monthly basis, meaning that the session information for an entire month is removed after the specified number of months. By default, the audit log is retained for 90 months. If the value is set to 0, audit log purging is disabled. There is no limit to specify maximum value for audit log retention, however, Micro Focus recommends to limit the value to 99 years (1188 months). The <*retentionValue*> sets the global variable "AuditLogRetention" to the number of months specified.

omnicc -chgblkdrvr_install [-force]

This option enables you to install the Changed block driver required for performing incremental block-based backup.

- [-force] executes the install command to forcibly install the driver without prompting you for additional inputs.

> **Important:** For the driver installation to complete, you must reboot the system after installing the driver.

omnicc -chgblkdrvr_uninstall

This option enables you to uninstall the Changed block driver from the system where you run the command.

> **Important:** For the driver uninstallation to complete, you must reboot the system after uninstalling the driver.

omnicc -chgblkdrvr_status

This option enables you to verify if the Changed block driver is installed on the system.

> **Important:** If you do not reboot the system after installing the driver, then the driver installation does not complete and the status command displays the message that the driver is installed on the system, but the system has not been rebooted. For the driver installation to complete, you must reboot the system.

omnicc -chgblkdrvr_remove_config <devName>

This option enables you to remove the Changed block driver configuration for Linux x86_64 devices and requires that you specify the name of the device.

omnicc -import_dp4cw HostName -port Port -user UserName -passwd Password

This option enables you to import a Data Protector for Cloud Workload server into a Data Protector Cell Manager.

omnicc -export_dp4cw HostName

This option enables you to export a Data Protector for Cloud Workload server from a Data Protector Cell Manager.

NOTES

If you change your licensing model from the traditional to the capacity based, the information about previously distributed traditional licenses will be overwritten.

EXAMPLES

The output for the omnicc -query, omnicc -check_license, omnicc -check_license -detail, and omnicc -password_info commands is displayed incorrectly due to the emergency license that is active even after applying a new license. To display the output correctly, remove the emergency license key and its annotation from the **lic.dat** file in the \programdata\config\server\cell\ (Windows) or /etc/opt/omni/server/cell/ (Linux) path.

The following examples illustrate how the omnicc command works.

1. To check if the licensing is covered within a Data Protector cell, execute:

   omnicc -check_license

   Sample output for omnicc -check_license when Product Edition is **Trial**:

   WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:34:43 PM Product Edition : Trial Licensing Mode : Local License Server : myserver License Type : Term Duration Left : 89 Days Summary ------- Licensing is covered. Total Protected Data : 0.00 TB

Sample output for `omnicc -check_license` when Product Edition is **Premium (Term based)**:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:00:55 PM Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Term Duration Left : 57 Days Summary ------- Licensing is covered. Total Protected Data : 0.00 TB
```

Sample output for `omnicc -check_license` when Product Edition is **Premium (Permanent)**:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:03:12 PM Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Permanent Total Capacity : 999 TB Summary ------- Licensing is covered. Total Protected Data : 0.00 TB
```

Sample output for `omnicc -check_license` when Product Edition is **Traditional**:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:34:43 PM Product Edition : Traditional Licensing Mode : Local License Server : myserver License Type : Traditional Summary ------- Description Licenses Needed Encryption Extension for one client system 1 Licensing is NOT covered. Total Protected Data : 0.00 TB
```

Sample output for `omnicc -check_license` when product edition is **Capacity**:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:00:55 PM Product Edition : Capacity Licensing Mode : Local License Server : myserver License Type : Term Duration Left : 57 Days Summary ------- Licensing is covered. Total Protected Data : 0.00 TB
```

Sample output for `omnicc -check_license` when product edition is **Capacity (Permanent)**:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 3:03:12 PM Product Edition : Capacity Licensing Mode : Local License Server : myserver License Type : Permanent TotalCapacity : 999 TB Summary ------- Licensing is covered. Total Protected Data : 0.00 TB
```

2. To get information about the Product Edition details, execute:

   `omnicc -check_license -detail`. Sample output:

```
WARNING: Calculation of total protected data size may take some time. Report Generated : 7/5/2018 4:11:44 PM Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Permanent Total Capacity : 999 TB ---------- License Category : Micro Focus Data Protector - capacity based per TB SW Licenses Capacity Installed : 999 TB Licenses Capacity In Use : 0 TB Add. Licenses Capacity Required : 0 TB Summary ------- Licensing is covered. Total Protected Data : 0.00 TB ---------- Backup Type | Total Protected Data | ---------- MS Filesystem | 2 GB ----------
```

   Sample output for `omnicc -check_license -detail` when product edition is **Capacity (Permanent)**:
   This command does not show encryption license details.

```
WARNING: Calculation of total protected data size may take some time. ReportGenerated : 7/5/2018 4:11:44 PM ProductEdition : Capacity LicensingMode : Local LicenseServer : myserver LicenseType : Permanent TotalCapacity : 999 TB ---------- LicenseCategory : Micro Focus Data Protector - capacity based per TB SW LicensesCapacityInstalled : 999 TB Licenses Capacity In Use : 0 TB Add. Licenses Capacity Required : 0 TB Summary ------- Licensing is covered. Total Protected Data : 0.00 TB ---------- Backup Type | Total Protected Data | ---------- MS Filesystem | 2 GB ----------
```

   Sample output for `omnicc -check_license -detail` when the product edition is **Premium (Term)** :

```
WARNING: Calculation of total protected data size may take some time. ReportGenerated : 7/5/2018 4:11:44 PM Product Edition : Premium LicensingMode : Local LicenseServer : myserver License Type : Term Duration Left : 57 Days ---------- LicenseCategory : Micro Focus Data Protector Premium - per TB LicensesCapacityInstalled : 999 TB Licenses Capacity In Use : 0 TB Add. Licenses Capacity Required : 0 TB Summary ------- Licensing is covered. Total Protected Data : 0.00 TB ---------- Backup Type | Total Protected Data | ---------- MS Filesystem | 2 GB ----------
```

3. To get information about the number of licenses available, execute:

   `omnicc -query`

   Sample output for `omnicc -query` when Product Edition is **Premium (Term based)**:

```
Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Term Duration Left : 57 Days Category Number of Licenses Micro Focus Data Protector - capacity based per TB SW 1
```

   Sample output for `omnicc -query` when Product Edition is **Premium (Permanent)**:

```
Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Permanent Total Capacity : 999 TB Category Number of Licenses Micro Focus Data Protector - capacity based per TB SW 999
```

Sample output for `omnicc -query` when Product Edition is **Traditional**:

```
Product Edition : Traditional Licensing Mode : Local License Server : myserver License Type : Traditional Category Number of Licenses Cell Manager for Linux 0 Cell Manager for Windows 1 Single Drive for UNIX / NAS / SAN 0 Single Drive for Windows / Linux 0 Multi-Drive Server for UNIX 0 ... ...
```

Sample output for `omnicc -query` when product edition is **Premium (Term based)** :

```
Product Edition : Premium Licensing Mode : Local License Server : myserver License Type : Term DurationLeft : 57 Days Category Number of Licenses Micro Focus Data Protector Premium - per TB 1
```

Sample output for `omnicc -query` when the product edition is **Capacity (Permanent)**

```
Product Edition : Capacity Licensing Mode : Local License Server : myserver License Type : Permanent TotalCapacity : 999 TB Category Number of Licenses Micro Focus Data Protector - capacity based per TB SW 999
```

Sample output for `omnicc -query` for when product edition is **Capacity (Term)**

```
Product Edition : Capacity Licensing Mode : Local License Server : myserver License Type : Term DurationLeft : 57 Days Category Number of Licenses Micro Focus Data Protector - capacity based per TB SW 20
```

4. To get information about the objects that are used to calculate the amount of data under protection in TB, execute:

   ```
   omnicc -cbl_detail
   ```

5. To get information about used GRE licenses, execute:

   ```
   omnicc -gre_license_info
   ```

6. To configure a Microsoft SharePoint 2010 farm administrator which will be used for backup or restore on a medium farm (two web front ends, one application and one sql server), execute:

   ```
   omnicc -impersonation -add_user web1.domain.com web2.domain.com indexapp.domain.com sql.domain.com -user MyDomain\MyUser -passwd MyPassword
   ```

7. To import an " X9000" NDMP server into a cell, execute:

   ```
   omnicc -import_ndmp lxdprnd5.ind.hp.com -type "HP X9000" -port 10000 -user root -passwd MyPassword
   ```

8. To check the value of the `DailyMaintenanceTime` option in the output of a debug text file named "CHECK", execute:

   ```
   omnicc -debug 20 CHECK.txt
   ```

9. (Data Protector Express only) To check the number of sockets used by the licensed hypervisor clients, execute:

   ```
   omnicc -socket_info
   ```

10. To check the number of on-line licenses, execute:
    ```
    omnicc -check_license -detail  -online
    ```

    Sample output:

    ```
    Report Generated : 10/31/2019 10:20:02 AM Product Edition : Traditional Licensing Mode : Local License Server : exampleserver.net License Type : Traditional ---------- License Category : On-line Extension for ONE UNIX system Licenses Installed : 0 Licenses Used : 0 Additional Licenses Required : 0 ---------- License Category : On-line Extension for ONE Windows / Linux system Licenses Installed : 4 Licenses Used : 5 Additional Licenses Required : 1 Details of Licenses Used : exampleserver1.net exampleserver2.net [Hypervisor] exampleserver3.net [Hypervisor] exampleserver4.net [Hypervisor] exampleserver5.net [Hypervisor] ---------- License Category : Direct Backup using NDMP for 1 TB Licenses Capacity Installed : 0 TB Licenses Capacity In Use : 0 TB Add. Licenses Capacity Required : 0 TB ----------
    ```

11. To check the total protected data for full backup beyond 90 days, execute:

    ```
    omnicc -check_license -detail -exact
    ```

    Sample output:

    ```
    omnicc -check_license  -detail -exact''' NOTE: Calculation of total protected data done as part of daily maintenance.  Report Generated           : 1/26/2020 8:12:31 PM Product Edition           : Capacity Licensing Mode            : Local License Server            : mytestserver.net License Type              : Permanent Total Capacity            : 999 TB  License Category             : Micro Focus Data Protector - capacity based per TB SW Licenses Capacity Installed    : 999 TB Licenses Capacity In Use       : 0 TB Add. Licenses Capacity Required : 0 TB  Summary Licensing is covered.  Total Protected Data    : 0.00 TB  Backup Type             |  Total Protected Data  | MS Filesystem           | 1.08 GB
    ```

12. To check the protected Data Protector for Cloud Workload data, execute:

    ```
    omnicc -dp4cw_data -detail
    ```

    Sample output:

    ```
    ---------- dp4cw Label | Protected Data | ---------- / | 0.00 GB ABCDEFGHIJKLMNOPQRSTUVWXYZ | 0.00 GB ABCDEFGHIJKLMNOPQRSTUVWXYZ123 | 0.00 GB CEPH | 4045432098816.00 GB mysql |
    ```

```
4096.00 GB OPENSHIFT | 5054464.33 GB ---------- dp4cw : 3950622224.00 TB
```

13. To import a Data Protector for Cloud Workload server into a Cell Manager, execute:

    ```
    omnicc -import_dp4cw dp4cw_host -port 8080 -user xyz -passwd xyz
    ```

14. To import a Data Protector for Cloud Workload server from a Cell Manager, execute:

    ```
    omnicc -export_dp4cw dp4cw_host
    ```

SEE ALSO

omnicellinfo(1), omnicheck(1M), omnidlc(1M), omnisv(1M)

omnicellinfo

omnicellinfo - displays configuration information about the Data Protector cell
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnicellinfo -version | -help

omnicellinfo -servers

omnicellinfo -group

omnicellinfo -object [schedule | no_schedule] [-group *Group*]

omnicellinfo -db

omnicellinfo -prepostinfocheck

omnicellinfo { -mm | -dev } [-detail]

omnicellinfo { -dlinfo [-group *Group*]} | -cell [brief] { -schinfo [*Backup_Specification* | -days *NumberDays* | -group *Group*]} | { -dlobj [-group *Group*]} | { -trees [-group *Group*]} | -allbdf | -acl

DESCRIPTION

The omnicellinfo command displays information about data objects, media pools, devices, clients, database, backup specifications and backup specification groups in the cell. It can be also used to display the cell managers in multicell environments.

Some options recognized by omnicellinfo are intended primarily for generating reports by shell/awk/perl scripts. Information produced is formatted in records with a newline as field separator and a blank line as record separator. Those options are: -dlinfo, -schinfo, -dlobj, -trees and -allbdf.

OPTIONS

-version

Displays the version of the omnicellinfo command.

-help

Displays the usage synopsis for the omnicellinfo command.

-servers

Displays the list of cell managers that are included in the multicell environment.

-group

Displays the backup specification groups that contain backup specifications. Note that the backup specification group named Default is not displayed.

-object [schedule | no_schedule]

Displays information about objects (filesystems, databases and disk images) in the cell. The report shows: Object (object type, client name, and mountpoint), Label, and Next Scheduled Backup Date. When you use the schedule option, the report only shows those objects which are scheduled for backup. When you use the -no_schedule option, the report only shows those objects which are not scheduled for backup. By default, all objects (scheduled and unscheduled) are listed.

-mm

Displays information about the media and media pools in the cell. The report shows for each pool: the Pool Name, Media Class, Media Usage Policy, Media Allocation Policy, and Amount of Free Space in the pool.

-dev

Displays information about the backup devices in the cell. The report shows for each device: the Device Name, Client Name, Device Type and Media Pool.

-db

Displays information about the Data Protector Internal Database (IDB). The database is divided in logical structures, for each of these structures the report shows: Disk Space Used, Records Used and Records Total.

-prepostinfocheck

Searches all worklists configured in the Data Protector cell and checks for security compliance of the commands executed during the session. The rules are defined in the "Pre and Post-Exec Commands for a Backup Specification" in *Data Protector Help* and enforced by Inet. You can execute this option after the patch installation to quickly figure out the Group or Name or command that is not proper.

Note PrePostInfoCheck validation includes file system path checking for defined pre and post scripts in data/bar lists. This is platform specific and it is recommended to execute checks on both Windows and Linux clients to check for errors that are reported for that platform.

-cell

Displays information about the configured clients in the cell. The report shows for each client: client name, operating system, cell console version, Disk Agent version, Media Agent version, GUI version, and all installed Data Protector integration versions. There is also a short summary which shows the total number of clients and, if the brief option was not specified, all possible Data Protector software components, together with the total number of every software component in the cell. If the brief option was specified, only the installed Data Protector software components together with the total number of every software component in the cell is listed.

The VADP feature introduced in Data Protector 8.14 provides enhanced reports for VMs. The VMware virtual machines are represented as Data Protector clients called VADP clients. The VADP clients display the information on the Guest OS of the virtual machine. If the VM tools are installed and running, and VM is powered on, the Host information section of the output displays information, such as the operating system, IP address, or hostname. If not, only the VM name is displayed.

-detail

The -detail option can be used in combination with the -dev and -mm options to produce a more detailed report.

-dlinfo

Shows information about backup specifications. For each backup specifications it lists the name of the backup specification, session owner, pre-exec and post-exec script. Session owner is in format *USER.GROUP@CLIENT*.

-schinfo [*Backup_Specification* | -days *NumberDays*]

Shows information about backup specification scheduling. If *Backup_Specification* and -days option are not specified, the command displays the next schedule time for each backup specification. If backup specification is specified the command lists all schedules in the next year for the specified backup specification. Option -days can be used to display schedules of all backup specifications for a specified number of days.

-dlobj

Shows information about all objects in backup specifications. For each object it lists object type, object name (in format *ClientName:PathName*), description, and the name of the backup specification. After this, the device and poolname fields are listed for each device used in the backup specification making the size of the records variable.

-trees

Shows information about all defined trees in backup specifications. For each tree, it lists filesystem name (in format *Client Name:Pathname*), tree, description, backup device, media pool and name of the backup specification.

-acl

Displays all Data Protector access permissions that the user running the command has.

-group *Group*

This option allows you to limit the output of the command to single backup specification group. The following options support this: -dlinfo, -schinfo, -dlobj, -trees and -object.

EXAMPLES

The following examples illustrate how the omnicellinfo command works.

1. To list detailed information about the selected objects, execute:

   omnicellinfo -object schedule

2. To list detailed information about the configured devices, execute:

   omnicellinfo -dev -detail

3. To display all virtual machines configured on ESXi servers or vCenters and imported to the Data Protector Cell Manager, execute:

   omnicellinfo –cell brief

SEE ALSO

omnicc(1), omnicheck(1M), omnidlc(1M), omnisv(1M)

omniclus

omniclus - manages load balancing in a cluster environment in the event of an application (Data Protector or other) failover (this command is available on systems with the Data Protector MS Cluster Support component installed (Windows systems) and on the Data Protector Cell Manager (UNIX systems))

SYNOPSIS

omniclus -version | -help

omniclus -clus *cluster_name* -session { * | *backup_specification* } -abortsess [-abortid { == | != } *application_id*]

omniclus -clus *cluster_name* -inhibit { * | 0 | *minutes* }

omniclus -clus *cluster_name* -session { * | *backup_specification* } -symlink { split | active }

NOTE: On UNIX systems, replace the wildcard (*) with the string '*' .

NOTE: On Windows systems, the -noclus option can be specified directly after -clus to prevent loading of the cluster dynamic library.

DESCRIPTION

The omniclus command, which is common to all platforms (Windows and UNIX systems), allows you to communicate the Data Protector Cell Manager special events that in certain way control its behavior and behavior of the backup sessions in a cluster environment. omniclus allows load balancing by offering additional (CLI) control of the Cell Manager in cluster environments:

- Aborting sessions
- Temporarily disabling the Cell Manager for backup sessions

Note that the system specified as the *cluster_name* argument of the -clus option must be a cluster-aware Data Protector Cell Manager.

OPTIONS

-version

Displays the version of the omniclus command
-help

Displays the usage synopsis for the omniclus command.
-clus *cluster_name*

Specifies the cluster-aware Cell Manager.
-session { * | *backup_specification* }

Specifies the session(s) to which the abort message should be sent.
-abortsess

Specifies the abort session command.
-abortid { == | != } *application_id*

Specifies the application identification.
-inhibit { * | 0 | *minutes* }

Specifies the number of minutes for Cell Manager backup inactivity, where * means forever and 0 means activate now.

NOTES

The omniclus command can only be used in cluster environments.

EXAMPLES

The following examples illustrate how the omniclus command works.

1. To abort all running sessions, execute:

   ```
   omniclus -clus cluster.domain.com -session * -abortsess
   ```

   NOTE: On UNIX systems, replace the wildcard (*) with the string '*'.

   The utility will connect to all running sessions and will send them abort messages. The state of the sessions can be then checked with the Data Protector omnistat utility.

2. To abort specific running sessions, execute:

   ```
   omniclus -clus cluster.domain.com -session mybackup -abortsess
   ```

   The utility will connect to backup session managers issuing abort messages and sending them additional information - the backup specification name. Each backup session manager checks whether the command addresses it and if this is the case it aborts.

3. To abort sessions (all or specific) with application identifications, execute:

   ```
   omniclus -clus obvs.domain.com -session * -abortsess -abortid != 10
   ```

   NOTE: On UNIX systems, replace the wildcard (*) with the string '*'.

   This way the user can define groups of sessions and abort only the ones that are actually related to the application that failed over. For example a backup session that performs a normal filesystem backup of a remote client is not aborted because an application server switches, while the application server backup can be aborted.

4. Temporarily disabling the Data Protector cell

   The following command will inhibit backup sessions for twenty minutes:

   ```
   omniclus -clus cluster.domain.com -inhibit 20
   ```

   The following command will inhibit backup sessions forever:

   ```
   omniclus -clus cluster.domain.com -inhibit *
   ```

   NOTE: On UNIX systems, replace the wildcard (*) with the string '*'.

   The following command will re-activate backup sessions immediately:

   ```
   omniclus -clus cluster.domain.com -inhibit 0
   ```

omnicreatedl

omnicreatedl - creates a filesystem backup specification file (datalist); or an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB backup specification file (datalist)
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnicreatedl -version | -help

FILESYSTEM BACKUP

omnicreatedl [-datalist *Name*] [-host *HostName1* [*HostName2* ...]] [-device *BackupDevice*]

MICROSOFT EXCHANGE SERVER 2003 ZERO DOWNTIME BACKUP

omnicreatedl -ex2000 -datalist *Name* [-device *Name*] { *P9000_DISK_ARRAY_XP_OPTIONS* | *P6000_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS* } *EXCHANGE_OPTIONS* [-force] [-virtualSrv *Name*]

P9000_DISK_ARRAY_XP_OPTIONS

1. ZDB-to-disk and ZDB-to-disk+tape sessions (Business Copy P9000 XP configurations):

-split_mirror -sse -local *app_sys bck_sys* [-mirrors *MU_numbers*] -instant_restore [-leave_enabled_bs] [-split | -establish]

2. ZDB-to-tape sessions (Business Copy P9000 XP configurations):

-split_mirror -sse -local *app_sys bck_sys* [-mirrors *MU_numbers*] [-keep_version [-leave_enabled_bs]] [-split | -establish]

3. ZDB-to-tape sessions (Continuous Access P9000 XP or combined (CA+BC P9000 XP) configurations):

-split_mirror -sse { -remote *app_sys bck_sys* | -combined *app_sys bck_sys* } [-keep_version [-leave_enabled_bs]] [-split | -establish]

P6000_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS

1. ZDB-to-disk sessions:

-snapshot -smis *app_sys bck_sys* -instant_recovery [-snapshots *number*]

2. ZDB-to-disk+tape sessions:

-snapshot -smis *app_sys bck_sys* -instant_recovery [-snapshots *number*] [-wait_clonecopy *number*]

3. ZDB-to-tape sessions:

-snapshot -smis *app_sys bck_sys* -snapshot_type { standard | vsnap | clone [-wait_clonecopy *number*]} -snapshot_policy { strict | loose } -replica_conf { local | combined [-ca_failover_option { follow_replica_direction | maintain_replica_location }]}

EXCHANGE_OPTIONS

-annotation { MIS | SRS | KMS }

{ -all_storage_groups | -storage_group *Storage_Group_Name1* [-store *Store1* [*Store2* ...]] [-storage_group *Storage_Group_Name2* [-store *Store1* [*Store2* ...]]...]}

DESCRIPTION

FILESYSTEM BACKUP

The omnicreatedl command creates a filesystem backup specification file (datalist). It searches all specified clients for local

mount points and puts them in the backup specification or on the stdout if no backup specification name is specified. If no client is specified, all clients in the Data Protector cell are searched.

MICROSOFT EXCHANGE SERVER 2003 ZERO DOWNTIME BACKUP

The omnicreatedl command is also used to create an Exchange Server ZDB backup specification file for disk arrays of theP9000 XP Disk Array Family:

When creating an Exchange ZDB backup specification file, if the circular logging is disabled for any storage group, an Exchange ZDB transaction logs backup specification file for each such storage group specified in the Exchange ZDB backup specification file is additionally created.

An Exchange ZDB backup specification file includes the stop/quiesce the application and restart the application scripts (omniEx 2000.exe) sections for dismounting/mounting backed up stores and checking their consistency. A backup specification can be edited later using the Data Protector GUI to modify backup devices, ZDB options, schedule, and so on.

For a Microsoft Exchange Server 2003 ZDB, the *final* decision on whether the created backup specification will start a ZDB-to-disk, ZDB-to-disk+tape or ZDB-to-tape session depends on the Data Protector omnib command options selection.

OPTIONS

-version

Displays the version of the omnicreatedl command.

-help

Displays the usage synopsis for the omnicreatedl command.

FILESYSTEM BACKUP

-datalist *Name*

Specifies the name of the backup specification file (datalist) for filesystem backup. The backup specification file is created on the Cell Manager in the default server configuration directory under datalists . If this option is not specified, backup specification objects are written to stdout .

-host *HostName1 [HostName2]*

List of all clients whose filesystems will be included in the backup specification. If this option is not specified, all clients from the cell are used.

-device *BackupDevice*

Specifies the backup device to be used for backup. If this option is not used, the backup device must be specified using the Data Protector GUI.

MICROSOFT EXCHANGE SERVER 2003 ZERO DOWNTIME BACKUP

-ex2000

Instructs the omnicreatedl command to create a Microsoft Exchange Server 2003 ZDB backup specification file and, if circular logging is disabled for any storage group specified, a Microsoft Exchange Server 2003 ZDB transaction logs backup specification file(s) for every such storage group.

-datalist *Name*

Specifies the name of the Microsoft Exchange Server 2003 ZDB backup specification file for the Microsoft Exchange Server 2003 ZDB. The file is created on the Cell Manager in the default server configuration directory under datalists .

The corresponding datalist for Microsoft Exchange Server 2003 logs for every storage group specified that has the circular logging disabled are also created in the same directory with the file name Storage_Group_Name (LOGS) app_sys .

If any of the thus created backup specification files (datalists) has a name that already exists, the omnicreatedl command issues a warning and, depending on whether the -force option is set or not, overwrites the existing backup specification files with the same name or aborts the action.

-force

Forces overwriting of an existing backup specification file with the same name.

-virtualSrv *Name*

The name of the Microsoft Exchange Server 2003 virtual server. This option is obligatory and used only in cluster configurations.

P9000_DISK_ARRAY_XP_OPTIONS

-split_mirror -sse

Instructs the omnicreatedl command to create an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB backup specification.

-local *app_sys bck_sys*

Specifies the Business Copy (BC) P9000 XP configuration, with the application system *app_sys* and the backup system *bck_sys*.

-remote *app_sys bck_sys*

Selects the Continuous Access (CA) P9000 XP configuration, with the application system *app_sys* and the backup system *bck_sys*.

-combined *app_sys bck_sys*

Selects the Combined (Continuous Access + Business Copy (CA+BC) P9000 XP) configuration, with the application system *app_sys* and the backup system *bck_sys*.

-mirrors *MU_numbers*

This option is only considered when the Business Copy (BC) P9000 XP configuration is chosen.

Specify the mirror unit (MU) number(s) of a replica or a replica set from which the Data ProtectorP9000 XP Agent, according to the replica set rotation, selects the replica to be used in the zero downtime backup session. The replica selection rule is described in the Data Protector Concepts Guide. The maximum number of replicas that can be created for the same source volumes is different for mirror copies and snapshots. Both limitations are imposed by the P9000 XP Disk Array Family storage system.

You can specify one or more non-negative integer numbers, one or more ascending ranges of such numbers, or any combination of both. Use a comma as the separator character. Examples:

5

7-9

4,0,2-3

When a sequence is specified, it does not define the order in which the replicas are used. If this option is not specified, the MU number 0 is used.

-instant_restore

When specified, this option enables ZDB to disk or ZDB to disk+tape. Consequently, instant recovery can be run using the created replica in the ZDB session. If the option is not specified, it is only possible to perform a ZDB to tape. However, this option does not influence the replica set rotation.

If this option is specified, the omnicreatedl command automatically sets the -keep_version option.

-keep_version

If configuring a ZDB to tape, specify this option to keep the replica on the disk array after the zero downtime backup session. The replica becomes part of a replica set (specify a value for the option -mirrors). Unless the additional option -instant_restore is specified, the replica is not available for instant recovery.

If this option is not specified, the replica is removed at the end of the session. In this case, it is also not possible to specify the -leave_enabled_bs option.

-leave_enabled_bs

To specify this option, the -keep_version option has to be specified.

By default, Data Protector dismounts the filesystems on the backup system after each ZDB session.

If this option is specified, the filesystems remain mounted after the backup. Thus, you can use the backup system for some data warehouse activity afterwards, but not for instant recovery.

-split

If this option is specified, the volumes of the replica selected for the current ZDB session are prepared for the zero downtime backup at the start of the current ZDB session: mirrors are resynchronized with the P-VOLs, and volumes to be used for snapshot storage are made empty.

If neither the -split option nor the -establish option is specified, Data Protector acts as if the -establish option was specified.

-establish

If this option is specified, if the volumes of the replica to be used in the next ZDB session are not ready for ZDB, they are prepared for ZDB at the end of the current ZDB session.

If neither the -split option nor the -establish option is specified, Data Protector acts as if the -establish option was specified.

EXCHANGE_OPTIONS

-annotation { MIS | SRS | KMS }

This option specifies the possible Microsoft Exchange Server 2003 annotations: Microsoft Information Store (MIS), Site Replication Service (SRS), and Key Management Service (KMS). MIS is the default setting and does not need to be specified in case when the MIS will be backed up.

-all_storage_groups

This option creates a backup specification for all databases relating to Microsoft Exchange Server 2003 Microsoft Information Store. It must be specified by the -annotation MIS parameter.

-storage_group *storage group name*

This option creates a backup specification for all stores relating to the specified storage group. Multiple declarations of the -storage_group parameter are possible to create a backup specification for the selected storage groups.

Logical storage group names can be obtained by using the Exchange System Administrator tool, which is a part of Microsoft Exchange Server 2003.

-store *Store1* [*Store2* ...]

When the -store parameter is specified, backup specification is created only for specified store(s) inside the storage group. List of stores can be specified after the -store parameter to create a backup specification for many stores.

Store names can be obtained by using Exchange System Administrator tool, which is a part of Microsoft Exchange Server 2003.

EXAMPLES

The following examples show how the omnicreatedl command works:

1. To create an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server 2003 running on client "computer1.company.com" with the backup system "computer2.company.com", to back up all storage groups relating to Microsoft Information Store, execute:

   omnicreatedl -ex2000 -datalist Exchange_example -all_storage_groups -split_mirror -sse -local computer1.company.com computer2.company.com

   The omnicreatedl command creates the P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file named "Exchange_example" and additional P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB transaction logs backup specification files (in case they do not already exist) for each storage group with disabled circular logging option.

2. To create an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server 2003 running on client "computer1.company.com" with the backup system "computer2.company.com", to back up entire First Storage Group and Test Storage Group (both have circular logging disabled), execute:

```
omnicreatedl -ex2000 -datalist Exchange_example -storage_group "First Storage Group" -storage group "Test Storage Group" -split_mirror -sse
-local computer1.company.com computer2.company.com
```

The omnicreatedl command creates the P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file (datalist) named "Exchange_example" and two additional P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB transaction logs backup specification files (if they do not already exist) named: "First Storage Group (LOGS) computer1.company.com" for First Storage Group log files backup and "Test Storage Group (LOGS) computer1.company.com" for Test Storage Group log files backup.

3. To create an P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server 2003 running on "computer1.company.com" with the backup system "computer2.company.com", overwriting the possible already existent backup specification files with the same name to back up First Mailbox Store, Public Folder Store, part of First Storage group and Test Mailbox Store, part of Test Storage Group, execute:

```
omnicreatedl -ex2000 -datalist Exchange_example -storage_group "First Storage Group" -store "First Mailbox Store" "Public Folder Store" -stora
ge group "Test Storage Group" -store "Test Mailbox Store" -split_ mirror -sse -local computer1.company.com computer2.company.com -force
```

The omnicreatedl command creates the P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB-to-tape backup specification file (datalist) "Exchange_example" and two additional P9000 XP Disk Array Family Microsoft Exchange Server 2003 ZDB transaction logs backup specification files if circular logging option is disabled for a particular storage group: "First Storage Group (LOGS) computer1.company.com" for First Storage Group log files backup and "Test Storage Group (LOGS) computer1.company.com" for Test Storage Group log files backup. Any possible already existent backup specification file with the same name is overwritten.

omnidb

omnidb - queries the Data Protector Internal Database (IDB)
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnidb -version | -help

omnidb -session [-datalist Datalist] [-type { restore | backup | verification }] [-user User] [-since Date -until Date | -last Number | -latest | -wo start duration] [-detail]

omnidb -session SessionID
[-report [warning | minor | major | critical] |
-detail |
-encryptioninfo |
-strip |
-purge |
-remove_msgs |
-change_protection Protection |
-change_catprotection Protection |
-media [-detail]]

omnidb { -object | -filesystem | -vprotect | -winfs | -vbfs | -winfsblockbased | -rawdisk | -sap | -sapdb | -saphana | -stream | -oracle8 | -mssql | -msese | -e2010 | -veagent | -mbx | -informix | -sybase | -lotus | -vss | -db2 | -mssps | -mssharepoint | -idb | -m365 | -integ MySQL | -integ PostgreSQL } [-detail | -encryptioninfo]

omnidb Object [[-since Date] [-until Date] | -last NumberOfDays | -latest] [-noexpand] [-detail | -encryptioninfo]

omnidb Object [[-since Date] [-until Date] | -last NumberOfDays] [-change_protection Protection | -change_catprotection Protection] [-noexpand]

omnidb Object [-noexpand] -strip NumberOfDays

omnidb -strip

omnidb -change_protection Protection

omnidb -change_catprotection Protection

omnidb { -filesystem | -vprotect | -winfs | -vbfs } Host:MountPoint Label -fileversions FileName... [-detail | -encryptioninfo] [-noexpand]

omnidb Object [-noexpand] -session SessionID [-copyid CopyID] [-report [warning | minor | major | critical] | -change_protection Protection | -change_catprotection Protection | -strip | -catalog | -encryptioninfo]

omnidb Object [-noexpand] -session SessionID [-copyid CopyID] -media [-detail]

omnidb Object [-noexpand] -session SessionID [-copyid CopyID] -listcopies [-detail | -encryptioninfo]

omnidb -filesearch [-n N] <client> <directory> <filename>

omnidb Object [-session SessionID] [-copyid CopyID] -listdir <directory>

omnidb -list_folders -session SessionID [-mailbox { MailboxName...}]

omnidb -veagent Host:Set -session SessionID [-copyid CopyID] [-catalog | -media] [-vdiskuuid DiskUuid]

omnidb -veagent Host:Set -session SessionID [-copyid CopyID] [-list_vdisks]

omnidb -rpt [SessionID [-detail]

omnidb -rpt -wo start duration

omnidb -addhost -servername ClientName -user UserName -passwd Password

omnidb -removehost -servername ClientName -user UserName

omnidb -listhost [-servername ClientName]

omnidb -auditing { -timeframe [StartDate] [EndDate] | -since Date [-until Date] | -last NumberOfDays } [-detail]

Object

{ -filesystem Host:MountPoint Label |

-winfs Host:MountPoint Label |

-vprotect Host:MountPoint Label |

-vbfs Host:MountPoint Label |

-rawdisk Host Label |

-winfsblockbased Host:MountPoint Label |

-stream Host:Set |

-sap Host:Set |

-sapdb Host:Set |

-saphana Host:Set |

-oracle8 Host:Set |

-mssql Host:Set |

-msese Host:Set |

-e2010 Host:Set [Label] |

-mbx Host:Set |

-informix Host:Set |

-sybase Host:Set |

-lotus Host:Set |

-vss Host:Set |

-db2 Host:Set |

-mssharepoint Host:Set |

-veagent Host:Set |

-m365 *Client:* Set |

-idb Host:Set |

-integ MySQL Host:Set |

-integ PostgreSQL Host:Set }

Protection

{ none | days n | weeks n | until Date | permanent }

Date

[YY]YY/MM/DD (1969 < [YY]YY < 2038)

DESCRIPTION

The omnidb command is used to query the IDB Log database.

This command can be used to:

- list sessions and their summary reports
- list backed up objects and their details (for example: client name, mountpoint, label, object type, object status, backup type, and so on), message logs, and media location
- search for all occurrences of a pathname pattern

The omnidb command performs basic IDB queries.

OPTIONS

-version

Displays the version of the omnidb command.

-help

Displays the usage synopsis for the omnidb command.

-datalist IntegrationName BackupSpecificationName

Lists the sessions resulting from backup specification backups created using this BackupSpecificationName .

Note: For non-filesystem backup specification (Microsoft Exchange Server, Microsoft SQL Server, Informix Server, and so on).

IntegrationName must be specified in front of BackupSpecificationName . Both must be in double quotes.

-type { restore | backup | verification }

If no SessionID is specified, the command lists either backup, restore, or verification sessions. If SessionID is specified for backup sessions, the c ommand lists the objects created for that backup session.

-user User

Lists only the sessions belonging to the specified user.

-since Date

Lists sessions since the given Date .

-until Date

Lists sessions until the given Date .

-last n

Lists sessions that occurred within the last n days.

-latest

Lists the last active Data Protector session.

-wo start duration

Start defines the start of the timeframe. Duration is the duration of the timeframe in seconds.

-detail

Displays detailed information about the selected query, such as backup type, protection, whether or not encrypted. The VADP feature introduced in Data Protector 8.14 provides enhanced reports for Virtual Machines. Reports on VMware virtual machines display VM objects in the command line output in the same way as regular Data Protector clients. The reports for each VM object displays additional information, such as VM name, VM path, VM UUID, ESXi server, and full object name.

-encryptioninfo

Displays detailed encryption information for objects meeting the query criteria.

-session SessionID

Displays session information. If no SessionID is specified, all sessions are shown. The report shows for each session: the ID, type, status and user (UNIX login, UNIX group and client). If a sessionID is specified, then objects that are backed up within this session are shown. This information includes: client name, mountpoint, label, object type and object status.

If the -detail option is specified, more information is shown, such as the backup type (full, incr,...), protection status, encryption status, and so on. For integration objects, the backup ID is also shown. For VADP clients, the object name must use the VM name as reported from omnicellinfo -cell brief command and this applies to all variations of omnidb -session, where object name is <hostname>:/<vCenter>/<path>/<vmname>[<UUID>]. Here, <hostname> is DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

If the -encryption option is specified, the encryption KeyID-StoreID is displayed for each encrypted object created during the specified session. SessionID is mandatory in this case.

-auditing

Lists auditing related information from the cell. The following information is listed for each backup, restore, copy, or consolidation session: name, specification, completion status, backup type, start time, end time, owner, and session type.

If the -detail option is specified, the command also lists used media and objects.

-copyid CopyID

>If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option is obligatory. It selects a specific copy.

-filesearch [-n N] ClientName DirectoryPath FileName

Lists all the backed up files and directories that match the selection criteria set by the ClientName DirectoryPath FileName parameters. Wildcards can be used. The list can be limited to a certain number of displayed objects by setting the -n option, where N is the number of objects to be displayed. The following information is displayed about each object: object type, object name, object description, pathname.
Note: DirectoryPath can be a complete or incomplete path. For example for file C:\Directory\Sub-directory\file.txt, DirectoryPath can be /, /Directory/ or /Directory/Sub-directory.

-listdir Directory

Lists all the backed up objects in the specified directory.

-list_folders

Microsoft Exchange Server Single Mailbox integration: displays a list of all single mailbox folders (including their subfolders) backed up within a particular session.

-mailbox MailboxName

Microsoft Exchange Server Single Mailbox integration: displays mailbox folders for a particular mailbox only. If the option is not specified, folders of all backed up mailboxes are listed.

-listcopies

Lists details on all existing object or mirror copies of the specified object for the specified session. The session ID, the CopyID, the time and the status of object copy or mirror sessions for the specified object are listed.

-rpt SessionID

Displays session information in a form specially suited for further use of awk, grep or perl. Records are separated with blank lines and line feed is the field separator. If no SessionID is specified, all backup sessions are shown. Each record contains the following fields: the ID, backup specification name, status, start time in format HH:MM and duration in hours as a floating point number.

-report Report

Lists all messages (of specified report level and higher) which were generated by the specified session. Messages are classified (in ascending order) as: warning, minor, major and critical. For example, if major is selected, only major and critical messages are reported. By default, all messages are reported.

-object

Displays information on all data objects. The report shows the client name, label, and object type.

If the -detail option is specified, more detailed information is displayed for each object, such as each session for which object versions were created, together with protection status, encryption status, and so on.

If the -encryptioninfo option is specified, for each object, the encryption KeyID-StoreID is displayed for each session in which object versions were created.

-filesystem Client:MountPoint Label

Displays information on all filesystem objects (displays the Client:MountPoint Label string for every filesystem object in the IDB). If a Client:MountPoint Label string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-vProtect Client:MountPoint Label

Displays information on all vProtect objects (displays the Client:MountPoint Label string for every vProtect object in the IDB). If a Client:MountPoint Label string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-winfs Client:MountPoint Label

Displays information on all Windows filesystem objects (displays the Client:MountPoint Label string for every Windows filesystem object in the IDB). If a Client:MountPoint Label string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-vbfs Client:MountPoint Label

Displays information on all Windows filesystem objects (displays the Client:MountPoint Label string for every Windows filesystem object in the IDB). If a Client:MountPoint Label string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-winfsblockbased Client:MountPoint Label

Displays information on the size of occupied data, path, and size of the block map file.

-rawdisk Client Label

Displays information on disk image objects (displays the Client Label string for every object in the IDB). If a Client Label string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-stream Client:Set

Displays information on stream objects (displays the Client:Set string for every stream object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-sap Client:Set

Displays information on SAP R/3 data objects (displays the Client:Set string for every SAP R/3 object in the IDB). If Client:Set is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-sapdb Client:Set

Displays information on SAP MaxDB data objects (displays the Client:Set string for every SAP MaxDB object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-oracle8 Client:Set

Displays information on Oracle objects (displays the Client:Set string for every Oracle object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the status, size of object, and the number of session errors reported.

-mssql Client:Set

Displays information on Microsoft SQL Server objects (displays the Client:Set string for every Microsoft SQL Server object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-msese Client:Set

Displays information on Microsoft Exchange Server objects (displays the Client:Set string for every Microsoft Exchange Server object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-e2010 Client:Set

Displays information on Microsoft Exchange Server 2010/2013 objects (displays the Client:Set string for every Microsoft Exchange Server 2010/2013 object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-mbx Client:Set

>Displays information on Microsoft Exchange Server objects - single mailboxes (displays the Client:Set string for every Microsoft Exchange Server object - single mailboxes in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.>

-informix Client:Set

Displays information on Informix Server objects (displays the Client:Set string for every Informix Server object in the IDB). If an Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-sybase Client:Set

Displays information on Sybase objects (displays the Client:Set string for every Sybase object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-lotus Client:Set

Displays information on Lotus Notes/Domino objects (displays the Client:Set string for every Lotus Notes/Domino object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-vss Client:Set

Displays information on Microsoft Volume Shadow Copy (VSS) objects (displays the Client:Set string for every VSS object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-db2 Client:Set

Displays information on IBM DB2 UDB objects (displays the Client:Set string for every IBM DB2 UDB object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-mssharepoint Client:Set

Displays information on Microsoft SharePoint Server 2010 objects (displays the Client:Set string for every Microsoft SharePoint Server 2010 object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the session ID, session start time, session duration, backup object status and size, and the number of session errors reported.

-veagent Client:Set

Displays information on virtual environment objects (displays the Client:Set string for every virtual environments object in the IDB). If a Client:Set string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the status, size of object, and the number of session errors reported.

>Reports display VMware virtual machines in the same way as Data Protector clients called VADP clients. The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

-idb [Client:Set]

Displays information on backup objects of the Internal Database type that are referenced in the IDB. In the omnidb output, such objects are marked with the IDB string.

If the argument Client:Set is not specified, omnidb lists the Client:Set string for every Internal Database backup object. If the Client:Set argument is specified, omnidb lists for each corresponding backup session its session ID, start time, duration, statuses and sizes of the backed up objects, and the number of errors reported.

-integ {MySQL | PostgreSQL} Client:Set

Displays information on backup objects of the MySQL or PostgreSQL type that are referenced in the IDB. In the omnidb output, such objects are marked with the MySQL or PostgreSQL string.

If the argument Client:Set is not specified, omnidb lists the Client:Set string for every MySQL or PostgreSQL backup object. If the Client:Set argument is specified, omnidb lists for each corresponding backup session its session ID, start time, duration, statuses and sizes of the backed up objects, and the number of errors reported.

Note: In the omnidb command output, MySQL pseudo-backup objects with metadata are denoted with the suffix :METADATA in their names.

-m365 [Client:Set]

Displays information on backup objects of the Microsoft 365 type that are referenced in the IDB. In the omnidb output, such objects are marked with the IDB string.

If the argument Client:Set is not specified, omnidb lists the Client:Set string for every Internal Database backup object. If the Client:Set argument is specified, omnidb lists session ID, start time, duration, statuses and sizes of the backed up objects, and the number of errors reported for each corresponding backup session.

-strip

This option works in three different ways. If SessionID is specified it strips the Detail Catalog of all the objects from the session with a specified session ID. If both SessionID and ObjectName are specified it strips the Detail Catalog of the object identified by ObjectName from the session with specified session ID. If no option is specified, it strips the Detail Catalog of all data objects that are no longer protected.

-strip NumberOfDays

This option can be used with ObjectName to strip the Detail Catalog of all versions of the specified object that are older than NumberDays days.

-fileversions FileName

Displays information on all sessions which contain the filesystem with specified file FileName , session ID, mode, date modified, size and type.

-noexpand

Use this option to display IPv6 hostnames in compressed format.

-media

Shows list of the media used in the backup session. If object is also specified then it only shows list of media containing that object.

-user_location

This option changes the output of media related reports to print out user defined location instead of physical location used by default.

-change_protection Protection

This option changes the current protection of the object versions identified by ObjectName and/or SessionID to the new protection defined as Protection. If it is specified without any other option then it changes protection for all Failed/Aborted objects. Protection can be none, permanent, until a specific date, or for a time interval. When the protection is until a specified date or for a time interval, you must specify the value. The Date form is YY/MM/DD. You can specify a date until which the data is to be protected, or you can specify a time interval, which is the number of days (after today) during which the data should not be overwritten.

> Note From Data Protector 9.05 onwards, the protection for any virtual machine can be modified for a specific VEAgent object. This option allows you to change the protection for all the VEAgent Disk objects, when the VEAgent object is selected.

-change_catprotection Protection

Changes the current protection of the catalog retention time. Protection can be none, same_as_data_protection, until a specific date, or for a time interval. same_as_data_protection means that catalog will stay until data is overwritten/exported. When the protection is until a specified date or for a time interval, you must specify the value. The Date form is YY/MM/DD. You can specify a date until which the data is to be protected, or you can specify a time interval, which is the number of days (after today) during which the data should not be overwritten.

Note From Data Protector 9.05 onwards, the catalog protection for any virtual machine can be modified for a specific VEAgent object. This option allows you to change the catalog protection for all the VEAgent Disk objects, when the VEAgent object is selected.

-catalog

Displays the Detail Catalog of a specified object - session combination. Use an object option (for example -filesystem) to specify the object and use the -session (and sessionID) to specify the session.

-purge

This option removes the session from the session list. All objects within the session become unprotected. It is still possible to make a restore from this session.

-timeframe StartDate EndDate

Lists the sessions that started within a specified timeframe.

-vdiskuuid diskUUID

This option can be used with the "-catalog" or "-media" to list the associated virtual machine disk objects. These options are supported for the VMware and Hyper-V.

-list_vdisks

Lists the disk information (disk name and disk UUID) for a backed up virtual machine object.

Note: Both -vdiskuuid diskUUID and -list_vdisks options are available only for VMware objects backed using Data Protector 9.05 and later, and Hyper-V RCT objects backed up using Data Protector 2020.11 onwards.

NOTES

With clustered objects, the Client argument must define name of the virtual host.

With virtual environment objects, the VM UUID displayed by the omnidb command refers to the instance UUID of the virtual machine.

The virtual machine objects and its associated disk objects constitute the VEAgent object size.

EXAMPLES

The following examples illustrate how the omnidb command works.

1. To see details for the backup sessions started by user "root" in last three days, execute:

   omnidb -session -user root -last 3 -type backup -detail

2. To see critical errors for the session with the sessionID "2013/05/14-17", execute:

   omnidb -session 2013/05/14-17 -report critical

3. To see all virtual machines used in backup as VEPA objects and its additional information, execute:

```
omnidb -session 2015/11/05-1 -detail
```

4. To see all virtual machines from all VEPA backups as objects, execute:

   ```
   omnidb –veagent
   ```

5. To display session information about a single virtual machine, execute:

   ```
   omnidb –veagent host.domain.name:/vcenter.domain.name/datacenter/path/example_host[c6a20393-159d-4b9a-8671-73a4490ab032]
   ```

   where, <hostname> is the DNS name of the guest virtual machine or IP address.

6. To see all objects of the type filesystem, execute:

   ```
   omnidb -filesystem
   ```

7. To see encryption information for all Windows filesystem objects, execute:

   ```
   omnidb -winfs -encryptioninfo
   ```

8. To see encryption information for objects created in session "2013/03/23-2" execute:

   ```
   omnidb -session 2013/03/23-2 -encryptioninfo
   ```

9. To see details for the filesystem "hpuljum.company.com:/ Label44" in the latest session, execute:

   ```
   omnidb -filesystem hpuljum.company.com:/ Label44 -latest -detail
   ```

10. To see catalog for the filesystem "bob:/" in the session "2012/07/14-6", execute:

    ```
    omnidb -filesystem bob:/ -session 2012/07/14-6 -catalog
    ```

11. To see information on the block map file of Volume E on host hostname.company.com in session 2016/11/20-10 , execute:

    ```
    omnidb -winfsblockbased hostname.company.com:/E "E:[New Volume]" -session 2016/11/20-10 -catalog
    ```

12. To see details of the sessions that used a Microsoft Exchange Server backup specification named "MSExchange test", execute:

    ```
    omnidb -session -datalist "E2010 MSExchange test" -details
    ```

13. To list all Microsoft Exchange Server mailbox folders in the mailbox "User 2", backed up in the session "2013/03/16-10", execute:

    ```
    omnidb -mbx -list_folders -session 2013/03/16-10 -mailbox "User 2"
    ```

14. To see information on Lotus Notes/Domino Server objects, execute:

    ```
    omnidb -lotus
    ```

15. To see which Lotus Notes/Domino Server files are contained in the Lotus Notes/Domino Server object "computer.company.com:DREAM::Databases:5" from the session "2012/08/26-2", execute:

    ```
    omnidb -lotus computer.company.com:DREAM::Databases:5 -session 2012/08/26-2 -catalog>
    ```

16. To see information on the SAP MaxDB object "machine.company.com:/instance1/Config/1", execute:

    ```
    omnidb -sapdb machine.company.com:/instance1/Config/1
    ```

17. To see information on the SAP HANA object "hanasys.company.com:H95:7", execute:

    ```
    omnidb -saphana machine.company.com:/instance1/Config/1
    ```

18. To see detailed information on media used for the Windows filesystem object "system.company.com:/C" with the label "DTS_T" in the session "2012/07/14-17", with CopyID "d5032390-baba-4b3f-8c67-1f5b9273b242/1015", execute:

    ```
    omnidb -winfs system.company.com:/C "DTS_T" -session 2012/07/14-17 -copyid d5032390-baba-4b3f-8c67-1f5b9273b242/1015 -media -detail
    ```

19. To see detailed information on all existing object or mirror copies of the Windows filesystem object "system.company.com:/D" with the label "D1" with the sessionID "2013/05/01-12", execute:>

    ```
    omnidb -winfs system.company.com:/D "D1" -session 2013/05/01-12 -listcopies -detail
    ```

20. To see information on Microsoft SharePoint Server 2010 configuration database objects, execute:

    ```
    omnidb -mssharepoint helios.company.com:SharePoint_Config/1:SharePoint_Config
    ```

21. To display information on backup sessions that backed up the Internal Database (more specifically, the set "DPSPECs:0") on the Cell Manager with the fully qualified domain name "cmsys.company.com", execute:

    ```
    omnidb -idb cmsys.company.com:DPSPECs:0
    ```

22. To display information on MySQL backup objects backed up with Data Protector, execute:

    ```
    omnidb -integ MySQL
    ```

23. To display information on Microsoft 365 backup objects backed up with Data Protector, execute:

    ```
    omnidb -m365
    ```

24. To display information on Microsoft 365 backup sessions for a mailbox abc@MyOrg.MyDomain.com , execute:

    omnidb -m365 MyOrg:Exchange/User/abc@MyOrg.MyDomain.com -detail

25. To display information on Microsoft 365 backup sessions for mailboxes abc@MyOrg.MyDomain.com and xyz@MyOrg.MyDomain.com, execute:

    omnidb -m365 MyOrg:Exchange/User/abc@MyOrg.MyDomain.com -detail MyOrg:Exchange/User/xyz@MyOrg.MyDomain.com -detail

26. To list disk information of a backed up virtual disk object hyperv.company.com from session 2020/11/01-1 , execute:

    omnidb - veagent hyperv.company.com -session 2020/11/01-1 -list_vdisks

27. To list catalog information of a virtual disk object hyperv.company.com from session 2020/11/01-1 , execute:

    omnidb - veagent hyperv.company.com -session 2020/11/01-1 -catalog -vdiskuuid <Disk_uuid>

28. To list media information of a virtual disk object hyperv.company.com from session 2020/11/01-1 , execute:

    omnidb - veagent hyperv.company.com -session 2020/11/01-1 -media -vdiskuuid <Disk_uuid>

29. To change the protection interval of a VEAgent object hyperv.company.com from session 2020/11/01-1 to 11 days, execute:

    omnidb - veagent hyperv.company.com -session 2020/11/01-1 -change_protection days 11

30. To change the catalog protection interval of a VEAgent object hyperv.company.com from session 2020/11/01-1 to 22 days, execute:

    omnidb - veagent hyperv.company.com -session 2020/11/01-1 -change_catprotection days 22

31. To see all objects of the type vProtect, execute:

    omnidb -vprotect

32. To see details for the vProtect object "hpuljum.company.com:/ Label44 " in the latest session, execute:

    omnidb -vprotect hpuljum.company.com:/ Label44 -latest -detail

33. To see catalog for the vProtect object "bob:/ " in the session "2021/10/28-1", execute:

    omnidb -vprotect bob:/ Label44 -session 2021/10/28-1 -catalog

omnidbp4000

omnidbp4000 - manages the configuration data which the Data Protector P4000 VSS Agent uses to connect to the CIMOM providers
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnidbp4000 --version | --help

omnidbp4000 --ompasswd --add *ClientName* [--ssl] [--port *PortNumber*] [--user *Username*] [--passwd *Password*] [--check [--host *ClientName*]]

omnidbp4000 --ompasswd --remove *ClientName* [--port *PortNumber*] [--user *Username*]

omnidbp4000 --ompasswd [--list [*ClientName*]]

omnidbp4000 --ompasswd --check [--host *ClientName*]

DESCRIPTION

The omnidbp4000 command enables you to manage configuration data which is used for connections between the Data Protector P4000 VSS Agent and the chosen Common Information Model Object Manager (CIMOM) providers. Such connections must be properly configured before storage systems of the P4000 SAN Solutions family can be used for zero downtime backup and instant recovery purposes.

Using omnidbp4000, you should configure the connection to the chosen CIMOM provider. Once configured, the connection configuration data corresponding to the chosen CIMOM provider is stored in a separate configuration file located on the Cell Manager in the directory:

Windows systems: Data_Protector_program_data\server\db80\smisdb\p4000\login

UNIX systems: /var/opt/omni/server/db80/smisdb/p4000/login

With omnidbp4000, you can also update or remove the connection configuration data, list the contents of the configuration files, and check if the connection to a particular CIMOM provider can be established. For these purposes, the omnidbp4000 command provides the basic options --add, --remove, --list, and --check. The option --add can be used for configuring a connection anew as well as updating the configuration data for an already configured connection.

OPTIONS

--version

Displays the version of the omnidbp4000 command.

--help

Displays the usage synopsis for the omnidbp4000 command.

--ompasswd --add *ClientName* [--ssl] [--port *PortNumber*] [--user *Username*] [--passwd *Password*] [--check [--host *ClientName*]]

Configures or reconfigures the data which the Data Protector P4000 VSS Agent uses to establish connection to a CIMOM provider whose service is running on the system *ClientName*. For *ClientName* you can specify either fully qualified domain name, host name, or IP address of the system. Host names are automatically expanded to fully qualified domain names before they are stored to the configuration files. If no additional options are specified, omnidbp4000 configures the connection as a non-SSL connection, using the port number 5988 as the CIMOM service listening port, and using administrator as the user name. In this case, omnidbp4000 prompts you to enter the password interactively, and omits the initial connection check.

If the option --ssl is specified, the connection is configured to use SSL.

If the option --port is specified, the connection is configured to use the port number *PortNumber*. If not specified, the default port number is used: 5988 for connections not using SSL, 5989 for connections using SSL. recommends you use the default port number.

If the option --user is specified, the connection is configured to use the user name specified in *Username*. In the opposite case, the default user name administrator is used. If the option --password is specified, the connection is configured to use the password *Password*. If not specified, omnidbp4000 prompts you to enter the password interactively,

If the option --check is specified, omnidbp4000 checks if the connection to the CIMOM provider can be established after storing the data to the connection configuration file. If the option --host is specified, the Data Protector P4000 VSS Agent checking the connections is started on the system *ClientName*, otherwise one of the systems with the Data Protector P4000 VSS Agent installed is chosen by Data Protector. For *ClientName* you can specify either fully qualified domain name or IP address of the system.

--ompasswd --remove *ClientName* [--port *PortNumber*] [--user *Username*]

Removes the connection configuration data, which has been added by omnidbp4000, for the CIMOM providers whose service is running on the system *ClientName*. For *ClientName* you can specify either fully qualified domain name or IP address of the system. If the option --port, the option --user, or both are specified in addition, only the configuration files corresponding to connections whose port number matches *PortNumber*, whose user name matches *Username*, or whose port number and user name both match the specified values are removed, respectively.

--ompasswd [--list [*ClientName*]]

Lists all existing connection configuration data for the CIMOM providers, which has been added by omnidbp4000. For each provider, the following information is displayed: the user name, the fully qualified domain name or IP address of the system hosting the CIMOM service, the port number of the CIMOM service listening port, and the indicator whether the connection uses SSL. You can narrow the output to only a particular system by specifying the argument *ClientName*. For *ClientName* you can specify either fully qualified domain name or IP address of the system.

--ompasswd --check [--host *ClientName*]

Triggers a check if the configured connections from the Data Protector P4000 VSS Agent to the CIMOM providers can be established. If the option --host is specified, the Data Protector P4000 VSS Agent checking the connections is started on the system *ClientName*, otherwise one of the systems with the Data Protector P4000 VSS Agent installed is chosen by Data Protector. For *ClientName* you can specify either fully qualified domain name or IP address of the system.

NOTES

The omnidbp4000 command is available on Windows systems only.

EXAMPLES

The following examples illustrate how the omnidbp4000 command works.

1. To configure a connection to the CIMOM provider hosted on the system "cimom_host1" in the local domain, so that the connection uses SSL, the CIMOM service port number "5989", the user name "administrator", and the password "secretstring" to connect to the CIMOM provider, execute:

   ```
   omnidbp4000 --ompasswd --add cimom_host1 --ssl --password secretstring
   ```

2. To update the configuration of the connection to the CIMOM provider hosted on the system "cimom_host3.company.com" that does not use SSL and uses the user name "storagesys_admin" to connect to the CIMOM provider, so that the Data Protector P4000 VSS Agent uses the new password "newsecretstring" to connect, execute:

   ```
   omnidbp4000 --ompasswd --add cimom_host3.company.com --password newsecretstring
   ```

3. To remove configuration data for connections to the CIMOM providers hosted on the system with the fully qualified domain name "cimom_host2.company.com" and for which the user name "backup_admin" is used, execute:

   ```
   omnidbp4000 --ompasswd --remove cimom_host2.company.com --user backup_admin
   ```

4. To list connection configuration data for connections to the CIMOM providers hosted on the system with the IP address "16.57.73.10", execute:

   ```
   omnidbp4000 --ompasswd --list 16.57.73.10
   ```

5. To trigger a check if the configured connections to the CIMOM providers can be established, and use the Data Protector

P4000 VSS Agent installed on the system "p4000_host1.company.com" for checking, execute:

```
omnidbp4000 --ompasswd --check --host p4000_host1.company.com
```

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1), omnidbutil(1M), omnidbvss(1), omnibdxp(1), omnidbzdb(1), omniofflr(1M)

omnidbvss

omnidbvss - queries the VSS database (VSSDB); browses, lists, saves, removes, and manages the items of the VSSDB (this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnidbvss -version | -help

omnidbvss -init

omnidbvss -list session [-barlist *BackupSpecName*]

omnidbvss -list session_persistent [-barlist *BackupSpecName*] [-older_than *YYYY/MM/DD*]

omnidbvss -get session { *SessionKey* [*SessionKey ...*] | -barlist *BackupSpecName* | -all } [-detail] [-save_metadata *Directory*]

omnidbvss -get session_persistent { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* [-older_than *YYYY/MM/DD*] | -all [-older_than *YYYY/MM/DD*]} [-save_metadata *Directory*]

omnidbvss -remove session { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* | -all } -force -reference

omnidbvss -remove session_persistent { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* -older_than *YYYY/MM/DD* | -all -older_than *YYYY/MM/DD* }

omnidbvss -disable session { *SessionKey* [*SessionKey ...*] | -barlist *BackupSpecName* | -all } [-force [-backhost *AlternativeBackupSystem*]]

omnidbvss -enable session { *SessionKey* [*SessionKey ...*] | -barlist *BackupSpecName* | -all } -backhost *BackupSystem* -mnt_target *MountPoint* [-mnt_sessionid_apphostname | -mnt_sessionid | -mnt_apphostname_sessionid | -mnt_apphostname | -mnt_direct] [-mnt_readwrite]

omnidbvss -resolve { -apphost *ApplicationSystem* | -all }

omnidbvss -resolve -session *SessionID*

SessionKey = *SessionID* [: *ClientName*]

DESCRIPTION

The omnidbvss command is used to query the VSSDB.

This command can be used to:

- list all available backup sessions (ZDB-to-disk, ZDB-to-disk+tape, and ZDB-to-tape)
- view information about a specific or all available backup sessions
- view details about a specific or all available ZDB-to-disk and ZDB-to-disk+tape sessions
- save backup components and writer metadata documents
- remove a specific or all available ZDB-to-disk and ZDB-to-disk+tape sessions, together with theirs replicas, from the VSSDB and from the disk array
- remove a reference to a specific or to all available backup sessions from the VSSDB
- disables the specified or all ZDB-to-disk or ZDB-to-disk+tape sessions
- enables the specified or all ZDB-to-disk, ZDB-to-disk+tape sessions
- initialize the VSSDB
- resolve the application systems in the Data Protector VSS integration cell.

OPTIONS

-version

Displays the version of the omnidbvss command.

-help

Displays the usage synopsis for the omnidbvss command.

-init

Initializes the VSSDB.

IMPORTANT: All data including sessions and created replicas is deleted from the VSSDB.

-list session [-barlist *barlist*]

Queries the VSSDB and lists all ZDB-to-disk and ZDB-to-disk+tape session IDs. If -barlist is specified, only the IDs of the ZDB-to-disk and ZDB-to-disk+tape sessions that were created using the backup specification are listed.

-list session_persistent [-barlist *barlist*] [-older_than *YYYY/MM/DD*]

Queries the VSSDB and lists all available backup session (ZDB to disk, ZDB to disk+tape, and ZDB to tape) IDs.

If -barlist is specified, only the IDs of the sessions that were created using the backup specification are listed.

If -older_than is specified, only the sessions IDs that were created before the specified date are listed.

-get session { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* | -all }

[-detail] [-save_metadata *Directory*]

Displays information about the ZDB-to-disk and ZDB-to-disk+tape sessions.

By specifying *SessionKey*, the -barlist, or the -all option, information about the backup components and disks about the sessions that match the given criteria will be displayed.

–detail displays detailed information (components, disks) about the specified session.

-save_metadata saves the backup components document (Backup Components Document.xml) and writer metadata document (writer_name.xml) to the specified directory.

-get session_persistent { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName*

[-older_than *YYYY/MM/DD*] | -all [-older_than *YYYY/MM/DD*]} [-save_metadata *Directory*]

Displays information about any backup session created using VSS software or the hardware provider.

By specifying *SessionKey*, the -barlist, or the -all option, information about the sessions that match the given criteria will be displayed.

-older_than displays information about the backup sessions, specified with the -barlist option, or all sessions that were created before the specified date.

-save_metadata saves the backup components document (Backup Components Document.xml) and writer metadata document (writer_name.xml) to the specified *directory*.

-remove session { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* | -all }

[-force] [-reference]

Removes the specified ZDB-to-disk or ZDB-to-disk+tape sessions and their replicas from the VSSDB (non-persistent metadata) and disk array.

By specifying the *SessionKey*, -barlist, or -all option, the information about the sessions that match the given criteria will be deleted from the VSSDB and the session's replicas will be deleted from the disk array.

If -reference is specified, only the reference information about the specified sessions and their replicas will be removed from the database. This option can be used to remove an entry that points to a replica that no longer exists.

The removing operation fails in the following cases, unless the -force option is used:

- If you have changed the disks' configuration manually after the backup (for example, the sessions target volumes were presented manually to some other system).

- If the target volumes cannot be dismounted because of a lock by some other process.

-remove session_persistent { *SessionKey* [*SessionKey...*] | -barlist

BackupSpecName [-older_than *YYYY/MM/DD*] | -all [-older_than *YYYY/MM/DD*]}

Removes the reference information about the specified sessions from the VSSDB (persistent metadata). It does not remove the session's replicas from the disk array.

By specifying the *SessionKey*, -barlist, or -all option, information about the sessions that match the given criteria will be removed.

-older_than removes the reference information about the backup sessions, specified by the -barlist option, or all sessions, that were created before the specified date.

-disable session { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* | -all }

[-force [-backhost *AlternativeBackupSystem*]]

Disables the specified ZDB-disk or ZDB-to-disk+tape sessions (if *SessionKey* is used), sessions created by the specified backup specification (if -barlist is used), or all sessions (if -all is used). Disabling means that the replicas (target volumes) created in the specified sessions or using the specified backup specification are dismounted and unpresented from the backup system.

The disabling operation fails in the following cases, unless the -force option is used:

- If you have changed the disks' configuration manually after the backup (for example, the sessions target volumes were presented manually to some other system).

- If the target volumes cannot be dismounted because of a lock by some other process.

Use -force -backhost *AlternativeBackupSystem* if the backup system from which you want to disable a backup session is not available. *AlternativeBackupSystem* specifies an alternative client system (any client in the Data Protector cell hat has the VSS integration component installed), from which the session will be disabled by force.

-enable session { *SessionKey* [*SessionKey...*] | -barlist *BackupSpecName* | -all }

-backhost *BackupSystem* -mnt_target *MountPoint* [-mnt_sessionid_apphostname | -mnt_sessionid | -mnt_apphostname_sessionid | -mnt_apphostname] [-mnt_direct] [-mnt_readwrite] [-force]

Enables the specified ZDB-disk or ZDB-to-disk+tape sessions (if *SessionKey* is used), or sessions created by the specified backup specification (if -barlist is used), or all sessions (if -all is used). Enabling means that the replicas (target volumes) created in the specified sessions or using the specified backup specification are presented and mounted to the specified backup system.

-backhost specifies the target client system where you want the target volumes to be presented.

-mnt_target specifies the directory on the *BackupSystem* where you want the target volumes to be mounted. By default, a new directory with the session ID is created in the specified directory and the disks are mounted there. If -mnt_direct is used, the disks are mounted to the specified directory. Use -mnt_direct only when mounting disks from only one backup session.

You can select the suffix of the mount directory by selecting one of the following options:

-mnt_sessionid_apphostname The name of the application system follows the session ID.

-mnt_sessionid Only the sessionID is used.

-mnt_apphostname_sessionid The sessionID follows the application system name.

-mnt_apphostname Only the application system name is used.

The enabling operation fails in the following cases, unless the -force option is used:

- When -mnt_direct is used and another disk is already mounted in the specified directory.

- If the session to be enabled is already enabled on another backup system.

- If you have changed the disks' configuration manually after the backup.

If you use the -force option to enable disks on your specified system even if they are already specified on some other system, note that the disks will not be dismounted on the other system and you will need to clean the environment manually.

By default, the disks are mounted in read-only mode. If -mnt_readwrite is specified, the disks will be mounted in read/write mode.

-resolve { -apphost *ApplicationSystem* | -all }

Resolves the specified application system (if -apphost is used) or all application systems (if -all is used) in the Data Protector cell.

The command applies only to instant recovery-enabled backup sessions and must be run always after:

- installing or upgrading Data Protector

- your source volumes configuration on the application system has changed (for example, you have modified the existing source volumes or you have presented new source volumes)

- you have added a new storage object (for example, a Microsoft Exchange Server storage group)

-resolve –session *SessionID*

Resolves the target volumes created in the specified backup session.

The command applies only to instant recovery-enabled backup sessions and must be run always after:

- installing or upgrading Data Protector

- your source volumes configuration on the application system has changed (for example, you have modified the existing source volumes or you have presented new source volumes)

- you have added a new storage object (for example, a Microsoft Exchange Server storage group)

EXAMPLES

1. To list the instant recovery–enabled sessions (ZDB to disk or ZDB to disk + tape) created using the backup specification "Backup1", execute:

   ```
   omnidbvss -list session -barlist Backup1
   ```

2. To get information about the backup components of all backup sessions created before February 1st, 2013, and to save information about the backup components and writer metadata to the directory "C:\metadata", execute:

   ```
   omnidbvss -get session_persistent -all older_than 2013/02/01 -save_metadata C:\metadata
   ```

   Note that the specified directory must exist before you execute the command.

3. To remove the reference information about the sessions "2013/02/11-1" and "2013/02/11-2" from the VSSDB and to remove the associated replicas from the disk array, execute:

   ```
   omnidbvss -remove session 2013/02/11-1 2013/02/11-2
   ```

4. To mount the target volumes from the session "2013/02/15-1" in the directory "C:\mnt\", present them on the client system "backupsys", and to leave the volumes mounted in read/write mode, execute:

   ```
   omnidbvss -enable session 2013/02/15-1 -backhost backupsys -mnttarget C:\mnt -readwrite
   ```

   Note that a new directory with the session ID is created and that the target volumes are mounted in the directory "C:\mnt\2013-02-15-1".

SEE ALSO

omnidb(1M), omnidbcheck(1M), omnidbinit(1M), omnidbp4000(1), omnidbsmis(1), omnidbutil(1M), omnidbxp(1), omnidbzdb(1), omniofflr(1M)

omnidbxp

omnidbxp - queries the ZDB database (XPDB), manipulates the P9000 XP LDEV exclude file, configures the P9000 XP Disk Array Family command devices usage, and manages the user authentication data which the Data Protector P9000 XP Agent uses to connect to specific disk arrays
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnidbxp -version | -help

omnidbxp -exclude { -put *filename* | -get *filename* | -check *SEQ LDEV* | -init | -delete }

omnidbxp [-ir] -session { -list | -show *sessionID* }

omnidbxp [-ir] -ldev { -list | -show *SEQ LDEV* }

omnidbxp -cm { -add *serial* { *CU:LDEV* | *LDEV* } *hostname* [*instance*] | -update *serial* { *CU:LDEV* | *LDEV* } *hostname* [*instance*]}

omnidbxp -cm -remove { all | *serial* [{ *CU:LDEV* | *LDEV* } [*hostname*]]}

omnidbxp -cm -list

omnidbxp -user -add *SEQ* -username *Username* [-password *Password*]

omnidbxp -user -check *SEQ* -host *ClientName*

omnidbxp -user -update *SEQ* -username *Username* [-password *Password*]

omnidbxp -user -list *SEQ*

omnidbxp -user -remove *SEQ*

DESCRIPTION

Using the omnidbxp command, you can perform various tasks related to the XPDB and your P9000 XP Disk Array Family storage system.

QUERYING THE INFORMATION ON BACKUP OBJECTS AND MANIPULATING THE LDEV EXCLUDE FILE

The omnidbxp command can be used to query the information stored in the ZDB database (XPDB), which stores the information about the configured LDEVs pairs (for both S-VOL types: mirror and snapshot) that is used during the Data Protector P9000 XP Disk Array Family backup and restore sessions. The XPDB is a set of plain text files stored on the Cell Manager in the default Data Protector ZDB database directory. The XPDB records contain data about the P-VOL – S-VOL pairs which have been put in the SUSPENDED state by the Data Protector P9000 XP Disk Array Family integration: the mirrors that have been split and the snapshots that have been created on the disk array. The XPDB is written to whenever a mirror is split or a snapshot is created. A pair is deleted from the XPDB whenever the Data Protector P9000 XP Agent resynchronizes a mirror (if the S-VOL is a mirror copy) or empties the volume that stores snapshot data (if the S-VOL is a snapshot).

The omnidbxp command can also be used to manipulate the P9000 XP LDEV exclude file. The P9000 XP LDEV exclude file enables disabling of using certain LDEVs on the backup system (S-VOL LDEVs) by Data Protector. Thus, it is possible to reserve certain LDEVs for other purposes than Data Protector backup and restore. The disabled LDEVs are, if used in a Data Protector session, ignored by Data Protector and such a session fails with critical error. The list of disabled LDEVs is kept in the P9000 XP LDEV exclude file on the Cell Manager: Data_Protector_program_data\server\db80\exclude\XPexclude (Windows systems) or /var/opt/omni/server/db80/xpdb/exclude/XPexclude (UNIX systems).

The omnidbxp options to be used for querying the XPDB and manipulating the P9000 XP LDEV exclude file are: -exclude , -put , -get , -check , -init , -delete , -session , -list , -show , -ir , -ldev , -show .

P9000 XP Disk Array Family COMMAND DEVICE HANDLING

An P9000 XP Disk Array Family command device is needed by any process that needs access to a disk array of the P9000 XP Disk Array Family. The information about P9000 XP Disk Array Family command devices is kept in the XPDB for the purpose of eliminating duplicate instance usage and overallocation. Data Protector provides the following mechanism to prevent duplicate instance usage and overallocation:

1. Whenever a session is started, Data Protector queries the XPDB for a list of command devices. If none is found in the XPDB (default behavior when the first session is started), Data Protector identifies command devices and generates a list of command devices in the XPDB as connected to every application system and every backup system in the cell.
2. Every command device is assigned an instance number (starting from 301) and the system (hostname) having access to it. If a command device can be accessed from more than one system, the hostname identifier enables Data Protector to be aware of the fact that the command device is already meant to be used by some other system; next available instance number is assigned to such a command device–hostname combination.
3. When the list is created, every disk array of the P9000 XP Disk Array Family which is attached to an application system or a backup system has a list of its command devices and systems having access to them (together with an instance number) assigned.
4. During a session, whenever an application system or a backup system needs access to a P9000 XP Array, it uses the first assigned command device with the instance number from the list. If the command device fails, the next command device from the list assigned to a particular system is used. If all of them fail, the session fails. The successful command device is used by a particular system until the end of the session and the list of command devices is used for all consecutive sessions.

Using the omnidbxp command, it is possible to:

1. Specify a particular command device (identified by the serial number of a P9000 XP Array and the LDEV number) to be used by a particular system. Optionally, an instance number can be assigned too. If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number. The entire information is written in the XPDB.
2. List all command devices in the XPDB.
3. Remove a specific or all command devices from the XPDB or update the information about a specific command device in the XPDB.

The omnidbxp option combinations to be used for command device handling begin with the -cm option. The options that can follow are: -add , -update , -remove , -list .

CONFIGURING THE USER AUTHENTICATION DATA

You can use the omnidbxp command to add user credentials of disk array user accounts to the XPDB and to manage stored credentials. For each particular disk array serial number, you can add user credentials of a single user account. The credentials are used by the P9000 XP Agent when it attempts to connect to a disk array through a command device which has the user authentication mode enabled. They must match those configured on the P9000 XP Array. The user credentials are required for the following types of Data Protector sessions:

- zero downtime backup and instant recovery sessions (involving only the Data Protector P9000 XP Agent)

- VSS instant recovery sessions (involving the Data Protector P9000 XP Agent and the Data Protector Microsoft Volume Shadow Copy Service integration)

Before running a particular Data Protector session, you can use the omnidbxp command to verify that the P9000 XP Agent can actually connect to the disk array using the preconfigured user credentials from the XPDB.

The omnidbxp option combinations to be used for configuring the user authentication data begin with the -user option. The options that can follow are: -add , -username , -password , -check , -host , -update , -list , -remove .

OPTIONS

-version

Displays the version of the omnidbxp command

-help

Displays the usage synopsis for the omnidbxp command.

-exclude -put *filename*

Sets the list of excluded LDEVs by reading the contents of the *filename*, checking its syntax and if the syntax is correct, copying the file to its position on the Cell Manager. If the syntax is not correct, the file is not copied.

-exclude -get *filename*

Prepares the P9000 XP LDEV exclude file for editing by reading the contents of the P9000 XP LDEV exclude file on the Cell Manager and saving it under the *filename*.

-exclude -check *SEQ LDEV*

Checks whether the specified LDEV, identified by its backup system disk array serial number (*SEQ*) and LDEV number (*LDEV*) is specified in the P9000 XP LDEV exclude file on the Cell Manager. The LDEV number must be specified as the CU#:LDEV in decimal format. If the queried LDEV is specified in the P9000 XP LDEV exclude file, the command returns the string YES!. If the queried LDEV is not specified in the P9000 XP LDEV exclude file, the command returns the string NO!.

-exclude -init

Overwrites the current P9000 XP LDEV exclude file on the Cell Manager with the template P9000 XP LDEV exclude file.

-exclude -delete

Deletes the contents of the P9000 XP LDEV exclude file on the Cell Manager.

-ir

Specifies that the current omnidbxp command is executed only for the LDEVs pairs marked for the instant recovery in the XPDB. If this option is not specified, the current command is executed for all LDEVs pairs in the XPDB.

-session -list

Lists all available sessions in the XPDB.

-session -show *sessionID*

Lists all backup system S-VOL LDEVs that were involved in the session with the *sessionID*.

-ldev -list

Lists all S-VOL LDEVs in the XPDB together with their corresponding backup session ID.

-ldev -show *SEQ LDEV*

Lists all available XPDB information about the S-VOL specified by its *SEQ* and *LDEV* identifiers. The following information is listed: session ID, timestamp (date and time), CRC data, instant recovery flag, the *SEQ* and *LDEV* identifiers and port number of the corresponding primary volume (P-VOL), mirror type, mirror unit (MU) number, fully qualified domain name (FQDN) of the application system name, and FQDN of the backup system.

-cm -add *serial* { *CU:LDEV* | *LDEV* } *hostname* [*instance*]

Adds the command device identified by the serial number of a P9000 XP Array (*serial*) and serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) to the XPDB, and assigns it the hostname of the system accessing it (*hostname*) and optionally the instance number (*instance*). If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number.

The instance number must be any number in the range between 301 and 399.

The command does not check whether the specified command device or system exist, it only checks if the optional instance number specified is within the correct range and if the command device together with the instance number is not already assigned to be used by some other system. If checks fail, the command fails with an appropriate error message.

-cm -update *serial* { *CU:LDEV* | *LDEV* } *hostname* [*instance*]

Updates the XPDB information about the command device identified by the serial number of a P9000 XP Array (*serial*), serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) and the specified hostname of the system accessing it (*hostname*), by assigning the newly specified instance number (*instance*) to the P9000 XP Array serial number, serial number of command device and hostname combination. If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number.

The instance number must be any number in the range between 301 and 399.

The command does not check whether the specified command device or system exist, it only checks if the optional instance number specified is within the correct range and if the command device together with the instance number is not already assigned to be used by some other system. If the checks fail, the command fails with an error message.

-cm -remove all

Removes the information about all command devices from the XPDB.

-cm -remove *serial* [{ *CU:LDEV* | *LDEV* } [*hostname*]]

If only the *serial* argument is specified, the command removes the information about command devices within a specific P9000 XP Array identified by the serial number of this P9000 XP Array (*serial*) from the XPDB.

If the *CU:LDEV* | *LDEV* and optionally *hostname* arguments are specified as well, the command removes the information about the command device identified by the serial number of the P9000 XP Array (*serial*), serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) and optionally by the hostname of the system (*hostname*).

When removing the information about the command device without specifying the system (*hostname*), the command deletes all entries for the specified command device, regardless of the system(s) assigned to it.

-cm -list

Lists all command devices in the XPDB.

-user -add *SEQ* -username *Username* [-password *Password*]

Adds user authentication data for the disk array with the serial number *SEQ* to the XPDB. For each particular disk array serial number, the XPDB can only contain authentication data of a single disk array user account.

If the option -password is specified, omnidbxp uses the password specified in the command line instead of prompting for it to be entered interactively.

-user -check *SEQ* -host *ClientName*

Checks if the P9000 XP Agent can connect to the disk array with the serial number *SEQ* from the system *ClientName* using the user authentication data configured for this disk array. *ClientName* can be a name of either an application system or the backup system. This action actually checks if the user name and password configured in the XPDB for this disk array match any of the user accounts that are configured on the disk array. If successful, omnidbxp reports the command device and the instance number that were used for the connection.

-user -update *SEQ* -username *Username* [-password *Password*]

Updates the user authentication data for the disk array with the serial number *SEQ* in the XPDB.

If the option -password is specified, omnidbxp uses the password specified in the command line instead of prompting for it to be entered interactively.

-user -list [*SEQ*]

Lists the user authentication records that are stored in the XPDB, in the form of serial number–user name pairs.

If the argument *SEQ* is specified, omnidbxp only lists the records that belong to the disk array with this particular serial number.

-user -remove *SEQ*

Removes the user authentication data for the disk array with the serial number *SEQ* from the XPDB.

EXAMPLES

1. To set or change the P9000 XP LDEV exclude file:

   a.) Use the following command on the application or backup system:

   ```
   omnidbxp -exclude -get c:\tmp\filename.txt
   ```

   This command reads the P9000 XP LDEV exclude file from the Cell Manager and saves it in the "c:\tmp\filename.txt" file.

   b.) Edit the `c:\tmp\filename.txt` file and save it when you are done editing.

   c.) Use the following command on the application or backup system:

   This command reads the contents of the "c:\tmp\filename.txt", checks its syntax and if the syntax is correct, copies the file to its position on the Cell Manager.

   ```
   omnidbxp -exclude -put c:\tmp\filename.txt
   ```

2. To check whether the LDEV identified by the serial number "12345" and the LDEV number "123" is specified in theP9000 XP LDEV exclude file, execute the following command:

   ```
   omnidbxp -exclude -check 12345 2864
   ```

3. To list all backup system LDEVs, regardless of they being marked for instant recovery or not, that were involved in the session with the sessionID "2013/05/18-22", execute:

   ```
   omnidbxp -session -show 2013/05/18-22
   ```

4. To list all command devices in the XPDB, execute:

   ```
   omnidbxp -cm -list
   ```

5. To add the command device identified by the P9000 XP Array serial number "00035371" and command device serial number "103" to the XPDB and assign it to be used on the "computer.company.com" system by the instance number "303", execute:

   ```
   omnidbxp -cm -add 00035371 103 computer.company.com 303
   ```

6. To remove the information about all command devices from the XPDB, execute:

   ```
   omnidbxp -cm -remove all
   ```

7. To add the user name "data_protector_admin_3" and the password "3drowssap2xelpmoc1ym" as the user authentication data for the disk array with the serial number "80134" to the XPDB, execute:

   ```
   omnidbxp -user -add 80134 -username data_protector_admin_3 -password 3drowssap2xelpmoc1ym
   ```

8. To check if the P9000 XP Agent installed on the system "p9500_bkp_sys.company.com" can connect to the disk array with the serial number "80134" using the user authentication data configured in the XPDB, execute:

   ```
   omnidbxp -user -check 80134 -host p9500_bkp_sys.company.com
   ```

9. To update the user authentication data that is configured in the XPDB for the disk array with the serial number "80134" with the user name "data_protector_admin_5" and a password that you will enter interactively, execute:

   ```
   omnidbxp -user -update 80134 -username data_protector_admin_5
   ```

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbp4000(1), omnidbsmis(1), omnidbutil(1M), omnidbvss(1), omnidbzdb(1), omniofflr(1M)

omnidbzdb

omnidbzdb - executes administrative tasks on the 3PAR StoreServe Storage and NetApp Storage and manages the configuration data which the integration agents use to connect to the CIMOM providers or to the storage systems (this command is available on systems with the Data Protector User Interface component installed).

SYNOPSIS

omnidbzdb --version | --help

omnidbzdb --diskarray *ArrayFamily* --ompasswd --add *ClientName* [--ssl] [--port *PortNumber*] [--namespace *Namespace*] [--user *Username*] [--passwd *Password*]

omnidbzdb --diskarray *ArrayFamily* --ompasswd --remove *ClientName* [--port *PortNumber*] [--user *Username*]

omnidbzdb --diskarray *ArrayFamily* --ompasswd [--list [*ClientName*]]

omnidbzdb --diskarray *ArrayFamily* --ompasswd --check [--host *ClientName*]

omnidbzdb --diskarray *ArrayFamily* --list { --session [--ir] [--excluded] [--original] | --datalist }

omnidbzdb --diskarray *ArrayFamily* --show { --session SessionID | -datalist BackupSpecName }

omnidbzdb --list --purge

omnidbzdb --purge [--force] [--host *ClientName*]

omnidbzdb --delete { --session *SessionID* | --datalist *BackupSpecName* } [--reference] [--preview] [--force] [--host *ClientName*]

omnidbzdb --sync_check [--host *ClientName*] [--session *SessionID* | --datalist *BackupSpec*]

omnidbzdb { --exclude | --include } --session *SessionID*

DESCRIPTION

The omnidbzdb command enables you to manage configuration data used for connections between a Data Protector 3PAR StoreServ Storage integration agent and the chosen Common Information Model Object Manager (CIMOM) providers, and for connection between Data Protector NetApp Storage integration agent and the chosen NetApp storage system. Such connections must be properly configured before a storage system can be used for zero downtime backup and instant recovery purposes. To integrate with these storage system families, Data Protector uses different integration agents, depending on the operating system running on the application and backup systems:

- **Data Protector 3PAR StoreServ Storage integration:** 3PAR VSS Agent for Windows systems and P6000 / 3PAR SMI-S Agent for Windows, Linux, and HP-UX systems.
- **Data Protector NetApp Storage integration:** NetApp Storage Provider, which is a plug-in to the Data Protector SMI-S Agent

Use omnidbzdb to configure the connection to the chosen CIMOM provider or NetApp storage system. Once configured, the connection configuration data for the chosen system is stored in a separate configuration file located on the Cell Manager in the directory:

- **Data Protector 3PAR StoreServ Storage integration:**

  Data_Protector_program_data\server\db80\smisdb\p10000\login (Windows) and /var/opt/omni/server/db80/smisdb/p10000/login (UNIX)

- **Data Protector NetApp Storage integration:**

  Data_Protector_program_data\server\db80\smisdb\netapp\login (Windows) and /var/opt/omni/server/db80/smisdb/netapp/login (UNIX)

With omnidbzdb, you can also update or remove the connection configuration data, list the contents of the configuration files, and check if the connection to a particular CIMOM provider or storage system can be established. For these purposes, the omnidbzdb command provides the basic options --add, --remove, --list, and --check. The option --add can be used for configuring a new connection and updating the configuration data for an already configured connection.

OPTIONS

--version

Displays the version of the omnidbzdb command.

--help

Displays the usage synopsis for the omnidbzdb command.

--diskarray *ArrayFamily*

Selects the disk array family on which to perform configuration data management. omnidbzdb of the current Data Protector product version supports 3PAR StoreServ Storage and NetApp Storage. You can select one of them by specifying the corresponding value for the *ArrayFamily* argument (P10000 or 3PAR for the 3PAR StoreServ Storage, NetApp for the NetApp Storage). In an omnidbzdb command line, this option must precede all other options and option combinations.

--ompasswd --add *ClientName* [--ssl] [--port *PortNumber*] [--namespace *Namespace*] [--user *Username*] [--passwd *Password*]

Configures or reconfigures the data, which the appropriate Data Protector ZDB integration agent uses to establish connection to a CIMOM provider running on the system *ClientName*, or to a storage residing on this system. For *ClientName* you can specify either fully qualified domain name, host name, or IP address of the system. Host names are automatically expanded to fully qualified domain names before they are stored to the configuration files. If no additional options are specified, omnidbzdb configures the connection as non-SSL, using the port number 5988 as a system listening port, and using administrator as the user name. In this case, omnidbzdb prompts you to enter the password interactively and omits the initial connection check.

If the option --ssl is specified, the connection is configured to use SSL.

If the option --port is specified for a CIMOM provider, the connection is configured to use the port number *PortNumber*. If not specified, the default port number is used: 5988 for connections not using SSL, 5989 for connections using SSL. recommends you use the default port number.

If the option --user is specified, the connection is configured to use the user name specified in *Username*.If not specified, the default user name administrator is used. If the option --password is specified, the connection is configured to use the password *Password*. If not specified, omnidbzdb prompts you to enter the password interactively.

--ompasswd --remove *ClientName* [--port *PortNumber*] [--user *Username*]

Removes the connection configuration data, which was added with omnidbzdb. For *ClientName* you can specify either fully qualified domain name or IP address of the system with running CIMOM providers services, or of the storage system. If you additionally specify the options --port, --user, or both, only those configuration files are removed where connection values match the specified ones.

--ompasswd [--list [*ClientName*]]

Lists all existing connection configuration data for the CIMOM providers or storage systems, which was added with omnidbzdb. For each system, the following information is displayed: the user name, the fully qualified domain name or IP address of the system hosting the CIMOM service or the storage, the port number of the listening port, and the indicator whether the connection uses SSL. You can narrow the output by specifying the argument *ClientName*. For *ClientName* you can specify either fully qualified domain name or IP address of the system.

--ompasswd --check [--host *ClientName*]

Triggers a check if the configured connections from the Data Protector integration agent to the CIMOM providers or to the storage systems can be established. If the option --host is specified, the connections check starts on system *ClientName*, otherwise it starts on one of the systems with the appropriate integration agent. For *ClientName* you can specify either fully qualified domain name or IP address of the system.

--list { -session [--ir] [--excluded] [--original] | --datalist }

Lists all zero downtime backup sessions running in the cell that matches the specified criteria, or the backup specifications that were used to create replicas. Specify the --ir option to list only sessions for which the "Track the replica for instant recovery" option was selected. To list excluded sessions, specify --excluded option. Specify the --original option to list only the sessions with the original volumes preserved on the disk array after a corresponding instant recovery session was performed. The --datalist option lists all ZDB backup specifications which were used to create the replicas that are part of replica sets with existing members.

-show { -session *SessionID* | -datalist *BackupSpecName*}

When used with --session option, the command lists expanded details of a session. When used with --datalist, the

command lists replicas that are a part of replica set identified by the backup specification name.

--list --purge

Lists virtual disks marked for purging.

--purge [--force] [--host *ClientName*]

Removes virtual disks marked for purge. The --force option removes elements marked for deletion even if they are presented to clients. Use the --host option to change location to start the SMISDB purge operation.

--delete { --session *SessionID* | --datalist *BackupSpecName* } [--reference] [--preview] [--force] [--host *ClientName*]

Deletes information about session or backup specification from the SMISDB. Specify the --session option to delete information about the session. Specify --datalist to delete replicas associated with the specified backup specification and the linked information from SMISDB. Specify the --reference option to only delete information about the replica from the SMISDB. Use this option to remove entries that point to replicas that no longer exist on the disk array, or to make existing replicas independent from the Data Protector operation. The --preview option lists the replicas that will be deleted, but does not delete them nor does it delete the information from the SMISDB. Specify the --force option to force deletion even if replicas are presented to other hosts. Use the --host option to change the location of the deleted actions when the system from the backup session is no longer available.

--sync_check [--host *ClientName*] [--session *SessionID* | --datalist *BackupSpec*]

Compares persistent data in SMISDB with the current state of the storage system and lists the differences for all ZDB sessions. In specific circumstances, the comparison output might be incorrect, so double check whether the results reflect the actual storage system state before taking any action based on the comparison results. The --host option changes the location of comparison. Use the --datalist to check for entries related to the specified backup specification or the --session option to lists the differences for the specified session.

{ --exclude | --include } --session *SessionID*

Excludes a replica from use or includes it back for use.

You cannot use an excluded replica to:

- participate in replica set rotation
- perform instant recovery
- delete information about its ZDB session from the SMISDB

To involve an excluded replica in replica set rotation, bring it back to use:

- make it available for instant recovery
- enable deletion of its ZDB session information from the SMISDB

EXAMPLES

The following examples illustrate how the omnidbzdb command works.

1. To configure a connection to the CIMOM provider available to the Windows system "cimom_host3" in the local domain, so that the connection uses the default CIMOM service port number "5989", the user name "Cimomuser", and the password "drowssapelpmis" to connect to the CIMOM provider, execute:

   ```
   omnidbzdb --diskarray 3PAR --ompasswd --add cimom_host3 --user Cimomuser --password drowssapelpmis
   ```

2. To configure a connection to the NetApp Storage residing on "netapp_box" in the local domain, so that the connection uses the default port number "5989", the user name "NetApp_admin", and the password "netapppwd4" to connect to the NetApp Storage, execute:

   ```
   omnidbzdb --diskarray NetApp --ompasswd --add netapp_box --user NetApp_admin --password netapppwd4
   ```

3. To update the configuration of the connection to the CIMOM provider available to the system "cimom_host5.company.com" that uses SSL and the user name "administrator" to connect to the CIMOM provider, so that the Data Protector 3PAR VSS Agent and the Data Protector P6000 / 3PAR SMI-S Agent use the new password "drowssapregnorts" to connect, execute:

   ```
   omnidbzdb --diskarray 3PAR --ompasswd --add cimom_host5.company.com --ssl --password drowssapregnorts
   ```

4. To remove configuration data for connections to the NetApp storage systems available to the Windows system with the fully qualified domain name "netapp_storage5.company.com" and for which the user name "backup_operator" is used, execute:

   ```
   omnidbzdb --diskarray NetApp --ompasswd --remove netapp_storage5.company.com --user backup_operator
   ```

5. To list connection configuration data for connections to the CIMOM providers available to the system with the IP address "19.105.89.43", execute:

```
omnidbzdb --diskarray 3PAR --ompasswd --list 19.105.89.43
```

6. To verify that the Data Protector NetApp Storage integration agent can connect to the NetApp storage system using the configured user authentication data, execute:

   ```
   omnidbzdb --diskarray NetApp --ompasswd --check
   ```

7. To list all ZDB sessions where the replica is tracked for instant recovery, execute:

   ```
   omnidbzdb --diskarray 3PAR -session --ir
   ```

8. To compare the information in the SMISDB with the current state of the 3PAR StoreServe Storage system from the system "Computer", execute:

   ```
   omnidbzdb --diskarray 3PAR --sync_check --host Computer
   ```

9. To list replicas that are to be deleted from a session 2012/12/1-2, execute:

   ```
   omnidbzdb --diskarray 3PAR --delete --session 2012/12/1-2 -preview
   ```

10. To exclude a replica from use, execute:

    ```
    omnidbzdb --diskarray 3PAR --exclude --session 2013/12/1-2
    ```

SEE ALSO

omnidb(1M), omnidbcheck(1M), omnidbinit(1M), omnidbp4000(1), omnidbsmis(1), omnidbutil(1M), omnidbvss(1), omnidbxp(1), omniofflr(1M)

omnidownload

omnidownload - downloads information about a backup device and a library from the Data Protector Internal Database (IDB) (this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnidownload -version | -help

omnidownload -list_devices [-detail]

omnidownload -dev_info

omnidownload -device *BackupDevice* [-file *FileName*]

omnidownload -list_libraries [-detail]

omnidownload -library *Library* [-file *FileName*]

DESCRIPTION

Allows the user to display information about backup devices or download the configuration of the specified backup device to an ASCII file. Used together with the omniupload utility, this command enables you to create and maintain backup devices using the command-line interface.

OPTIONS

-version

Displays the version of the omnidownload command.
-help

Displays the usage synopsis for the omnidownload command.
-device *BackupDevice*

Specifies the name of the backup device you want to download to an ASCII file.
-library *Library*

Specifies the name of the library you want to download to an ASCII file.
-file *FileName*

Specifies the name of the target ASCII file for the backup device. By default, the file is created in the local directory. If this option is omitted, the data is sent to the standard output.
-list_devices

Displays information about the Data Protector backup devices. The report includes the following information for each device: device name, client, device type and pool.
-dev_info

Same as -list_devices option. Used only for compatibility with old Data Protector releases.
-list_libraries

Displays information about the Data Protector libraries. The report includes the following information for each device: library name, client and library type.

-detail

This option can be used in combination with the -list_devices and -list_libraries options to display more detailed information about the Data Protector backup devices or libraries.

EXAMPLES

The following examples illustrate how the omnidownload command works.

1. To download backup device "DAT1" into file "/tmp/DAT1", execute:

   omnidownload -device DAT1 -file /tmp/DAT1

2. To review the information about a virtual tape library named "VTL" in ASCII format that will be saved as the file "libVTL.txt" to the directory "C:\Temp", execute:

   omnidownload -library VTL -file C:\Temp\libVTL.txt

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omniiso

omniiso - primarily serves as a post-exec script to prepare the ISO image file for Enhanced Automated Disaster Recovery (EADR); can also be used as a standalone command to automate your backup and disaster recovery process
(this command is available on systems with the Data Protector Automatic Disaster Recovery component installed)

SYNOPSIS

omniiso -version | -help

omniiso [-session *FSSessionID* [*IDBSessionID*]] [-host *ClientName* [-remotehost *ClientName*]] [-cd | -net] [-out *ISOImagePath*] [-srd *SRDPath*] [-rset *P1SPath ImgPath*] [-autoinject] [-waik *WAIKPath*] [-inject_drivers *DriverPath_1 DriverPath_2* ...] [-use_raw_object] [-move_to *Path*] [-unique_name] [-exec_script *ScriptFilePath*] [-password [*Passwd*]] [-anyobj]

DESCRIPTION

The omniiso command can be used as a:

STANDALONE COMMAND

Although all functionality of the command is also available through the Disaster Recovery Wizard in the Data Protector GUI, it can also be used as a standalone command to automate your backup and disaster recovery process.

The command merges

- the recovery set (the data required for temporary DR OS installation and configuration that is created during a full client backup),
- the SRD file (a file that contains all required backup and restore object information to perform the restore),
- and the P1S file (a file that contains information on how to format and partition all disks installed in the system)

with disaster recovery installation into a disaster recovery ISO image or creates a network recovery image and saves the created image to a file on disk. By default, the DR OS image files are created in the Data Protector temporary files directory and are used to perform disaster recovery.

Such DR OS image can also be created using the EADR Wizard in the Data Protector GUI instead of this command (recommended).

POST-EXEC SCRIPT

If the command is used as a post-exec script in the EADR Wizard in the Data Protector GUI to prepare the disaster recovery ISO image, you do not have to specify parameters as their values are automatically obtained from the environment.

Tip You cannot use omniiso in a pre-exec or post-exec script to create ISO image on the Cell Manager because the IDB is backed up in a separate session.

OPTIONS

-version

Displays the version of the omniiso command.

-help

Displays the usage synopsis for the omniiso command.

-session *FSSessionID* [*IDBSessionID*]

Specifies IDs of the backup sessions that serve as the basis for updating the DR OS image file. All object backed up in the specified sessions and included in the SRD file are used for the update.

If you are updating the DR OS image file for a Data Protector client, specify the *FSSessionID* argument for the most recent full or incremental filesystem backup session that involves the entire client. If you are updating the DR OS image file for the Data Protector Cell Manager, additionally specify the *IDBSessionID* argument for an appropriate full or incremental Data Protector Internal Database backup session.

CAUTION: The specified Data Protector Internal Database backup session must be a session that was run after the specified filesystem backup session had completed. To ensure the highest consistency of the included data, the time frame between both sessions' start times should be minimal.

-host *ClientName*

Specifies the client system for which the DR OS image is created. If not specified, the local system (the system on which the command is executed) is used.

-remotehost *ClientName*

Specifies the client system where the DR OS image is created. If not specified, the system specified with -host is used.

-cd

If this option is specified, omniiso creates an ISO file that can be written to a CD-ROM. If this option is not specified, the command creates disaster recovery ISO file to be written on a backup medium.

-net

If this option is specified, omniiso creates a network recovery image file that can be then used to boot the target system over the network. If this option is not specified, the command creates disaster recovery ISO file to be written on a backup medium.

-out *ISOPath*

Specifies the location where the DR OS image is created. If this option is not specified, the DR OS image file is created in the Data Protector temporary files directory.

-srd *SRDPath*

Specifies the path to the SRD file. If the -srd option is not specified, the command creates a SRD file on the system, where omniiso is running and uses it to create the disaster recovery ISO image. If the -remotehost option is specified, the SRD file is created on the remote client.

-rset *P1SPath* *ImgPath*

Specifies the full path to the P1S file and the recovery set. If this option is not specified, the command creates the P1S file and the recovery set on the system, where omniiso is running and uses them to create the disaster recovery ISO image. If the -remotehost option is specified, the P1S and recovery set parameters specify the path on the remote client.

-autoinject

Automatically injects drivers into the DR OS image.

This option is available only for supported Windows systems.

-waik *WAIKPath*

Specifies the Windows Automated Installation Kit (WAIK) or Assessment and Deployment Kit (ADK) installation directory. If the -remotehost option is specified, the path is searched on the remote client.

This option is available only for supported Windows systems.

-inject_drivers *DriverPath_1* *DriverPath_2* ...

Injects additional drivers into the DR OS image. You must specify a full path to the driver. A maximum of 50 paths can be specified. If the -remotehost option is specified, the paths are searched on the remote client.

This option is available only for supported Windows systems.

-use_raw_object

If the specified backup session contains both filesystem and disk image backup objects for the same volume, this option specifies that a disk image backup object should be used. If this option is not specified, filesystem backup objects have a higher priority. If only one backup object for the same volume is present in the specified backup session, this option is ignored.

-anyobj

Enables you to create a recovery image even if the specified backup session does not contain all client volumes. Note that all host critical volumes must be part of the specified backup session:

- the boot and system volumes
- the Data Protector installation volume
- the volume where the CONFIGURATION object is located
- the Active Directory database volume (in case of an Active Directory controller)
- the quorum volume (in case of a Microsoft Cluster)

-password [*Passwd*]

Specifies the password that is used during the creation of the recovery media. By using a password you can prevent unauthorized use of the recovery media after boot. If you only specify the -password option without a password, the command will prompt you to provide one at the start of the image creation process.

-move_to *Path*

Moves the DR OS image file to the specified location.

-unique_name

Renames the ISO image file to a unique name consisting of the platform type (Windows, Linux), followed by the client name, platform type (amd64, ia64), the date and time when the image was created, and the system BIOS UUID. All name components are separated by the '#' character. For example:

windows#computer.company.com#amd64#2013-04-25-09-03#844D978B-1D69-BC7D- EB0D-3B93628059A1.iso

-exec_script *ScriptFilePath*

Executes the specified script after the DR OS file is created. The executed script receives the full path of the DR OS recovery image. You can use scripts to automate various image post-processing tasks.

> Some options, like move_to Path , -exec_Script ScriptFilePath , and -unique_name , are not applicable to remote ISO generation, but applicable to only local ISO generation.

NOTES

- The omniiso command is available on Windows and Linux systems only.
- If the BTRFS volume is detected, you get the following **Warning** message:

  Warning: BTRFS volume detected. Make sure that you have included all the BTRFS sub volumes in the specified version.

EXAMPLES

The following examples illustrate how the omniiso command works.

- To create and save a disaster recovery ISO file for a Data Protector Windows client in the CD-ROM-ready format at "C:\iso\dr\omnidr.iso" on the local system, containing objects backed up in the session with the session ID "2013/05/16-23", using information stored in the SRD and P1S files stored in "C:\iso\dr\srd\machine101.company.com" and "C:\iso\dr\p1s\machine101.company.com", using the recovery set stored in "C:\iso\dr\img\machine101.company.com.img", execute:

```
omniiso -session 2013/05/16-23 -cd

-out c:\iso\dr\omnidr.iso

-srd C:\iso\dr\srd\machine101.company.com

-rset C:\iso\dr\p1s\machine101.company.com

C:\iso\dr\img\machine101.company.com.img
```

- To create and save a disaster recovery ISO file for a Data Protector Windows client in the CD-ROM-ready format at "C:\iso\dr\omnidr.iso" on the local system, containing objects backed up in the session with the session ID "2013/05/22-23", using information stored in the SRD and P1S files stored in "C:\iso\dr\srd\machine102.company.com" and "C:\iso\dr\p1s\machine102.company.com", using the recovery set stored in "C:\iso\dr\img\machine102.company.com.img" where the drivers are automatically injected, execute:

  ```
  omniiso -session 2013/05/22-23 -cd

  -out C:\iso\dr\omnidr.iso

  -srd C:\iso\dr\srd\machine102.company.com

  -rset C:\iso\dr\p1s\machine102.company.com

  C:\iso\dr\img\machine102.company.com.img -autoinject
  ```

- To create and save a disaster recovery ISO file for a Data Protector Linux client in the CD-ROM-ready format at "/data/iso/dr/omnidr.iso" on the local system, containing objects backed up in the session with the session ID "2013/04/12-35", using information stored in the SRD and P1S files stored in "/etc/opt/omni/server/dr/srd/machine106.company.com" and "/etc/opt/omni/server/dr/p1s/machine106.company.com", using the recovery set stored in "/etc/opt/omni/server/dr/p1s/machine106.company.com.img", execute:

  ```
  omniiso -session 2013/04/12-35 -cd

  -out /tmp/omnidr.iso

  -srd /etc/opt/omni/server/dr/srd/machine106.company.com

  -rset /etc/opt/omni/server/dr/p1s/machine106.company.com

  /etc/opt/omni/server/dr/p1s/machine106.company.com.img
  ```

- To create and save a disaster recovery network image for the Data Protector Cell Manager system “machine202.company.com” at "C:\iso\dr\omnidr.iso", containing objects backed up in the sessions with the session IDs "2013/04/12-43" and "2013/04/12-44", using information stored in the SRD and P1S files stored in "C:\iso\dr\srd\machine102.company.com" and "C:\iso\dr\p1s\machine102.company.com", using the recovery set stored in "C:\iso\dr\img\machine102.company.com.img" where the drivers are automatically injected, and with the image protected by a password which must be provided from the command prompt, execute:

  ```
  omniiso -session 2013/04/12-43 2013/04/12-44 -net

  -host machine202.company.com

  -out C:\iso\dr\omnidr.iso

  -srd C:\iso\dr\srd\machine102.company.com

  -rset C:\iso\dr\p1s\machine102.company.com

  C:\iso\dr\img\machine102.company.com.img -autoinject -password
  ```

- To create and save a disaster recovery ISO file for a Data Protector Microsoft Windows client in the CD-ROM-ready format at "C:\iso\dr\omnidr.iso" on the local host "10.1.1.1", containing objects backed up in the remote host "10.1.1.2" with the session ID "2019/01/11-2", using information stored in the SRD and P1S files in "c:\recovery.srd", using the recovery set stored in "c:\recovery.img", execute:

  ```
  omniiso -session 2019/01/11-2 -cd

  -out C:\iso\dr\omnidr.iso

  -host 10.1.1.1

  -remotehost 10.1.1.2

  -rset C:\Temp\10.1.1.2

  -srd C:\recovery.srd C:\recovery.img

  -waik "C:\Program Files\Windows AIK"
  ```

- To run `omniiso` from a post-exec script, execute:

  ```
  omniiso -cd -out /export/EADR_$HOSTNAME.iso
  ```

  Ensure that the required user rights in the Data Protector user list are included. To allow `omniiso` to be executed from a backup session, the following user rights are required, else the error message `Error updating SRD file objects [error: -10]. Aborting` is displayed:

Linux clients : The operator group membership is required for user root and group root.

Windows clients: The user SYSTEM , group NT AUTHORITY .

SEE ALSO

omnidr(1M), omniofflr(1M), omnisrdupdate(1M), omniusb(1)

omnimcopy

omnimcopy - makes a copy of a Data Protector medium using Data Protector backup devices as the source and destination (this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnimcopy -version | -help

omnimcopy -copy *BackupDevice* [-slot *Slot* ...] -from *BackupDevice* [-src_slot *Slot* ...] [*BasicOptions*] [*LabelOptions*]

BasicOptions

-pool *PoolName*

-location *Location*

-force

-size *SpecSize*

-encrypt

-eject

-permanent | -until *Date*

Date = [YY]YY/MM/DD (1969 < [YY]YY < 2038)

LabelOptions

-label *UserLabel* [-no_barcode_as_label] | -autolabel | -[no_]barcode_as_label

DESCRIPTION

The omnimcopy copies a Data Protector medium. It reads data from the input medium and writes the data to the output medium. Note that the output medium is first initialized. During initialization, a medium is assigned a:

- Data Protector Medium Label: Depending on the selected options, the media labels can be user defined or generated automatically. By default, Data Protector automatically generates media labels from the media pool names, unless the Use barcode as media label during initialization option is selected in the library properties. This behavior can be changed during the initialization of media using -barcode_as_label , -no_barcode_as_label and MediumLabel options.
- Medium ID (system-assigned)
- Location

The physical devices used for the input and output must be the same device type and have the same block size. This copy functionality allows the user to use multiple tapes in order to implement vaulting with Data Protector. This copy function is a separate function within Data Protector and cannot be done automatically during backup. Main advantage of this implementation is that all devices can be used during backup (better performance).

The source and destination devices are backup devices which means they can be located everywhere in the Data Protector cell. During the copy the destination tape will be initialized before all data from the source tape is copied.

The writing destination tape will ignore the early end of tape mark and will write until the physical EOT is reached. If the space on the destination is not sufficient to keep the whole original tape the copy has to be restarted with a new tape.

After a copy operation both media are tracked in the media management database.

This enables also a listing of the copies for an original media as well as the listing of the original tape for a copy. If a mount request is issued during a restore session all tapes which contains the data will be listed (original and copies).

After the operation copy both tapes become nonappendable.

A copy of a copy is not possible.

If the original media get obsolete in the database, which means it is overwritten or it is exported from the cell, the first copy becomes automatically the original tape.

OPTIONS

-version

Displays the version of the omnimcopy command
-help

Displays the usage synopsis for the omnimcopy command
-copy *BackupDevice* [-slot *Slot* ...]

Specifies the output backup device - the device used to create a copy of the medium (target medium).
-from *BackupDevice* [- src_slot *Slot* ...]

Specifies the input backup device - the device which is used as a source. You can specify only one slot. The -src_slot parameter takes the barcode value of the source tape.
-pool *PoolName*

Specify the poolname to which the copy of the medium is added. By default the medium is added to the source media poolname.
-location *Location*

Specifies the location of the media, when you keep them out of the library. Used for the vaulting purposes.
-force

Overwrites the data on the target medium even if this data is still protected by the Data Protector media management system. Note that this option must be used with an unprotected medium as well.
-size *SpecSize*

This option specifies the size of the target medium.
-encrypt

This option turns on hardware encryption on all destination drives.
-eject

Ejects the target medium from the drive after the medium is copied.
-permanent

This backup protection option provides permanent protection of backup media. This means that the data is permanently protected from being overwritten.
-until *Date*

This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.

-label *UserLabel*

Manually specify the medium label for the copy of the medium. A description can have a maximum of 80 characters, including any keyboard character or space. If the Use barcode as medium label on initialization option is selected in the library properties, you have to specify also the -no_barcode_as_label option.

-autolabel

If this option is specified, the medium is labeled automatically by the Data Protector media management system.

-barcode_as_label

Data Protector uses barcode as a medium label during the initialization of the medium instead of generating media labels based on the media pools names. This option is supported only on library devices with enabled barcode support.

-no_barcode_as_label

Data Protector does not use barcodes as a medium label during the initialization of the medium, but generates media labels based on the media pools names. This option can be used to override the Use barcode as medium label on initialization option (if it is selected) in the library properties in the Data Protector GUI.

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omniminit

omniminit - initializes a Data Protector medium
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniminit -version | -help

omniminit -init *BackupDevice* [*MediumLabel*] [*BasicOptions*] [*SlotOptions*] [-no_barcode_as_label]

omniminit -init *BackupDevice* [*BasicOptions*] [*SlotOptions*] [-barcode_as_label]

omniminit -init_magazine *BackupDevice* [*MagazineDescription*] [*BasicOptions*]

omniminit -init_mag_medium *BackupDevice* *MagazineDescription* [*BasicOptions*] [*SlotOptions*]

omniminit -preerase *BackupDevice* [*SlotOptions*] [-eject]

BasicOptions

-force

-pool *PoolName*

-size *n*

-location *OffLineLoc*

-wipe_on_init

-eject

SlotOptions

-slot *SlotID* [*Side*]

DESCRIPTION

The omniminit command initializes a backup medium. During initialization, a medium is assigned a:

- Data Protector Medium Label: Depending on the selected options, the media labels can be user defined or generated automatically. By default, Data Protector automatically generates media labels from the media pool names, unless the Use barcode as media label during initialization option is selected in the library properties. This behavior can be changed during the initialization of media using -barcode_as_label , -no_barcode_as_label and MediumLabel options.
- Medium ID (system-assigned)
- Location

This information is added to the Data Protector Internal Database (IDB) and the medium is added to a Data Protector media pool. Medium ID is its unique identifier. The Medium Label does not necessarily have to be unique, but it is recommended. The medium location is optional, and can be used to define an offline location for the medium.

OPTIONS

-version

Displays the version of the omniminit command.

-help

Displays the usage synopsis for the omniminit command.

-init *BackupDevice* [*MediumLabel*]

Specifies two items: the name of the *BackupDevice* where the medium is mounted and the *MediumLabel* which is assigned to the medium by Data Protector after initialization. The *MediumLabel* can be up to 32 characters long. Any printable character, including spaces, can be used. The text must be enclosed in quotation marks.

-init_magazine *BackupDevice* [*MagazineDescription*]

Specifies two items: the name of the *BackupDevice* where the magazine is mounted and the *MagazineDescription* (optional) which is assigned to the magazine. Note that the *MagazineDescription* must be unique for each magazine. The description is also used for assigning *MediumLabel* to each medium.

-init_mag_medium *BackupDevice MagazineDescription*

Initializes single medium from magazine. *BackupDevice* specifies the device where the magazine is mounted. *MagazineDescription* must also be specified to identify the magazine. Note that single medium from the magazine can be initialized only if the magazine has been initialized before and therefore has a unique *MagazineDescription*.

-preerase *BackupDevice*

Pre-erases the optical disk. Pre-erasing a medium enables backups which are twice as fast. This is because the pre-erase step is removed from the backup process. For best performance, optical disks should be pre-erased before each backup.

-force

Overrides the initialization safety checks. By default, a medium containing protected data or being in a non-Data Protector format cannot be initialized.

-pool *PoolName*

Specifies the name of the media pool to which this medium will be added. If no *PoolName* is specified, the medium is added to the default pool for the specified backup device.

-slot *SlotID* [*Side*]

Specifies the *SlotID* of the exchanger backup device where the medium is mounted. This option is only valid for this backup device type, but must be given for magneto-optical devices. To specify the side of the platter in this slot, use the additional *Side* parameter. Values of *Side* are A or B.

-size *n*

Specifies the medium capacity in MB. If not specified, Data Protector uses the standard capacity of the media class used with the backup device selected for initialization. The size is later used to calculate the free space remaining on the medium. (FreeSpace = Size - SpaceUsed)

-location *OffSiteLoc*

Specifies the location of the medium. This information is useful if media is stored off-site. The location can have maximum 32 characters. Any printable character, including spaces, can be used. The text must be enclosed in quotation marks.

-wipe_on_init

Wipes the data on medium after it has been initialized. This is done by overwriting the data on medium so it is impossible to restore the original data on medium after it has been wiped.

-barcode_as_label

Data Protector uses barcode as a medium label during the initialization of the medium instead of generating media labels based on the media pools names. This option is supported only on library devices with enabled barcode support.

-no_barcode_as_label

Data Protector does not use barcodes as a medium label during the initialization of the medium, but generates media labels based on the media pools names. This option can be used to override the Use barcode as medium label on initialization option (if it is selected) in the library properties in the Data Protector GUI.

EXAMPLES

The following examples illustrate how the omniminit command works.

1. To initialize slot "4" of backup device "ADIC" with medium label "Label4", in location "Backup Room", execute:

   omniminit -init ADIC Label4 -slot 4 -location "Backup Room"

2. To preerase slot "8" side "A" of magneto-optical tape library unit "MO_Changer", execute:

   omniminit -preerase MO_Changer -slot 8 A

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnimlist

omnimlist - lists the contents of a Data Protector medium
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnimlist -version | -help

omnimlist -device *BackupDevice* [-slot *SlotID* [*Side*]] [-monitor] [-detail]

omnimlist -device *BackupDevice* [-slot *SlotID* [*Side*]] [-header] [-monitor]

omnimlist -device *BackupDevice* -session [-slot *SlotID* [*Side*]] [-monitor] [-detail]

omnimlist -device *BackupDevice* -session *SessionID* [-slot *SlotID* [*Side*]] [-monitor] [-detail]

omnimlist -device *BackupDevice* -catalog [-slot *SlotID* [*Side*]] [-monitor]

omnimlist -device *BackupDevice* -catalog *DiskAgentID* [-slot *SlotID* [*Side*]] [-monitor]

DESCRIPTION

The omnimlist command lists the contents of a Data Protector medium. The command scans the catalog (index) of the medium and shows all objects and sessions on the medium.

The command can also be used to display the Data Protector medium tape header. If used for such purpose, the command reads the first block of the tape and then displays the information.

OPTIONS

-version

Displays the version of the omnimlist command.

-help

Displays the usage synopsis for the omnimlist command.

-device *BackupDevice*

Specifies the *BackupDevice* where the medium is mounted. If no other option is specified the command lists all sessions and all their objects.

-slot *SlotID* [*Side*]

Specifies the *SlotID* of the library where the medium is mounted. This option is only valid for this backup device type, but must be given for magneto-optical devices. To specify the side of the platter in this slot, use the additional *Side* parameter. Values of *Side* are A or B .

-session [*SessionID*]

Displays information about the sessions on the medium. If no *SessionID* is specified, all sessions are shown. This reports shows for each session: the *SessionID*, Session Type, Session Status. For the user who initiated the session it shows: the UNIX Login, UNIX Group, and ClientName. If a *SessionID* is specified, the objects for that session are shown. The session report shows for each object: the Client, Mountpoint, Object Label, Disk Agent ID and Object Status.

-catalog [*DiskAgentID*]

Displays the Detail Catalog for single or multiple objects. The catalog shows file information for all the files included in the backup of the object in that session. The *DiskAgentID* is used to uniquely identify the backup object-session combination. If not specified all found objects are processed.

-monitor

Displays information about the Medium (Pool, Medium ID, Medium Label, Location, and Initialization date/time), the Session (Session ID, Owner, Datalist used, and Start date/time), Objects (Type, Start date/time, Backup Mode), and Session (Client, Mountpoint, Object Label, Disk Agent ID, and Object Status).

-header

The command first checks if the media header is in Data Protector format and if it is corrupted. If the media header is not in Data Protector format or if it is corrupted, an appropriate message is displayed. Otherwise the following information from the media header is displayed: medium ID, medium label, medium location, initialization date, last access date, last write date, last overwrite date, number of writes, number of overwrites, pool label, device information, device capacity, tape format version, medium ID from original tape (for replicated media only), medium data format type and medium data format subtype. For random access media, date and time information (last access date, last write date and last overwrite date) is updated every time the medium is accessed/written/overwritten. For all other media, header information is not updated except when initializing the medium.

-detail

Displays detailed information about the selected query.

NOTES

For the -header option, the following limitation applies: the command displays the header information stored on the medium, ignoring possible updates in the Data Protector Internal Database (IDB).

EXAMPLES

The following examples show how the omnimlist command works.

1. To list sessions and corresponding Disk Agents from device "DAT2", execute:

   omnimlist -device DAT2 -monitor

2. To list sessions on slot "43" side "B" of a magneto-optical tape library unit "MO_Changer", execute:

   omnimlist -device MO_Changer -slot 43 B -session

3. To list all Disk Agents for the session "2013/05/13-23" on the device "Exa8500", execute:

   omnimlist -device Exa8500 -session 2013/05/13-23

4. To list the catalog for the object-session combination with the DiskAgentID "774226832", from the medium located in slot "7" of device "Herstal2", execute:

```
omnimlist -device Herstal2 -slot 7 -catalog 774226832
```

5. To display media header for the medium in the backup device named "dev_1", execute:

```
omnimlist -device dev_1 -header
```

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnimm

omnimm - provides media management for Data Protector
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnimm -version | -help

omnimm -create_pool *PoolName* [AmazonS3Glacier_Pool | AmazonS3Deep_Pool | B2D_Pool] *MediaType* [S3-Glacier-Compatible | S3-Glacier-Deep-Archive-Compatible | Deduplication store] [*Policy AgeLimit MaxOverWrites*] [-[no_]alloc_uninit_first] [-[no_]free_pool [*FreePoolName*]] [-[no_]move_free_media]

omnimm -modify_pool *PoolName NewPoolName* [*Policy AgeLimit MaxOverWrites*] [-[no_]alloc_uninit_first] [-[no_]free_pool [*FreePoolName*]] [-[no_]move_free_media]

omnimm -create_free_pool *PoolName MediaType* [*AgeLimit MaxOverWrites*]

omnimm -modify_free_pool *PoolName NewPoolName* [*AgeLimit MaxOverWrites*]

omnimm -create_mag_pool *PoolName MediaType* [*Policy AgeLimit MaxOverWrites*]

omnimm -modify_mag_pool *PoolName NewPoolName* [*Policy AgeLimit MaxOverWrites*]

omnimm -remove_pool *PoolName*

omnimm -remove_mag_pool *PoolName*

omnimm -show_pools [*PoolName*]

omnimm -move_medium *Medium ToPoolName*

omnimm -move_magazine *MagazineDescription NewPoolName*

omnimm -modify_medium *Medium NewMediumLabel NewLocation*

omnimm -modify_magazine *MagazineDescription NewLocation* [*NewMagazineDescription*]

omnimm -reset_poor_medium *Medium*

omnimm -reset_wp_medium *Medium*

omnimm -list_pool [*PoolName*] [-detail]

omnimm -show_pool_alloc *PoolName*

omnimm -list_scratch_media *PoolName* [-detail]

omnimm -show_repository_alloc *Library PoolName* [-detail]

omnimm -list_media *Medium* [-detail | -encryptioninfo]

omnimm -list_appendable_media *PoolName*

omnimm -list_copy *Medium*

omnimm -media_info *Medium* [-detail | -encryptioninfo]

omnimm -list_magazines_of_pool *PoolName* [-detail]

omnimm -list_media_magazine *MagazineDescription* [-detail]

omnimm -catalog *Medium*

omnimm -check_protection *Medium*

omnimm -recycle *Medium*

omnimm -recycle_magazine *MagazineDescription*

omnimm -export *Medium*

omnimm -export_magazine *MagazineDescription*

omnimm -copy_to_mcf { *Medium1* [*Medium2...*]} [-output_directory *Pathname*]

omnimm -import *LogicalDevice* [-slot *SlotID* [*Side*]] [-no_log | -log_dirs | -log_file | -log] [-pool *PoolName*] [-import_as_original]

omnimm -import_catalog *LogicalDevice* [-slot *SlotID* [*Side*]] [-no_log | -log_dirs | -log_file | -log]

omnimm -import_magazine *LogicalDevice* [*MagazineDescription*] [-slot *SlotID* [*Side*]] [-no_log | -log_dirs | -log_file | -log] [-pool *PoolName*] [-import_as_original]

omnimm -import_from_mcf { *File* ...} [[-pool_prefix *PoolPrefix*] | [-no_pool_prefix]] [-[no_]orig_pool] [-import_as_original]

omnimm -disable_lockname *LockName*

omnimm -enable_lockname *LockName*

omnimm -disable_device *DeviceName* [-ignore_lockname]

omnimm -enable_device *DeviceName* [-ignore_lockname]

omnimm -repository *LibraryName*

omnimm -repository_barcode_scan *LibraryName*

omnimm -repository_update *DriveName* [-slot *SlotID* [*Side*]]

omnimm -add_slots *LibraryName* { *Slot* ... | *FromSlot-ToSlot* ...}

omnimm -remove_slots *LibraryName* { *Slot* ... | *FromSlot-ToSlot* ...}

omnimm -silo_query *LibraryName* [-range *FromSlot-ToSlot*]

omnimm -silo_enter *LibraryName* -cap *CapID*

omnimm -silo_eject *LibraryNme* { *Volser* ... | *FromVolser-ToVolser* ...} -cap *CapID* [-location *Location*]

omnimm -enter *LibraryName* { *Slot* ... | *FromSlot-ToSlot* ...}

omnimm -eject *LibraryName* { *Slot* ... | *FromSlot-ToSlot* ...} [-location *Location*]

omnimm -group *PoolName* *MagazineDescription* *Medium* ...

omnimm -ungroup *MagazineDescription*

omnimm -reload_serial_number *DeviceName*

omnimm -show_locked_devs [-all]

omnimm -delete_unprotected_media [Library|-all] [-force]

omnimm -merge_library sourceLibrary destinationLibrary [-nofallback]

Policy =

Loose |

Strict |

App+Loose |

App+Strict |

AppIncr+Loose |

AppIncr+Strict

Medium =

Medium_Label |

Barcode |

Medium ID

Basic Options =

-force

-pool *PoolName*

-size *n*

-location *OffLineLoc*

-eject

DESCRIPTION

The main purpose of *media management* is to protect valuable user data.

To achieve this goal Data Protector provides the following functionality: protecting data from being overwritten, detecting and tracking bad or old media, utilizing and reporting space in auto changers, use of media within pools, drive cleaning, detecting standard tape and magneto-optical format. All this information is stored into the Data Protector Internal Database.

The omnimm command manages media pools, checks the protection of a medium, maintains and updates the contents of the repository in the library.

Protecting data is more than just stopping Data Protector from overwriting the tape. The detection of an old and poor media informs the administrator before data loss so that he can react before he needs to restore the data and tape will never be used for backups again. This means protection of data which are on Data Protector tapes and protection for data which is still on the system and needs to be backed up.

Data Protector has the concept of *media pools* to manage large numbers of cartridges. Pools are logical collection of cartridges with same common media or data properties. One pool can only contain media of one type. Data Protector support several media *pool policies* :

- *Loose* (loose, non-appendable); When Data Protector prompts for a medium and loose policy is selected, any medium in the defined pool will be accepted.
- *Strict* (strict, non-appendable); Data Protector decides which medium must be inserted for backup and only this medium will be accepted.
- *App+Loose* (loose, appendable);
- *App+Strict* (strict,appendable);
- *AppIncr+Loose* (loose, appendable for incrementals);
- *AppIncr+Strict* (strict, appendable for incrementals).

OPTIONS

-version

Displays the version of the omnimm command

-help

Displays the usage synopsis for the omnimm command

-create_pool *PoolName MediaType* [*Policy AgeLimit MaxOverWrites*]

Creates a new pool with *PoolName* for the medium of *MediaType* with the policy defined by *Policy*. Supported policies are: Loose, Strict, App+Loose, App+Strict, AppIncr+Loose and AppIncr+Strict. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

-[no_]alloc_uninit_first

Option -noalloc_uninit_first sets/resets "Use uninitialized media first" pool policy. This option can be used with *Loose* policy only.

-[no_]free_pool [FreePoolName]

If -free_pool is set, the pool is linked to the free pool specified with FreePoolName in order to share free media. Condition factors are inherited from the free pool. If the -no_free_pool is set, the pool is not linked. The default setting is -no_free_pool .

-[no_]move_free_media

The -move_free_pool option can only be set if the -free_pool option was set. If -move_free_media is set, de-allocation of free media from a regular to a free pool is done automatically. If -no_move_free_media is set, there is no automatic de-allocation of free media. The default setting is -no_move_free_media .

-modify_pool *PoolName NewPoolName* [*Policy AgeLimit MaxOverWrites*]

Renames the pool *PoolName* into *NewPoolName*. The *Policy*, *AgeLimit* and *MaxOverWrites* can also be changed. Supported policies are: Loose, Strict, App+Loose, App+Strict, AppIncr+Loose and AppIncr+Strict. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

-create_free_pool *PoolName MediaType* [*AgeLimit MaxOverWrites*]

Creates a new free pool with *PoolName* for the medium of *MediaType*. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

-modify_free_pool *PoolName NewPoolName* [*AgeLimit MaxOverWrites*]

Renames the free pool *PoolName* into *NewPoolName*. The *AgeLimit* and *MaxOverWrites* can also be changed. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

-create_mag_pool *PoolName MediaType* [*Policy AgeLimit MaxOverWrites*]

Creates pool *PoolName* with magazine support.

-modify_mag_pool *PoolName NewPoolName* [*Policy AgeLimit MaxOverWrites*]

Renames the magazine pool *PoolName* into *NewPoolName*. The *Policy*, *AgeLimit* and *MaxOverWrites* can also be changed. *Age Limit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

-remove_pool *PoolName*

Removes the pool specified by *PoolName*.

-remove_mag_pool *PoolName*

Removes the magazine pool specified by *PoolName*.

-show_pools [*PoolName*]

Shows media from the specified *PoolName* pool or from all pools if *PoolName* is omitted.

-move_medium *Medium ToPoolName*

Moves medium from the current pool to the pool specified by *ToPoolName*.

-move_magazine *MagazineDescription NewPoolName*

Moves magazine *MagazineDescription* from the current pool to the pool specified by *NewPoolName*.

-modify_medium *Medium NewMediumLabel NewLocation*

Modifies medium with the specified *Medium*. Note that you should always enter the medium label *NewMediumLabel* and location *NewLocation* in that sequence.

-modify_magazine *MagDescription NewLocation* [*NewMagDescription*]

Changes the location of the magazine *MagDescription* to *NewLocation*. If *NewMagDescription* is specified, it is assigned to the magazine as a new MagazineDescription. Note that each magazine must have a unique MagazineDescription.

-reset_poor_medium *Medium*

Resets the media condition factors. Once the medium has expired (its maximum usage criteria), it is marked as poor and can no longer be used for backup. This option resets the medium quality status, thus enabling it to be used for backup. You have to be very cautious using this option, because a backup stored on an expired medium might not be recoverable.

-reset_wp_medium *Medium*

Removes the write-protected flag for the specified medium from the MMDB, thus making the medium available for writing.

-list_pool [*PoolName*] [-detail]

Displays all the media from pool *PoolName*. The report shows: medium label, status, location, appendability and protection. Appendability is shown under item FULL. If displayed status under FULL is "YES" then medium is unappendable, otherwise it is appendable. If *PoolName* is not specified, the command lists all the configured media pools. This report shows: pool name, status, media class, the number of media and free space in pool.

-detail

Displays information in a more detailed format.

-show_pool_alloc *PoolName*

Displays the sequence in which the media from the specified pool will be used for backup. The report shows: sequence, medium label and location.

-list_scratch_media *PoolName*

Displays media from the specified pool which are not protected and can be used for backup. The report shows sequence, medium label and location.

-show_repository_alloc *Library PoolName*

Displays the order in which the media in the repository of the specified *Library* and *pool* will be used. The report shows: sequence, medium label, location and slot number.

-list_media *Medium*

Displays all the objects, their type and their protection status for the medium you specified. If an object is spanned across more than one media, the returned Object size refers to the absolute size of the Object, and not the size stored on a specific media.

The VADP feature provides enhanced reports for Virtual Machines. The reports display VMware virtual machines in the same way as Data Protector clients called VADP clients. The object name must use the VM name as reported from `omnicell info -cell brief` command, where object name is `<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]`. Here, `<hostname>` is DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

-list_appendable_media *PoolName*

Displays all appendable media from the specified media pool.

-list_copy *Medium*

List all copies of the given medium.

-media_info *Medium*

Displays information on the given medium.

-encryptioninfo

Displays detailed encryption information for objects on the specified medium.

-list_magazines_of_pool *PoolName*

Lists magazines of the pool *PoolName*.

-list_media_magazine *MagazineDescription*

Lists all the media in specified magazine.

-catalog *Medium*

Lists catalog for all object versions located on the specified medium. Only files located on this medium are displayed.

-recycle *Medium*

Resets the protection of data on medium. The present data can now be overwritten and medium can be used to store new data.

-recycle_magazine *MagazineDescription*

Recycles all media of specified magazine.

-export *Medium*

Purges from the database all data associated with the medium and the object versions it contains. This option is used when the medium will no longer be used for backup in this cell. A medium containing protected data cannot be exported.

-export_magazine *MagazineDescription*

Exports all media of specified magazine.

-copy_to_mcf *Medium*

Copies media-related catalog data into media container format (MCF) files, which you can transfer to anotherCell Manager, thus enabling you to import all media-related information on anotherCell Manager where it is then available for browsing. The media-related catalog data are not removed from the original Cell Manager. You can specify one or more media by either medium ID or medium label.

-output_directory *Pathname*

Specifies the directory where MCF files are stored. You must specify a full path to the files. If not specified, the files are by default copied on the Cell Manager to the directory Data_Protector_program_data\Config\Server\export\mcf (Windows systems) or /var/opt/omni/server/export/mcf (UNIX systems).

-import *LogicalDevice*

Imports a medium from a different cell. The medium is put in the default pool of the specified backup device. Information about the new medium is added to the database. Slot side must be specified for magneto-optical devices.

-no_log

Used with the -import option, this option omits the detail part of the catalog from the import.

-log

Used with the -import option, this option logs all detailed information of the backed up directory such as versions, numbers, and attributes.

-log_dirs

Used with the -import option, this option imports only the detail part of the directories.

-pool *PoolName*

Specifies the name of the pool.

-import_catalog *LogicalDevice*

Rereads the Detail Catalog from the specified device into the database, in case this information has been deleted. If the Detail Catalog for the specified medium already exists in the database, import will fail.

-import_magazine *LogicalDevice* [*MagazineDescription*]

Imports a magazine from a different cell. The magazine is put in the default pool of the specified backup device. Information about the new magazine and its media is added to the database.

-import_from_mcf *File* ...

Imports one or more MCF files that contain copies of media-related catalog data from the originalCell Manager. You must specify full paths to the files on the current Cell Manager.

-pool_prefix

Specifies an optional prefix for a media pool to which you want to import MCF files with media-related catalog data copies. If this option is not specified, the default prefix IMPORTED is used.

If the -no_pool_prefix option is set, no prefix is generated for a pool.

-[no_]orig_pool

Specifies a media pool for import. By default, the -orig_pool option is set.

It can be disabled with the -[no_]orig_pool option.

-import_as_original

Imports a medium copy or a medium-related catalog data copy as original if an original medium does not exist in a database.

-disable_lockname *LockName*

Disables devices with the *LockName* for any operation. The *LockName* must be defined using the Data Protector GUI or using the omniupload command.

-enable_lockname *LockName*

Enables devices with the *LockName*. The *LockName* must be defined using the Data Protector GUI or using the omniupload command.

-disable_device *DeviceName* [-ignore_lockname]

Disables the device with the *DeviceName* for any operation. The *DeviceName* must be defined using the Data Protector GUI or using the omniupload command. Unless the option -ignore_lockname is specified, if the device has a lockname defined, all devices with the same lockname are also disabled.

-enable_device *DeviceName* [-ignore_lockname]

Enables the device with the *DeviceName*. The *DeviceName* must be defined using the Data Protector GUI or using the omniupload command. Unless the option -ignore_lockname is specified, if the device has a lockname defined, all devices with the same lockname are also enabled.

-repository *LibraryName*

This option is used to specify the repository backup device that you want to check. This information is then used to update the database.

-repository_barcode_scan *LibraryName*

If this option is used then barcode reader is used to update the database. This option should be used only with devices that have enabled barcode reader.

-repository_update *DriveName*

Updates the database by reading all the slots (loads media in drive) in the device repository. If you additionally specify the slot number of the slot that is defined for a CL cartridge, then a cleaning operation is performed on the specified drive.

-slot *SlotID* [*Side*]

Specifies the *SlotID* of the library where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter in this slot, use the additional *Side* parameter. Slot *SlotID* must be specified for magneto-optical devices. Values of *Side* are A or B.

-add_slots *LibraryName* { *Slot*... | *FromSlot*-*ToSlot*...}

Adds slots to the selected library. With ADIC/GRAU DAS or StorageTek ACS libraries, this option adds volsers to the selected library. Make sure you use a format supported by your library. For example, when adding slots to a SCSI library, do not use letters or leading zeros.

-remove_slots *LibraryName* { *Slot*... | *FromSlot*-*ToSlot*...}

Removes slots from the selected library.

-silo_query *LibraryName*

Queries ACS/DAS server for the list of currently resident volsers and updates the Data Protector repository of specified library. This option is not recommended to be used with an ACS/DAS Server when querying logical libraries configured for the same physical library. In such a case, use the -add_slots option to add volsers manually.

With DAS Server, however, when logical libraries are not configured using Data Protector, but using the DAS utilities, the Data Protector query operation can safely be used on such libraries instead of adding volsers manually.

-silo_enter *LibraryName*

Moves ACS/DAS media from the CAP (ACS) or insert/eject area (DAS) to the repository.

-cap *CapID*

ID of Control Access Port of ACS or insert/eject area of DAS library.

-silo_eject *LibraryName* { *Volser* ... | *FromVolser* - *ToVolser* ...}

Moves media from the ACS/DAS repository into the CAP.

-location *Location*

Specifies the new location for the ejected media. Only media with barcode will be updated.

-enter *LibraryName* { *Slot* ... | *FromSlot* - *ToSlot* ...}

Moves media from the mail slots to the repository slots. This option is available only for SCSI libraries.

-eject *LibraryName* { *Slot* ... | *FromSlot* - *ToSlot* ...}

Moves media from the repository slots into the mail slots. This option is available only for SCSI libraries.

-group *PoolName MagazineDescription Medium* ...

Creates a magazine *MagazineDescription* out of the specified non-magazine media. Note that all specified media must be resident in the same SCSI library at the time. The magazine is added to the pool *PoolName* which must be configured to support magazines.

-ungroup *MagazineDescription*

Splits the magazine *MagazineDescription* so that the magazine media become non-magazine media.

-reload_serial_number *DeviceName*

Reloads the device serial number and overwrites the serial number stored in the Internal Database. A physical device can therefore be replaced without changing the logical device properties.

-show_locked_devs [-all]

Lists all locked devices, target volumes, media, and slots in the Data Protector cell. The -all option applies only when you execute the command on a MoM system, in which case locked devices, target volumes, media, and slots from all cells are listed.

-delete_unprotected_media [Library|-all] [-force]

This option is used for deleting unprotected media. This process is automatically carried out by Data Protector during its maintenance window. To trigger it when required, use the command with the options shown here.

Library - This option deletes all unprotected media for a specific B2D library.

all - This option deletes all unprotected media belonging to all the B2D devices.

force - This option makes Data Protector delete a medium from the IDB, even if the deletion process reports an error for that entry.

-merge_library sourceLibrary destinationLibrary [-nofallback]

This option is used to merge gateways of StoreOnce Backup system or Data Domain Boost devices (configured using FC identifiers) to IP- based devices. This enables the gateways to support multi-interface access.

After migration is complete, all gateways from the source library are, by default, set to use the FC paths, with an option to fall back to an IP path.

Note that you can *only* merge from DDBoost to DDBoost or StoreOnce to StoreOnce and only from FC to IP. Also, the media pools for the migrated gateways are not changed. If required, you can change the gateway pools using the DP GUI.

sourceLibrary - The library configured with an FC interface (DDBoost or StoreOnce System).

destinationLibrary - The library configured with an IP interface (DDBoost or StoreOnce System).

nofallback - This option can be specified to prevent migrated gateways from falling back to IP paths in case of errors.

RETURN VALUES

See the man page omniintro for return values.

Additional return values of the omnimm command are:
1 - Program failed, user error.

2 - Program failed, environmental malfunction.

3 - Program failed, internal malfunction.

4 - Program failed, reason unknown.

NOTES

Make sure that the *PoolName* does not exceed a limit of 32 characters.

The omnimm command displays the virtual machine object and its associated disk objects. Other commands will not display the same.

EXAMPLES

The following examples illustrate how the omnimm command works.

1. To create pool "DDS_Pool" of the class "DDS", with policy "App+Loose". Media in the pool will be usable for 12 months or for 100 overwrites., execute:

   omnimm -create_pool DDS_Pool "DDS" App+Loose 12 100

2. To modify the medium with label "Label23" changing the label to "LABEL23" and location to "Backup Room", execute:

   omnimm -modify_medium Label23 LABEL23 "Backup Room"

3. To list detailed information for medium "dat1", execute:

   omnimm -list_media dat1 -detail

4. To list the virtual machine objects and disk objects for medium "medId", execute:

   omnimm -list_media medId -detail

5. To list encryption information for medium "MediaPool1_10", execute:

   omnimm -list_media MediaPool1_10 -encryptioninfo

6. To import a medium in the backup device "Pool1" into pool "Default DDS", execute:

   omnimm -import Pool1 -pool "Default DDS"

7. To copy media catalogs of media "DefaultFile_1" and "MyDLT_35" to the MCF directory on a UNIX system, execute:

   omnimm -copy_to_mcf "DefaultFile_1" "MyDLT_35" -output_directory /tmp/mcf

8. To import media-related catalog data copies "2401110a_47d7f516_0aa0_0001.mcf" and "2401110a_47e26bc2_0a74_0002.mcf" from the default MCF directory on a supported Windows system into a new media pool with prefix "MCF_" located on another Cell Manager, execute:

   omnimm -import_from_mcf "C:\Program Files\OmniBack\Config\ Server\import\mcf\2401110a_47d7f516_0aa0_0001.mcf" "C:\ProgramData\Om

niBack\Config\Server\import\mcf\ 2401110a_47e26bc2_0a74_0002.mcf" -pool_prefix "MCF_" -no_orig_pool

9. To create an Amazon S3 Glacier pool of *S3 Glacier compatible* media type, run the following command:

   omnimm -create_pool "AmazonS3Glacier_Pool" "S3-Glacier-Compatible"

10. To create an Amazon S3 Glacier Deep Archive pool of *S3-Glacier-Deep-Archive-Compatible* media type, run the following command:

    omnimm -create_pool "AmazonS3Deep_Pool" "S3-Glacier-Deep-Archive-Compatible"

11. To create a B2D_pool of Deduplication store media type with policy App+Loose, run the following command:

    omnimm -create_pool "B2D_pool" "Deduplication store" App+Loose

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnimnt

omnimnt - responds to a Data Protector mount requests for a medium
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnimnt -version | -help

omnimnt -device *BackupDevice* -session *SessionID* [-cancel]

DESCRIPTION

The omnimnt command satisfies or aborts a Data Protector mount request. A mount request is issued by a backup device once it has filled all the available media. A mount request is a prompt to mount a new medium. Once the requested medium is inserted in the device drive, the omnimnt command should be used to confirm that the correct medium is inserted. The mount request can also be canceled which is done by canceling device. If you cancel device, all data objects associated with the backup device that issued the mount request will not be processed any further. To view information on currently active sessions, use the omnistat command.

OPTIONS

-version

Displays the version of the omnimnt command

-help

Displays the usage synopsis for the omnimnt command

-cancel

Cancels the device. This will terminate processing of all objects that are associated with the backup device which issued the request.

-device *BackupDevice*

References the backup device *BackupDevice* which issued the mount request, in order to confirm mount request or cancel the device.

-session *SessionID*

Specifies the session using the backup device which issued the mount request.

EXAMPLES

The following examples illustrate how the omnimnt command works.

1. To satisfy a mount request issued by device "DAT1" in a session with SessionID "R-2013/05/05-275", execute:

   omnimnt -device DAT1 -session R-2013/05/05-275

2. To cancel device for the backup device "Juke" in the session with SessionID "R-2013/05/25-3", execute:

   omnimnt -device Juke -session R-2013/05/25-3 -cancel

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnimver

omnimver - verifies data on a medium
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnimver -version | -help

omnimver -device *BackupDevice* [-slot *SlotID* [*Side*]] [-eject]

DESCRIPTION

The omnimver command is used to verify the contents of a Data Protector backup medium. It reads the data and verifies that data is written in the Data Protector format. If the -crc option was used to back up the data, it also checks the CRC for each block.

OPTIONS

-version

Displays the version of the omnimver command

-help

Displays an extended usage synopsis for the omnimver command

-device *BackupDevice*

Specifies the backup device where medium is located.

-slot *SlotID* [*Side*]

Specifies the *SlotID* of the Exchanger backup device where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter in this slot, use the additional *Side* parameter. Slot *Side* must be specified for magneto-optical devices.

-eject

Ejects the medium from the drive after the verification.

EXAMPLES

1. To verify slot 32 of backup device "Spectra60", execute:

   omnimver -device Spectra60 -slot 32

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omniupload(1), sanconf(1M), uma(1M)

omniobjconsolidate

omniobjconsolidate - consolidates Data Protector backup objects into synthetic full backups
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniobjconsolidate -version | -help

omniobjconsolidate -consolidationlist *ConsolidationSpecificationName* -scheduled [*GeneralOptions*]

omniobjconsolidate -consolidationlist *ConsolidationSpecificationName* -postbackup -session *SessionID* [*GeneralOptions*]

omniobjconsolidate [*GeneralOptions*] [*Device* ...] *Object* [*Object* ...]

GeneralOptions

[-dynamic *min max*]

[-protect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }]

[-[no_]log | -log_dirs | -log_file]

[-recycle]

[-locationpriority *MediumLocation* [*MediumLocation* ...]]

[-no_monitor]

[-priority *NumValue*]

MediumLocation

= "= *MediumLocation* " | "< *MediumLocation* "

Device

-targetdevice *LogicalDevice* [*DeviceOptions*]

DeviceOptions

[-concurrency *ConcurrencyNumber*]

[-crc]

[-encrypt]

[-pool *PoolName*]

[-prealloc *MediumID* [*MediumID* ...]]

Object

{ -filesystem | -winfs } *Client:MountPoint Label*

-session *SessionID*

[-copy *CopyID*]

[-sourcedevice *BackupDevice*]

-consolidationdevice *LogicalDevice*

[-targetdevice *LogicalDevice*]

[-protect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }]

[-[no_]log | -log_dirs | -log_file]

[-[no_]recycle]

OtherOptions

Date = *[YY]YY/MM/DD (1969 < [YY]YY < 2038)*

DESCRIPTION

The omniobjconsolidate command creates synthetic full backups from full and incremental backups. It can be used to:

- consolidate objects that you specify
- start a post-backup object consolidation specification
- start a scheduled object consolidation specification

To consolidate an object to a specific point in time, specify only the incremental version of that point in time. The restore chain is retrieved automatically.

To obtain the information about all backed up objects or sessions containing the objects you want to consolidate, use the omnidb command.

OPTIONS

-version

Displays the version of the omniobjconsolidate command.

-help

Displays the usage synopsis of the omniobjconsolidate command.

-consolidationlist *ConsolidationSpecificationName*

Specifies the object consolidation specification identified by *ConsolidationSpecificationName* for object consolidation.

-scheduled

Immediately starts a scheduled object consolidation specification.

-postbackup

Immediately starts a post-backup object consolidation specification specified by the -session *SessionID* option.

-session *SessionID*

If specified with the -postbackup option, provides the session ID for the post-backup object consolidation session.

If specified as part of the object definition, selects the point in time for object consolidation.

-dynamic *min max*

Specifies how many devices are locked prior to starting a session. Devices that are specified per object through the -target device option are locked in any case. The *max* value is increased by Data Protector if the number of statically assigned devices is higher than the specified *max* value.

Min specifies the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be started) required for starting the session. If fewer devices are available than specified here, the session will queue. The default is 1.

Max specifies the maximum number of available devices that Data Protector will use in the session. The highest number you can specify is 32. The default is 5. Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. If this option is not specified, the default value for *max* is the number of specified devices.

-protect { none | weeks *n* | days *n* | until *Date* | permanent }

Sets a period of protection for the consolidated data on the backup medium to prevent the data from being overwritten. If this option is not specified, the data protection of the consolidated objects is the same as the protection of the full backup of the objects. If a relative period of protection was set for the full backup, such as *n* days or weeks, the same protection period is counted from the creation time of the synthetic full backup.

-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }

Specifies file catalog retention time. If you do not want to save the file catalog, use the -no_log option. If this option is not specified, the catalog protection of the consolidated objects is the same as the catalog protection of the full backup of the objects. If a relative period of catalog protection was set for the full backup, such as *n* days or weeks, the same protection period is counted from the creation time of the synthetic full backup.

-log

Specifies the logging level of the object consolidation session. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

If the logging level is not specified, the logging level of the source object is used.

-no_log

Specifies the logging level of the object consolidation session. No information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

-log_dirs

Specifies the logging level of the object consolidation session. All detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring.

-log_file

Specifies the logging level of the object consolidation session. All detailed information about backed up files and directories (filenames and file versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

-[no_]recycle

The -recycle option removes data and catalog protection of the objects on the source media. When there are no more protected objects on the media, the media can be overwritten. The -no_recycle option is available as part of the object definition if the -recycle option is specified as part of *GENERAL_OPTIONS*.

IMPORTANT: If you recycle data protection of source objects, the recycled points in time will no longer be available. Unless copies of these points in time exist, you will be able to restore only to the latest (consolidated) point in time.

-locationpriority *MediumLocation* [*MediumLocation*]

The order in which media are selected for object consolidation in case copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

The priority must be specified in the form "=MediumLocation" (equal to) or "<MediumLocation" (lower priority than).

If you specify -locationpriority "=Loc1" "< Loc2" "=Loc3" "< Loc4", than Loc1 has the highest priority, Loc2 and Loc3 have a lower priority, and Loc4 has the lowest priority.

-no_monitor

If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.

-priority *NumValue*

In case multiple running sessions request access to a specific device at the same time, this option determines the order in which the sessions will be queued. The *NumValue* can be any value from 1 (the highest priority) to 6000 (the lowest priority). In case the option is not specified, the default value of 3000 is set. If a low priority session is running when a high priority session starts queuing, the currently running session is allowed to finish. When more sessions request access to a device with the same priority, any of these sessions might acquire access first.

-filesystem *Client:MountPoint Label*

Selects the filesystem identified with *Client:MountPoint Label* for object consolidation.

-winfs *Client:MountPoint Label*

Selects the Windows filesystem identified with *Client:MountPoint Label* for object consolidation.

-copy *CopyID*

Selects the copy identified with *CopyID*. If not specified, Data Protector automatically selects the most appropriate copy as the source for object consolidation.

-sourcedevice *LogicalDevice*

Specifies a logical device to be used for reading full object versions from the source media. If this option is not specified, Data Protector uses the logical device that was used for writing the objects.

-consolidationdevice *LogicalDevice*

Specifies a logical device that will read incremental object versions and perform object consolidation.

-targetdevice *LogicalDevice*

Specifies a logical device that will be used for writing consolidated object versions to the target media. If specified as a part of *GeneralOptions*, the device is used for all objects. In this case, you can also specify device options. If you specify several devices, the devices will be dynamically assigned to objects.

If specified as part of *Object*, the device is used only for this object.

You can combine static and dynamic assignment of devices by specifying some devices as part of *GeneralOptions*, and for some objects, specifying a device per object.

-concurrency *ConcurrencyNumber*

Specifies the number of restore Media Agents that can send data to a device concurrently.

The maximum concurrency value is 32.

-crc

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during object consolidation. The CRC checks enables you to verify the media after the operation. Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying the media.

-encrypt

If this option is used, the backup Media Agent enables hardware encryption on the device. Consolidated data is encrypted and written to media.

-pool *PoolName*

Selects a specific media pool for object consolidation. If not defined, a default media pool from the device definition will be used.

-prealloc MediumID [*MediumID*]...

Defines the prealloc list. This is a subset of media used for object consolidation in the specified sequence.

When using the prealloc list and the strict media allocation policy with the backup device, Data Protector expects the sequence of the media in the device to correspond with that specified in the prealloc list. If the media are not available in this sequence, Data Protector issues a mount request. If no media are specified in this list, the Data Protector allocation procedure is used to allocate media.

NOTES

All options specified before the first *Object* are applied to all objects. Options specified as a part of an *Object* are applied only to that object and may override general options.

RETURN VALUES

See the man page omniintro for return values.

Additional return values of the omniobjconsolidate command are:
10 - There was an error while consolidating some files. All agents completed successfully.
11 - One or more agents failed, or there was a database error.
12 - None of the agents completed the operation.
13 - Session was aborted.

EXAMPLES

1. To start an object consolidation session that consolidates the WinFS object versions for "OBJECT1" on the host "system1.company.com" to the point in time defined with the session ID "2013/05/06-1", using the device "LTO3" as the source device and the file library "FILEDEV1" as the consolidation device, and writes the consolidated objects to the device "LTO4", use:

   omniobjconsolidate -winfs system1.company.com:/C 'OBJECT1' -session 2013/05/06-1 -sourcedevice 'LTO3' -consolidationdevice 'FILEDEV1' -targetdevice 'LTO4'

2. To start an interactive object consolidation session for the filesystem object "system1.company.com:/ 'Label42'" from the session "2013/05/01-2", using the device "DEV1" to read the source object and the device "DEV2" to consolidate the object, and write the consolidated object to the device "DEV3", use:

   omniobjconsolidate -filesystem system1.company.com:/ 'Label42' -session 2013/05/01-2 -sourcedevice 'DEV1' -consolidationdevice 'DEV2' -targetdevice 'DEV3'

3. To immediately start a post-backup object consolidation specification named "post_BU1" for the session "2013/05/03-1", execute:

```
omniobjconsolidate -consolidationlist post_BU1 -postbackup -session 2013/05/03-1
```

4. To immediately start a scheduled object consolidation specification named "Consolidation_16_Spec", execute:

```
omniobjconsolidate -consolidationlist Consolidation_16_Spec -scheduled
```

SEE ALSO

omnib(1), omnikeytool(1M), omniobjcopy(1), omniobjverify(1), omnir(1)

omniobjcopy

omniobjcopy - creates additional copies of objects backed up with Data Protector on a different media set (this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniobjcopy -version | -help

omniobjcopy -copylist *CopySpecificationName* -scheduled [*[GENERAL_OPTIONS*]

omniobjcopy -copylist *CopySpecificationName* -postbackup -session *SessionID* [*[GENERAL_OPTIONS*]

omniobjcopy -replist *ReplicationSpecificationName* -scheduled [*[GENERAL_OPTIONS*]

omniobjcopy -replist *ReplicationSpecificationName* -postbackup -session *SessionID* [*[GENERAL_OPTIONS*]

omniobjcopy -restart *SessionID*

omniobjcopy [*GENERAL_OPTIONS*] *Device* ... *Object* [*Object*]...

GENERAL_OPTIONS

[-replication]

[-dynamic *min max*]

[-targetprotect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }]

[-[no_]log | -log_dirs | -log_file]

[-sourceprotect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-locationpriority *MediumLocation* [*MediumLocation* ...]]

[-no_monitor]

[-no_auto_device_selection]

[-session Session ID]

-replication

-targetcs HostName

-targetcsdevice DeviceName

[-priority *NumValue*]

MediumLocation

= "= *MediumLocation* " | "< *MediumLocation* "

Device

= -targetdevice *LogicalDevice* [*DeviceOptions*]

DeviceOptions

[-concurrency *ConcurrencyNumber*]

[-crc]

[-encrypt]

[-pool *PoolName*]

[-prealloc *MediumID* [*MediumID* ...]]

Object

{ -filesystem | -winfs } *Client:MountPoint Label*

-session *SessionID*

[-copyid *N* [-fixedcopy ...]]

[-sourcedevice *LogicalDevice*]

[-targetdevice *LogicalDevice*]

[-targetprotect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }]

[[-no_]log | -log_dirs | -log_file]

[-sourceprotect { none | weeks *n* | days *n* | until *Date* | permanent | keep }]

[-full]

Object

-rawdisk *Client Label*

-session *SessionID*

[-copyid *N* [-fixedcopy ...]]

[-sourcedevice *LogicalDevice*]

[-targetdevice *LogicalDevice*]

[-targetprotect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-sourceprotect { none | weeks *n* | days *n* | until *Date* | permanent | keep }]

Object

{ -sap | -oracle8 | -integ {MySQL | PostgreSQL} | -informix | -msese | -e2010 | -mssql | -lotus | -mbx | -sapdb | -saphana | -msvssw | -db2 | -sybase | -mssharepoint | m365 | -veagent | -idb } *Client:Set*

-session *SessionID*

[-copyid *N* [-fixedcopy ...]]

[-sourcedevice *LogicalDevice*]

[-targetdevice *LogicalDevice*]

[-targetprotect { none | weeks *n* | days *n* | until *Date* | permanent }]

[-sourceprotect { none | weeks *n* | days *n* | until *Date* | permanent | keep }]

OtherOptions

Date = *[YY]YY/MM/DD (1969 < [YY]YY < 2038)*

DESCRIPTION

The omniobjcopy command creates additional copies of objects backed up using Data Protector. You can use the omniobjcopy command to copy objects such as filesystems (UNIX or Windows), very big file systems, disk image sections, and Data Protector Internal Database (IDB) to an additional media set. The command can be also used for copying the integration objects (SAP R/3, Oracle, Informix Server, VMware vSphere, Microsoft Hyper-V, Microsoft Exchange Server, Microsoft Exchange Server single mailboxes, Microsoft SharePoint Server, Microsoft 365 mailboxes, Microsoft SQL Server, Lotus, Sybase, DB2, Microsoft Volume Shadow Copy Service, SAP MaxDB, and SAP HANA Appliance).

To obtain the information about all backed up objects or sessions containing the objects you want to copy, use the omnidb command.

This command starts an interactive or automated object copy session. Use this command to immediately start an automated (scheduled or post-backup) object copy specification.

From Data Protector 9.05 onwards for VMware and Hyper-V integrations, the virtual machine disks are considered as objects that run in parallel. When the virtual machine object is selected for object copy operations, its associated disk objects are also considered for these copy operations.

OPTIONS

-version

Displays the version of the omniobjcopy command.

-help

Displays the usage synopsis for the omniobjcopy command.

-copylist *CopySpecificationName*

Specifies the name of the object copy specification identified by *CopySpecificationName* for object copying.

-replist *ReplicationSpecificationName*

Specifies the name of the replication specification identified by *ReplicationSpecificationName* for replication.

-scheduled

Immediately starts a scheduled object copy specification.

-postbackup

Immediately starts a post-backup object copy specification specified by the -session *SessionID* option.

-replication

Enables replication for supported B2D devices in interactive sessions.

-session *SessionID*

Selects the session ID for the -postbackup option or for the object definition.

-restart *SessionID*

Tries to restart a failed non-interactive object copy session, specified by its session ID.

-dynamic *min max*

Specifies how many devices are locked prior to starting a session. Devices that are specified per object through the -target device option are locked in any case. The *max* value is increased by Data Protector if the number of statically assigned devices is higher than the specified *max* value.

Min specifies the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be started) required for starting the session. If fewer devices are available than specified here, the session will queue. The default is 1.

Max specifies the maximum number of available devices that Data Protector will use in the session. The highest number you can specify is 32. The default is 5. Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. If this option is not specified, the default value for *max* is the number of specified devices.

-targetprotect { none | weeks *n* | days *n* | until *Date* | permanent }

Sets the level of protection for the copy object. The media containing this object copy session cannot be overwritten until the protection expires. By default (if this option is not specified), the protection is the same as the original protection for the source object.

-keepcatalog { weeks *n* | days *n* | until *Date* | same_as_data_protection }

Specifies file catalog retention time. If you do not want to save the file catalog at all, use the -no_log option. By default (if this option is not specified), the protection is the same as for the source object.

-log

Specifies the logging level of the object copy session. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the Data Protector Internal Database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

If the logging level is not specified, it is set to the same logging level as for the source object.

-no_log

Specifies the logging level of the object copy session. Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log_dirs

Specifies the logging level of the object copy session. If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

-log_file

Specifies the logging level of the object copy session. All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector Internal Database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape. It also does not take much space since some information on file details (file attributes) is not logged to the database.

-sourceprotect { none | weeks *n* | days *n* | until *Date* | permanent | keep }

Sets the level of protection for the source object after a successful copy. The media containing this source object cannot be overwritten until the protection expires. By default (if this option is not specified), the protection is not changed.

The none option specifies that protection is removed from the source object immediately, allowing recycling.

The keep option can only be specified at the object level and specifies that the protection for that source object should not be changed.

-locationpriority *MediumLocation* [*MediumLocation*]

The order in which media are selected for the object copy in case that the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

The priority must be specified in the form "=MediumLocation " (equal to) or "<MediumLocation " (lower priority than).

If you specify -locationpriority "=Loc1" "< Loc2" "=Loc3" "< Loc4" , than Loc1 has the highest priority, Loc2 and Loc3 have a lower priority, and Loc4 has the lowest priority.

-no_monitor

If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.

-no_auto_device_selection

If this option is specified, Data Protector does not automatically replace unavailable devices with available devices of the same device tag.

-priority *NumValue*

In case multiple running sessions request access to a specific device at the same time, this option determines the order in which the sessions will be queued. The *NumValue* can be any value from 1 (the highest priority) to 6000 (the lowest priority). In case the option is not specified, the default value of 3000 is set. If a low priority session is running when a high priority session starts queuing, the currently running session is allowed to finish. When more sessions request access to a device with the same priority, any of these sessions might acquire access first.

-concurrency *ConcurrencyNumber*

Specifies the number of restore Media Agents that can send data to a device concurrently.

The maximum concurrency value is 32.

-crc

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during an object copy. The CRC checks enables you to verify the media after the operation. Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and the media.

-encrypt

If this option is used, the backup Media Agent enables hardware encryption on the device. Data is encrypted and copied.

-pool *PoolName*

Selects a specific media pool for object copy. If not defined, a default media pool from the device definition will be used.

-prealloc *MediumID* [*MediumID*]...

Defines the prealloc list. This is a subset of media used for object copy in the specified sequence.

When using the prealloc list and the strict media allocation policy with the backup device, Data Protector expects the sequence of the media in the device to correspond with that specified in the prealloc list. If the media are not available in this sequence, Data Protector issues a mount request. If no media are specified in this list, the Data Protector allocation procedure is used to allocate media.

-filesystem *Client:MountPoint Label*

Selects the filesystem identified by the *Client:MountPoint Label* string for object copying.

-winfs *Client:MountPoint Label*

Selects the Windows filesystem identified by the *Client:MountPoint Label* string for object copying.

-copyid *N* [-fixedcopy]

Selects the specified object copy as a source for object copying.

If -fixedcopy option is not specified, Data Protector selects the needed media set automatically. If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option is obligatory.

-sourcedevice *LogicalDevice*

Specifies a logical device different from the one used for the backup to be used for reading backed up objects from the source media. By default (if this option is not specified), the same backup device is used for backing up and reading backed up objects from the source media.

-targetdevice *LogicalDevice*

Specifies a backup device that will be used for writing object copies to the target media.

-full

Selects the whole restore chain of full and incremental backups for the object copy operation. This option is not supported for Data Protector application integrations.

-sap *Client:Set*

Selects the SAP R/3 object identified by the *Client:Set* string for object copying.

-informix *Client:Set*

Selects the Informix Server object identified by the *Client:Set* string for object copying.

-e2010 *Client:Set*

Selects the Microsoft Exchange Server 2010/2013 object identified by the *Client:Set* string for object copying.

-mssql *Client:Set*

Selects the Microsoft SQL Server object identified by the *Client:Set* string for object copying.

-lotus *Client:Set*

Selects the Lotus Notes/Domino Server object identified by the *Client:Set* string for object copying.

-mbx *Client:Set*

Selects the Microsoft Exchange Server single mailbox object identified by the *Client:Set* string for object copying.

-sapdb *Client:Set*

Selects the SAP MaxDB object identified by the *Client:Set* string for object copying.

-msvssw *Client:Set*

Selects the Microsoft Volume Shadow Copy Service object identified by the *Client:Set* string for object copying.

-db2 *Client:Set*

Selects the DB2 object identified by the *Client:Set* string for object copying.

-sybase *Client:Set*

Selects the Sybase object identified by the *Client:Set* string for object copying.

-mssharepoint *Client:Set*

Selects the Microsoft SharePoint Server 2010 object identified by the *Client:Set* for object copying.

-veagent *Client:Set*

Selects the virtual environment object identified by the *Client:Set* string for object copying. On selecting an object for copying, the associated disk objects are also considered.

-idb *Client:Set*

Selects the Internal Database backup object identified by the *Client:Set* string for object copying.

-saphana *Client:Set*

Selects the SAP HANA backup object identified by the *Client:Set* string for object copying.

-integ {MySQL | PostgreSQL} *Client:Set*

Selects the MySQL or PostgreSQL backup object identified by the *Client:Set* string for object copying.

RETURN VALUES

For common return values, see the omniintro man page.

Additional return values of the omniobjcopy command are:

10 - There was an error while copying some files. All agents completed successfully.
11 - One or more agents failed, or there was a database error.
12 - None of the agents completed the operation.
13 - Session was aborted.

EXAMPLES

1. To start an interactive object copy session for copying two WinFS objects "system.company.com:/C 'Object1'" and "system.company.com:/C 'Object1'" from two different sessions to the device "DEV1", so that the source object version for "Object1" is then recycled, execute:

   omniobjcopy -winfs system.company.com:/C 'Object1' -session 2013/04/01-3 -targetdevice 'DEV1' -recycle -winfs systems.company.com:/C 'Object2' -session 2013/04/25-9 -targetdevice 'DEV1'

2. To start an interactive object copy session for copying the whole restore chain of full and incremental backups for the filesystem object "system1.company.com:/ 'Label42'" from the session "2013/05/01-2", using the device "DEV1" to read the source objects and the device "DEV2" copy the objects, execute:

   omniobjcopy -filesystem system1.company.com:/ 'Label42' -session 2013/05/01-2 -sourcedevice 'DEV1' -targetdevice 'DEV2' -full

3. To start an interactive replication session for copying the whole restore chain of full and incremental backups from the session "2013/05/01-2", using the device "B2D1" as the source and the device "B2D2" as the target device, execute:

   omniobjcopy -replication -session 2013/05/01-2 -sourcedevice 'B2D1' -targetdevice 'B2D2' -full

4. To immediately start a post-backup object copy specification named "post_BU1" for the session "2013/05/03-1", and to make the devices available to this session with the highest priority in case of resource conflicts, execute:

   omniobjcopy -copylist post_BU1 -postbackup -session 2013/05/03-1 -priority 1

5. To immediately start a scheduled object copy specification named "CopySpec", use:

   omniobjcopy -copylist CopySpec -scheduled

6. To immediately start a scheduled replication specification named "ReplicSpec", use:

   ```
   omniobjcopy -replist ReplicSpec -scheduled
   ```

7. To restart a failed post-backup object copy specification "2013/03/16-10", use:

   ```
   omniobjcopy -restart "2013/03/16-10"
   ```

8. To start an interactive object copying session for the MySQL object " mysqlsys.company.com:MYSQL56.1408541577" from the session "2014/11/20-21", setting the level of protection for the object copy to five weeks, and suppressing messages from the command output, execute:

   ```
   omniobjcopy -no_monitor -integ MySQL mysqlsys.company.com:MYSQL56.1408541577 -session 2014/11/20-21 -targetproctect weeks 5
   ```

9. To start an object copying session for the virtual environment object " hyperv .company.com " from the session " 2020/11/01-1 ", to the target device " target_device1 ", execute:

   ```
   omniobjcopy -veagent  hyperv.company.com -session 2020/11/01-1  -targetdevice target_device1
   ```

SEE ALSO

omnib(1), omnikeytool(1M), omniobjconsolidate(1), omniobjverify(1), omnir(1)

omniobjverify

omniobjverify - verifies Data Protector backup objects, either interactively or using pre-configured post-backup, or scheduled verification specifications
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniobjverify -version | -help

omniobjverify -verificationlist *VerificationSpecificationName* -scheduled [*GENERAL_OPTIONS*]

omniobjverify -verificationlist *VerificationSpecificationName* -postbackup -session *SessionID* [*GENERAL_OPTIONS*]

omniobjverify [*GENERAL_OPTIONS*] *Object[[Object]...]*

GENERAL_OPTIONS

[{ -verify_on_source | -verify_on_mahost | -verify_on_host *hostname* }]

[-locationpriority *MediumLocation* [*MediumLocation*]...]

[-no_monitor]

[-priority *NumValue*]

MediumLocation = "= *MediumLocation*" | "< *MediumLocation*"

Object{

{ -filesystem | - vprotect | -winfs | -rawdisk }
Client:ObjectName Label

| { -sap | -oracle8 | -integ {MySQL | PostgreSQL} | -informix | -msese | -e2010 | -mssql | -lotus | -mbx | -sapdb | -saphana | -msvssw | -db2 | -sybase | -mssharepoint | m365 | -veagent | -idb } *Client:ObjectName*

-session *SessionID*

[-copyid *N* [-fixedcopy]]

[-sourcedevice *LogicalDevice*]

}

DESCRIPTION

The omniobjverify command verifies backup objects that have been created by Data Protector backup, object copy, or object consolidation sessions. You can use the omniobjverify command to verify objects such as filesystems (UNIX or Windows), vProtect, very big file systems, disk image sections, and the Data Protector Internal Database (IDB).

The command can be also used to verify integration objects (SAP R/3, Oracle, MySQL, PostgreSQL, Informix Server, VMware vSphere, Microsoft Hyper-V, Microsoft Exchange Server, Microsoft Exchange Server single mailboxes, Microsoft SharePoint Server, Microsoft 365 mailboxes, Microsoft SQL Server, Lotus, Sybase, DB2, Microsoft Volume Shadow Copy Service, SAP MaxDB, and SAP HANA Appliance). It verifies the data integrity of the objects and the ability of Data Protector to deliver them to the application integration, not the application integration's ability to restore them.

To obtain the information about all backed up objects or sessions containing the objects you want to verify, use the omnidb command.

This command can be used to start an interactive object verification session or immediately start an automated (scheduled or post-backup) object verification specification.

From Data Protector 9.05 onwards for VMware integrations, the virtual machine disks are considered as objects that run in parallel. When the virtual machine object is selected for object copy operations, its associated disk objects are also considered for these copy operations. This is the case for Hyper-V RCT virtual machines as well.

OPTIONS

-version

Displays the version of the omniobjverify command.

-help

Displays the usage synopsis for the omniobjverify command.

-verificationlist *VerificationSpecificationName*

Specifies the name of the verification specification, identified by *VerificationSpecificationName*, for object verification.

-scheduled

Immediately starts a scheduled verification specification.

-postbackup

Immediately starts a post-backup verification specification specified by the -session *SessionID* option.

-session *SessionID*

Selects the session ID for the -postbackup option or for the object definition.

-verify_on_source

Specifies the original backup object source host as the host on which the object verification process will be performed.

-verify_on_mahost

Specifies the Media Agent host as the host on which the object verification process will be performed.

-verify_on_host *hostname*

Specifies the host identified by *hostname* as the host on which the object verification process will be performed.

-locationpriority *MediumLocation* [*MediumLocation*]

The order in which media are selected for object verification if the same object version exists in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally match the conditions of the media set selection algorithm.

The priority must be specified in the form "=MediumLocation" (equal to) or "<MediumLocation" (lower priority than).

If you specify -locationpriority "=Loc1" "< Loc2" "=Loc3" "< Loc4", then Loc1 has the highest priority, Loc2 and Loc3 have a lower priority, and Loc4 has the lowest priority.

-no_monitor

If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.

-priority *NumValue*

In case multiple running sessions request access to a specific device at the same time, this option determines the order in which the sessions will be queued. The *NumValue* can be any value from 1 (the highest priority) to 6000 (the lowest priority). In case the option is not specified, the default value of 3000 is set. If a low priority session is running when a high priority session starts queuing, the currently running session is allowed to finish. When more sessions request access to a device with the same priority, any of these sessions might acquire access first.

-filesystem *Client:ObjectName Label*

Selects the filesystem identified by *Client:ObjectName Label* for object verification.

-vProtect *Client:ObjectName Label*

Selects the vProtect node identified by *Client:ObjectName Label* for object verification.

-winfs *Client:ObjectName Label*

Selects the Windows filesystem identified by the *Client:ObjectName Label* string for object verification.

-rawdisk *Client:ObjectName Label*

Selects the disk image identified by the *Client:Label* string for object verification. *ObjectName* is blank in this case

-copyid *N* [-fixedcopy]

Selects the specified copy of an object version as a source for object verification.

If -fixedcopy option is not specified, Data Protector selects the needed media set automatically. If several copies of the same object version exist in one session as a result of the object copy or object mirror operation, this option is obligatory.

-sourcedevice *LogicalDevice*

Specifies a logical device different from the one used for the backup to be used for reading backed up objects from the source media. By default (if this option is not specified), the original backup device is used for reading backed-up objects from the source media.

-sap *Client:ObjectName*

Selects the SAP R/3 object identified by the *Client:ObjectName* string for object verification.

-oracle8 *Client:ObjectName*

Selects the Oracle object identified by the *Client:ObjectName* string for object verification.

-informix *Client:ObjectName*

Selects the Informix Server object identified by the *Client:ObjectName* string for object verification.

-e2010 *Client:ObjectName*

Selects the Microsoft Exchange Server object identified by the *Client:ObjectName* string for object verification.

-m365 *Client:ObjectName*

Selects the Microsoft 365 object identified by the *Client:ObjectName* string for object verification.

-mssql *Client:ObjectName*

Selects the Microsoft SQL Server object identified by the *Client:ObjectName* string for object verification.

-lotus *Client:ObjectName*

Selects the Lotus Notes/Domino Server object identified by the *Client:ObjectName* string for object verification.

-mbx *Client:ObjectName*

Selects the Microsoft Exchange Server single mailbox object identified by the *Client:ObjectName* string for object

verification.

-sapdb *Client:ObjectName*

Selects the SAP MaxDB object identified by the *Client:ObjectName* string for object copying.

-msvssw *Client:ObjectName*

Selects the Microsoft Volume Shadow Copy Service object identified by the *Client:ObjectName* string for object verification.

-db2 *Client:ObjectName*

Selects the DB2 object identified by the *Client:ObjectName* string for object verification.

-sybase *Client:ObjectName*

Selects the Sybase object identified by the *Client:ObjectName* string for object verification.

-mssps *Client:ObjectName*

Selects the Microsoft SharePoint Portal Server object identified by the *Client:ObjectName* string for object verification.

-mssharepoint *Client:ObjectName*

Selects the Microsoft SharePoint 2010 Server object identified by *Client:ObjectName* string for object verification.

-veagent *Client:ObjectName*

Selects the virtual environment object identified by the *Client:ObjectName* string for object verification.

-idb *Client:Set*

Selects the Internal Database backup object identified by the *Client:Set* string for object verification.

-saphana *Client:Set*

Selects the SAP HANA backup object identified by the *Client:Set* string for object verification.

-integ {MySQL | PostgreSQL} *Client:Set*

Selects the MySQL or PostgreSQL backup object identified by the *Client:Set* string for object verification.

RETURN VALUES

For common return values, see the omniintro man page.

Additional return values of the omniobjverify command are:

10 - There was an error while copying some files. All agents completed successfully.
11 - One or more agents failed, or there was a database error.
12 - None of the agents completed the operation.
13 - Session was aborted.

EXAMPLES

1. To start an interactive object verification session for verifying one WinFS object "system.company.com:/C 'Object1'" from session 2013/02/06-1, using the original host as the verification host, execute:

   ```
   omniobjverify -winfs system.company.com:/C 'Object1' -session 2013/02/06-1
   ```

2. To start an interactive verification session for verifying two filesystem objects "system1.company.com:/ 'Label1'" and "system1.company.com:/ 'Label2'" from session 2013/03/01-2, on host "system2.company.com", execute:

omniobjverify -verify_on_host system2.company.com -filesystem system1.company.com:/ 'Label1' -session 2013/03/01-2 -filesystem system1.company.com:/ 'Label2' -session 2013/03/01-2

3. To immediately start a post-backup verification specification named "post_bu_verify1" for the session "2013/01/03-1", execute:

   omniobjverify -verificationlist post_bu_verify1 -postbackup -session 2013/01/03-1

4. To immediately start a scheduled verification specification named "sched_verify1", execute:

   omniobjverify -verificationlist sched_verify1 -scheduled

5. To start an object verification session for the MySQL object " mysqlsys.company.com:MYSQL58.1411047241" from the session "2014/11/21-5", using the backup device "FastestDriveOfAll ",execute:

   omniobjverify -integ MySQL mysqlsys.company.com:MYSQL58.1411047241 -session 2014/08/21-5 -sourcedevice FastestDriveOfAll

6. To start an object verification session to verify a virtual object on the host host.company.com from the session 2020/11/01-1 , execute:

   omniobjverify -verify_on_host host.company.com -veagent <veagent_object> -session 2020/11/01-1

7. To start an object verification session to verify a virtual object on the MA host mahost.company.com from the session 2020/11/01-1 , execute:

   omniobjverify -verify_on_mahost mahost.company.com -veagent <veagent_object> -session 2020/11/01-1

8. To start an object verification session to verify a virtual object on the source source.company.com from the session 2020/11/01-1 , execute:

   omniobjverify -verify_on_source source.company.com -veagent <veagent_object> -session 2020/11/01-1

9. To start an interactive object verification session for verifying one vProtect object "system.company.com:/ 'Object1 '" from session 2021/10/07-1 , using the original host as the verification host, execute:

   omniobjverify -vProtect system.company.com:/ 'Object1' -session 2021/10/07-1

10. To start an interactive verification session for verifying two vProtect objects "system1.company.com:/ 'Label1 '" from session 2021/10/07-1 and " system1.company.com:/ 'Label2 '" from session 2021/10/07-2 , on host " system2.company.com", execute:

    omniobjverify -verify_on_host system2.company.com -vProtect system1.company.com:/ 'Label1' -session 2021/10/07-1 -vProtect system1.company.com:/ 'Label2' -session 2021/10/07-2

11. To start an interactive verification session for verifying one vprotect object "system1.company.com:/ 'Label1 '" from session 2021/10/07-1 and one WinFS object " system1.company.com:/ 'Label2 '" from session 2021/10/07-3 , using the original host as the verification host, execute:

    omniobjverify -vprotect system1.company.com:/ 'Label1' -session 2021/10/07-1 -winfs system1.company.com:/ 'Label2' -session 2021/10/07-3

12. To start an interactive verification session for verifying a vProtect object "system1.company.com:/ 'Label1 '" from session 2021/10/20-1 on the source host:

    omniobjverify -vprotect system1.company.com:/ 'Label1' -session 2021/10/20-1 -verify_on_source

SEE ALSO

omnib(1), omnidb(1), omnikeytool(1M), omniobjconsolidate(1), omniobjcopy(1), omnir(1)

omnir

omnir - this command is available on systems with the Data Protector User Interface component installed. It is used to restore objects such as filesystems, blocks, disk images, the Data Protector Internal Database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Server, Microsoft 365 mailboxes, MySQL, PostgreSQL, SAP R/3, SAP MaxDB, Informix Server, VMware vSphere, H3C CAS, Microsoft Hyper-V, Lotus, IBM DB2 UDB, and NDMP objects backed up with Data Protector. The command is also used to start the instant recovery process. To restore a Sybase database, see the **syb_tool** man page.

SYNOPSIS

omnir -version | -help

omnir SESSION_OPTIONS [-noexpand] *Object* [*Object* ...]

SESSION_OPTIONS

-[no_]preview

-report { warning | minor | major | critical }

FILESYSTEM RESTORE

Object

{ -filesystem | -winfs | -vprotect } Host:MountPoint Label

-session *SessionID* [-copyid *CopyID*]

-tree *TreeName* ...

[*DATA_OPTIONS*]

[*FILESYSTEM_OPTIONS*]

[*GENERAL_OPTIONS*]

[*SPLIT_MIRROR_OPTIONS*]

Object

{ -filesystem | -winfs | -vprotect } Host:MountPoint Label

-full [-session *SessionID*]

-tree *TreeName* ...

[*DATA_OPTIONS*]

[*FILESYSTEM_OPTIONS*]

[*GENERAL_OPTIONS*]

[*SPLIT_MIRROR_OPTIONS*]

Object

{ -filesystem | -winfs | -vprotect } Host :MountPoint Label

-omit_deleted_files [-session *SessionID* [-copyid *CopyID*]]

-overwrite

-tree *TreeName* ...

[*DATA_OPTIONS*]

[*FILESYSTEM_OPTIONS*]

[*SPLIT_MIRROR_OPTIONS*]

[*GENERAL_OPTIONS*]

Object

{ -filesystem | -winfs | -vprotect } Host :MountPoint Label

-tree *TreeName* ...

MEDIUM_OPTIONS

[*DATA_OPTIONS*]

[*FILESYSTEM_OPTIONS*]

[*GENERAL_OPTIONS*]

Object

-host *Hosttname*

-session *SessionID*

[-full | -omit_deleted_files -overwrite]

[*FILESYSTEM_OPTIONS*]

[*GENERAL_OPTIONS*]

Object

-resume SessionId

DISK IMAGE RESTORE

Object

-rawdisk *Host Label*

-session *SessionID* [-copyid *CopyID*]

-section [*ToSection1=*] *Section1* [-section *ToSection2= Section2* ...]

[*SPLIT_MIRROR_OPTIONS*]

[*GENERAL_OPTIONS*]

Object

-rawdisk *Host Label*

-section [*ToSection1=*] *Section1* [-section *ToSection2= Section2* ...]

MEDIUM_OPTIONS

[*GENERAL_OPTIONS*]

INSTANT RECOVERY

omnir -host *ClientName*

-session *SessionID*

-instant_restore

[*P9000_DISK_ARRAY_XP_OPTIONS* | *3PAR_DISK_ARRAY_OPTIONS* | *NETAPP_DISK_ARRAY_OPTIONS* | *DELLEMCUNITY_DISK_ARRAY_OPTIONS*]

[*ORACLE_SPECIFIC_OPTIONS*]

[*SAP_SPECIFIC_OPTIONS*]

P9000_DISK_ARRAY_XP_OPTIONS

-keep_version

-check_config

3PAR_DISK_ARRAY_OPTIONS

{ -copyback wait_clonecopy *Minutes* }

{ -check_config | -no_check_config }

[-force_prp_replica]

[-force_restore_volset]

NETAPP_DISK_ARRAY_OPTIONS

{ -check_config | -no_check_config }

[-force_prp_replica]

[-force_restore_volset]

DELLEMCUNITY_DISK_ARRAY_OPTIONS

{ -check_config | -no_check_config }

[-force_prp_replica]

[-force_restore_volset]

SAP_SPECIFIC_OPTIONS

-sap

-user *UserName* -group *GroupName*

-recover { now | time *MM/DD/YY hh:mm:ss* | logseq *LogSeqNumber* thread *ThreadNumber* | SCN *Number* } [-open [-resetlogs]]

-appname *ApplicationDatabaseName*

ORACLE_SPECIFIC_OPTIONS

-oracle

-user *UserName* -group *GroupName*

-recover { now | time *MM/DD/YY hh:mm:ss* | logseq *LogSeqNum* thread *ThreadNum* | SCN *Number* } [-open [-resetlogs]]

-appname *ApplicationDatabaseName*

-parallelism *Number*

NDMP RESTORE

Object

-filesystem *Host:MountPoint Label*

-full [-session *SessionID*]

-device *BackupDevice*

-tree *TreeName* ...

[*NDMP_DATA_OPTIONS*]

[*NDMP_GENERAL_OPTIONS*]

Object

-filesystem *Host:MountPoint Label*

-session *SessionID* [-full]

-device *BackupDevice*

-tree *TreeName* ...

[*NDMP_DATA_OPTIONS*]

[*NDMP_GENERAL_OPTIONS*]

NDMP_DATA_OPTIONS

-into *PathName*

-ndmp_env *FileName*

NDMP_GENERAL_OPTIONS

-server *ServerName*

-no_monitor

-variable *VariableName VariableValue*

SAP R/3 FILE RESTORE

Object

-sap *Client:Set*

-session *SessionID* [-copyid *CopyID*]

-tree *FileName* ...

[*DATA_OPTIONS*]

[*FILESYSTEM_OPTIONS*]

[*GENERAL_OPTIONS*]

VIRTUAL ENVIRONMENT RESTORE

omnir -veagent

-virtual-environment { vmware | hyperv | vcd | h3ccas }

-barhost *BackupHost*

-apphost *OriginalAppHost*

-instance *OriginalDatacenter*

-method { vStorageImage | vCDvStorageImage | vStorageImageOpenStack | h3ccasImage -non-cached | h3ccasImage -cached|HyperV-RCT }

[-session *BackupID* |

-fromsession *BackupID* -untilsession *BackupID*]

VirtualMachine [*VirtualMachine* ...]

[*NewInstance* | *Directory* | *NewOrganization*]

[*RESTORE_OPTIONS*]

[*COMMON_OPTIONS*]

VirtualMachine

-vm *vmpath* -instanceUUID *vmInstanceUUID* [-versionID *VersionID*] [-new_name *NewVirtualMachineName*] [-disk *DiskName* ...]

NewInstance

-newinstance { *TargetDatacenter* | *TargetHostpool* }

[-store { *TargetDatastore* | *TargetStoragePool* }]

[-network_name *TargetNetwork*]

[-destination *RestoreClient*]

[-host_cluster *HostOrCluster*]

[-resourcePool *ResourcePool*]

[-specificHost *SpecificHost*]

[-targetstoragepath *TargetStoragePathOfAllHyper-V-VMs*]

[-targetVM *TargetH3CCASVM*]

NewOrganization

-neworganization *TargetOrganization*

[[-virtual_datacenter_path | -virtual_datacenter_uuid] *TargetVDC*]

[[-vapp_path | -vapp_uuid] *TargetVApp*]

[[-vcenter_path | -vcenter_uuid] *TargetVCenter*]

[[-network_name | -network_uuid] *TargetNetwork*]

Directory

-directory *RestoreDirectory*

[-overwrite | -skip | -latest]

RESTORE_OPTIONS

[-deletebefore | -deleteafter | -skip | -keep_for_forensics]

[-removeSnapshots]

COMMON _OPTIONS

[-consolidate]

[-register]

[-poweron]

[-skipTagAttach | { [-categoryName CategoryName] [-tagName TagName] | [-tagId TagId]}]

SAP MAXDB RESTORE

omnir -sapdb

-barhost *ClientName*

[-user user:group]

[-instance InstanceName]

[-destination ClientName]

[-newinstance DestinationInstanceName]

[-session BackupID]

[-recover [-endlogs | -time: YYYY-MM-DD.hh.mm.ss] [-from_disk]]

[-nochain]

[-from_disk]

[-force]

[-config]

[GENERAL_OPTIONS]

INFORMIX SERVER RESTORE

omnir -informix

-barhost *ClientName*

-barcmnd *PathName*

-user *User:Group*

-appname *ApplicationDatabaseName*

-barарg *OnBarRestoreArguments*

[*SESSION_OPTIONS*]

[*GENERAL_OPTIONS*]

SESSION_OPTIONS

-report { warning | minor | major | critical }

-load { low | medium | high }

-no_monitor

MICROSOFT 365 MAILBOX RESTORE

omnir -m365
-m365-environment {exchange}

- organization Organization

-barhost *BackupHost*

-tenantname TenantName

-mailbox <mailbox> -session <backupsessionId> -type <User | Group> ...

- azureapp *AzureApplicationName*

-destinationfolder *RestorePath*

MICROSOFT EXCHANGE SERVER 2010/2013 RESTORE

STANDARD RESTORE

omnir -e2010

-barhost *ClientName*

Database [*Database* ...]

[-user *User:Domain*]

[*VSS_EXCHANGE_SPECIFIC_OPTIONS*]

[*GENERAL_OPTIONS*]

INSTANT RECOVERY

omnir -e2010

-barhost *ClientName*

-instant_restore

Database [*Database* ...]

[-user *User:Domain*]

[*VSS_INSTANT_RECOVERY_OPTIONS*]

[*VSS_EXCHANGE_SPECIFIC_OPTIONS*]

[*GENERAL_OPTIONS*]

Database

{ -db_name *SourceDatabaseName* | -db_guid *SourceDatabaseGUID* }

[-source *SourceClientName*]

{ -repair | -latest | -pit | -new | -temp } *E2010_METHOD_OPTIONS*

E2010_REPAIR_METHOD_OPTIONS

[-no_resume_replication]

E2010_LATEST_METHOD_OPTIONS

[-node *TargetNode...* | -all]

[-no_resume_replication]

[-no_recover]

[-no_mount]

[*E2010_IR_SPECIFIC_OPTIONS*]

E2010_PIT_METHOD_OPTIONS

-session *ID*

[-node *TargetNode...* | -all]

[-no_resume_replication]

[-no_recover]

[-no_mount]

[*E2010_IR_SPECIFIC_OPTIONS*]

E2010_NEW_METHOD_OPTIONS

-session *ID*

-client *TargetClientName*

-location *TargetDatabasePath*

-name *TargetDatabaseName*

[-recoverydb]

[-no_recover]

[-no_mount]

[*E2010_IR_SPECIFIC_OPTIONS*]

E2010_TEMP_METHOD_OPTIONS

-session *ID*

-client *TargetClientName*

-location *TargetDatabasePath*

[-no_chain]

[-edb_only]

[-no_recover]

[*E2010_IR_SPECIFIC_OPTIONS*]

E2010_IR_SPECIFIC_OPTIONS

[-from_session *SessionID*]

MICROSOFT EXCHANGE SINGLE MAILBOX RESTORE

omnir -mbx

-barhost *HostName*

[-destination *HostName*]

-mailbox *MailboxName* -session *BackupID* [*MAILBOX_OPTIONS*]...

-public -session *BackupID* [*PUBLIC_FOLDERS_OPTIONS*]

[*GENERAL_OPTIONS*]

MAILBOX_OPTIONS

-folder *FolderName*

-exclude *FolderName*

-originalfolder { -keep_msg | -overwrite_msg }

-destmailbox *DestMailboxName*

-chain

PUBLIC_FOLDERS_OPTIONS

-folder *FolderName*

-exclude *FolderName*

-originalfolder { -keep_msg | -overwrite_msg }

-chain

MICROSOFT SQL SERVER RESTORE

omnir -mssql

-barhost *ClientName*

[-destination *ClientName*]

[-instance *SourceInstanceName*]

[-destinstance *DestinationInstanceName*]

{ -base *DBName* -session *BackupID* [*MSSQL_OPTIONS*]... | -base *DBName* -datafile *GroupName*|*DataFileName* -session *BackupID* [*DATAFILE_OPTIONS* ...]}

[*GENERAL_OPTIONS*]

MSSQL_OPTIONS

-asbase *NewDBName* { -file *LogicalFileName1* *PhysicalFileName1* [-file *LogicalFileName2* *PhysicalFileName2* ...]}

-replace

-singleuser

-nochain

-recovery { rec | norec }

-stopat yyyy/mm/dd.hh:mm:ss

-standby *File*

-tail_log *BackupSpecificationName*

DATAFILE_OPTIONS

-replace

-singleuser

-nochain

-recovery { rec | norec }

MICROSOFT SHAREPOINT SERVER 2010/2013 RESTORE

omnir -mssharepoint

-barhost *HostName*

[-destination *RestoreClientName*]

-user *User* : *Group*

[-session *BackupID*]

[-replace]

[-byserver *ServerName* [-byserver *ServerName* ...]]

-farmname *FarmName*

[*Component* [*Component* ...]]

[*GENERAL_OPTIONS*]

Component

-configdb |

-webapplication *WebApplicationName* [WEB_APPLICATION_OPTIONS] [*ContentDatabase* [*ContentDatabase* ...]] |

-ssp *SSPName* [*SSP_OPTIONS*] [-index *INDEX_OPTIONS*] [*Database* [*Database* ...]]

[-webapp *WebApplicationName* [*WEB_APPLICATION_OPTIONS*] [*ContentDatabase* [*ContentDatabase* ...]]]

-wsssearch [*Database*] |

-ssodb [*DB_OPTIONS*]

ContentDatabase

-db *DBName* -host *DBHostName* [-unlink] [*DB_OPTIONS*]

Database

-db *DBName* -host *DBHostName* [*DB_OPTIONS*]

WEB_APPLICATION_OPTIONS

-as *WebApplicationName*

-url *WebApplicationURL*

-poolusername *Username* [-poolpassword *Password*]

-replace

DB_OPTIONS

-sqllogin *Username* [-sqlpassword *Password*]

-instance *SourceInstanceName*

-as *NewDBName*

-tohost *DBHostName*

-newinstance *DestinationInstanceName*

-todir *NewDirectoryName*

-replace

SSP_OPTIONS

-ssplogin *Username* [-sspassword *Password*]

-as *SSPName*

-mysiteurl *MySiteWebAppUrl*

INDEX_OPTIONS

-tohost *IndexServerHostName*

-todir *NewDirectoryName*

LOTUS RESTORE

omnir -lotus

-barhost *ClientName*

[-user *User:Group*]

[-destination *ClientName*]

[-parallelism *n*]

-domino_server *srv_name*

-appname

-db *db1* [-db *db2* ...]

[-NSF] [-NTF] [-BOX] [-ALL]

[-direx *direx1* [-direx *direx2* ...]]

[-r_dest *restore_dir*]

[-recover | recovery_time *yyyy/mm/dd.hh:mm:ss*]

[-reset_replica]

[-session *BackupID*]

MICROSOFT VOLUME SHADOW COPY SERVICE RESTORE

STANDARD RESTORE

omnir -vss

-barhost *ClientName*

-session *BackupID1* { *Tree* [*Tree* ...]}

[-session *BackupID2* { *Tree* [*Tree* ...]}...]

[-no_recovery]

[-into *PathName*]

[-destination *ClientName*]

[*VSS_EXCHANGE_SPECIFIC_OPTIONS*]

[*GENERAL_OPTIONS*]

INSTANT RECOVERY

omnir -vss

-instant_restore

-barhost *ClientName*

-session *SessionID1* { *Tree* [*Tree* ...]}

[-session *SessionID2* { *Tree* [*Tree* ...]}...]

[-no_recovery]

[-destination *ClientName*]

[*VSS_INSTANT_RECOVERY_OPTIONS*]

[*VSS_EXCHANGE_SPECIFIC_OPTIONS*]

[*GENERAL_OPTIONS*]

Tree

-tree *TreeName* [*VSS_EXCHANGE_2010_SPECIFIC_OPTIONS*]

VSS_INSTANT_RECOVERY_OPTIONS

[-conf_check { strict | non-strict | disabled }]

[-no_retain_source]

[-use_vds | -use_vss | *VSS_P9000_DISK_ARRAY_XP_OPTIONS* | *VSS_P10000_OPTIONS* | *VSS_P4000_OPTIONS*]

VSS_P9000_DISK_ARRAY_XP_OPTIONS

-copy_back -no_retain_source [-no_diskarray_wait]

VSS_P10000_OPTIONS

-copy_back

VSS_P4000_OPTIONS

-copy_back

VSS_EXCHANGE_SPECIFIC_OPTIONS

[-exch_check [-exch_throttle *Value*] | -exch_checklogs]

VSS_EXCHANGE_2010_SPECIFIC_OPTIONS

[[-target_tree *TargetStoreName* | -exch_RSG *LinkedStoreName*] -target_dir *Directory*]

DB2 RESTORE

omnir -db2

-barhost *ClientName*

-instance *InstName*

{[-dbname *DBName* [-session *BackupID*] [-newdbname *NewDBName* ...]] [-tsname *DBName*TSName* [-session *BackupID*] [-offline ...]] [-logfile *DBName*LogFileName* [-session *BackupID* ...]]}

[*DB2_OPTIONS*]

DB2_OPTIONS

-destination *ClientName*

-rollforward [-time *YYYY-MM-DD.hh.mm.ss*]

-frominstance *InstName*

MYSQL RESTORE

omnir SESSION_OPTIONS

-integ MySQL

-barhost *TargetMySQLHostname*

-appname *TargetInstanceName*

-user *Username:GroupName*

-options MYSQL_OPTIONS

[GENERAL_OPTIONS]

SESSION_OPTIONS

[-report {warning | minor | major | critical}]

MYSQL_OPTIONS

-source_client *SourceMySQLHostname*

-source_instance *SourceInstanceName*

-database *DATABASE_OPTIONS* | -binary_log *BINARY_LOG_OPTIONS*

DATABASE_OPTIONS

–session *SessionID*

{ –staging [CustomStagePath]

[–copy_back [–target_dir NonOriginalTargetPath]

–import] |

–inplace [–target_dir NonOriginalTargetPath]}

[–include {DatabaseName | DatabaseName.TableName}] ...

[–roll_forward [YYYY–MM–DD hh:mm:ss]]

BINARY_LOG_OPTIONS

-include BinaryLogFilename [-include BinaryLogFilename] ...

[-target_dir NonOriginalTargetPath]

POSTGRESQL RESTORE

omnir SESSION_OPTIONS

-integ *PostgreSQL*

-barhost *TargetPostgreSQLHostname*

-appname *TargetInstanceName*

-user *Username:GroupName*

-options *POSTGRESQL_OPTIONS*

[GENERAL_OPTIONS]

SESSION_OPTIONS

[-report {warning | minor | major | critical}]

POSTGRESQL_OPTIONS

-source_client *SourcePostgreSQLHostname*

-source_instance *SourceInstanceName*

-target_dir *NonOriginalTargetPath*

[-session SessionID] |

[–roll_forward [YYYY–MM–DD hh:mm:ss]]

DATA_OPTIONS

-exclude *PathName* ...

-skip *MatchPattern* ...

-only *MatchPattern* ...

-as *Pathname*

-into *Pathname*

MEDIUM_OPTIONS

-device *BackupDevice*

-medium *MediumID*

-id *DiskAgentID*

-slot *SlotID* [*Side*]

FILESYSTEM_OPTIONS/FILESYSTEM_OPTIONS_BLOCKBASED

-touch

-lock

-no_protection

-[no_]overwrite | -merge

-catalog

-sparse

-move_busy

-no_share[_info]

-omit_unrequired_object_versions

-[no_]resumable

IDB RESTORE

-idb

-barhost *ClientName*

[-restoredb [*RESTORE_DB_OPTIONS*]]

[-restoreconf [*RESTORE_CONF_OPTIONS*]]

[-restoredcbf [*RESTORE_DCBF_OPTIONS*]]

[-client *SourceClientName*]

[-until *YYYY* - *MM* - *DD* [*hh* . *mm* . *ss*]]

[-pre *PathName*]

[-post *PathName*]

[*GENERAL_OPTIONS*]

RESTORE_DB_OPTIONS

-targetdir *TargetDataFolderPath*

-port *TargetDatabasePort*

[-nodbrecover | -nouseasnewidb]

RESTORE_CONF_OPTIONS

[-keeprecent | -nooverwrite | -overwrite]

[-session *SessionID*]

[-targetdir *TargetConfFolderPath*]

[-name *FileOrFolderName* ...]

RESTORE_DCBF_OPTIONS

[-targetdir *TargetDCBFFolderPath*]

GENERAL_OPTIONS

-device *BackupDevice*

-no_auto_device_selection

-server *ServerName*

-target *Client*

-profile

-load { low | medium | high }

-pre_exec *PathName*

-post_exec *PathName*

-variable *VariableName VariableValue*

-no_monitor

[-priority *NumValue*]

-s3_tier *S3RestoreTier*

-s3_tier_policy *S3RestoreTierPolicy*

-s3_rate *S3RestoreTierPolicyRate (GB/Hour)*

SPLIT_MIRROR_OPTIONS

-sse

-remote *ApplicationSystem BackupSystem* | -local *ApplicationSystem BackupSystem* | -combined *ApplicationSystem BackupSystem*

[-quiesce *cmd*]

[-restart *cmd*]

[-mirrors *list*]

[-discovery]

[-re_establish_links_before_restore]

[-disable_disks]

[-restore_links_after_restore]

DESCRIPTION

The omnir command restores objects backed up using Data Protector. You can use the omnir command to restore filesystems, vProtect objects, very big file systems, disk image sections, NDMP objects, and Data Protector Internal Database (IDB) to their original or different location. It can also be used for restoring application integration objects (SAP R/3, Microsoft Exchange Server 2010/2013, Microsoft Exchange Server single mailboxes, Microsoft SQL Server, Microsoft SharePoint Server 2010/2013, Lotus, Informix Server, VMware vSphere, Microsoft Hyper-V, IBM DB2 UDB, MySQL, or SAP MaxDB), or to start the instant recovery process. To restore a Sybase database, see the syb_tool man pages.

If several copies of the same object version exist, you can let Data Protector select which media set will be used for the restore. You can also specify the media set from which you want to restore the data, except when restoring the IDB or an integration object. It is not possible to specify the media set created as a result of the media copy operation.

The omnir command also supports parallel restore. You can achieve this by specifying more than one object using the command line options. It is not possible to use the -medium option when performing a parallel restore. The number of objects for parallel restore is limited by the MaxSessions global option.

Note It is not allowed to specify the same object more than once within the same omnir command. To differentiate options for the same object (for example, the -tree option) specify these options for the same object as many times as needed.

Information about all backed up objects can be obtained from the IDB by using omnidb command or, in the case of the instant recovery, from a ZDB database or VSS database by using the omnidbxp , omnidbsmis , or omnidbvss command. For more information on these commands, see the related man pages. For most restore actions you need to specify the *SessionID* of the session containing the object you want to restore, which can be obtained by the omnidb command.

Note When restoring integration objects, provide the *SessionID* of the backup session. In case of object copies, do not use the object copy session ID, but the object's *BackupID* , which equals the original object's backup session ID. If imported backup media are used for restoring an object, do not specify the new session ID which is assigned to the imported backup session, but the object's BackupID which is the original backup session ID for that object.

To restore objects from a medium that is not in the IDB, use the -medium *MediumID* option, instead of the *SessionID* .

Note The -medium option is not possible when performing a parallel restore.

To get the *MediumID* and *DiskAgentID* from the medium, use the omnimlist command to read the medium. See the omnimlist man page for more information on this command.

Note When restoring a Microsoft SQL Server with the -tail_log option specified, a tail log backup session is performed before the actual restore session starts.

SAP specific global option

With Data Protector 10.01, a new global option SessSuccessfulWhenSAPNoArchiveLogsBackedUp is added. By enabling this option, the SAP backup session is marked as successful, even if 0 archive logs were backed up.

OPTIONS

-version

Displays the version of the omnir command.

-help

Displays the usage synopsis of the omnir command.

-resume *SessionID*

Starts a new session that continues with the restore from where the failed session *SessionID* left off, using the same options as used in the failed session. This functionality is supported for filesystem restore sessions and Data Protector Oracle Server integration restore sessions.

FILESYSTEM RESTORE

-filesystem *Client:MountPoint Label*

Selects the filesystem identified with *Client:MountPoint Label* for restore.

-vProtect *Client:MountPoint Label*

Selects the vProtect object identified with *Client:MountPoint Label* for restore.

-winfs *Client:MountPoint Label*

Selects the Windows filesystem identified with *Client:MountPoint Label* for restore.

-winfsblockbased *Client:MountPoint Label*

Selects the Windows blocks identified with *Client:MountPoint Label* for restore.

-session *SessionID*

Specifies the session to be used for restore.

-copyid *CopyID*

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

-tree *TreeName*

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must

be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives). For example: -tree /usr/temp (UNIX systems) and -tree /temp/Filesystem/E (Windows systems).

-full

Specifies that the selected object will be restored from the last full backup and all incremental backups related to this full backup.

-omit_deleted_files

This option can only be used in combination with the -overwrite option. For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

If this option is specified, Data Protector recreates the state of the backed up directory tree at the time of the chosen incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are not restored.

If this option is not specified, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

If you use this option in combination with the -as or -into option, carefully choose the restore location to prevent accidental removal of existing files.

-host *ClientName*

Restores all objects of the specified client that were backed up in the specified session. This option is only valid for the filesystem restore.

DISK IMAGE RESTORE

-rawdisk *Client Label*

Selects the disk image identified by *Client* and *Label* for restore.

-session *SessionID*

Specifies the session to be used for restore.

-copyid *CopyID*

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

-section [*ToSection* =] *Section*

Specifies the disk image section to be restored. To restore the section to a new section, include both the source and destination section.

NDMP RESTORE

-full

Specifies that the selected object will be restored from the last full backup and all incremental backups related to this full backup.

-filesystem *Client:MountPoint Label*

Selects the filesystem identified with *Client:MountPoint Label* for restore.

-session *SessionID*

Specifies the session to be used for restore.

-tree *TreeName*

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives). For example: -tree /usr/temp (UNIX system) and -tree /temp/Filesystem/E (Windows system).

-into *Pathname*

Restores the selected fileset into the given directory.

-ndmp_env *FileName*

Specifies the filename of file with NDMP environment variables for specific NDMP implementations.

SAP R/3 FILE RESTORE

-sap *Client:Set*

Selects the SAP R/3 object identified by *Client:Set* for restore.

-session *SessionID*

Specifies the session to be used for restore.

-copyid *CopyID*

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

-tree *TreeName*

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives). For example: -tree /usr/temp (UNIX system) and -tree /temp/Filesystem/E (Windows system).

INFORMIX SERVER RESTORE

-informix

Selects the Informix Server object for restore.

-barhost *ClientName*

Specifies the Informix Server client from which the data was backed up.

-barcmnd *PathName*

The value of the barcmnd option has to be set to ob2onbar.pl .

-user *UserName:GroupName*

Specifies *Username* and *GroupName* that started the script specified by the -barcmnd option.

-appname *ApplicationDatabaseName*

Specifies the database server name of Informix Server to be restored.

-bararg *OnBarRestoreArguments*

Specifies the onbar restore arguments. Each onbar restore argument has to be put in double quotes.

MICROSOFT 365 RESTORE

- organization OrganizationName

Specifies the name of the Microsoft 365 organization as registered in Azure Active Directory (AD).

-barhost *ClientName*

Specifies the Microsoft 365 client from which the data was backed up.

-tenantname *TenantName*

Specifies the name of the Microsoft 365 publisher domain.

-mailbox *MailboxName*

Specifies the name of the Microsoft 365 mailbox for restore.

-session *backupsessionID*

Specifies the ID of the backup session that you want to restore, for example, 2020/10/23-2 .

-azureapp *AzureApplicationName*

Specifies the name of the Azure application under which the backup session was created.

-restorelocation RestoreFolder

Specifies the name of the folder for restoring the data.

MICROSOFT EXCHANGE SERVER 2010 RESTORE

-msese

Selects the Microsoft Exchange Server object for restore.

-barhost *ClientName*

Specifies the Microsoft Exchange Server client from which the data was backed up.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-appname *full_application_name*

Specifies a Microsoft Exchange Server Information Store, Site Replication Service or Key Management Service for the restore. The name of the Store/Service (*full_application_name*) must be provided in double quotes as follows:

- For the Information Store: Microsoft Exchange Server (Microsoft Information Store)
- For the Site Replication Service: Microsoft Exchange Server (Microsoft Site Replication Service)
- For the Key Management Service: Microsoft Exchange Server (Microsoft Key Management Service)

-base *DBName*

Specifies the Microsoft Exchange Server store or logs for restore.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2011/10/09-2 .

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

This option must be set for every -base option specified.

-logpath *path*

Specifying this option, you set the temporary directory for the Microsoft Exchange Server log files. Data Protector restores the log files to this directory. Using this directory, the Microsoft Exchange Server then recovers the database - this operation is referred to as hard recovery.

-last

Hard recovery is performed after the restore of the Microsoft Exchange Server object. Use this option if you are restoring the last set of files. If you do not set this option, you have to start the recovery manually by running the eseutil /cc /t utility from the directory for temporary log files. If this option is not specified, soft recovery is performed after the restore.

-mount

The restored Microsoft Exchange Server databases will be automatically mounted after the soft or hard recovery.

-consistent

Restores the database to its last consistent state. The latest log files, created after backup, are applied to the restored database during recovery.

MICROSOFT EXCHANGE SERVER 2010/2013 RESTORE

-e2010

Selects the Microsoft Exchange Server 2010/2013 object for restore.

-barhost *ClientName*

Specifies on which client to start the Data Protector Microsoft Exchange Server 2010 integration agent (e2010_bar.exe). This can be any client that has the MS Exchange Server 2010+ Integration component installed.

-instant_restore

Performs an instant recovery.

-user *User:Domain*

Specifies which Windows domain user account to use to start the restore session. Ensure that the specified user has appropriate Microsoft Exchange Server permissions, is added to the Data Protector admin or operator user group, and is saved to a Windows Registry on the Microsoft Exchange Server client on which the integration agent (e2010_bar.exe) will be started (see the Data Protector omnicc command).

If this option is not specified, the restore session is started under the user account under which the Data Protector Inet service is running.

{ -db_name *SourceDatabaseName* | -db_guid *SourceDatabaseGUID* }

Specifies which database to restore. If the database no longer exists, use the -db_guid option.

-source *SourceClientName*

Specifies from which client the database was backed up. For databases that are part of a DAG, specify the DAG virtual system (host). If this option is not specified, Data Protector assumes that the database was backed up from the client specified with the -barhost option.

{ -repair | -latest | -pit | -new | -temp }

Specifies which restore method to use:

repair : Available only for databases that are part of a Microsoft Exchange Server Database Availability Group (DAG). Automatically restores all the corrupt passive copies (copies with the status Failed or FailedAndSuspended).

latest : Restores a corrupt database to the latest possible point in time.

pit : Restores an existing database to a specific point in time.

new : Restores files to a different database, either because the original database no longer exists or in order to move the data elsewhere.

temp : Restores files to a location of your choice.

-no_resume_replication

Specifies that the replication between the active and passive copies should not be resumed after the restore session

completes.

-node *TargetNode ...* | -all

Specifies which clients (that is, database copies) to restore.

-no_recover

Specifies that logs should not be applied to the database file after the restore completes.

-no_mount

Specifies that the database should not be mounted after the database recovery completes.

-session { *BackupID* | *SessionID* }

Specifies from which backup data to restore, for example, 2012/10/09-2 .

For standard restore, specify *BackupID* . A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

If a differential backup session is selected, the .log files backed up in the selected differential backup session are restored.

If an incremental backup session is selected, the .log files backed up in all subsequent incremental backup sessions, up to the selected incremental backup session, are restored.

For instant recovery, specify *SessionID* of a ZDB-to-disk or ZDB-to-disk+tape session.

-client *TargetClientName*

Specifies to which client to restore.

-location *TargetDatabasePath*

Specifies to which directory to restore.

-name *TargetDatabaseName*

Specifies which name to use for the new database. If another database with the same name already exists, the restore is not performed.

-recoverydb

Restores files to a Microsoft Exchange Server recovery database.

Although multiple recovery databases can exist in parallel, only one recovery database can be mounted to the Microsoft Exchange Server at a time.

-no_chain

Restores only the files backed up in the selected session.

By default, the complete chain is restored.

-edb_only

Restores only the database file (.edb). Logs (.log) and checkpoint files (.chk) are not restored.

-from_session

An instant recovery specific option that specifies which full or copy ZDB session to use as a starting session in a restore chain.

Use this option if the session that you specified for instant recovery is an incremental or a differential session. If you do not use it, the integration agent uses the last full or copy session as the starting point in a restore chain for instant recovery.

MICROSOFT EXCHANGE SINGLE MAILBOX RESTORE

-mbx

Selects Microsoft Exchange Server single mailboxes and Public Folders for restore.

-barhost *ClientName*

Specifies the Microsoft Exchange Server client from which the data was backed up.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-mailbox *MailboxName*

Specifies the Microsoft Exchange Server single mailboxes for restore.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2 .

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

-public

Specifies the Microsoft Exchange Server Public Folders for restore (as part of the Microsoft Exchange Server single mailbox restore).

-folder *FolderName*

Specifies folders to be restored. Note that the subfolders are also restored. If this option is not specified, all backed up folders are restored.

-exclude *FolderName*

Specifies the folders to be excluded from restore.

-originalfolder { -keep_msg | -overwrite_msg }

If this option is selected, Data Protector restores Exchange Server items to the same folders in which they were when the backup was performed.

If -keep_msg is selected, the messages in the mailbox or Public Folders are not restored, even if they are different from their backed up version.

If -overwrite_msg is selected, all messages are restored, replacing their current versions (if they exist). If different versions of the same message exist in the mailbox or Public Folders (for example, if you have a copy of the message), only one is replaced with the backed up version and all other versions remain intact.

The messages in the mailbox that were not backed up in the specified backup session (or the restore chain of backup sessions) always remain intact.

If -originalfolder is not specified, Data Protector creates a new folder in the root of the mailbox or in the root of All Public Folders and restores Exchange items into it. For a mailbox restore, the folder is named Data Protector BackupDate *BackupTime*, and for a Public Folders restore, it is named Data Protector BackupDate *BackupTime* - public folder. If you restore a mailbox or Public Folders from the same backup several times, a number is appended to the folder name. For example, in the second restore session of a mailbox, the folder Data Protector BackupDate *BackupTime* (1) is created.

-destmailbox *DestMailboxName*

Specifies the destination mailbox, into which data will be restored. The destination mailbox must exist on the target Microsoft Exchange Server. If this option is not specified, data is restored to the original mailbox.

-chain

If this option is specified, data is restored not only from the specified backup session, but also from the latest full, the latest incremental1 (if exists), and all incremental backups from the last incremental1 up to the specified version.

LOTUS RESTORE

-lotus

Selects the Lotus Notes/Domino Server object for restore.

-barhost *ClientName*

Specifies the Lotus Notes/Domino Server client from which the data was backed up.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-parallelism *n*

Sets the number of restore streams, running in parallel. The default is 1.

-domino_server *srv_name*

Sets the name of the Lotus Notes/Domino Server which you want to restore.

-appname

Specifies the Lotus Notes/Domino Server instance source.

-db *db*

Sets the restore of an individual Lotus Notes/Domino Server database.

-NSF

Sets the restore of all NSF (Notes Storage Facility) databases.

-NTF

Sets the restore of all NTF (Notes Templates Facility) files.

-BOX

Sets the restore of all BOX files.

-ALL

Sets the restore of all objects, NSF databases, NTF files and BOX files.

-dir *dir*

Sets the Lotus Notes/Domino data directories that you want to include in the restore. Enter their relative pathnames to the Lotus Notes/Domino data directory.

-direx *direx*

Sets the Lotus Notes/Domino data directories that you want to exclude from the restore. Enter their relative pathname to the Lotus Notes/Domino data directory.

-r_dest *restore_dir*

Sets the relative pathname to the restored database directory.

-recover

Specify this option to perform the recovery of the restored database to the last possible consistent state.

-recovery_time *yyyy/mm/dd.hh:mm:ss*

Sets a point in time to which you want the database to be recovered.

-reset_replica

This option should be used only when restoring to the last possible consistent state. If the option is specified, each restored storage database (NSF database) is assigned a new replica ID.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2 .

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

DB2 RESTORE

-db2

Selects the IBM DB2 UDB object to restore.

-barhost *ClientName*

Specifies the IBM DB2 UDB client from which the data was backed up.

-instance *InstName*

Sets the name of the database instance that was backed up.

-dbname *DBName*

Sets the name of the DB2 database that you want to restore.

-newdbname *NewDBName*

Specify this option if you want to restore the whole DB2 database into a new database.

-tsname *DBName*TSName*

Sets the name of the DB2 table space that you want to restore. To specify the table space you would like to restore, write the name of the database, then the "*" character and finally the name of the table space (without spaces).

-logfile *DBName*LogFileName*

Sets the name of the DB2 Log file that you want to restore. It should not be used with the -rollforward option. To specify the Log file you would like to restore, write the name of the database, then the "*" character and finally the name of the Log file (without spaces).

-offline

Specify this option if you want to restore a table space offline.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-rollforward [time: *YYYY-MM-DD.hh.mm.ss*]

Specify the point in time when you want a rollforward to be performed to. The rollforward point in time *must* be entered in local time (as it is set on the DB2 target server) and not in coordinated universal time (UTC). If you specify a rollforward option without time argument, a rollforward will be performed to the end of the logs.

-frominstance *InstName*

Sets the name of the DB2 instance from which you want to restore the data.

MICROSOFT VOLUME SHADOW COPY SERVICE RESTORE

-vss

Selects the VSS object for restore.

-barhost *ClientName*

Specifies the system on which the backup session was originally performed.

-session { *BackupID* | *SessionID* }

Specifies from which backup data to restore, for example, 2012/10/09-2 .

For standard restore, specify *BackupID* . A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

For instant recovery, specify *SessionID* of a ZDB-to-disk or ZDB-to-disk+tape session.

-tree *TreeName*

Specifies the file, component, or tree to restore. For example, to specify a component, you can use: -tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/StoreOne"

When specifying trees, the trees must be specified without the drive letter.

-into *Pathname*

Restores the selected files, component, or tree into the given directory.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up. If not specified, the components are always restored to the server from where they were backed up. Note that all objects in one restore session must be restored to the same system.

-instant_restore

Selects instant recovery for ZDB and VSS integrations.

-conf_check { strict | non-strict | disabled }

Defines the configuration check mode. If this option is specified, Data Protector checks whether the individual components can be selectively restored using the instant recovery functionality. The check detects whether there is more than one component on the volume or there is any data besides the component's data on the volume. If the check fails, the instant recovery session will fail. Specify the strict mode to check each file or folder. Specify the non-strict mode to check each folder. Disable configuration check only if instant recovery cannot be performed with an enabled configuration check and only after you make sure that this will not result in a loss of data. In case of a data loss, the data that does not belong to a component, but resides on the same volume, will be lost.

-no_recovery

Leaves the application database in the recovery mode after completion of the restore session, enabling you to manually apply transaction logs to the database.

This option is available only for the SQL Server writer.

-use_vds

Switches a replica from the specified backup session with the source volume. Once switched, the replica is not available for another instant recovery session and also information about this replica is deleted from the database (VSSDB). Does not use a ZDB array specific options or agents.

With disk arrays of the P9000 XP Disk Array Family, this option must be used after the backup created with the P9000 XP Array provider in the VSS compliant mode.

-use_vss

The instant recovery is performed by the VSS hardware provider (VSS LUN resync). The actual instant recovery method depends on the disk array and VSS hardware provider settings. The VSS LUN resync functionality must be supported by the operating system and the VSS hardware provider.

VSS_P9000_DISK_ARRAY_XP_OPTIONS

-copy_back

Performs resynchronization of the disk pair, copying data from the target volume (backup disk) to the source volume. This option must be specified if the data was backed up with VSS provider in the resync mode.

-no_retain_source

Deletes the source volume during restore. This option must be specified if the data was backed up with VSS provider in the resync mode since there is no possibility to retain the source during re-synchronization of replica and source disk.

-no_diskarray_wait

If this option is specified, the source volume is immediately available while the synchronization or copy process is running in the background (quick restore). The SSE Agent does not wait for the synchronization or copy process to complete. If this option is not specified, there is a 60–minute delay before the background processes can run.

VSS_P10000_OPTIONS

-copy_back

Performs a restore of snapshot data to the source volume.

VSS_P4000_OPTIONS

-copy_back

Performs a restore of snapshot data to the source volume.

NOTE: All snapshots dependent on the snapshot being used for restore are deleted.

VSS_EXCHANGE_SPECIFIC_OPTIONS

-exch_check

Performs the consistency check of the Microsoft Exchange Server database replicated datafiles. The Microsoft Exchange Server database backup is considered as successful only if the consistency check succeeds. Use this option if consistency check was not performed during backup.

-exch_throttle *Value*

Throttles down the consistency check to lessen impact on restore performance. Set the number of input/output operations, after which the check is stopped for one second.

-exch_checklogs

Performs the consistency check of the log files only, which is enough for Microsoft Exchange Server to guarantee backup data consistency.

VSS_EXCHANGE_2010_SPECIFIC_OPTIONS

-target_tree *TargetStoreName*

Specifies the target component to which the source component will be restored and enables you to restore a subcomponent to a different component than the one from which it was backed up. This option can be used only once for each -tree option and cannot be specified together with -exch_RSG .

TreeName and its *TargetStoreName* pair must always be fully expanded subcomponents representing an Exchange store or logs. To get a list of available targets on a specific host, execute the command:

vssbar -appsrv:HostName -perfom:browse -all

Potential targets can be identified by the string "RESTOREMODE = 1".

NOTE: You cannot restore only a store without logs to a different location. If you specify a target store for an original store, you must also specify logs with an additional -tree TreeName -target_tree TargetStoreName pair.

The option must be specified together with -target_dir .

-exch_RSG *LinkedStoreName*

Creates a new Recovery Storage Group (RSG) and links it to *LinkedStoreName* . This option can be used only once for each -tree option and cannot be specified together with -target_tree . Only one storage group per session can be restored with this option due to an Exchange limitation. *LinkedStoreName* and its *TreeName* pair must always be fully expanded subcomponents, representing an Exchange store or logs.

IMPORTANT: If the RSG already exists, it is removed and a new one is created. Any existing data in it will be lost. NOTE: You cannot restore only a store without logs to a different location. If you specify a target store for an original store, you must also specify logs with an additional -tree TreeName -target_tree TargetStoreName pair.

The option must be specified together with *-target_dir* .

-target_dir *Directory*

During an instant recovery session, the replica will be mounted to *Directory* . The target directory for one session must always be the same, for example, you cannot specify one target directory for the store(s) and another one for the logs.

SAP MAXDB RESTORE

-sapdb

Selects the SAP MaxDB object for restore.

-barhost *ClientName*

Specifies the SAP MaxDB client from which the data was backed up.

-instance *InstName*

Sets the name of the database instance that was backed up.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-newinstance *DestinationInstanceName*

Performs a restore to the SAP MaxDB instance with the instance name *DestinationInstanceName*. This option is to be used only when a restore to an instance other than the one that was backed up is to be performed. Note that the specified instance must already exist and must be configured for use with Data Protector. This option does not create a new instance.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2.

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

If this option is not specified, backup data created in the last backup session is restored regardless of the -endlogs or the -time option selection.

-recover [-endlogs | -time: *YYYY-MM-DD.hh.mm.ss*]

Specify this option to recover the restored SAP MaxDB database by applying the restored (if the -from_disk option is not specified) or client-resident logs (if the -from_disk option is specified) to the last available log (the default behavior, or if the -endlogs option is specified), or to the specified point in time (if the -time: option is specified).

Make sure that the backup session selected by the -session option will restore enough data for the integration to apply the redo logs until the last available log or until the specified point in time.

When this option is not specified, the following happens after the restore:

- If archive logs are not restored (if restore from a full backup session is performed), the database remains in the Admin mode after the restore.

- If archive logs are restored, the database is, if the restored archive logs allow it, switched to the Online mode. If the database, however, cannot be switched to the Online mode (because the restored archive logs do not allow it), it remains in the Admin mode.

-endlogs

Specify this option to recover the database until the last log. This is the default option.

-time: *YYYY-MM-DD.hh.mm.ss*

Specify the -time: option to recover the database until the point specified by the *YYYY-MM-DD.hh.mm.ss* argument.

Note that the specified time is the system time on the system running the Data Protector CLI. If the system to be recovered is not in the same time zone as the system running the Data Protector CLI, the point of recovery is adjusted to the local time setting on the system to be restored.

-from_disk

Specify this option to apply the existing archive logs on the SAP MaxDB Server to SAP MaxDB Server redo logs.

If this option is not specified, the backed up archive logs on backup media are applied to the redo logs (if trans backup session is restored), or the redo logs are left intact together with the existing archive logs on the SAP MaxDB Server (if full or diff backup session is restored).

When a transactional backup session is selected for restore or when it is a part of the needed restore chain, and the this

option is specified at the same time, the archive logs from Data Protector media are applied to the redo logs. Thereafter, the archive logs on the SAP MaxDB Server are applied to redo logs.

This option is ignored in case of SAP MaxDB migration, thus allowing only for the restore of redo logs from the backed up archive logs on backup media (if trans backup session is restored).

-nochain

This option instructs the command to restore only the selected or last backup session; the integration does not restore the whole restore chain of full, differential, and transactional backups.

MICROSOFT SQL SERVER RESTORE

-mssql

Selects the Microsoft SQL Server object, identified with *DBName*, for restore.

-barhost *ClientName*

Specifies the Microsoft SQL Server client from which the data was backed up.

-destination *ClientName*

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

-instance *SourceInstanceName*

Sets the name of the Microsoft SQL Server instance to be restored. omnir takes the (DEFAULT) instance by default.

The *SourceInstanceName* is case-sensitive; it has to be the same as the name of the SQL Server instance that you specified in the backup specification.

-destinstance *DestinationInstanceName*

Specify this option to determine an Microsoft SQL Server instance into which the data will be restored. omnir takes the (DEFAULT) instance by default.

-base *DBName*

Specifies the SQL Server database for restore. The database name is case–sensitive.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2.

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

-datafile *GroupName*|*DataFileName*

Specifies an SQL Server data file for restore. *GroupName* is the name of the group the data file belongs to.

-asbase *NewDBName* { -file *LogicalFileName1* *PhysicalFileName1*

[-file *LogicalFileName2 PhysicalFileName2*]...}

This option can only be used for database restore.

Enables restore of the Microsoft SQL Server database under a new name and restore of files to a new location. If the -asbase option is used, all logical and physical filenames have to be specified with the -file option.

-replace

Specify this option if a database with the same name but a different internal structure already exists at the target Microsoft SQL Server instance.

If this option is not specified, the Microsoft SQL Server does not let you overwrite the existing database - the restore will fail.

If you are restoring a data file from the PRIMARY group to an existing database, you must specify the option at the data file level.

When using this option, ensure that the most recent logs are backed up before the restore.

-singleuser

Disconnects all users that are connected to the target Microsoft SQL Server database and puts the database in the single user mode. Note that if the database is not in the simple recovery mode, the -replace option should also be specified.

-nochain

Microsoft SQL Server integration: Restores only the data identified by the -session option. If the option -session is not specified, backup data created in the latest backup session is restored.

-recovery { rec | norec }

Specifies the state (recovered, nonrecovered) of the Microsoft SQL Server database after the restore. The default value for this option is rec .

-stopat *yyyy/mm/dd.hh:mm:ss*

This option is only available for database objects.

Specifies the exact time when the rollforward of transactions will be stopped. Therefore, to enable database recovery to a particular point in time, the backup you restore from must be a transaction log backup.

You cannot use this option with norecovery or standby. If you specify a stop at time that is after the end of the restore log operation, the database is left in a non-recovered state (as if the restore log is run with norecovery).

-standby *File*

This option can only be used for database restore.

Specifies the standby state of the Microsoft SQL Server database after the restore.

-tail_log *BackupSpecificationName*

Specify this option to perform a tail log backup session before the actual restore session starts.

MYSQL RESTORE

-integ MySQL

Selects a MySQL backup object for restore.

-barhost TargetMySQLHostname

Specifies the Data Protector client to restore data to. You can specify any client that hosts MySQL database management system and has the Data Protector MySQL Integration component installed. On this client, the Data Protector MySQL integration agent is started at the beginning of the restore session.

-appname TargetInstanceName

Specifies the name of the MySQL instance you want to restore data to. If the instance does not exist yet, Data Protector automatically creates and registers it at the end of the restore session.

-user Username:GroupName

Specifies the username of the operating system user account to use for the restore session. The chosen account must be granted appropriate privileges as a MySQL database administrator and be a Data Protector user with the proper user rights for the restore scenario (Start restore , Restore from other users , Restore to other clients , and so on). If no value is specified, username of the Data Protector Inet account on the target client is used.

-source_client SourceMySQLHostname

Specifies the Data Protector client from which MySQL data was backed up.

-source_instance SourceInstanceName

Specifies the name of the original MySQL instance whose data was backed up.

-database

Enables Data Protector to primarily restore MySQL databases, database tables, or both, as opposed to restoring MySQL binary log files only. The MySQL integration agent is used in this process. If the -roll_forward option is also specified, Data Protector also restores and applies all the required binary log files according to the chosen time period. In this case, the Disk Agent is additionally used to restore binary log files.

-binary_log

Enables Data Protector to restore one or more MySQL binary log files only, as opposed to MySQL databases, database tables, or both. The Disk Agent is used in this process.

-session SessionID

This option can only be used in combination with the -database option.

Enables Data Protector to process the restore chain from its beginning up to end including the MySQL backup session with the specified session ID. Ensure the session ID belongs to a valid backup session.

-staging [CustomStagePath]

This option can only be used in combination with the -database option.

If the additional option -copy_back is not specified, performs the first phase of a staged restore. In this scenario, data from valid backup images of the restore chain is placed to an intermediate location on the target client leaving MySQL production data intact.

If the additional option -copy_back is specified, performs a complete staged restore.

If the additional option -import is specified, performs data migration of the database and/or database tables.

Specify the CustomStagePath parameter to use a custom folder for staging the restored data, instead of the Data Protector default folder for temporary files.

-copy_back

This option can only be used in combination with the -database and -staging options.

Performs the complete staged restore. Data from backup images of the restore chain is placed to an intermediate location on the target client first. Afterwards, this data is copied to the target location. The binary log is filtered and only the content applicable to the selected tables is recovered. The system tablespace is always restored regardless of the restore scope.

This restore method requires more storage space from an in-place restore, but can better prevent potential data inconsistency in the event something goes wrong.

Use the -target_dir option to redirect restore to a location that differs from the original one

-target_dir NonOriginalTargetPath

This option can only be used in combination with the -copy_back , -inplace , or -include option.

Redirects restore of databases, database tables, or binary log files to a location that differs from the original one.

-import

This option can only be used in combination with the -database and -staging options.

Imports the selected MySQL databases, database tables, or both to the target MySQL instance. The database tables with the same name should not exist on the target instance. The target MySQL instance should be offline during the restore session.

The binary log is filtered and only the content applicable to the selected tables is recovered.

This options is supported with MySQL 5.6.6 and later versions.

-inplace [CustomStagePath]

This option can only be used in combination with the -database option.

Performs an in-place restore of MySQL data, as opposed to one or both phases of a staged restore. In this scenario, data from the backup images of the restore chain overwrites the MySQL production data (if it exists). Such restore process requires less storage space from a complete staged restore, but is more prone to potential data inconsistency in the event something goes wrong.

Note With this option selected, you can restore only the entire backup image to the target location regardless of the restore scope.

Use the -target_dir option to redirect restore to a location that differs from the original one.

-include {DatabaseName | DatabaseName.TableName}

This option can only be used in combination with the -database and -copy_back or -import options.

Narrows the scope of the restore process to the specified databases or database tables. Other MySQL entities are not restored even if they exist in the backup images of the restore chain. You can specify the -include option and a corresponding parameter more than once.

If this option is not specified, all backup data is included in the restore process.

-roll_forward [EndDateTime]

This option can only be used in combination with the -database option.

Recovers the restored MySQL entity (instance, database, or database table) by rolling it forward using transactions from the corresponding binary log files that Data Protector restores as needed. If you want Data Protector to bring the entity to a certain point in time (not the latest available state), specify the EndDateTime parameter to stop the rollforward at that particular date and time. For EndDateTime , use local time on the source client, not the coordinated universal time (UTC).

-include BinaryLogFilename

This option can only be used in combination with the -binary_log option.

Specifies the name of the binary log file which you want to restore. You can specify the -include option and a corresponding parameter more than once, thus restoring multiple binary log files in the same session.

VIRTUAL ENVIRONMENT RESTORE

-veagent

Selects the virtual environment objects for restore.

-virtual-environment { vmware | hyperv | vcd | h3ccas }

Specifies the virtual environment type.

-barhost *BackupHost*

Specifies the client with the Virtual Environment Integration component installed to control the restore session.

-apphost *OriginalAppHost*

Specifies the client that the virtual machine objects were backed up from.

-instance { *OriginalDatacenter* | *OriginalHostpool* }

Specifies the instance from which the virtual machines were backed up.

-method { vStorageImage | vCDvStorageImage | vStorageImageOpenStack | h3ccasImage -non-cached | h3ccasImage -cached|HyperV-RCT }

This is a VMware, H3C CAS, and Hyper-V specific option.

Specifies the method that is used for backup and restore.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2 .

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

If you specify the session ID of an incremental or differential backup session, all backup data from the corresponding backup chain is restored as well.

-fromsession *BackupID1* -untilsession *BackupID2*

Restores from the backup data created in the time interval between *BackupID1* and *BackupID2*.

-vm *vmpath*

For VMware and H3C CAS virtual machines, *vmpath* is the complete virtual machine path (for example, /MyVirtualMachines/VMname).

For Microsoft Hyper-V virtual machines, *vmpath* is the GUID (for example, 991B483A-C177-4EB0-9DBE-998E96692783).

-instanceUUID *vmInstanceUUID*

This is a VMware and H3C CAS specific option.

Specifies the instanceUUID of virtual machine for restore.

Note You should not specify the instanceUUID parameter for restore while restoring the virtual machine backed up from Data Protector 8.1 and below.

-versionID *VersionID*

This is a VMware specific option.

Specifies the version of a backed up object selected for the restore.

-new_name *NewVirtualMachineName*

This is a VMware and H3C CAS specific option.

Restores a virtual machine under a new name.

-disk *DiskName*

For VMware virtual machines, DiskName refers to the name of the disk. For example, scsi0:0 .

For Microsoft Hyper-V virtual machines, DiskName refers to the path of the disk. For example, c:\Disk1.vhdx. If the path of the disk contains special characters, the path must be enclosed in a single quote.

-newinstance { *TargetDatacenter* | *TargetHostpool* }

This is a VMware and H3C CAS specific option.

Specifies the datacenter or hostpool that the virtual machines are restored to. If this option is not specified, the virtual machines are restored to the original datacenter or hostpool.

-store { *TargetDatastore* | *TargetStoragePool* }

This is a VMware and H3C CAS specific option.

Specifies the datastore or storage pool to which the virtual machines should be restored. You can choose among all datastores or storage pools that are accessible by the specified restore target host. If this option is not specified, the virtual machines are restored to the original datastore or storage pool.

-destination *DifferentAppHost*

Specifies the client that the virtual machines are restored to. If you specify an ESX(i) Server system, the virtual machines are registered in and restored to it. If you specify a vCenter Server system, the virtual machines are registered in the vCenter Server but restored to one of its ESX(i) Server systems. If you specify a CAS server system (CVM), the virtual machines are restored to it.

If this option is not specified, the virtual machines are restored to the original client where they were backed up from.

-host_cluster *HostOrCluster*

Specifies the ESX(i) Server system, H3C CAS host or the cluster that the virtual machines are restored to. If this option is not specified, the virtual machines are restored to the original ESX(i) Server system, H3C CAS host or cluster.

-resourcePool *ResourcePool*

Specifies the resource pool on the ESX(i) Server system or the cluster that the virtual machines are restored to. If this option is not specified, the virtual machines are restored to the original resource pool.

-specificHost *SpecificHost*

Specifies the specific ESX(i) Server system or H3C CAS host in the cluster that the virtual machines are restored to. If this option is not specified, the virtual machines are restored to the original ESX(i) Server system or H3C CAS host.

-targetstoragepath *TargetStoragePathOfAllHyper-V-VMs*

This is a Hyper-V specific option.

Specifies the complete path for a different location where the virtual machines should be restored to. The original path is appended to the specified path. For example, if the original path is C:\VMStorage and the target path is D:\Restore, the virtual machines will be restored to D:\Restore\C\VMStorage.

-targetVM TargetH3CCASVM

This is a H3C CAS specific option.

Specifies the VM to which you want to restore individual disks. This option is applicable only with H3C CAS cached method.

-neworganization *TargetOrganization*

This is a VMware specific option.

Specifies the organization in vCloudDirector to which the virtual machines should be restored. If this option is not specified, the virtual machines are restored to the original organization.

-virtual_datacenter_path *TargetVDC*

This is a VMware specific option.

Specifies the path of the vDatacenter to which the virtual machines should be restored. If this option is not specified, the virtual machines are restored to the original vDatacenter.

-virtual_datacenter_uuid *TargetVDC*

This is a VMware specific option.

Specifies the UUID of the vDatacenter to which the virtual machines should be restored.

-vapp_path *TargetVApp*

This is a VMware specific option.

Specifies the path of the vApp to which the virtual machines should be restored. If this option is not specified, the virtual machines are restored to the original vApp.

Note that the virtual machines are restored as a new vApp if the original vApp is no longer available or all virtual machines of the selected vApp are restored.

-vapp_uuid *TargetVApp*

This is a VMware specific option.

Specifies the UUID of the vApp to which the virtual machines should be restored.

-vcenter_path *TargetVCenter*

This is a VMware specific option.

Specifies the path of the vCenter to which the virtual machines should be restored.

-vcenter_uuid *TargetVCenter*

This is a VMware specific option.

Specifies the UUID of the vCenter to which the virtual machines should be restored.

-network_name *TargetNetwork*

This is a VMware specific option.

VMware vSphere behavior:

Specifies the name of the network that enables virtual machines communication.

The target network can be selected for all virtual machines specified in the restore session.

If an individual virtual machine does not have a network adapter, no action is taken.

If an individual virtual machine has multiple network adapters, the first in the list is selected.

If you leave this option empty, the virtual machine is connected to the network available at the time of backup even though it might not be available anymore.

-network_uuid *TargetNetwork*

This is a VMware specific option.

Specifies the UUID of the network that enables virtual machines communication.

If an individual virtual machine is restored into an existing vApp, the vApp network is specified.

If all virtual machines of the selected vApp are restored, the Organization network is specified.

-consolidate

This is a VMware specific option.

Commits all snapshots (including non-Data Protector ones) to the virtual machine base once a virtual machine is restored.

-register

This is a VMware and H3C CAS specific option.

Registers the virtual machines once they are restored. If this option is not specified, you need to manually recover the restored virtual machines. By default, the option is selected.

-poweron

Puts the newly restored virtual machines online once they are restored.

-skipTagAttach

This is a VMware specific option. Skips attaching of a tag to the restored VM.

[-deletebefore | -deleteafter | -skip | -keep_for_forensics]

VMware and H3C CAS behavior:

The -deletebefore option deletes an existing virtual machine before it is restored, even if it resides in a different datacenter than your target datacenter, and then restores it from new. This is the space efficient option, but is less secure, since the old virtual machine is not available if the restore fails. Therefore, it should be selected with caution.

The -deleteafter option deletes an existing virtual machine after it is restored, even if it resides in a different datacenter than your target datacenter. If the restore fails, the existing virtual machine is not deleted. This is not supported with H3C CAS VM restore, but it is supported with H3C CAS individual disk restore using cached method.

The -skip option skips the restore of an existing virtual machine. This allows you to restore missing virtual machines without affecting existing ones.

The -keep_for_forensics option marks an existing virtual machine with a timestamp. The virtual machine which is kept for forensics is powered off after the restore and remains at the original location. It does not affect consecutive backups of the original virtual machine. This is not supported with H3C CAS.

If none of these options are specified, an existing virtual machine is deleted after the restore completes. If the restore fails, the existing virtual machine is not deleted.

Hyper-V behavior:

The -deletebefore option deletes an existing virtual machine before it is restored and then restores it from new.

The -skip option skips the restore of an existing virtual machine. When restoring multiple virtual machines, selecting this option enables you to restore only the virtual machines that do not exist at restore time.

If none of these options are specified, the behavior is the same as with the -deletebefore option (an existing virtual machine is deleted before the restore by default).

[-removeSnapshots]

This is an Hyper-V specific option.

The -removeSnapshots option consolidates all snapshots before disk restore.

-directory *RestoreDirectory*

Restores virtual-machine files to a directory on the backup host. After such a restore, the virtual machines are not functional.

[-overwrite | -skip | -latest]

These are VMware and H3C CAS specific options.

The -overwrite option overwrites existing files with those from the backup. By default, this option is used.

The -skip option leaves an existing file intact if it is more recent than the one from the backup. Otherwise, it overwrites the file with the one from the backup.

For H3C CAS, this option leaves an existing file intact if the backup image already exists in same directory.

The -latest option preserves an existing file (the file is not restored from the backup). This is a VMware specific option.

-tagName TagName

This is a VMware specific option.

Specifies the tag which should be attached to the virtual machines to be restored. If this option is not specified, the tags from the backed up information is attached. To attach multiple tags, specify multiple tagNames seperated by a comma character.

-tagId TagId

This is a VMware specific option.

You can also use the tagId to specify a tag for restore. You can access the tagId by running the vepa_util.exe command to list tags. To attach multiple tags, specify multiple tagIds seperated by a comma character.

-categoryName CategoryName

This is a VMware specific option.

Specifies the name of the category which contains the tag. To specify the tagName, you must also specify the categoryName.

MICROSOFT SHAREPOINT SERVER 2010/2013 RESTORE

-mssharepoint

Selects the Microsoft SharePoint Server object for restore.

-barhost *HostName*

Specifies the front-end Web server system that was used during backup.

-destination

Specifies the client on which the Data Protector Microsoft SharePoint Server integration agent should be started. It also specifies to which farm the components are restored.

-user

Specifies the Windows domain user under which the Data Protector Microsoft SharePoint Server integration agent should run. This user must be a farm administrator.

-webapplication

Specifies a Web application for restore. Shows the original Web application name.

-session *BackupID*

Specifies from which backup data (*BackupID*) to restore, for example, 2012/10/09-2 .

A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the object *copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

-db

Specifies different options for different databases.

-ssodb

Specifies the Microsoft SharePoint Server single sign-on database for restore.

-ssp

Specifies the Shared Services Provider (SSP) for restore.

-wsshelpsearch

Specifies the Windows SharePoint Services (WSS) Help Search for restore.

-tohost *Client*

Specifies the client to restore to. When you restore Microsoft SQL Server databases, the client must be an SQL Server system.

-instance *SourceInstanceName*

Specifies the original Microsoft SQL Server instance name.

-newinstance *DestinationInstanceName*

Specifies the Microsoft SQL Server instance to which the database should be restored.

-as *NewDBName*

Specifies the name under which the database should be restored. By default, the Microsoft SQL Server databases are restored under the original name. You can restore the Microsoft SQL Server database under a different name.

-todir *NewDirectoryName*

Specifies the path to the directory to which the files (database files, index files) should be restored. By default, index files are restored to their original directories.

-replace

Overwrites any existing database. Overwrites all the existing redirection options specified for the selected component. A restore to the original location is performed.

INSTANT RECOVERY

-instant_restore

Restores data on a disk array using instant recovery.

-host *ClientName*

Restores all objects of the specified client that were backed up in the specified session.

-session *SessionID*

Specifies the session to be used for restore.

3PAR_DISK_ARRAY_OPTIONS

-copyback [wait_clonecopy *Minutes*]

If this option is specified, the instant recovery method of copying replica data (the “copy-back” method) is used in the instant recovery session. With this method, volumes of the replica are copied to the disk group of the current source volumes. If mirrorclones were used in the corresponding zero downtime backup session, volumes of the replica are copied to the disk group of the original volumes, not mirrorclones.

Before the actual data copy operation, storage for the replica to be restored is allocated. Although the copy of the

replica is only virtual at that time, it is immediately available for use. In the background, however, a process is still copying data from the replica to the source location (the replica normalization process). The copy process may degrade the disk array performance, and indirectly the application system performance as well. To reduce a potential degradation of the application system performance, specify the option wait_clonecopy *Minutes* to make Data Protector wait for the copy to complete before the session continues. If the copy process completes before the delay expires, the session continues immediately. Additionally, you can control the copy process by setting appropriate omnirc options.

-switch

If this option is specified, the instant recovery method of switching the disks (the “switch” method) is used in the instant recovery session. With this method, volumes of the replica replace the source volumes.

Note that if this option is specified, and the target volumes to be used in the instant recovery session are standard snapshots or vsnaps, the session automatically uses the instant recovery method of copying replica data instead. In such a case, Data Protector does not wait for the copy to complete, and the instant recovery session continues or finishes immediately.

{ -leave_source | -no_leave_source }

These options determine whether original data from the source volumes is preserved on the disk array after instant recovery or not. For example, you can specify the option -leave_source to investigate why the original data got corrupted.

If the -no_leave_source option is specified, the source volumes are either overwritten with data from the replica (with the “copy-back” instant recovery method) or deleted (with the “switch” instant recovery method) during the instant recovery session. In case of the “copy-back” instant recovery method in which the replica used consists of snapclones, the source volumes are converted into containers before being overwritten, provided that the source and target volumes match in size, redundancy level, and belong to the same disk group.

CAUTION

If you decide to perform instant recovery by copying replica data and not to preserve source volumes after the session (the options -copyback and -no_leave_source are specified), and the instant recovery session fails, a data loss on the source volumes may occur.

{ -check_config | -no_check_config }

These options determine whether a sanity check and a comparison of current volume group configuration of the volume groups participating in the instant recovery session and the volume group configuration information kept in the SMISDB after the corresponding zero downtime backup session are performed or not. If the sanity check fails or the volume group configuration has changed since the zero downtime backup session, the instant recovery session aborts.

In an Serviceguard cluster, when performing instant recovery to some other node than the one from which data was backed up, you must specify the -check_config option. In such circumstances, the current volume group configuration on the node to which data is to be restored differs from the volume group configuration kept in the SMISDB. Consequently, the SMISDB volume group configuration data is replaced by the current volume group configuration data on the node to which data is to be restored, and the instant recovery session succeeds.

-force_prp_replica

If this option is specified and any target volume containing data to be restored is presented to a system other than the backup system, the 3PAR SMI-S Agent removes such presentation. If the option is not specified, the instant recovery session fails in such circumstances.

If this option is specified and a target volume containing data to be restored is presented to the backup system, but cannot be dismounted in an operating system-compliant way, the 3PAR SMI-S Agent performs a forced dismount. If the option is not specified, the instant recovery session fails in such circumstances.

-force_restore_volset

If this option is specified and a source volume (a member of the volume set) is exported to the application host using volume set, the 3PAR SMI-S Agent removes all volumes that are part of the volume set presentation during instant recovery and adds them back after the restore completes. If the option is not specified, the instant recovery session fails in such circumstances.

Note that if this option is selected during remove presentation, none of the volumes part of the volume set can be accessed.

P9000_DISK_ARRAY_XP_OPTIONS

-keep_version

If this option is specified, the LDEV pairs involved in the current instant recovery session are split and left in the SUSPENDED state after the restore of data is complete. In the opposite case, the LDEV pairs are left in the PAIR state.

Even if the instant recovery is successful, it is recommended to keep the replica until the next ZDB session.

On Linux systems, you must specify this option if the replica set consists of more than a single replica.

-check_config

If this option is specified, the current configuration of the participating volume groups is compared with the volume group configuration as it was during the ZDB session and which is stored in the XPDB. If the configuration has changed since the ZDB session, the instant recovery session aborts. Additionally, the CRC check information for the selected LDEV pairs stored in the XPDB is compared to the current CRC check information. If the items compared do not match, the session aborts. A RAID Manager Library flag, which is set whenever the selected mirror LDEV is accessed/changed by any process (including non-Data Protector processes) is checked. If the flag is set, the session fails with an appropriate warning.

In Serviceguard clusters, if instant recovery is performed to some other node than the one from where the volumes were backed up, the current volume group configuration on the target node is different from the volume group configuration kept in the XPDB. In such a case, the XPDB volume group configuration data is replaced by the current volume group configuration data on the target node, and the session does not abort. When performing instant recovery to some other node than the one that was backed up, specify this option.

ORACLE/SAP_SPECIFIC_OPTIONS

-oracle

Selects the Oracle options for instant recovery.

-sap

Selects the SAP R/3 options for instant recovery.

-recover { now | time *Time* | logseq *LogSeqNumber*

thread *ThreadNumber* | SCN *Number* }

Selects the point in time to which the database is recovered. The following options are available:

now

All existing archive logs are applied.

time MM/DD/YY hh:mm:ss

Specifies an incomplete recovery. Archive logs are applied only to a specific point in time.

logseq LogSeqNumber thread ThreadNumber

Specifies an incomplete recovery. Archive logs are applied only to the specified redo log sequence and thread number.

SCN Number

Specifies an incomplete recovery. The archive logs are applied only to the specified SCN number.

-open

Opens the database after recovery.

-resetlogs

Resets the logs after the database is opened. Available only if the -open option is specified. This option is not

available if the -recovery option is set to now.

The following are recommendations on when to reset the logs.

Always reset the logs:

- After an incomplete recovery, that is if not all archive redo logs will be applied.

- If a backup of a control file is used in recovery.

Do not reset the logs:

- After a complete recovery where a backup of a control file is not used in recovery.

- If the archive logs are used for a standby database. If you must reset the archive logs, then you have to recreate the standby database.

-user *UserName* -group *GroupName*

Specifies the username and group name of the account under which Data Protector starts instant recovery. Required only for UNIX clients.

-appname *ApplicationDatabaseName*

Name of the backed up database.

ORACLE_SPECIFIC_OPTIONS

-parallelism *Number*

Selects the parallelism for the restore of archive logs and restore from incremental backups.

DATA_OPTIONS

-exclude *TreeName*

Excludes the specified tree from the restore. This option is not supported with the Data Protector NDMP server integration.

-skip *MatchPattern*

Excludes files matching *MatchPattern* from restore. This option is not supported with Data Protector NDMP server integration.

-only *MatchPattern*

Restores only files that match the given *MatchPattern*. This option is not supported with Data Protector NDMP server integration.

-as *Pathname*

Restores the selected fileset as the specified tree.

-into *Pathname*

Restores the selected fileset into the given directory.

SESSION_OPTIONS

-noexpand

Use this option to display IPv6 hostnames in compressed format.

-preview

Checks the restore parameters without performing the actual restore.

Restore preview is not available for Internal Database restore sessions.

-report { warning | minor | major | critical }

Sets the level of error notification for the session. Errors are classified (in ascending order) as: warning, minor, major and critical. When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if major is selected, only major and critical errors are reported. By default, all errors are reported.

MEDIUM_OPTIONS

-device *BackupDevice*

Specifies the backup device where the backup medium is mounted.

-medium *MediumID*

Specifies the medium from which data will be restored.

This option is not possible when performing a parallel restore.

-slot *SlotID* [*Side*]

Specifies the *SlotID* of the tape library unit where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter in this slot, use the additional *Side* parameter. Slot *Side* must be specified for magneto-optical devices. Values for side are `A` or `B`.

-id *DiskAgentID*

Specifies the ID of the Disk Agent which should be used for restore.

FILESYSTEM_OPTIONS

-touch

Updates the access date/time of the file during the restore. By default the access date/time of the backup version is used.

-lock

When performing a restore of a file, the Disk Agent tries to lock the file. By default the file is not locked.

-no_protection

Do not restore protection of the backed up files, instead use the default protection settings.

-overwrite

Overwrites files with the same name in the specified fileset on the disk.

-no_overwrite

Does not overwrite existing files with the same name.

-merge

This option merges files from the backup medium to the target directory and replaces older versions that exist in the directory with newer (if they exist on the medium) files. Existing files are overwritten if the version on the medium is newer than version on disk. No existing directory is deleted.

If a directory or file doesn't exist on disk (but is on the backup medium) it is restored (created).

-catalog

Displays the restored files and directories.

-sparse

Restores sparse files in their original form.

-move_busy

This option is useful only in case the option -overwrite is specified. A problem can occur if, for example, a file to be overwritten cannot be deleted because it is currently in use. Setting this option causes busy files to be moved to a filename starting with # . The original file can thus be deleted as the lock is transferred to the corresponding file starting with # sign. For example, /tmp/DIR1/DIR2/FILE would be moved to /tmp/DIR1/DIR2/omnir#FILE .

-no_share[_info]

If this option is specified, share information for directories on Windows is not restored. If a directory was shared on the network when a backup was run with the Backup share information for directories option set (by default), it will be automatically shared after restore, unless this option is selected for restore.

-omit_unrequired_object_versions

This option applies if you select directories for restore and the backup was performed with the logging level -log or -log_files . If specified, Data Protector checks in the IDB for each backup in the restore chain if there are any files to restore. Backups with no object versions to restore are skipped. Note that this check may take some time. If not specified, each backup in the restore chain is read, even if there was no change since the previous backup. To restore empty directories, do not specify this option.

-[no_]resumable

By default, Data Protector creates checkpoint files during the restore session. The checkpoint files are needed if the restore session fails and you want to restart the failed session, using the Data Protector resume session functionality. If you specify the option -no_resumable , the checkpoint files are not created.

If you have changed the default using the global option ResumableRestoreDefault , specify the option -resumable if you want checkpoint files to be created.

IDB RESTORE

-idb

Selects the Internal Database backup object for restore.

-barhost *ClientName*

Specifies the Cell Manager system to which the Internal Database (IDB) should be restored to, in case of aCell Manager migration. For *ClientName* you can specify either fully qualified domain name, host name, or IP address.

-restoredb

Instructs Data Protector to restore the basic IDB parts: the Catalog Database (CDB), the Media Management Database (MMDB), and the Session Messages Binary Files (SMBF).

If no additional options -nodbrecover and -nouseasnewidb are specified, after a successful restore Data Protector starts the Internal Database Service, performs recovery of the basic IDB parts using both the backed up and the not yet backed up IDB archived log files, and finally starts using the recovered IDB as the new Internal Database of the cell.

However, if the restored database is not used as a new Internal Database (-nouseasnewidb option), then along with restore of Internal Database files (files in PG,IDB and JCE folder), all backed up Session Messages Binary files (SMBF) and all backed up Data Protector IDB specific files (DPSPEC) will be restored to the temporary location (the specified Restore location).

DPSPEC files are all Data Protector Internal Database specific files and these are not Postgres related files, DCBFs, SMBFs and Configuration files. These are usually: Auditing files, Data Protector logs, keystore, log files, meta, reportdb, smisdb, sqldb, sysdb, vssdb, and xpdb files.

If needed, this restored database can be used as an Internal Database. However, before switching over to the new Internal Database, all SMBF and DPSPEC files should be copied from the temporary location to the original location. This is required for the Cell manager functionality.

-restoreconf

Instructs Data Protector to restore the Cell Manager configuration data. A prerequisite for this operation is a successful restore of the basic Internal Database part in the same session (if the latter is also selected for restore).

-restoredcbf

Instructs Data Protector to restore the Detail Catalog Binary Files (DCBF) part of the IDB. A prerequisite for this operation is a successful restore of the basic Internal Database part in the same session (if the latter is also selected for restore).

-client *SourceClientName*

Specifies the Cell Manager system from where the Internal Database (IDB) was backed up. This system should be running on the same operating system version as the original Cell Manager system. For *SoruceClientName* specify the fully qualified domain name.

-until *YYYY*-*MM*-*DD*[*hh*.*mm*.*ss*]

Specifies that a point-in-time restore should be performed, returning the IDB to the state it was in at the specified date (and optional time).

If this option is not specified, the restore process creates a copy of the IDB in the latest backed up state. Additionally, in this case, the not yet backed up IDB archived log files are copied from the original IDB location to the target restore location.

Important: After a point-in-time IDB restore session, copy specific files from the auditing_IDBRestoreSessionID_*NNNNNNNNN* directory to the original auditing directory. This will make auditing information consistent with the state of the restored IDB. The following audit logs should be copied:

YYYY_*MM*_*DD*.med

YYYY_*MM*_*DD*.obj

YYYY_*MM*_*DD*.ses

In the above filenames, the *YYYY*, *MM*, and *DD* strings correspond the date specified with the -until option.

-pre *PathName*

Specifies the path name of the pre-exec command or script on theCell Manager system. This command is invoked on the Cell Manager before the IDB restore process is initiated.

-post *PathName*

Specifies the path name of the post-exec command or script on theCell Manager system. This command is invoked on the Cell Manager after the IDB restore process is completed.

RESTORE_DB_OPTIONS

-targetdir *TargetDataFolderPath*

Specifies the target directory on the Cell Manager where the basic IDB parts (CDB, MMDB, SMBF) should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space. Note that the *TargetDataFolderPath* length should not exceed 80 characters.

Important: Do not reuse the original IDB directory as the target directory.

-port

Specifies the number of the port that is temporarily used for the Internal Database Service during the restore process. After the process completes, this service is restarted on the original port defined during Data Protector Cell Manager installation.

Important: Do not reuse the original Internal Database Service port as the temporary port. recommends to use the port 7114 for this purpose.

-nodbrecover

If specified, this option instructs Data Protector not to start the Internal Database Service after a successful restore. Thus, recovery of the basic IDB parts (CDB, MMDB, SMBF) using the IDB archived log files is not performed.

-nouseasnewidb

This option can only be specified if the -nodbrecover option is not specified.

If specified, this option instructs Data Protector not to use the recovered IDB as the new Data Protector Internal

Database in the cell.

RESTORE_CONF_OPTIONS

-keeprecent

Instructs Data Protector to keep the most recent version of each Cell Manager configuration file: the existing version on the Cell Manager system (when newer from the version in the IDB backup image) or the backed up version (when newer from the version that already exists on the Cell Manager system). This is the default behavior when neither -keeprecent , nor -nooverwrite , nor the -overwrite option is specified.

-nooverwrite

Instructs Data Protector to preserve each existing Cell Manager configuration file even when its counterpart is present in the IDB backup image.

-overwrite

Instructs Data Protector to unconditionally overwrite each existing Cell Manager configuration file with its counterpart from the IDB backup image. You can use this selection in the event that only a few configuration files are missing on the Cell Manager.

-session *SessionID*

This option must be specified if the -restoredb option is not specified.

If the -session option is specified, Data Protector processes the restore chain of the IDB backup session with the specified session ID. Ensure your session ID belongs to a valid backup session.

If the -session option is not specified, Data Protector automatically selects and processes the restore chain that suits your restore chain selection for the basic IDB parts (CDB, MMDB, SMBF).

-targetdir *TargetConfFolderPath*

Specifies the target directory on the Cell Manager where the Cell Manager configuration data should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space.

If this option is not specified, the original Cell Manager configuration data location is used for the restore session.

-name *FileOrFolderName* ...

If specified, narrows the scope of the Cell Manager configuration data restore to the specified files or folders.

RESTORE_DCBF_OPTIONS

-targetdir *TargetDCBFFolderPath*

Specifies the target directory on the Cell Manager where the DCBF part of the IDB should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space.

If this option is not specified, the original DCBF location is used for the restore session.

SPLIT_MIRROR_OPTIONS

-sse

Selects the P9000 XP Disk Array Family split mirror restore.

-local *ApplicationSystem BackupSystem*

If the -sse option is specified, this option selects the Business Copy (BC) P9000 XP configuration.

-combined *ApplicationSystem BackupSystem*

If the -sse option is specified, this option selects the combined Continuous Access+Business Copy (CA+BC) P9000 XP

configuration.

-mirrors *list*

Specifies the mirror unit (MU) number of a specific replica to be used in the restore session, or the MU numbers of a range or sequence of replicas which define a replica set from which the integration, according to the replica set rotation, selects one replica to be used in the restore session. If this option is not specified, the MU number 0 is used.

-quiesce *cmd*

Specifies the command/script to be run before the LDEV pairs are split (put into the SUSPENDED state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for stopping the application, dismounting the file systems not to be restored in the active session, but belong to the same volume group or disk, or preparing the volume group for deactivation.

If this command/script fails, the command/script specified with the option -restart is not executed. Therefore, you need to implement a cleanup procedure in this command/script. Note that if the omnirc option ZDB_ALWAYS_POST_SCRIPT is set to 1, the command/script specified with the option -restart is always executed.

-restart *cmd*

Specifies the command/script to be run immediately after the LDEV pairs are resynchronized (put into the PAIR state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for restarting the application or mounting the filesystems.

-re-establish_links_before_restore

Directs the Data Protector disk array agent to synchronize the LDEV pairs, that is, to copy the application data to the disks which store backup data. This is necessary to prepare the disks for restore and to enable consistent data restore. If the paired LDEVs have been split (put into the SUSPENDED state) before the restore, and only some files need to be restored, then this option updates the backup system. This will ensure that the correct data is resynchronized to the application system. If this option is not specified, the synchronization is not performed.

-disable_disks

Directs the Data Protector disk array agent to disable disks on the application system, that is, dismount the filesystems and deactivate the volume groups. This is performed before the LDEV pairs are split. The disks are enabled after the links are restored. Note that only filesystems selected for restore are dismounted. If other filesystems exist on the volumes of the volume group or on the disk, appropriate commands/scripts must be used to dismount these filesystems (specified with the options -quiesce and -restart). You must always select this option for restore when you want to copy data from the backup system to the application system, that is, to incrementally restore links. The application system disks have to be disabled to provide data integrity after the links are restored, that is, data is copied.

-restore_links_after_restore

Directs the Data Protector disk array agent to incrementally restore the links for the LDEVs that Data Protector has successfully restored to the backup system. The P9000 XP Agent also incrementally re-establishes links for the LDEVs for which the Data Protector restore failed.

GENERAL_OPTIONS

-device *BackupDevice*

Specifies the backup device where the backup medium is mounted.

-no_auto_device_selection

If this option is specified, Data Protector does not automatically replace unavailable devices with available devices of the same device tag.

-server *ServerName*

Selects the Cell Manager with the client name *ServerName* as the Cell Manager. Use this option to perform a restore to a client that is not in the current Data Protector cell.

-target *Client*

Restores the selected fileset to the specified client.

-profile

Displays restore statistics.

-load { low | medium | high }

Specifies the level of network traffic generated by a session during a time period. High level generates as much traffic as allowed by the network, resulting in a faster restore. A low level has less impact on network performance, but results in a slower restore. By default, this option is set to high .

-pre_exec *PathName*

Instructs the Disk Agent to execute this command before restoring the data object. The complete pathname of the command should be specified.

-post_exec *PathName*

Instructs the Disk Agent to execute this command after restoring the data object. The complete pathname of the command should be specified.

-variable *VariableName VariableValue*

This option lets you specify a variable name and its value for proper operation of some platforms and integrations. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

-no_monitor

By default the command monitors the session and displays all messages. If this option is used, the command displays only the session ID.

-priority *NumValue*

In case multiple running sessions request access to a specific device at the same time, this option determines the order in which the sessions will be queued. The *NumValue* can be any value from 1 (the highest priority) to 6000 (the lowest priority). In case the option is not specified, the default value of 3000 is set. If a low priority session is running when a high priority session starts queuing, the currently running session is allowed to finish. When more sessions request access to a device with the same priority, any of these sessions might acquire access first.

-s3_tier *S3RestoreTier*

This option specifies the tier for AWS S3 Glacier or Deep Archive restore. S3RestoreTier can be**Standard**, **Expedited** or **Bulk** for AWS S3 Glacier and **Standard** or **Bulk** for Deep Archive. Default value is '*Standard*'.

-s3_tier_policy *S3RestoreTierPolicy*

This option specifies the restore tier policy for AWS Glacier restore. This option is applicable only to the**Standard** tier. *S3RestoreTierPolicy* can be **free_tier**, **no_retrieval_limit** or **max_retrieval_rate**. Default value is **no_retrieval_limit**.

-s3_rate *S3RestoreTierPolicyRate (GB/Hour)*

This option specifies the restore tier policy rate in GB/Hour for AWS Glacier restore. This option is applicable only for **Standard** tier and **max_retrieval_rate** policy. The default value is 1 GB/Hour.

RETURN VALUES

See the man page omniintro for return values.

Additional return values of the omnir command are:

10 - There was an error while copying some files. All agents completed successfully.
11 - One or more agents failed, or there was a database error.
12 - None of the agents completed the operation.
13 - Session was aborted.

EXAMPLES

The following examples illustrate how the omnir command works.

1. To restore trees "/tree1" and "/tree2" of the root filesystem on "fs", with the label "lb1", from data created in the session "2013/05/12-33", as the trees "/tmp/tree1" and "/tmp/tree2", skipping ".xyz" files, execute:

   ```
   omnir -filesystem fs:/ lb1 -session 2013/05/12-33 -tree /tree1 -as /tmp/tree1 -tree /tree2 -as /tmp/tree2 -skip *.xyz
   ```

2. To perform a full restore of tree "/ac" on filesystem "bb:/", with no label, from data created in the session "2013/05/12-2, execute":

   ```
   omnir -filesystem bb:/ -full -session 2013/05/12-2 -tree /ac
   ```

3. To perform restore of the section "/dev/rdsk/c201d6s0" of the disk image labeled "RawRoot" on the client "machine" from data created in the backup session "2013/05/23-12", execute:

   ```
   omnir -rawdisk machine "RawRoot" -section /dev/rdsk/c201d6s0 -session 2013/05/23-12
   ```

4. To use parallel restore for restoring two objects, execute:

   ```
   omnir -filesystem client1:/ -session 2013/04/17-2 -tree /users -into /tmp -filesystem client2:/opt -session 2013/04/17-3 -tree /opt -into /tm
   p
   ```

5. To perform an instant recovery to the system named "machine" from data created in the backup session "2013/03/08-1", keeping the replica on the disk array, execute:

   ```
   omnir -host machine -session 2013/03/08-1 -instant_restore -keep_version
   ```

6. To perform an instant recovery of filesystem backup data on a disk array of theP9000 XP Disk Array Family to the system named "computer" from data created in the backup session "2013/05/02-1", keeping the replica on the disk array, execute:

   ```
   omnir -host computer -session 2013/05/02-1  -instant_restore  -keep_version
   ```

7. To perform a point in time recovery of the database "dbase.nsf" and all Lotus Notes/Domino Server NTF files of the Lotus Notes/Domino Server "BLUE" from the system "computer", to the original location with parallelism 4, execute:

   ```
   omnir -lotus -barhost computer -domino_server BLUE -parallelism 4 -db dbase.nsf -NTF -recovery_time 2012/08/15.15:00:00
   ```

8. To perform an Informix Server restore of the database server "ol_computer" on the UNIX system "computer" with the bar argument "-r rootdbs", and to make the devices available to this session with the highest priority in case of resource conflicts, execute:

   ```
   omnir -informix -barhost computer -barcmnd ob2onbar.pl -user informix:informix -bararg "-r rootdbs" -appname ol_computer -priority 1
   ```

9. The Microsoft Information Store with the "/First Storage Group/STORE/Public Folder Store" store and "/First Storage Group/LOGS/Logs" logs is to be restored to the system called "computer.company.com" (where it was backed up), from data created in the backup session "2013/05/07-13". The Microsoft Exchange Server log files are to be restored to "c:\temp" directory, the hard recovery is to be performed after the restore has finished. The database is to be mounted after the hard recovery. Execute:

   ```
   omnir -msese -barhost computer.company.com -appname "Microsoft Exchange Server(Microsoft Information Store)" -base "/First Storage
   Group/LOGS/Logs" -session "2013/05/07-13" -base "/First Storage Group/STORE/Public Folder Store" -session "2013/05/07-13" -logpath c:\t
   emp -last -mount
   ```

10. Microsoft Exchange Server 2010/2013 restore: Suppose you want to restore the backup of the database "DB1" to a recovery database that should be created on the client "exchange2.company.com" and named "Recovery1", with the files in the "C:\Recovery1Folder" directory. Suppose the database "DB1" was backed up in the session "2013/5/14-1" from a DAG whose virtual system name was "dag0.company.com". To also ensure that the integration agent (`e2010_bar.exe`) is started on the client "exchange1.company.com", execute:

    ```
    omnir -e2010 -barhost exchange1.company.com -db_name DB1 -source dag0.company.com -new -session 2013/5/14-1 -client
    exchange2.company.com -location C:\Recovery1Folder -name Recovery1 -recoverydb
    ```

11. Microsoft Exchange Server 2010/2013 restore (instant recovery): Suppose you want to restore the corrupt standalone database "DB1", which resides on the client "exchange1.company.com". The database was backed up in the ZDB session "2013/05/20-3". To ensure that the integration agent (`e2010_bar.exe`) is started on the client "exchange1.company.com", and that the database is restored to the latest state, using the copy-back instant recovery method, execute:

    ```
    omnir -e2010 -barhost exchange1.company.com -instant_restore -copy_back -db_name DB1 -latest
    ```

12. Virtual Environment (VMware vSphere) restore: Suppose you want to restore the virtual machine "/vm/machineA" and the individual disks ("scsi0:0" and "scsi0:1") of the virtual machine "/vm/machineB". At the time of backup, the virtual machines were running on the ESX Server systems that belonged to the datacenter "/MyDatacenter" managed by the vCenter Server system "vcenter.company.com". The virtual machines were backed up with the "vStorageImage" backup method.

    To restore them to the original location, using the backup session "2013/01/11-1" and to ensure that the newly restored virtual machines are put online when the session completes, execute:

    ```
    omnir -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacente
    r -method vStorageImage -session 2013/1/11-1 -vm -instanceUUID vmInstanceUUID /MyDatacenter/vm/machineA -vm MyDataCenter/vm/
    machineB -disk scsi0:0 -disk scsi0:1 -register -poweron
    ```

13. Virtual Environment (VMware vSphere) restore: Suppose the virtual machines "/MyVirtualMachines/machineA" and "/MyVirtualMachines/machineB" were backed up in the session "2013/02/12-5" from the datacenter "/MyDatacenter" that is managed by the vCenter Server system "vcenter.company.com", using the "vStorageImage" backup method. To restore the virtual machines outside the datacenter, to the directory "C:\tmp" on the backup host

"backuphost.company.com", execute:

```
omnir -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method vStorageImage -session 2013/2/12-5 -vm -instanceUUID vmInstanceUUID /MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB -directory c:\tmp
```

14. Virtual Environment (H3C CAS) restore using VMs to a directory using non-cached method: Suppose the virtual machines /MyVirtualMachines/machineA and /MyVirtualMachines/machineB were backed up in the session 2018/10/06-6 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage non-cached backup method. To restore the virtual machines outside of the host pool, to the directory C:\tmp on the backup host backuphost.company.com, execute:

```
omnir -veagent -virtual–environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -session 2018/10/06-6 -vm /MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB -directory c:\tmp
```

15. Virtual Environment (H3C CAS): Restoring multiple virtual machines from a single session.

    Suppose the Virtual Machines /MyVirtualMachines/machineA, /MyVirtualMachines/machineB and /MyVirtualMachines/machineC were backed up in the session 2018/12/14-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore all three virtual machines in a single session, execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -method "h3ccasImage -non-cached" -session 2018/12/14-13 -vm /MyVirtualMachines/machineA -instanceUUID 893a8e41-015c-47df-8d9f-a70b3d12fdf6 -vm /MyVirtualMachines/machineB -instanceUUID e41021aa-2447-4cf3-8336-084b2eb46c8e -vm /MyVirtualMachines/machineC -instanceUUID 37f164cc-ade7-4544-af61-5674fe04ea8c -register
    ```

16. Virtual Environment (H3C CAS): Restoring multiple virtual machines from multiple sessions.

    Suppose the Virtual Machines /MyVirtualMachines/machineA, /MyVirtualMachines/machineB and /MyVirtualMachines/machineC were backed up from sessionID 2018/12/14-7 to sessionID 2018/12/14-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore all three virtual machines in multiple sessions, execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -method "h3ccasImage non-cached" -fromsession 2018/12/14-7 untilsession 2018/12/14-13 -vm /MyVirtualMachines/machineA -instanceUUID 893a8e41-015c-47df-8d9f-a70b3d12fdf6 -vm /MyVirtualMachines/machineB -instanceUUID e41021aa-2447-4cf3-8336-084b2eb46c8e -vm /MyVirtualMachines/machineC -instanceUUID 37f164cc-ade7-4544-af61-5674fe04ea8c -register
    ```

17. Virtual Environment (H3C CAS): Restoring virtual machine to a new CAS server using non-cached method.

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine to a new CAS server cvm1.company.com, execute:

    ```
    omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -destination cvm1.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost cvknode1 -store /StoragePool1 -method h3ccasImage -non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637efba -register
    ```

18. Virtual Environment (H3C CAS): Restoring virtual machine with the same name to a new CAS server where the virtual machine already exists (using -deletebefore option).

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine with the same name to a new CAS server cvm1.company.com using the -deletebefore option, execute:

    ```
    omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -destination cvm1.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost cvknode1 -store /StoragePool1 -method h3ccasImage-non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637efba -register -deletebefore
    ```

19. Virtual Environment (H3C CAS): Restoring virtual machine with the same name to a new CAS server where the virtual machine already exists (using -skip option).

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine with the same name to a new CAS server cvm1.company.com using the -skip option, execute:

    ```
    omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool -destination cvm1.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost cvknode1 -store /StoragePool1 -method h3ccasImage -non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637efba -register -skip
    ```

20. Virtual Environment (H3C CAS): Restoring virtual machine with a new name to a new CAS server.

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine with a new name machineB to a new CAS server cvm1.company.com, execute:

```
omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool
-destination cvm1.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost cvknode1 -store /StoragePool1 -method
h3ccasImage -non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637ef
ba -new_name machineB -register
```

21. Virtual Environment (H3C CAS): Restoring virtual machine with a new name to the same CAS server.

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine with a new name machineB to the same CAS server cvm.company.com, execute:

    ```
    omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool
    -destination cvm.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost cvknode1 -store /StoragePool1 -method h
    3ccasImage -non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637efb
    a -new_name machineB -register
    ```

22. Virtual Environment (H3C CAS): Restoring virtual machine with a new name to a specific host in the same CAS server.

    Suppose the Virtual Machine /MyVirtualMachines/machineA was backed up from sessionID 2019/03/19-7 to sessionID 2019/03/19-13 from the host pool /MyHostPool that is managed by the CAS management Server system cvm.company.com, using the h3ccasImage -non-cached backup method. To restore the Virtual Machine with a new name machineB to a specific host cvknode2 in the same CAS server cvm.company.com, execute:

    ```
    omnir.exe -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost cvm.company.com -instance /MyHostPool
    -destination cvm.company.com -newinstance /MyHostPool2 -host_cluster Cluster2 -specificHost cvknode2 -store /StoragePool1 -method h
    3ccasImage -non-cached -session 2019/03/19-7 -vm /MyVirtualMachines/machineA -instanceUUID 7d9ae6ad-5f7f-4294-8b35-00f31637efb
    a -new_name machineB -register
    ```

23. Virtual Environment (H3C CAS): Restoring virtual machine as a new virtual machine.

    Suppose the virtual machine /MyVirtualMachines/machineA was backed up in the session 2020/02/10-18 from the Host pool /MyHostpool that is managed by the H3C CAS management Server system h3ccas.company.com, using the H3CCAS cached backup method. To restore as a new virtual machine execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -
    method h3ccasImage-cached -session 2020/02/10-18 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -new_n
    ame NewVMName -register
    ```

24. Virtual Environment (H3C CAS): Restoring virtual machine disks to a different virtual machine within the same H3C CAS server:

    Suppose an individual disk /vms/images/DiskA in a virtual machine /vm/machineA was backed up in the session 2021/07/07-13. To restore the disk to a different virtual machine /vm/machine1 within the same H3C CAS server in store /vm/images, execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -
    method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /
    vm/images/DiskA -targetVM /vm/machine1 -store /vm/images -specificHost cas1 -poweron -deletebefore
    ```

25. Virtual Environment (H3C CAS): Restoring virtual machine disks to the same virtual machine, but to a different storage pool, within the same H3C CAS server:

    Suppose an individual disk /vms/images/DiskA in a virtual machine /vm/machineA was backed up in the session 2021/07/07-13. To restore the disk to the same virtual machine within the same H3C CAS server, but in a different storage pool, execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -
    method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /
    vm/images/DiskA -store /vm/images -specificHost cas1 -poweron -deletebefore
    ```

26. Virtual Environment (H3C CAS): Restoring virtual machine disks to a virtual machine in a different H3C CAS server:

    Suppose an individual disk /vms/images/DiskA in a virtual machine /vm/machineA was backed up in the session 2021/07/07-13. To restore the disk to a virtual machine /vm/machine1 in a different H3C CAS server h3ccas2.company.com, execute:

    ```
    omnir -veagent -virtual-environment H3CCAS -barhost backuphost.company.com -apphost h3ccas.company.com -instance /MyHostpool -
    method h3ccasImage-cached -session 2021/07/07-13 -vm /vm/machineA -instanceUUID 15e597fd-d309-4901-b11e-e2d2c63a5d44 -disk /
    vm/images/DiskA -targetVM /vm/machine1 -store /vm/images -specificHost cas1 -destination h3ccas2.company.com -newinstance /Host_P
    ool1 -deletebefore
    ```

27. Virtual Environment (Restoring virtual machines to a Microsoft Hyper-V system): Suppose you want to restore the virtual machines "VM1" with the GUID "62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C" and "VM2" with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130". At the time of backup, the virtual machines were running on the Microsoft Hyper-V system "hyperv1.company.com". The virtual machines were backed up with the "Hyper-V Image" backup method.

    To restore the virtual machines to the Microsoft Hyper-V system "hyperv2.company.com" to the default location, using backup data created in the backup session "2013/01/11-1" and to power the newly restored virtual machines on when the session completes, execute:

    ```
    omnir -veagent -virtual-environment hyperv -barhost backuphost.company.com -apphost hyperv1.company.com -instance hyperv -sessio
    n 2013/1/11-1 apphost hyperv1.company.com -instance hyperv -session 2013/1/11-1 -vm 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C -v
    ```

m 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination hyperv2.company.com -poweron

28. Virtual Environment (Restoring virtual machines outside a Microsoft Hyper-V system): Suppose the virtual machines "VM1" with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130" was backed up in the session "2013/02/12-5" from the Microsoft Hyper-V system "hyperv.company.com", using the "Hyper-V Image" backup method. To restore the virtual machine outside the Microsoft Hyper-V system, to the directory "c:\tmp" on the restore client "client.company.com", execute:

    omnir -veagent -virtual-environment hyperv -barhost client.company.com -apphost hyperv.company.com -instance hyperv -session 2013/2/12-5 -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -directory c:\tmp

29. Virtual Environment (Restoring individual virtual machine disks to a directory in a Microsoft Hyper-V system):

    Suppose the virtual machine VM1 with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130" was backed up in the Microsoft Hyper-V system "hyperv.company.com" using the "Hyper-V Image" backup method in session "2016/02/02-5". To restore disks (DiskPath1 "C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx" and DiskPath2 "c:\Disk2.vhdx") to the directory "C:\tmp" on the restore client "client.company.com", execute:

    omnir -veagent -virtual-environment hyperv -barhost client.company.com -apphost hyperv.company.com -instance hyperv -destination hyperv.company.com -session 2016/02/02-5 -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -disk C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx -disk c:\Disk2.vhdx -directory C:\tmp

30. Virtual Environment (Restoring individual virtual machine disks to original location in a Microsoft Hyper-V system)

    Suppose the virtual machine VM1 with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130" was backed up in the Microsoft Hyper-V system "hyperv.company.com" using the "Hyper-V Image" backup method in session "2016/02/02-5". To restore disks (DiskPath1 "C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx" and DiskPath2 "c:\Disk2.vhdx") to its original location on the restore client "client.company.com", execute:

    omnir -veagent -virtual-environment hyperv -barhost client.company.com -apphost hyperv.company.com -instance hyperv -destination hyperv.company.com -session 2016/02/02-5 -removeSnapshots -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -disk C:\Hyper-V\Virtual Hard Disks\Disk1.vhdx -disk c:\Disk2.vhdx

    > **Note** If the disk path (DiskPath1 and DiskPath2 in example) contains special characters, the path must be enclosed in a single quote.
    >
    > The `-removeSnapshots` option removes existing snapshots from the virtual machine.

31. Virtual Environment (Restoring virtual machines to a Microsoft Hyper-V system): Suppose you want to restore the virtual machines "VM1" with the GUID "62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C" and "VM2" with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130". At the time of backup, the virtual machines were running on the Microsoft Hyper-V system "hyperv1.company.com". The virtual machines were backed up with the "Hyper-V RCT" backup method. To restore the virtual machines to the Microsoft Hyper-V system "hyperv2.company.com" to the default location, using backup data created in the backup session "2013/01/11-1" and to power the newly restored virtual machines on when the session completes, execute:

    omnir -veagent -virtual-environment hyperv -method HyperV-RCT -barhost backuphost.company.com -apphost hyperv1.company.com -instance hyperv -session 2013/1/11-1 apphost hyperv1.company.com -instance hyperv -session 2013/1/11-1 -vm 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination hyperv2.company.com -poweron

32. Virtual Environment (Restoring virtual machines outside a Microsoft Hyper-V system): Suppose the virtual machines "VM1" with the GUID "54C22930-E3B9-43AA-AFCD-1E90BB99F130" was backed up in the session "2013/02/12-5" from the Microsoft Hyper-V system "hyperv.company.com", using the "Hyper-V RCT" backup method. To restore the virtual machine outside the Microsoft Hyper-V system, to the directory "c:\tmp" on the restore client "client.company.com", execute:

    omnir -veagent -virtual-environment hyperv -method HyperV-RCT -barhost client.company.com -apphost hyperv.company.com -instance hyperv -session 2013/2/12-5 -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -directory c:\tmp

33. To perform a VSS restore of the "Registry Writer" and "System Writer" trees from the backup session "2013/05/20-3" and the "Event Log Writer" tree from data created in the backup session "2013/05/27-1", which were both performed on the client "system1.company.com" to the client "system2.company.com" into the "c:\tmp directory", execute:

    omnir -vss -barhost system1.company.com -session 2013/05/20-3 -tree /"Registry Writer" -tree /"System Writer" -session 2013/05/27-1 -tree /"Event Log Writer" -destination "system2.company.com" -into c:\tmp

34. To start an online restore of a DB2 database called "TEMP" from instance "DB2Inst" on the client "splendid" and roll it forward till the 16th March 2013, 9:15 a.m., execute:

    omnir -db2 -barhost splendid -instance DB2Inst -dbname TEMP -rollforward -time 2013-03-16.09.15.00

35. To restore the contents of a mailbox called "FIRST" residing on an Microsoft Exchange Server system called "infinity.ipr.company.com" from data created in the backup session 2013/01/10-1, into the new mailbox called "TEMP", execute:

    omnir -mbx -barhost infinity.ipr.company.com -mailbox FIRST -session 2013/01/10-1 -destmailbox TEMP

36. To restore all messages from the "Inbox" folder (and all subfolders) from the "User 1" mailbox residing on the Microsoft Exchange Server system called "exchange.hp.com", into the original location, from data created in the backup session "2013/03/10-18", without overwriting the messages, execute:

```
omnir -mbx -barhost exchange.hp.com -mailbox "User 1" -session 2013/03/10-18 -folder Inbox -originalfolder -keep_msg
```

37. To restore all messages from the "User 2" mailbox residing on the Microsoft Exchange Server system called "exchange.hp.com", except for the messages in the folder "Deleted Items", into a new location, from data created in the backup session "2013/03/10-19" (for example, performed at 13:47:00), execute:

    ```
    omnir -mbx -barhost exchange.hp.com -mailbox "User 2" -session 2013/03/10-19 -exclude "Deleted Items"
    ```

    The messages will be restored in the "Data Protector 03/10/13 13:47:00" mailbox on the "exchange.hp.com" Microsoft Exchange Server.

38. To start an online restore of an SAP MaxDB database called "TEMP" on the client "splendid" and roll it forward till the 10th January 2013, 9:15 a.m. from the archive logs already residing on the client, execute:

    ```
    omnir -sapdb -barhost splendid -instance TEMP -recover -time: 2013-01-10.09.15.00 -from_disk
    ```

39. With disk arrays of the P9000 XP Disk Array Family, to recover an Oracle database "DB1" on the Windows client "san32" using the user account "sys" that belongs to the "sysgroup" user group, from data created in the backup session "2013/02/05-18", until the most recent time, to open the database after the recovery, to keep the replica on the disk array, and to use "1" as the parallelism setting, execute:

    ```
    omnir -host san32 -session 2013/02/05-18 -instant_restore -keep_version -oracle -user sys -group sysgroup -recover now -open -appname DB1 -parallelism 1
    ```

40. To perform restore of the section "/dev/rdsk/c201d6s0" of the disk image labeled "Raw" on the client "system1" from data created in the backup session "2013/05/23-12" using the media set containing the object copy with ID "d5032390-baba-4b3f-8c67-1f5b9273b242/1013", execute:

    ```
    omnir -rawdisk system "Raw" -section /dev/rdsk/c201d6s0 -session 2013/05/23-12 -copyid d5032390-baba-4b3f-8c67-1f5b9273b242/1013
    ```

41. Exchange 2010 VSS restore to a different storage group:

    To restore the Exchange 2010 Writer logs on the system "exch2010.company.com" from the storage group copy "Replicated Storage Group" created by LCR, from data created in the backup session "2013/04/08-12", to storage group "Original Storage Group", and with the files restored in the "C:\Omni" directory, execute the following command:

    ```
    omnir -vss -instant_restore -use_vds -barhost exch2010.company.com -session 2013/04/08-12 -tree "/Microsoft Exchange Writer(Exchange Replication Service)/Microsoft Information Store/Replicated Storage Group/Logs" -target_tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/Original Storage Group/Logs" -target_dir "C:\Omni"
    ```

42. Exchange 2010 VSS instant recovery to a non-Exchange location:

    To perform instant recovery of the Exchange 2010 Writer store "StoreOne" from the storage group "First Storage Group" from data created in the backup session "2013/04/08-9" on the system "exch2010.company.com", to the system "server2.company.com", and with the replicas mounted to "C:\Omni_Mnt", execute:

    ```
    omnir -vss -instant_restore -use_vds -barhost exch2010.company.com -destination server2.company.com -session 2013/04/08-9 -tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/StoreOne" -target_dir "c:\mnt" -tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/Logs" -target_dir "C:\Omni_Mnt"
    ```

43. Exchange 2010 VSS restore to a non-Exchange location and creating RSG:

    To restore the Exchange 2010 Writer store "Store One" from the storage group named "First Storage Group" from data created in the backup session "2013/04/10-9" that was performed on the system "exch2010.company.com", and to create the Recovery Storage Group "DP RSG" that links restored store to "Store Two" in storage group "Second Storage Group", and with the files restored in the "C:\Omni" directory, execute:

    ```
    omnir -vss -instant_restore -use_vds -barhost exch2010.company.com -session 2013/04/10-9 -tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/Store One" -exch_RSG "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/Second Storage Group/Store Two/" -target_dir "c:\mount" -tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/Logs" -exch_RSG "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/Second Storage Group/Logs" -target_dir "C:\Omni"
    ```

44. To perform a full restore of the tree "/vol/vol1" of the NDMP client alpha.hp.com, from data created in the backup session "2013/05/12-2", using the device "LTO" connected to the client beta, execute:

    ```
    omnir -filesystem alpha.hp.com:/vol/vol1 /vol/vol1 -full -session 2013/05/12-2 -tree “/vol/vol1” -device LTO
    ```

45. To restore an entire Microsoft SharePoint Server server (moss.domain.com) from the latest session, execute:

    ```
    omnir -mssharepoint -barhost wfe1.domain.com -server moss.domain.com
    ```

46. To restore a Microsoft SharePoint Server 2010 Web application content database from the latest session to the alternate location, changing a name, sql server, an instance and a data file path, execute:

    ```
    omnir -mssharepoint -barhost wfe1.domain.com -webapplication "SharePoint - 2224" -db "WSS_Content_2224" -as "WSS_new_DB" -tohost mosssql2.domain.com -newinstance moss1 -todir "f:\program files\SQL\data"
    ```

47. To restore the database "TEST1" on the Microsoft SQL Server instance "TEST_INSTANCE" and client "system1.company.com", and to perform a tail log backup session before the actual restore session starts, by using the backup specification "DB1_Backup", execute:

    ```
    omnir -mssql -barhost system1.company.com -instance TEST_INSTANCE -base TEST1 -tail_log DB1_Backup
    ```

48. To perform online restore of the entire Internal Database (IDB) and the Cell Manager configuration files backed up

from the Windows system "cmsys-win.company.com", by restoring the basic IDB parts (CDB, MMDB, SMBF) to the path "D:\Data_Protector_temp\idb", by restoring the Cell Manager configuration files and the DCBF part of the IDB to their original location, by restoring to the latest state that was backed up before 24 May 2013, using the temporary port "7114", and without performing the IDB recovery, execute:

```
omnir -idb -barhost cmsys-win.company.com -restoredb -targetdir D:\Data_Protector_temp\idb -port 7114 -until 2013-05-24 -nodbrecover -restoreconf -restoredcbf
```

49. To perform online restore of the basic IDB parts (CDB, MMDB, SMBF) backed up from the UNIX system "cmsys-ux.company.com", by restoring the data to the path "/var/tmp/Data_Protector_temp/idb", by restoring to the latest backed up state, using the temporary port "7114", and by performing the IDB recovery without putting the recovered IDB into use as the new IDB in the cell, execute:

    ```
    omnir -idb -barhost cmsys-ux.company.com -restoredb -targetdir /var/tmp/Data_Protector_temp/idb -port 7114 -nouseasnewidb
    ```

50. To perform online restore of the DCBF part of the IDB backed up from the system "cmsysx.company.com" to its original location, and to the latest state that was backed up before 12 April 2013 at 16:00, execute:

    ```
    omnir -idb -barhost cmsys.company.com -restoredcbf -until 2013-04-12.16.00.00
    ```

51. To support restore of object names with instanceUUID in its name, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance instanceName -method vStorageImage -session sessionID -vm vmPath –instanceUUID vmInstanceUUID -register -poweron -deletebefore
    ```

52. To restore OpenStack Nova Instances backed up as virtual machines from the VMware vCenter, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost barHostName -apphost appHostName -instance /Datacenter -method vStorageImageOpenStack -session sessionID -vm vmPath -instanceUUID vmInstanceUUID -register -poweron -deletebefore
    ```

53. To restore the MySQL database "db1" and database table "db2.table1" of the "MYSQL56" instance to the original system "winsys.company.com" as a new instance named "MYSQL56 _NEW " using the user account "MYSQLDOMAIN\Administrator" in a complete staged restore session, to use the restore chain of the backup session with the ID "2014/11/22-13", and to roll the restored data forward until the last available state in the backup images of the corresponding binary log files, execute:

    ```
    omnir -integ MySQL -barhost winsys.company.com -appname MYSQL56 _NEW -user Administrator:MYSQLDOMAIN -options -source_client winsys.company.com -source_instance MYSQL56 -database -session 2014/11/22-13 -staging -copy_back -include db1 -include db2.table1 -roll_forward
    ```

54. To restore the MySQL binary log stored in the "mysql-bin.000001" file of the "MYSQL55" instance to the non-original target system "linuxsys2.company.com" and to the non-original path " C:\Users\MySQL\temp" using the user account with which the Data Protector `Inet` service is running, execute:

    ```
    omnir -integ MySQL -barhost linuxsys2.company.com -appname MYSQL55 -options -source_client linuxsys1.company.com -source_instance MYSQL55 -binary_log -include mysql-bin.000001 -target_dir C:\Users\MySQL\temp
    ```

55. To restore a VM to its original location with the backed up tags attached to the restored VM, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -register -poweron
    ```

56. To restore to original location and to skip attachment of tags to the restored VM, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -skipTagAttach register -poweron
    ```

57. To restore VM to a different location and to attach a tag "Gold" of category "DP", execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -categoryName DP -tagName Gold -register –poweron
    ```

58. To restore to a different location and to attach a custom tag using the tagId "`urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST`" , execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST -register –poweron
    ```

59. To attach multiple tags to a VM by specifying multiple tagIds, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStore -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -tagId urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST2,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST3,urn:vmomi:InventoryServiceTag:c03d4f1b-a589-47e2-ad9a-77d53bf328fa:TEST4 -register –poweron
    ```

60. To attach multiple tags to a VM by specifying multiple tag names, execute:

    ```
    omnir.exe -veagent -virtual-environment vmware -barhost backuphost.company.com -apphost vcenter.company.com -instance /MyDatacenter -destination vcenter2.company.com -newinstance /MyHostPool1 -host_cluster Cluster1 -specificHost esx.company.com -store MyStor
    ```

e -method VStorageImage -session 2020/06/23-1 -vm vmPath -instanceUUID vmInstanceUUID -categoryName myCategory -tagName MyTagName1,MyTagName2,MyTagName3,MyTagName4 -register –poweron

61. To restore the contents of mailboxes ("Mailbox1" and "Mailbox2") residing in a publisher domain called "test.onmicrosoft.com" from data created in the backup session 2020/06/23-2 under Azure application "app1", in restore folder "MyTempfolder", execute:

    omnir -m365 -m365-environment exchange -barhost ExampleHost.net -mailbox Mailbox1@test.onmicrosoft.com -session 2020/06/23-2 -azureapp app1 -mailbox Mailbox2@test.onmicrosoft.com -session 123 -restorelocation "MyTempfolder" -debug 1-500 Debug.txt

62. To perform online restore of the vProtect object backed up from the system "cmsysx.company.com" from session 2021/10/18-1 to its original location with overwrite, execute:

    omnir -vprotect cmsysx.company.com "/" -overwrite -session 2021/10/18-1 -tree /

63. To perform restore of the vProtect object backed up from the system "cmsysx.company.com " from session 2021/10/18-1 to the location / tmp/res1 without overwrite, execute:

    omnir -vprotect cmsysx.company.com "/" -no_overwrite -session 2021/10/18-1 -tree / -into /tmp/res1

SEE ALSO

omnib(1), omnikeytool(1M), omniobjconsolidate(1), omniobjcopy(1), omniobjverify(1)

omnirpt

omnirpt command is available on systems with the Data Protector User Interface component installed. It generates various reports about the Data Protector environment. For example: about backup, object copy, object consolidation, and object verification sessions in a specific time, session specifications, media, Data Protector configuration, and single sessions.

SYNOPSIS

omnirpt -version | -help

omnirpt -report ReportName ReportOptions [*FormatOptions*][*MethodOptions*] [-header] [-multicell] [-[no]_multiple]

omnirpt -rptgroup ReportGroup

omnirpt -smtp_config -add SMTPOptions

omnirpt -smtp_config -list

omnirpt -smtp_config -remove

omnirpt -smtp_config -test

FormatOptions:

-ascii |

-html |

-tab |

-short

MethodOptions:

-email *EmailAddress...* |

-smtp *EmailAddress...* |

-snmp *Hostname...* |

-broadcast *Hostname...* |

-log *Filename...* |

-external *CommandName...*

ReportName:

list_sessions |

session_flow |

device_flow |

used_media |

used_media_extended |

host_statistics |

session_statistics |

session_errors |

dl_trees |

obj_nobackup |

obj_copies |

obj_lastbackup |

obj_avesize |

fs_not_conf |

dl_info |

dl_sched |

db_size |

cell_info |

hosts_unused |

dev_unused |

lookup_sch |

hosts_not_conf |

licensing |

host |

media_list |

media_list_extended |

media_statistics |

pool_list |

single_session |

session_objects |

session_hosts |

session_devices |

session_media |

session_objcopies

ReportOptions:

SessionOption:

-session *SessionID*

PoolOption:

-pool *Poolname...*

LabelOption:

-label *Label*

LocationOption:

-location *Location...*

LibraryOption:

-[no_]library *Library...*

ProtectionOption:

-[no_]protection *NoOfDays*

MediaClassOption:

-class *MediaClass*

MediaStatusOption:

-status *MediaStatus*

SpecificationOptions:

-datalist *BackupSpecificationName...*

-copylist_sch *ScheduledCopySpecificationName...*

-copylist_post *PostbackupCopySpecificationName...*

-verificationlist_sch *ScheduledVerificationSpecificationName...*

-verificationlist_post *PostbackupVerificationSpecificationName...*

-conslist_sch *ScheduledConsolidationSpecificationName...*

-conslist_post *PostbackupConsolidationSpecificationName...*

-no_datalist

-no_copylist

-no_verificationlist

-no_conslist

DatalistGroupOption:

-group *BackupSpecificationGroup*

LookupSchedulesOption:

-schedule *NoOfdays*

NetworkOption:

-network *IP_Address...*

HostsOption:

-hosts *Hostname...*

HostOption:

-host *Hostname*

LevelOption:

-level *Level*

ObjectCopiesOption:

-num_copies { *less* | *equal* | *more* } *NumberOfCopies*

TimeframeOption:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

LatestObjectOption:

-days *NoOfdays*

Level: { warning | minor | major | critical }

Day: *[YY]YY/MM/DD*

Hour: *HH:MM*

SMTPOptions:

-server_name *SMTPServerHostName...*

[-server_port *SMTPServerPort...*]

-user_name *UserName...*

-email_id *SenderEmailAddress...*

DESCRIPTION

The omnirpt command generates reports such as the following about Data Protector environment. It also allows you to configure secure SMTP credentials for securely sending reports via SMTP:

- data protector configuration
- media configuration
- specifications about backup, object copy, object consolidation and object verification
- sessions about backup, object copy, object consolidation and object verification
  You can generate the session reports for a specific time or to query a single session information.

Each report definition includes its name -report *ReportName* and a set of options that specify report parameters (as described below). The reports support four different formats: ASCII, HTML, tabulator separated format, and short ASCII format.

Each report includes the following two parts:

- **Input:** What you have to/may specify to configure a report?
- **output:** The content of the report.

Input items that are included within square brackets ([ ]) are optional, while all others are required.

The following *report categories* are available:

Sessions in Timeframe

Sessions in Timeframe reports offer reports about backup, object copy, object consolidation, and object verification activities completed in past over a certain time. You can define this time either in relative terms (such as last 24 hours) or absolute (**15/03/12 00:00** - **16/03/12 00:00**).

Two other common report options for all **Sessions in Timeframe** reports include backup specification and backup specification group. These two limit the report to selected backup specifications.

- Client Statistics (host_statistics)
- Device Flow Report (device_flow)
- Extended Report on Used Media (used_media_extended)
- List of Sessions (list_sessions)
- Object Copies Report (obj_copies)
- Report on Used Media (used_media)
- Session Errors (session_errors)
- Session Flow Report (session_flow)
- Session Statistics (session_statistics)

Session Specifications

Session Specifications reports offer different configuration reports based on backup, object copy, object consolidation, and object verification specifications. By default, it uses backup, object copy, object consolidation, and object verification specifications, but you may choose to limit a report to a certain session specification. Selection of a backup specification group is only for backup specifications.

- Average Backup Object Sizes (obj_avesize)
- Filesystems Not Configured for Backup (fs_not_conf)
- Object's Latest Backup (obj_lastbackup)
- Objects Without Backup (obj_nobackup)
- Session Specification Information (dl_info)
- Session Specification Schedule (dl_sched)
- Trees in Backup Specification (dl_trees)

Internal Database

The Internal Database Size Report (db_size) report includes information about Data Protector Internal Database (IDB) size.

Configuration

Configuration reports include various reports about Data Protector environment:

- Cell Information (cell_info)
- Client Backup Report (host)
- Clients not Configured for Data Protector (hosts_not_conf)
- Configured Clients not Used by Data Protector (hosts_unused)
- Configured Devices not Used by Data Protector (dev_unused)
- Licensing report (licensing)
- Look up Schedule (lookup_sch)

Pools and Media

"Pools and Media" reports offer reports that search through Data Protector pools for media matching the search criteria. The default is to list all media or pools and each report option can then limit the search to a certain set of media.

- Extended List of Media (media_list_extended)
- List of Pools (media_list)
- List of Media (pool_list)
- Media Statistics (media_statistics)

Single Session

"Single session" reports include information about single Data Protector backup, object copy, object consolidation, or object verification sessions. These reports are mostly used as End of Session notification. In this case, Data Protector uses the session ID of the current session (the one that generated the End of Session event) to create the appropriate report.

- Session Devices Report (session_devices)
- Session Media Report (session_media)
- Session Object Copies Report (session_objcopies)
- Session Objects Report (session_objects)
- Session per Client Report (session_hosts)
- Single Session Report (single_session)

OPTIONS

-version

Displays the version of the omnirpt command.

-help

Displays the usage synopsis for the omnirpt command.

-header

This option is not used for the reports that have no required or optional report options. If this option is set, the output of the report will display report options too. If it is not set, only the output of the report is displayed.

-multicell

This option is only used with **Manager-of-Managers**. If this option is specified, the report will be generated for all Cell Managers configured in the MoM environment (multicell report).

-[no_]multiple

This option is only used for enterprise reports (multicell) and for Session per Client reports. If this option is specified, the report will be divided into sections. For enterprise reports the report will be divided by Cell Manager and for Session per Client reports it will be divided by client.

SMTP Options

-server_name SMTPServerHostName

Use this option to specify the SMTP server host name.

--user_name UserName

Use this option to specify the username configured on the SMTP server.

-email_id SenderEmailAddress

Use this option to specify the email address configured on the SMTP server.

[-server_port SMTPServerSecurePort]

The default SMTP server secure port is 587. Use this option to specify a different SMTP server secure port.

Configure SMTP

-add SMTPOptions

Use this option to add the secure SMTP credentials as per the details provided in SMTPOptions.

-list

Use this option to check or verify the secure SMTP credentials configured using the add option.

-remove

Use this option to remove the existing secure SMTP credentials.

-test

Use this option to test the secure connection to SMTP server based on the configured credentials.

Report names

list_sessions

Lists all sessions in the specified time frame. The report is defined by set of options that specify report parameters. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName ...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName ...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-verificationlist_sch *ScheduledVerificationSpecificationName...*]

[-verificationlist_post *PostbackupVerificationSpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_verificationlist]

[-no_conslist]

session_flow

Graphically presents duration of each session specified in certain time frame. Flow chart of the backup, object copy, object consolidation and object verification sessions matching search criteria is shown. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-verificationlist_sch *ScheduledVerificationSpecificationName...*]

[-verificationlist_post *PostbackupVerificationSpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_verificationlist]

[-no_conslist]

device_flow

Graphically presents usage of each device. Flow chart of the backup, object copy, and object consolidation sessions matching search criteria is shown. If you set the RptShowPhysicalDeviceInDeviceFlowReport global option to 1, the same physical devices (presented by their lock names or serial numbers) are grouped together. If there is no lock name or serial number specified, the logical name is displayed. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

used_media

Lists destination media that have been used by backup, object copy, and object consolidation sessions in the specific time frame together with their statistics. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

used_media_extended

Gives extended information on destination media that have been used by backup, object copy, and object consolidation sessions in the specific time frame, as well as the session type and subtype. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

host_statistics

Lists of clients and their backup status - only clients that were used by the backup sessions matching the search criteria are displayed.

Additionally, clients can be limited also with the -hosts report option.

The **VADP** feature introduced in Data Protector 8.14 offers enhanced reports for Virtual Machines. Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients. The VM name is the client name.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-hosts]

session_statistics

Shows statistics about backup, object copy, and object consolidation status in the selected time frame, limited to sessions matching the search criteria. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

session_errors

Shows list of messages that occur during backup, object copy, object consolidation, and object verification sessions in the specified time frame for selected session specifications. The messages are grouped by clients (for all selected clients). By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

[-verificationlist_sch *ScheduledVerificationSpecificationName...*]

[-verificationlist_post *PostbackupVerificationSpecificationName...*]

[-hosts *Hostname...*]

[-level *Level*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

[-no_verificationlist]

obj_copies

Lists object versions that are created in the specified time frame with the number of their valid copies. The number of copies includes the original object version. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients. The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

Report options are:

-timeframe { *Start Duration* | *Day Hour Day Hour* }

-num_copies { *less* | *equal* | *more* } *NumberOfCopies*

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

dl_trees

Lists all trees in the specified backup specification. It also shows names of drives and the name of a tree.

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients. The report displays all the VM names for VMware objects.

Report options are:

[-datalist *BackupSpecificationName* ...]

[-group *BackupSpecificationGroup*]

obj_nobackup

Lists all objects, specified for backup in selected backup specifications, which do not have a valid backup. A valid backup means that the backup completed successfully and its protection has not expired. For each object that does not have a valid protected full backup, the following items are shown: backup specification, an object type, an object name and a description. Only objects from the selected backup specification are used for the report. If HOST object is used: Host object is expanded (get disks) and report checks that expanded objects are in database. Unix and Windows filesystems are supported. This option is not available for backup specifications for integrations.

Report options are:

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-days *NoOfDays*]

obj_lastbackup

Lists all objects in the IDB. For each object, it displays the last full and the last incremental backup time, the last full and the last incremental object copy time, and the last object consolidation time.

Objects of the Client System type (host backup) are expanded; it means that the information is listed for each volume separately. As for objects of the Filesystem type (filesystem objects), only the Unix and Windows filesystems are supported.

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients. The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

You can narrow the scope of objects listed using the following report options:

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-days *NoOfDays*]

However, note the following:

–Filesystem objects that do not match the condition in the object creation time filter are listed anyway. However, in this case, the object creation time fields remain empty.

– If you clear certain filesystem objects from a backup specification, these filesystem objects will not be included in the report even if the objects exist in the IDB.

The above note is not applicable for objects of the Bar type (integration objects).

obj_avesize

Lists all objects, specified for backup in selected backup specifications, which have a valid backup. A valid backup means that the backup completed successfully and its protection has not expired. For each object average full and average incremental backup size is displayed. If HOST object is used: Host object is expanded (get disks) and report checks that expanded objects are in database. Unix and Windows filesystems are supported.

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients.

The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

Report options are:

[-datalist *BackupSpecificationName* ...]

[-group *BackupSpecificationGroup*]

[-days *NoOfDays*]

fs_not_conf

Displays a list of mounted filesystems which are not in selected backup specifications. Output is a list of filesystems. If HOST object is used, the report will not report any disk from client as not configured (assuming that HOST backup will backup all disks). If HOST object is used, the report will not report any disk from client as not configured (assuming that HOST backup will backup all disks).

Report options are:

[-datalist *BackupSpecificationName* ...]

[-group *BackupSpecificationGroup*]

dl_info

Shows information about all selected backup, object copy, object consolidation, and object verification specifications, such as type (for example, IDB, MSESE, E2010), session type, session specification name, group, owner, and pre & post exec commands. Host does not influence the report. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup...*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-verificationlist_sch *ScheduledVerificationSpecificationName...*]

[-verificationlist_post *PostbackupVerificationSpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_verificationlist]

[-no_conslist]

dl_sched

Shows information about all selected backup, object copy, object consolidation, and object verification specifications and their next scheduled time up to one year in advance (type, session type, session specification name, group, next execution, and backup operation time). HOST does not influence report. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

[-datalist *BackupSpecificationName...*]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName...*]

[-copylist_post *PostbackupCopySpecificationName...*]

[-verificationlist_sch *ScheduledVerificationSpecificationName...*]

[-verificationlist_post *PostbackupVerificationSpecificationName...*]

[-conslist_sch *ScheduledConsolidationSpecificationName...*]

[-conslist_post *PostbackupConsolidationSpecificationName...*]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_verificationlist]

[-no_conslist]

db_size

Displays information about the MMDB, CDB, archived log files, datafiles, and information for DCBF and SMBF in a table

format.

The Used columns in this report show the percentage of used items for each IDB part. This figure is calculated as the current number of items divided by the number of maximum items for particular IDB part in percents. In case the number of items is unlimited, this figure is always 0%. To find out whether certain parts of IDB are running out of space, you can additionally configure the IDB Space Low notification.

hosts_unused

Lists configured clients that are not used for backup and do not have any device configured.

dev_unused

Lists configured destination devices that are not used for backup, object copy, or object consolidation at all.

lookup_sch

List of backup, object copy, and object consolidation specifications that are scheduled to start in the next n number of days up to one year in advance (where n is the number of days specified by user).

Report option is:

[-schedule *NoOfDays*]

hosts_not_conf

List of clients in selected domain(s) that are not configured for Data Protector. Note that Data Protector will display also routers and other machines that have IP address in selected domain.

Report option is:

-network *IP_Address* ...

licensing

Lists all licenses and the available number of licenses.

host

Report output is all end-user backup related information about specific client: list of filesystems not configured for selected clients, list of all objects configured in backup specifications for the selected client, list of all objects with a valid backup for specified client with times and average sizes.

Note that Client Backup reports do not include information about application integration backup objects and backup specifications.

Report option is:

-host *HostName*

media_list

List of all media matching the search criteria. Displays the following information for each medium:
ID, label, location, status, protection, used and total MB, the time when media was last used, the media pool, and media class.

Report options are:

[-label Label]

[-location *Location...]*

[-pool *PoolName...]*

[-class *MediaClass...]*

[-status *MediaStatus]*

[-[no_]protection *NoOfDays]*

[-timeframe { *Start Duration* | *Day Hour Day Hour* }]

[-[no_]library *Library* ... *]*

media_list_extended

List of all media matching the search criteria. Displays the following information for each medium:
ID, label, location, status, protection, used and total MB, the time when media was last used, the media pool and media type, session specifications that have used this medium for backup, object copy, or object consolidation, as well as the session type and subtype.

By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

[-label *Label*]

[-location *Location* ...]

[-pool *Pool Name* ...]

[-class *MediaClass*]

[-status *MediaStatus*]

[-[no_]protection *NoOfDays*]

[-timeframe { *Start Duration* | *Day Hour Day Hour* }]

[-[no_]library *Library* ...]

[-datalist *BackupSpecificationName* ...]

[-group *BackupSpecificationGroup*]

[-copylist_sch *ScheduledCopySpecificationName* ...]

[-copylist_post *PostbackupCopySpecificationName* ...]

[-conslist_sch *ScheduledConsolidationSpecificationName* ...]

[-conslist_post *PostbackupConsolidationSpecificationName* ...]

Report filtering options are:

[-no_datalist]

[-no_copylist]

[-no_conslist]

media_statistics

Reports the statistics on the media matching the search criteria. Displays the following information: number of media; number of scratch media; number of protected, good, fair and poor media; number of appendable media; and total, used, and free space on media.

Report options are:

[-label Label]

[-location *Location* ...]

[-pool *PoolName* ...]

[-class *MediaClass*]

[-status *MediaStatus*]

[-[no_]protection *NoOfDays*]

[-timeframe { *Start Duration* | *Day Hour Day Hour* }]

[-[no_]library *Library* ...]

pool_list

Lists all pools matching a specified search criteria. Displays the following information for each pool: pool name, description, media type, total number of media, number of full and appendable media containing protected data, number of free media containing no protected data, number of poor, fair and good media.

Report options are:

[-pool *PoolName* ...]

[-location *Location* ...]

[-class *MediaClass*]

[-[no_]library *Library* ...]

[-timeframe { *Start Duration* | *Day Hour Day Hour* }]

single_session

Report displays all relevant information about single Data Protector backup, object copy, object consolidation, and object

verification sessions.

Report option is:

-session *SessionID*

[-level *Level*]

session_objects

Returns all information about all backup, object copy, or object consolidation objects that took part in a selected session.

Returns information about VM name and VM path for VMware virtual machines manifested as Data Protector clients called **VADP** clients.

Report option is:

-session *SessionID*

session_hosts

Displays information for each client that took part in the selected backup session: statistics about backup status for the client, list of objects and their related information for the client, error messages for the client.

All information is grouped for each client separately. Using the -multiple option, this report can be split into smaller reports, one for each client (see section Notifications for details).

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients.

The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

Report option is:

-session *SessionID*

[-level *Level*]

session_devices

Displays information about all devices that took part in a selected session.

Report option is:

-session *SessionID*

session_media

Displays information about all destination media that took part in a selected session.

Report option is:

-session *SessionID*

session_objcopies

Lists object versions that are created in the selected backup, object copy, and object consolidation session with the number of their valid copies.

Reports display VMware virtual machines in the same way as Data Protector clients called **VADP** clients.

The new object name format is as follows:

<hostname>:/<vCenter>/<path>/<vmname>[<UUID>]

Here, <hostname> is the DNS name of the guest virtual machine. If the DNS name is unknown, the IP address or VM name is used.

Report option is:

-session *SessionID*

Method options

-email *EmailAddress*

Sends the report to the specified *EmailAddress*.

On Windows systems, you need a configured MAPI profile. You can either use an existing mail profile or create a new one, named Omniback. To use an existing profile, edit the omnirc option OB2_MAPIPROFILE.

On Unix systems, /usr/bin/mail is used for sending the e-mails.

-smtp *EmailAddress*

The recommended option for sending reports by e-mail. Sends the report to the specified *EmailAddress* using the SMTP protocol.

By default, the SMTP server address is set to the Cell Manager address. To change the SMTP server, edit the SMTPServer global option. The server must be accessible from the Cell Manager system, but does not need to be part of the Data Protector cell.

-snmp *Hostname*

Report is send as an SNMP (Simple Network Mailing Protocol) trap.

-broadcast *Hostname*

Report is broadcasted to the selected machine. NOTE: Only Windows machines can be specified as broadcast destination.

-log *Filename*

Report is saved in to the log file specified with *Filename*.

-external *CommandName*

Specifies a script which receives the report. Optionally the script can than parse the report and forward it to user configured recipient. Usually, TAB report format is used in combination with -external option.

Report options

-rptgroup *ReportGroup*

This option executes the specified *ReportGroup*.

-session *SessionID*

This option is used to specify the session ID.

-pool *Poolname* ...

This option is used to specify the media pool name.

-label *Label*

This option is used to specify the medium label.

-location *Location* ...

This option is used to specify the medium location.

-[no_]library *Library* ...

This option is used to specify the library. If it is set to -no_library, all libraries in the cell are selected for the report.

-[no_]protection *NoOfDays*

This option is used to specify the protection. The number of days in which the protection will expire can be specified. If it is set to no_protection, all media in the cell will be selected for the report.

-class *MediaClass*

This option is used to specify the media class. It can have one of the following values: DDS, QIC, Exabyte, AIT, SAIT, T3480/T4890/T9490, Optical, File, T9840, Tape, DLT, SD-3, T3590, T3592, LTO-Ultrium, SuperDLT, VXA, DTF, T9940, T10000, StoreOnceSoftware, DataDomainBoost or ObjectStore.

-status *MediaStatus*

This option is used to specify the media status. It can have one of the following values: poor, fair, or good.

-datalist *BackupSpecificationName...*

This option is used to specify the backup specifications for the report. If you specify more than one backup specification, separate the specification names with spaces.

-copylist_sch *ScheduledCopySpecificationName...*

This option is used to specify the scheduled object copy specifications for the report. If you specify more than one scheduled object copy specification, separate the specification names with spaces.

-copylist_post *PostbackupCopySpecificationName...*

This option is used to specify the post-backup object copy specifications. If you specify more than one post-backup object copy specification, separate the specification names with spaces.

-verificationlist_sch *ScheduledVerificationSpecificationName...*

This option is used to specify the scheduled object verification specifications for the report. If you specify more than one scheduled object verification specification, separate the specification names with spaces.

-verificationlist_post *PostbackupVerificationSpecificationName...*

This option is used to specify the post-backup object verification specifications. If you specify more than one post-backup object verification specification, separate the specification names with spaces.

-conslist_sch *ScheduledConsolidationSpecificationName...*

This option is used to specify the scheduled object consolidation specifications. If you specify more than one scheduled object consolidation specification, separate the specification names with spaces.

-conslist_post *PostbackupConsolidationSpecificationName...*

This option is used to specify the post-backup object consolidation specifications. If you specify more than one post-backup object consolidation specification, separate the specification names with spaces.

-group *BackupSpecificationGroup*

This option is used to specify backup specification group for the report.

-schedule *NoOfDays*

This option is used to specify the number of days for which to display the schedule information.

-network *IP_Address* ...

This option specifies one or more IP addresses. Valid IP address forms are:

- a.b.c.d – a complete IPv4 address (for example, 10.17.1.1)
- a.b.c – an IPv4 C-class network address (for example, 10.17.1)
- IPv6 addresses in any valid form (for example, ::1, td10::abba:1603, and so on)

You can specify more than one IP address by using spaces in between.

-hosts *Hostname* ...

Select the client systems for which you want to create the report.

-host *Hostname*

Select the client system for which you want to create the report.

-level *Level*

Select the level of warnings that should be included in the report. The levels are warning , minor , major , and critical .

-num_copies { *less* | *equal* | *more* } *NumberOfCopies*

This option is used to specify the number of valid object versions copies. Note that you can specify more than, equal to, or less than the selected number of copies.

-timeframe *Start Duration*

This option is used to specify a relative time frame. It is useful for recurrent reports, for example you can use -timeframe 24 24 each day to set the time frame to last 24 hours.

-timeframe *Day Hour Day Hour*

This option is used to specify an absolute time frame.

-days *NoOfDays*

The report will filter objects that have been backed up recently. Specify the number of days.

Report filtering options

-no_datalist

This option is used to exclude all backup specifications from the report.

-no_copylist

This option is used to exclude all object copy specifications from the report.

-no_verificationlist

This option is used to exclude all object verification specifications from the report.

-no_conslist

This option is used to exclude all object consolidation specifications from the report.

Report Formats

-ascii

Specifies report format: ASCII

-html

Specifies report format: HTML

-tab

Specifies report format: TAB

-short

Specifies report format: SHORT

NOTES

The virtual machine objects and its associated disk objects constitute the VEAgent object size. The other fields in the omnirpt output for the VMware objects display the details of the virtual machine object, and not the disk objects.

EXAMPLES

1. To list all backup sessions that have started in the last 24 hours and display the report in the default ASCII format, execute:

   ```
   omnirpt -report list_sessions -timeframe 24 24 -no_copylist -no_conslist -no_verificationlist
   ```

2. To list all objects from session "2012/11/16-1" in tabulator separated format, which is useful for additional parsing or can be used with other tools for analysis, execute:

   ```
   omnirpt -report session_objects -session 2012/11/16-1 -tab
   ```

3. To list all media of class DLT with location string "COMPANY", for which protection will expire in the next 5 days, execute:

   ```
   omnirpt -report media_list -protection 5 -class DLT -location COMPANY
   ```

   This report can be used as a base for the vaulting process, as it can list you media that need to be taken to the vault.

4. To send "Internal Database Size Report" in HTML format to the user "name@domain.com" using the SMTP protocol, execute:

   ```
   omnirpt -report db_size -html -smtp name@domain.com
   ```

5. To execute the report group named "MyReportGroup", execute:

   ```
   omnirpt -rptgroup MyReportGroup
   ```

6. To graphically present the usage of devices that were used for backup and object consolidation (but not object copy) sessions in the last 48 hours in HTML format that will be sent as the file "session1#$filename|" to the directory "C:\Temp", execute:

   ```
   omnirpt -report device_flow -timeframe 48 48 -no_copylist -html >C:\Temp\session1#$filename|
   ```

7. To list all the media used only for object copy and object consolidation sessions, execute:

   ```
   omnirpt -report media_list_extended -no_datalist
   ```

8. To list all object versions created in the last 72 hours that have less than 5 valid copies, execute:

```
omnirpt -report obj_copies -timeframe 72 72 -num_copies less 5
```

9. To list all destination media that were used only for scheduled object copy specification named "Alpha" in the last 2 days, execute:

   ```
   omnirpt -report used_media -timeframe 48 48 -copylist_sch Alpha -no_datalist -no_conslist
   ```

10. To show statistics about backup status (but not object copy, object consolidation, and object verification) in the last 24 hours, execute:

    ```
    omnirpt -report session_statistics -timeframe 24 24 -no_copylist -no_conslist -no_verificationlist
    ```

11. To graphically present duration of all object consolidation sessions in the last 24 hours in HTML format that will be sent as the file "session_flow1#$filename|" to the directory "C:\Temp", execute:

    ```
    omnirpt -report session_flow -timeframe 24 24 -no_datalist -no_copylist -no_verificationlist -html  >C:\Temp\session_flow1#$filename|
    ```

12. To show all virtual machines selected in the VEPA backup specifications, execute:

    ```
    omnirpt –report dl_trees
    ```

13. To show the backup information about vCenters, ESXi servers and virtual machines in the last 24 hours, execute:

    ```
    omnirpt –report host_statistics –timeframe 24 24
    ```

14. To show copy IDs for backed up virtual machines in the last 24 hours, execute:

    ```
    omnirpt –report obj_copies –timeframe 24 24
    ```

15. To list information about the latest backup for all objects including virtual machines, execute:

    ```
    omnirpt –report obj_lastbackup
    ```

16. To list average object size for all objects including virtual machines, execute:

    ```
    omnirpt –report obj_avesize
    ```

17. To list information about objects including virtual machines for a given session, execute:

    ```
    omnirpt -report session_objects -session 2015/10/14-1
    ```

18. To list virtual machines as clients included in the selected backup session, execute:

    ```
    omnirpt -report session_hosts -session 2015/10/14-1
    ```

19. To list object versions of backed up virtual machines for the selected session, execute:

    ```
    omnirpt -report session_objcopies -session 2015/10/14-1
    ```

SEE ALSO

omnihealthcheck(1M), omnitrig(1M)

omnistat

omnistat - displays the status of active Data Protector backup and restore sessions
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnistat -version | -help

omnistat -session *SessionID* [-status_only | -monitor | -detail]

omnistat [-user *Username*] [-mount] [-error] [-detail]

omnistat -previous [-user *Username*] [{ -since *Date* | -until *Date* } | -last *Number*] [-failed]

Date

[*YY*] *YY/MM/DD*

DESCRIPTION

The omnistat command displays information on active sessions. You can view all active sessions (default) or only details of a specific session. An active session is referenced by its *SessionID*.

OPTIONS

-version

Displays the version of the omnistat command.

-help

Displays the usage synopsis for the omnistat command.

-session *SessionID*

Displays detailed information on the single active session identified by this *SessionID*.

-monitor

omnistat connects to the specified active session and starts monitoring the progress of the session.

-status_only

Displays only the overall status of the active session.

-detail

Displays detailed information about all current sessions.

-user *Username*

Displays information on active sessions belonging to the specified user.

-failed

Displays information on sessions containing data objects that failed due to errors.

-error

Displays information on active sessions with the status "In Progress (errors)"

-mount

Displays all active sessions with mount requests pending.

-previous

Lists all sessions from the Data Protector Internal Database (IDB).

-since *Date*

Lists all sessions since the specified *Date*.

-until *Date*

Lists all sessions until the specified *Date*.

-last *n*

Lists all sessions within the last *n* days.

EXAMPLES

The following examples illustrate how some options of the omnistat command work.

1. To view sessions that are currently active and have mount requests pending, execute:

   omnistat -mount

2. To see detailed information for the session with the SessionID "2013/04/24-32", execute the following commands. The SessionID can be specified in two different formats. If the short format is used, the ID refers to the session that was run in the same day:

omnistat -detail -session 2013/04/24-32

omnistat -detail -session 32

3. To see an overview of the sessions that occurred in last 3 days and were run by user root, execute:

   omnistat -previous -user root -last 3

4. To see information regarding the sessions that occurred within the last 3 days and had objects that have failed, execute:

   omnistat -previous -last 3 -failed

5. To see only the status of session with this SessionID, execute:

   omnistat -status_only -session 2

6. To monitor the session with the SessionID "R-2013/05/13-8", execute:

   omnistat -session R-8 -monitor

SEE ALSO

omniabort(1)

omniupload

omniupload - uploads information about a backup device from an ASCII file to the Data Protector Internal Database (IDB) (this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omniupload -version | -help

omniupload -create_device *FileName*

omniupload -modify_device *BackupDevice* [-file *FileName*]

omniupload -remove_device *BackupDevice*

omniupload -create_library *FileName*

omniupload -modify_library *Library* [-file *FileName*]

omniupload -remove_library *Library*

omniupload -create_cloudoptions [-cloud_type *[S3Glacier | S3GlacierDeepArchive]* -s3url *S3urlValue* -accesskey *AccessKeyID* -secretkey *SecretKeyID*]

DESCRIPTION

Uploads a backup device file to the Data Protector Internal Database (IDB).

Information on Data Protector backup devices is stored in the IDB. To configure a backup device, information on this device must be downloaded into a file. This is done using the omnidownload command. The file is then modified and uploaded back to the IDB.

OPTIONS

-version

Displays the version of the omniupload command.

-help

Displays the usage synopsis for the omniupload command.

-create_device *FileName*

Specifies the ASCII file containing the information about the backup device. This option is used to create a new backup device. If - is specified as *FileName* then data is read from stdin.

-modify_device *BackupDevice*

Uses the information in the uploaded file to modify an existing backup device in the IDB. If no filename is specified using the -file option the command searches the current directory for a file with the same name as the *BackupDevice*. Note that

the media class may not be changed.

-file *FileName*

Specifies the ASCII file that will be parsed for information about the backup device (library). This option is used to modify an existing backup device (library). If - is specified as *FileName* then data is read from stdin.

-remove_device *BackupDevice*

Removes information about the *BackupDevice* from the IDB.

-create_library *FileName*

Specifies the ASCII file containing the information about the library. This option is used to create a new library. If - is specified as *FileName* then data is read from stdin.

-modify_library *Library*

Uses the information in the uploaded file to modify an existing library in the IDB. If no filename is specified using, the -file option the command searches the current directory for a file with the same name as the *Library*. Note that the media class may not be changed.

-remove_library *Library*

Removes information about the *Library* from the IDB.

-create_cloudoptions

Creates a cloud options string.

-cloud_type *CloudTypeValue*

Specifies the cloud device type.

-s3url *S3urlValue*

Specifies the s3 url value.

-accesskey *AccessKeyID* -secretkey *SecretKeyID*

Specifies the access key ID and the secret key ID that is needed to create while creating a cloud device.

EXAMPLES

The following examples illustrate how the omniupload command works.

1. To create a backup device using the information in the file "/tmp/Device", execute:

```
omniupload -create_device /tmp/Device
```

2. To modify library "Exabyte1" using the information in the file "/tmp/EXA", execute:

   ```
   omniupload -modify_library Exabyte1 -file /tmp/EXA
   ```

3. To remove backup device "Stacker", execute:

   ```
   omniupload -remove_device Stacker
   ```

4. To create a virtual tape library named "VTL16" using the information in the file "lib16.txt", execute:

   ```
   omniupload -create_library lib16.txt
   ```

5. To modify the library capacity of a virtual tape library named "VTL" in an ASCII file named "libVTL.txt" in the directory "C:\Temp" to 50 TB, set the VTLCAPACITY parameter to 50:

   ```
   VTLCAPACITY 50
   ```

   and execute:

   ```
   omniupload -modify_library VTL -file C:\Temp\libVTL.txt
   ```

   Note that the VTLCAPACITY value in terabytes (TB) must be an integer.

6. To create an Amazon s3 Glacier cloud options string, run the following command:

   omniupload -create_cloudoptions [-cloud_type *S3Glacier* -s3url *https//:s3.us-east-1.amazonaws.com/* -accesskey *AccessKeyID* -secretkey *SecretKeyID*]

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), sanconf(1M), uma(1M)

omniusb

omniusb - writes the DR ISO image to a USB drive, and makes the drive bootable
(this command is available on systems with the Data Protector Automatic Disaster Recovery component installed)

SYNOPSIS

omniusb --version | --help

omniusb --iso *Path* { --drive *VolumePath* | --disk *DiskNumber* } [--silent]

DESCRIPTION

The omniusb writes the disaster recovery OS, converted from the DR ISO image – which was created using the GUI or the omniiso command – , to a USB drive, and makes the drive bootable. You can then use the bootable USB drive to start your recovery process.

You can use this command to automate your backup and disaster recovery preparation.

Alternatively, you can create a bootable USB drive can using the EADR Wizard from the Data Protector GUI.

OPTIONS

--version

Displays the version of the omniiso command.

--help

Displays the usage synopsis for the omniiso command.

--iso *Path*

Specifies the location where the disaster recovery ISO image file is located.

--drive *MountPath*

Specifies the mount path to which the USB drive is mounted, for example E:\.

--disk *DiskNumber*

Specifies the USB drive by its disk number as reported by the Windows Disk Management Extension.

--silent

Suppresses any user interaction. This option is applicable if the command is used in a pre--exec script.

NOTES

The omniusb command is available on Windows systems only.

EXAMPLES

The following examples illustrate how the omniusb command works.

1. To save the USB drive image created from a disaster recovery ISO file, located in "C:\iso\dr\omnidr.iso", to a USB drive, mounted under "G:", execute:

   omniusb --iso c:\iso\dr\omnidr.iso --drive G:

2. To save a disaster recovery ISO file, located in "C:\iso\dr\omnidr.iso", to a USB drive with the disk number "6", execute:

   omniusb --iso c:\iso\dr\omnidr.iso --disk 6

SEE ALSO

omniiso(1), omnidr(1M), omniofflr(1M), omnisrdupdate(1M)

omniusers

omniusers - adds or removes Data Protector users to or from an existing Data Protector user group, or lists the configured Data Protector users.

This command does not support the following:

- adding LDAP user and LDAP group.
- modifying LDAP group.
- listing/displaying LDAP group

Restart the Data Protector services if you perform any of the add, modify, or delete operations. Use the command omnisv -restart .

(This command is available on non-Windows systems with the Data Protector User Interface component installed.)

SYNOPSIS

omniusers -version | -help

omniusers -add -type { U | W } -usergroup *DPUserGroup* -name *UserName* -group *GroupOrDomainName* -client *ClientName* [-desc *Description*] [-setpass | -pass *password*]

omniusers -remove -name *WebUserName*

omniusers -modify -usergroup *DPUserGroup* -name WebUserName [-desc Description] [-newname NewUserName] [-newclient newClientName] [-newgroup newGrouporDomainName] [-newusergroup newDPUserGroup]

omniusers -list

omniusers -resetpass -name *WebUserName* [-pass password] [-oldpass oldpassword] [-targetCell targetCellManager]

omniusers -clearpass -name WebUserName [-targetcell targetCellManager]

omniusers -ldap_config -add -name *LdapConfigName* -vendor ActiveDirectory -server *LdapServer* -port *PortNumber* -usersDN *UserDistinguishedName* -bindDN *BindDistinguishedName* -rolesDN *rolesCtxDN* -bindcred *Password*

omniusers -ldap_config -remove -name *LdapConfigName*

omniusers -ldap_config -modify -name *LdapConfigName* [-newusersDN *NewUserDistinguishedName*] [-newbindDN *NewBindDistinguishedName*] [-newbindcred *NewPassword*]

omniusers -ldap_config -list

omniusers -ldap_config -testconn -server LdapServer -port PortNumber

omniusers -ldap_config -testauth -server LdapServer -port PortNumber -bindDN BindDistinguishedName -bindcred Password

DESCRIPTION

The command adds, removes, or lists the Data Protector users configured on the Cell Manager. It does not create or remove Data Protector user groups.

Use the command to remotely add a new Data Protector user account from a system where the Data Protector GUI is not supported. You can then use the account to start the Data Protector GUI on another system, and connect to the Cell Manager.

OPTIONS

-version

Displays the version of the omniusers command.

-help

Displays the usage synopsis for the omniusers command.

-add

Adds a user to the specified Data Protector user group.

-remove

Removes a user from its Data Protector user group.

-name *UserName*

Specifies username of the user to be added/removed. By specifying asterisk (*) as the username, all users from the specified group (on UNIX systems) or domain (on Windows systems) will be granted/revoked access from the specified clients to the Cell Manager.

* corresponds to <Any> in the Data Protector GUI. Note that in some shells, backslash and asterisk (*) must be used instead of *.

Note: Usernames and usernames of the configured Data Protector users are case-sensitive.

-type {U|W}

Specifies the user type: a UNIX user (U) or a Windows user (W).

-group *GroupOrDomainName*

A group (on UNIX systems) or a domain (on Windows systems) the specified user belongs to. By specifying asterisk (*) as the group or domain name, the specified user will be granted/revoked access from any group or domain from the specified clients.

* corresponds to < Any> in the Data Protector GUI. In some shells, backslash and asterisk (*) must be used instead of *.

Note that domain names of Windows GUI clients that are used with an LinuxCell Manager must be in capital letters.

-client *ClientName*

Specifies the name of the client system from where the specified user will have access to theCell Manager. By specifying asterisk (*) as the client name, the specified user will be granted/revoked access to the Cell Manager from any Data Protector client system.

* corresponds to < Any> in the Data Protector GUI. Note that in some shells, backslash and asterisk (*) must be used instead of *.

If this option is used with the -remove option, *ClientName* must contain the fully qualified domain name (FQDN) of the client system.

-usergroup *DPUserGroup*

Specifies the Data Protector user group the user(s) will be added to.

-desc *Description*

Specifies the description for the added user(s).

-passwd *Password*

Specifies the password for the added user.

-list

Lists users in all configured Data Protector user groups in the cell and updates the userlist file. For each configured Data Protector user the username, UNIX group or Windows domain, fully qualified domain name (FQDN) of the client system from which the user has granted access, and the user description are displayed. Asterisk (*) corresponds to the < Any> string in the Data Protector GUI.

-ldap_config

Configures LDAP for the user.

-name *LdapConfigName*

Specifies the name for LDAP configuration.

-vendor [ActiveDirectory]

Specifies the LDAP server vendor as ActiveDirectory.

-server *LdapServer*

Specifies the URL of the LDAP server in the following format: ldap://<server>:<port> .

-port *PortNumber*

Specifies the URL of the LDAP server in the following format: ldap://<server>:<port> .

-usersDN *UserDistinguishedName*

Specifies the distinguished name (DN) of the LDAP location that contains the users.

-bindDN *BindDistinguishedName*

Specifies the DN of an LDAP user that is used by the login module to perform the initial LDAP bind. You must have the required permission to search the LDAP location of the users and groups to obtain the users and their groups.

-bindcred *Password*

Specifies the password for the LDAP user provided in the BindDN option.

-rolesDN *rolesCtxDN*

Specifies the DN of the LDAP location that contains the user groups. Modifying Roles Context DN is not supported.

Important By default, the asterisk (*) option to specify all users, groups, domains or clients is disabled. To enable this option, manually change the value of global option EnableAnyOptionUserCtx to **1** in the global options file available at:

- *Windows*: <PROGRAMDATA>\Config\Server\Options
- *Linux*: /etc/opt/omni/server/options .

By selecting to enable and use the **<Any>** or asterisk (*) option for user, group or client fields in User Management context, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and hold Micro Focus harmless for the same.

In case of enabling and using the **<Any>** or asterisk (*) option for user, group or client fields in User Management context, Micro Focus encourages you to add relevant protection measures against risks associated with user privileges, which is not provided by Micro Focus. By not implementing relevant protection measures, you may be exposing the system to increased security risks. You understand and agree to assume all associated risks and hold Micro Focus harmless for the same. It remains at all times your sole responsibility to assess your own regulatory and business requirements. Micro Focus does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to you in conducting your business.

RETURN VALUES

The return values of the omniusers command are:
0 - The command operation completed successfully.
1 - A generic error occurred.
2 - The operation for adding or removing a user failed.
4 - Error parsing options.

EXAMPLES

The following examples illustrate how the omniusers command works.

1. To add the Windows user "win_user" from the domain "domain1" to the Data Protector "admin" user group and allow access only from the client system "client.company.com", execute:

   omniusers -add -type W -name win_user -usergroup admin -group domain1 -client client.company.com

2. To add the UNIX user "root" from the "sys" group to the Data Protector "admin" user group and allow access only from the client system "client.company.com", execute:

   omniusers -add -type U -name root -usergroup admin -group sys -client client.company.com

3. To add the UNIX user "root" to the Data Protector "admin" user group and allow access from any UNIX group but only from the system "client.company.com", execute:

   omniusers -add -type U -name root -usergroup admin -group * -client client.company.com

4. To display the Data Protector users in all configured Data Protector user groups or to update the userlist file, execute:

   omniusers -list

5. To add LDAP configuration using the LDAP server from ActiveDirectory, execute:

   omniusers -ldap_config -add -name ADname -vendor ActiveDirectory -server 15.218.114.127 -port 389 -usersDN "CN=Users,DC=mytestlab,DC=net" -rolesDN "OU=Groups,DC=mytestlab,DC=net" -bindDN "CN=testuser1,CN=Users,DC=mytestlab,DC=net" -bindcred mypassword

6. To display the LDAP configuration information, execute:

   omniusers -ldap_config -list

SEE ALSO

ob2install(1M), omnigui(5), omniintro(9), omnimigrate.pl(1M), omnisetup.sh(1M), upgrade_cm_from_evaa(1M)

SharePoint_VSS_backup.ps1

SharePoint_VSS_backup.ps1 - creates backup specifications and starts backup sessions for Microsoft SharePoint Server (this command is available on systems with the Data Protector MS Volume Shadow Copy Integration component installed)

SYNOPSIS

SharePoint_VSS_backup.ps1 –help | -version

SharePoint_VSS_backup.ps1 –createonly *CreateOptions*

SharePoint_VSS_backup.ps1 –backuponly *BackupOptions*

SharePoint_VSS_backup.ps1 -preview [–resumefarm] | -resumecert

CreateOptions

{ -device *DevName* | -hardware { no_keep | keep | ir } [-device *DevName*]}

[-overwrite]]

[-prefix *PrefixName*]

[-excludeindex]

BackupOptions

[-outfile *PathToFile*]

[-prefix *PrefixName*]

[-preview]

[-snapshot { diskonly | disktape | tapeonly }]

[-reduce]

[-mode { full | incremental | incremental1 ... | incremental9 }]

[-timeout *Timeout*]

DESCRIPTION

The SharePoint_VSS_backup.ps1 command creates backup specifications and start backup sessions for Microsoft SharePoint Server, using the Data Protector Volume Shadow Copy Service integration.

When you execute the command, Data Protector first queries for information about the Microsoft SharePoint Server environment. Then it creates backup specifications.

The newly created backup specifications are named SharePoint_VSS_backup_ClientName and have the same backup device specified for use (the one that you specified at command runtime). Once the backup specifications are created, the command starts backup sessions (one session for each backup specification).

You can also only create the backup specifications first, modify them in the Data Protector GUI if necessary and then start the backup sessions.

OPTIONS

-help

Displays the SharePoint_VSS_backup.ps1 command usage.

-version

Displays the SharePoint_VSS_backup.ps1 version.

–createonly

If this option is specified, Data Protector only creates backup specifications. Backup is not started.

–backuponly

If this option is specified, Data Protector only starts backup sessions using the existing backup specifications. The -device option is not required.

-device *DevName*

Specifies which Data Protector device to use for backup. You can specify only one device.

-hardware { no_keep | keep | ir }

Specifies that the hardware provider should be used (instead of the software provider with -device option specified) and, consequently, ZDB options set. The default values for ZDB options are as follows:

- Keep the replica for instant recovery: selected if ir is specified.
- Keep the replica after the backup: selected if ir or keep is specified.
- Configuration check mode: Strict
- Replica type: Mirror/Clone (Plex)
- Numbers of replica rotated: 3

The default ZDB backup types are as follows (provided a device is also specified):

- no_keep : ZDB-to-tape
- keep : ZDB-to-disk+tape
- ir : ZDB-to-disk+tape

–overwrite

By default, Data Protector does not create backup specifications if they already exist. If this option is specified, Data Protector overwrites the existing backup specifications with the newly-created ones. Not applicable if –backuponly is specified.

-prefix *PrefixName*

With this option specified, the backup specifications are created under a different name: SharePoint_VSS_backup_PrefixName_*ClientName*.

In case of backup, this option specifies which backup specifications to use: those which name contains *PrefixName*.

Non-ASCII characters in *PrefixName* are not supported.

-outfile *PathToFile*

If this option is specified, backup specification names, errors, sessions outputs, and omnir restore commands are written to the specified file.

-preview

If this option is specified, Data Protector displays information about the Microsoft SharePoint Server environment and describes the related actions without actually performing them.

-snapshot { diskonly | disktape | tapeonly }

Applicable when starting ZDB backup sessions (that is, sessions that use backup specifications in which a hardware provider is specified for use). Performs a ZDB-to-disk (diskonly), ZDB-to-tape (tapeonly) or ZDB-to-disk+tape (disktape) session.

-reduce

Microsoft SharePoint Server 2010: If this option is specified, the command excludes mirrored query components from backup to reduce the backup size.

Microsoft SharePoint Server 2013: If this option is selected, the command selects primary index replicas of each index partition to reduce the backup size.

-excludeindex

Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010). If this option is specified, Data Protector excludes data_index folder contained in the FASTSearch home folder from backup specification. This way, the backup is faster, but the restore is more time consuming. The option enables balancing between a backup size and a time to recovery.

-mode { full | incremental | incremental1 ... | incremental9 }

Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010). With this option specified, either a Full or Incremental or leveled incremental backup can be started. By default, the Full backup is performed.

When the incremental option is specified and the Full backup does not exist, the option is ignored and the Full filesystem backup of the FAST Search index files is started.

-resumecert

Applicable only to Microsoft FAST Search Server 2010. If this option is specified, the FAST Search certificates for the content and the query connectors are reinstalled.

-resumefarm

To be used after restore. This option returns the farm to a working state by resuming all background activities and crawling, unlocking sites, and starting Microsoft SharePoint Server services.

-timeout *Timeout*

This option sets the timeout in minutes after which the crawl of the FAST Search index files is aborted and the farm is resumed. If not specified, the default timeout is 15 minutes.

NOTES

The SharePoint_VSS_backup.ps1 command is available on Windows systems only.

EXAMPLES

Creating backup specifications:

1. To create backup specifications in which the backup device “filelib_writer1” is specified for use, execute:

   SharePoint_VSS_backup.ps1 –createonly –device filelib_writer1

2. To create backup specifications with the label “weekly” in their names and in which the backup device “dev1” is specified for use, execute:

SharePoint_VSS_backup.ps1 –createonly –device dev1 –prefix weekly

3. To create ZDB backup specifications in which the backup device “dev1” and the hardware provider (ZDB disk array) are specified for use, and in which the ZDB option “Keep the replica for instant recovery” is enabled, execute:

   SharePoint_VSS_backup.ps1 –createonly -hardware ir –device dev1

4. Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010).

   To create filesystem backup specifications in which the backup device “dev1” is specified for use and with the “data_index” folder, contained in the “FASTSearch” home folder, excluded from the backup of the FAST Search index files, execute:

   SharePoint_VSS_backup.ps1 –createonly –device dev1 -excludeindex

Starting backup sessions:

1. To preview the actions that are performed when a backup session is started, execute: SharePoint_VSS_backup.ps1 –backuponly –prefix dev –preview
2. To start backup sessions using the existing backup specifications that have no prefix in their names, execute:

   SharePoint_VSS_backup.ps1 –backuponly

3. To start backup sessions using the existing backup specifications that have the prefix weekly in their names, execute:

   SharePoint_VSS_backup.ps1 –backuponly –prefix weekly

4. To start backup sessions using the existing backup specifications that have no prefix in their names and to save the output of the sessions and the associated restore commands to the file “c:\logs\shp.log”, execute:

   SharePoint_VSS_backup.ps1 –backuponly –outfile C:\logs\shp.log

5. To start ZDB-to-disk backup sessions using the existing ZDB backup specifications that have no prefix in their names, execute:

   SharePoint_VSS_backup.ps1 –backuponly -snapshot diskonly

6. To start incremental filesystem backup sessions of the FAST Search index files (Microsoft SharePoint Server 2010), execute:

   SharePoint_VSS_backup.ps1 -backuponly -mode incremental

SEE ALSO

omnib(1)

syb_tool

syb_tool - a utility used to get ISQL command needed to restore a Sybase database that was backed up by Data Protector (this command is available on systems with the Data Protector Sybase Integration component installed)

SYNOPSIS

syb_tool *dbname servername*

-date *YYYY/MM/DD.hh:mm:ss*

[-new_db *dbname*]

[-new_server *servername*]

[-file *filename*]

[-media]

DESCRIPTION

The syb_tool is used to get the data needed for restore of Sybase databases.

OPTIONS

dbname

The name of Sybase database.

servername

The name of Sybase database server on which the backup was performed.

-date *YYYY/MM/DD.hh:mm:ss*

The date until which your database will be restored. syb_tool will find the first backup done after this date.

-new_db *dbname*

The name of the database that you want to restore to.

-new_server *servername*

The name of the server that you want to restore to.

-file *filename*

The name of the file where the ISQL statement needed for restore of desired database will be written to. The ISQL command can be started with the option -i , followed by the name of the file.

See also the section "Notes".

-media

This option returns the list of all media needed for restore.

NOTES

If the names of backed up objects contain characters that cannot be displayed using the current language group (on Windows) or code page (on UNIX):

1. Set the encoding used on the terminal to UTF-8.
2. *Windows systems:* Set the environment variable `OB2_CLI_UTF8` to `1`.
3. Redirect the output of the `syb_tool` command to a text file using the `-i` option.

   If you need to edit the file containing the load command, use a UTF-8 aware editor that does not set the first byte ("BOM"), since such a file is not supported by `isql`. Note that the Windows Notepad editor cannot be used.
4. When restoring the objects, add the `-i file_name -J utf8` options to the `isql` command, where *file_name* is the file with the load command.

EXAMPLES

1. To get the ISQL statement needed for the restore of the last backup of the database named "database1" on the Sybase Adaptive Server named "server", execute:

   ```
   syb_tool database1 server -date
   ```
2. To get the ISQL statement needed for the restore of the database named "database1" on the Sybase Adaptive Server named "server", using the first backup performed after midday of May 07 2013, execute:

   ```
   syb_tool database1 server -date 2013/05/07.12:00:00
   ```
3. To get the ISQL statement needed for the restore of the database named "database1" on the Sybase Adaptive Server named "server", using the first backup performed after midday of May 07 2013 and restoring it as "database_one" on the Sybase server called "server_one", execute:

   ```
   syb_tool database1 server -date 2013/05/07.12:00:00 -new_db database_one -new_server server_one
   ```
4. To get the ISQL statement needed for the restore of the last backup performed for database named "database1" on the Sybase Adaptive Server named "server", saving the ISQL statement to file "/tmp/stat.isql", and getting the list of media IDs needed for restore, execute:

   ```
   syb_tool database1 server -date -file /tmp/stat.isql -media
   ```

   To start the restore, start the ISQL command, specifying the input file "/tmp/stat.isql" in the following way:

   ```
   isql -Usa -P -Sserver -i /tmp/stat.isql
   ```

Section 1M: Administrative commands

This section includes the following topics:

DPDUtils

DPDUtils - configures a Data Protector Deduplication store.

SYNOPSIS

DPDUtils -version | -help

DPDUtils -restart -s <storeName>

DPDUtils -restart -w <storeName>

DPDUtils -shutdown_all

DPDUtils -shutdown <storeName>

DPDUtils -shutdown_portUnifier

DPDUtils -list_stores

DPDUtils -list_stores -s <storeName>

DPDUtils -stat <storeName>

DPDUtils -stat <storeName> -status

DPDUtils -stat <storeName> -dedupe_ratio

DPDUtils -stat <storeName> -capacity

DPDUtils -stat <storeName> -base_path

DPDUtils -unifyPort_all

DPDUtils -unifyPort <storename>

OPTIONS

-version

Displays version info of the DPDUtils command.

-help

Displays the usage synopsis of the DPDUtils command.

-restart -s <storeName>

Restarts the specified deduplication store and restores files from cloud storage if the backend cloud store supports it.

-restart -w <storeName>

Restarts the specified deduplication store and syncs with all the files in cloud.

-shutdown_all

Shuts down all deduplication stores running on the server.

-shutdown <storeName>

Shuts down the specified deduplication store running on the server.

-shutdown_portUnifier

Shuts down the portUnifier.

-list_stores

Lists all the deduplication stores.

-list_stores -s <storeName>

Prints information about the specified deduplication store.

-stat <storeName>

Prints the statistics of deduplication store.

-stat <storeName> -status

Prints the status of deduplication store.

-stat <storeName> -dedupe_ratio

Prints the dedupe ratio of deduplication store.

-stat <storeName> -capacity

Prints the capacity of deduplication store.

-stat <storeName> -base_path

Prints the base path where deduplication store resides.

-unifyPort_all

Adds all deduplication stores on the server to a unified port.

-unifyPort <storeName>

Adds the specified deduplication store to a unified port.

EXAMPLES

1. To print the statistics of the deduplication store DedupeStore, execute:

   DPDUtils -stat *DedupeStore*

2. To list all the available deduplication stores or a specific store, execute:

   DPDUtils -list_stores -s *DedupeStore*

util_hana.pl

util_hana.pl - configures a SAP HANA database and prepares the environment for backup, and checks the configuration of the database. This command is available on systems with the Data Protector SAP HANA Integration component installed.

SYNOPSIS

util_hana.pl -help | -version

util_hana.pl -APP

util_hana.pl -config -sid <InstanceName> -instance <InstanceNumber> -instance_base_path <InstanceBasePath> -sysuser <SystemUsername> -syspassword <SystemPassword> -client <HostName> -port <PortNumber>

util_hana.pl -econfig -sid <InstanceName> -instance <InstanceNumber> -instance_base_path <InstanceBasePath> -sysuser <SystemUsername> -syspassword <EncodedPassword> -client <HostName> -port <PortNumber>

util_hana.pl -CHKCONF <InstanceName or SID>

util_hana.pl -OBJS0 <InstanceName or SID>

OPTIONS

-help

Displays usage synopsis of the util_hana.pl command.

-version

Displays the binary version of the util_hana.pl command.

-APP

Displays the configured SAP HANA SIDs. This has an additional optional option to specify the base path.

-config

Configures the SAP HANA database with the parameters which are provided.

-econfig

Configures the SAP HANA database parameters which are provided, along with the encoded password.

-CHKCONF

Checks the configuration details of the SAP HANA database. This option reqiures SID to be passed as an additional parameter.

-OBJS0

Lists the databases configured for the given SAP HANA instance. This option reqiures SID to be passed as an additional parameter.

cjutil

cjutil - starts, stops, and queries the Windows Change Journal
(this command is available on systems with the Data Protector Disk Agent component installed)

SYNOPSIS

cjutil -volume *vol* { -start [-maxsize *max* -delta *del*] | -stop [-wait] | -query }

DESCRIPTION

The cjutil command is used to control and administer the Change Journal.

OPTIONS

-volume *vol*

Defines the volume name in the form /C or /C:\mounted_folder .

-start [-maxsize *max* -delta *del*]

Starts the Change Journal on the specified volume.

The -maxsize *max* option sets the maximum size of the Change Journal in bytes. The highest possible value is 4 GB (4 294 967 296 bytes). Any specified value greater than 4 GB will be rounded down to 4 GB. Note that a reasonable size for a 100 GB drive is an 85 MB Change Journal.

The -delta *del* option specifies the size in bytes to be purged from the Change Journal when it reaches its maximum size. recommends the value be approximately one-eighth to one-quarter the value of the maximum size but not greater than one quarter the size of the maximum size. This value may be automatically adjusted to better correspond to the volume cluster size.

-stop [-wait]

Stops the Change Journal asynchronously.

The -wait specifies that the Change Journal will be stopped synchronously. The call returns only after the Change Journal has been deleted.

-query

Queries the status of the Change Journal.

NOTES

If the -start option is specified and the Change Journal is already active, the Change Journal is adjusted to the value of the maximum size and delta. Note that these values can only be adjusted to increase.

When starting the Change Journal, if you not specify -maxsize and -delta , or specify 0 for these parameters, the system chooses a default value based on the volume size.

As an alternative to the Data Protector cjutil command, you can also use the Windows fsutil command for administering the Change Journal.

EXAMPLES

1. To start the Change Journal with the maximum size of 8 MB (in bytes) and specify the size of 1 MB (in bytes) to be purged from the Change Journal when it reaches the specified maximum size, execute:

   ```
   cjutil -start -maxsize 8388608 -delta 1048576
   ```

SEE ALSO

omnicjutil(1M)

omniasfix

To fix the inconsistent Application Server configuration, use the Application Server reconfiguration utility located as follows.

- **Windows:** <*DP_HOME*>\bin\perl.exe <*DP_HOME*>\bin\omniasfix.pl -help
- **Linux:** /opt/omni/bin/perl /opt/omni/sbin/omniasfix.pl -help

Important: Before executing this utility, consider the effort involved in configuring any invalidated or removed configurations again.

Micro Focus recommends that you use this utility only after consulting with Micro Focus Support. Use this utility when the configuration of the Application Server is corrupt though all other configured services run without any issues. When you execute this utility, the Application Server reconfigures and results in the following:

- existing custom certificate configurations are invalidated
- existing LDAP configurations are removed
- any existing Reporting Server configurations with the Cell Manager are invalidated
- any existing Edge Service configurations with the Cell Manager are invalidated

Prerequisite

Collect the debug logs using the following command and send them to Micro Focus Support for analysis of the Application Server configuration issues during upgrade:

- **Windows:** <DP_HOME>\bin\omnidlc.exe -no_filter
- **Linux:** /opt/omni/lbin/omnidlc -no_filter
  By default, it creates the packed debugs as dlc.pck in the current working directory from which you run the omnidlc command

Synopsis

omniasfix.pl -version|-help

omniasfix.pl [-port <port>]

-port option will be useful if the Data Protector installation used non default port for Application Server.

Post configuration

1. For the Cell Manager installation having custom certificates configured for Application Server, you must reconfigure the certificates. See Configure custom certificates.
2. For the Cell Manager installation having LDAP configured, reconfigure it. See User authentication and LDAP.
3. For the Cell Manager installation configured with the Reporting Server, perform the following:
   a. Set the reporting user password using reportingutil.pl utility
      Windows: <DP_HOME>\bin\perl.exe <DP_HOME>\bin\reportingutil.pl -resetpass [-password Password]
      Linux: /opt/omni/bin/perl /opt/omni/bin/reportingutil.pl -resetpass [-password Password]
   b. Set the same password as in previous step for user in Cell Manager by running the omniusers command:
      Windows: < DP_HOME>\bin\omniusers.exe -resetpass -name WebUserName [-pass password] [-oldpass oldpassword]
      Linux: /opt/omni/bin/omniusers -resetpass -name WebUserName [-pass password] [-oldpass oldpassword]
      Note: Repeat this on all the cell managers imported into the reporting server.
   c. Using a browser access the following URL and extract the public_key information for the cell manager.
      https://<Cell Manager>:<AppServer Port>/auth/realms/DataProtector
      Example: {"realm":"DataProtector","public_key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDtpQ9y38DqpqqOKv1n60JbCDiIC7vWS19v9pHyUO97IIEOMLMLx98Oj1AV8CXH2YHvwI01vrg30Ryiy1pxSfZtLeXEgiwPLLW9TYOFYW7kw1wP4/gPtENz4PModTyUdg81NHCHjzuRKQXcFNlKkmqC1W+I22Has69dgPVMv2Tf5QIDAQAB","token-service":https://cellmanager.net:7116/auth/realms/DataProtector/protocol/openid-connect,"account-service":https://cellmanager:7116/auth/realms/DataProtector/account,"tokens-not-before":0}.
   d. Set the Cell Manager public key information on the Reporting Server using the reportingutil.pl utility
      Windows: <DP_HOME>\bin\perl.exe <DP_HOME>\bin\reportingutil.pl -updatecm -cellmanager CellManager [-realmpubkey RealmPublicKey]
      Linux: /opt/omni/bin/perl /opt/omni/bin/reportingutil.pl -updatecm -cellmanager CellManager [-realmpubkey RealmPublicKey]
   e. Copy the CA certificate from the Cell Manager from the following path and copy it to a directory in the reporting server.
      Windows: <DP_DATA>\Config\Server\certificates\ <Cell Manager>_cacert.pem
      Linux: /etc/opt/omni/server/certificates/ <Cell Manager>_cacert.pem
   f. On the reporting server run the following command to add the cell manager CA certificate into the reporting server trust store.
      Windows: <DP_HOME>\bin\perl.exe <DP_HOME>\bin\reportingutil.pl -updatecm -cellmanager CellManager [-cacert PathtoCMCACert]
      Linux: /opt/omni/bin/perl /opt/omni/bin/reportingutil.pl -updatecm -cellmanager CellManager [-cacert PathtoCMCACert]
4. For Cell Manager configured with Edge Service, do the following:
   a. Launch the Data Protector Manager and connect to the Cell Manager. In **Dashboard** > **Clients,** choose the Edge Service client and export it from cell manager.
   b. On the Edge Service client, run the following script to reconfigure the keystore and trust store:
      <DP_HOME>\bin\perl.exe <DP_HOME>\bin\esgencert.pl
   c. Using **Dashboard** > **Clients** in the Data Protector Manager, import the Edge Service client back into the Cell

Manager.

ob2install

ob2install - runs installation, removal, upgrade, or installation check of the specified Data Protector components to/from/on a remote Linux and Windows systems using the specified Installation Server
(this command is available on the Data Protector Installation Server)

SYNOPSIS

ob2install -version | -help

ob2install -server *InstallationServer* -input *Filename*

DESCRIPTION

The ob2install command can be used to remotely install, remove, upgrade, or check the installation of Data Protector components to/from/on a remote Linux and Windows systems. To run the desired operation, you need to specify a Linux or Windows Installation Server appropriate for the platform the remote system is using.

During installation, if the password is unavailable in the input file then the system prompts 3 times for the valid password. The installation stops after 3 failure attempts.

OPTIONS

-version

Displays the version of the ob2install command.

-help

Displays the usage synopsis for the ob2install command.

-server *InstallationServer*

Specifies the Installation Server used for the installation session. The Installation Server must belong to local cell.

Note: If the Cell Manager and the Installation Server are two different systems in the cell, the Cell Manager hostname must be listed on the Installation Server in the file /etc/opt/omni/client/cell_server (Linux systems), Data_Protector_program_data\Config\client\cell_server (Windows systems).

Note: If the Cell Manager and the Installation Server are two different systems in the cell, the Cell Manager hostname must be listed on the Installation Server in the file /etc/opt/omni/client/cell_server .

-input *Filename*

Specifies the input file (plain text file) containing the data for the client installation. Each client is described in the input file with a newline-separated ASCII string, using the format described below.

INPUT FILE FORMAT SYNOPSIS

-host *Hostname* - *Component* *Version* [- *Component* *Version* ...] [-encryption EncryptionFlag] -push_inst *RemoteInstallationParameters*

INPUT FILE OPTIONS

-host *Hostname*

Specifies the system to which remote installation will be performed. The *Hostname* must be enclosed in double quotes.

- *Component* *Version*

Specifies the components for the installation. The *Version* argument specifies the version of the product. Specify only the components that are supported on the target Data Protector system. The available components are:

cc – User Interface

da – Disk Agent

ndmp – NDMP Media Agent

ma – General Media Agent

sap – SAP R/3 Integration

sapdb – SAP MaxDB Integration

saphana – SAP HANA Appliance Integration

oracle8 – Oracle Integration

sybase – Sybase Integration

mysql – MySQL Integration

postgresql – PostgreSQL Integration

ssea – P9000 XP Agent

informix – Informix Integration

lotus – Lotus Integration

db2 – DB2 Integration

smisa – 3PAR SMI-S Agent

netapp – NetApp Storage Provider

vmwaregre_agent – VMware Granular Recovery Extension Agent

vepa – Virtual Environment Integration

StoreOnceSoftware – StoreOnce software deduplication

autodr – Automatic Disaster Recovery

docs – English Documentation (Guides, Help)

jpn_ls – Japanese Documentation (Guides, Help)

fra_ls – French Documentation (Guides, Help)

chs_ls – Simplified Chinese Documentation (Guides, Help)

-push_inst *RemoteInstallationParameters*

This option specifies all parameters that are crucial for a successful remote client installation. The option must be used with all its parameters.

Note: All arguments except *GeneralInstallationType* and *InstallationType* must be enclosed in double quotes (" ").

SITE SPECIFIC PATCH TEST MODULE (SSPTM) OPTIONS

- *testmodule Version* - *tm_ssp_num SSPTMNAME*

Specifies the components for SSPTM package installation. The *Version* argument specifies the version of the product. The *SSPTMNAME* argument specifies the SSPTM package name without any extension.

Note The SSPTM specific options takes precedence over the "-Component Version" options. Therefore, the "-Component Version" options are ignored when the SSPTM specific options are provided.

RemoteInstallationParameters

InstallPath

Specifies the main installation path for remote installation to Windows systems-the *Data_Protector_home* directory. The path must end with a backslash (\). For remote installation to Linux or Windows systems, for which this argument is ignored, you can use a placeholder ("-").

This argument is currently ignored. You can use a placeholder ("-").

InstallDataPath

Specifies the additional installation path for remote installation to specific Windows systems-the *Data_Protector_program_data* directory. The path must end with a backslash (\). For remote installation to Linux systems or Windows systems for which this argument is ignored, you can use a placeholder ("-").

UserName

Specifies the user name that is used by the Installation Server for remote installation. If not specified, a default value is used: `root` for Linux systems and `Administrator` for Windows systems. If not specified, the default value `root` is used. If you perform remote installation using secure shell, use a placeholder ("-").

Password

Specifies the password that is used by the Installation Server for remote installation. If not specified, the `ob2install` command prompts for it during the installation process. If you want `ob2install` to prompt for the password interactively or you perform remote installation using secure shell, use a placeholder ("-").

Note For more information on password caching functionality, refer to the *Password Caching* section in *Data Protector Installation Guide*.

CellManagerName

Specifies the name of the Cell Manager to whose cell the remote system will be added. To only install components on the remote system without adding it to a cell, use a placeholder ("-").

GeneralInstallationType

Specifies the general installation type:

`1` – currently unused value (reserved for future extensions)

`2` – client installation

InstallationType

Specifies the installation type:

`1` – new installation

`2` – update

`3` – delete

`4` – check installation

EXAMPLES

The following examples illustrate how the `ob2install` command works.

Note The latest MR release version has to be provided in the input file.

1. To start a remote installation to the Linux system "linuxsys.company.com" using the Installation Server "issys.company.com" and import the client into the cell of the Cell Manager "cmsys.company.com", use the default remote installation user name, make `ob2install` prompt for the password interactively, where the input file is named "infile.txt" and the specified components are User Interface, Disk Agent, and General Media Agent, execute the following command:

```
ob2install -server issys.company.com -input infile.txt
```

The input file "infile.txt" must contain the following line:

```
-host "linuxsys.company.com" -cc A.10.10 -da A.10.10 -ma A.10.10 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1
```

2. To start a remote installation to a supported Windows system "winsys.company.com" using theInstallation Server "issys2.company.com" and import the client into the cell of the Cell Manager "cmsys.company.com", use the user name "Administrator" and the password "q1w2e3r4", where the input file is named "infile.txt" and the specified components are P6000 / 3PAR SMI-S Agent, Automatic Disaster Recovery, and French Documentation (Guides, Help), execute the following command:

   ```
   ob2install -server issys2.company.com -input infile.txt
   ```

   The input file "infile.txt" must contain the following line:

   ```
   -host "winsys.company.com" -smisa A.10.10 -autodr A.10.10 -fra_ls A.10.10 -push_inst "-" "-" "Administrator" "q1w2e3r4" "cmsys.company.com" 2 1
   ```

3. To start a remote installation to the Linux system "linuxsys.company.com" using theInstallation Server "issys.company.com" and import the client into the cell of the Cell Manager "cmsys.company.com", use the default remote installation user name, password as specified in the NOTE, where the input file is named "infile.txt" and the specified SSPTM package is "QXCMUX0001", execute the following command:

   ```
   ob2install -server issys.company.com -input infile.txt
   ```

   The input file "infile.txt" must contain the following line:

   ```
   -host "linuxsys.company.com" -testmodule A.09.00 -tm_ssp_num QXCMUX0001 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1
   ```

   > **Note** You need not specify the password while installing SSPTM modules as Data Protector is already installed on your system. However, in case of connectivity issues to the remote host, the ob2install prompt interactively requests for a new password (if required).

4. To start remote installation on windows hosts, winsys1.company.com, winsys2.company.com, winsys3.company.com and winsys4.company.com, using the Installation Server "issys2.company.com" and import the client into the cell of the Cell Manager "cmsys.company.com", where the input file is named "infile.txt" and the specified components are P6000 / 3PAR SMI-S Agent, Automatic Disaster Recovery, and French Documentation (Guides, Help), execute the following command:

   ```
   ob2install -server issys2.company.com -input infile.txt
   ```

   The input file "infile.txt" must contain the following line:

   ```
   -host "winsys1.company.com" -smisa A.10.10 -autodr A.10.10 -fra_ls A.10.10 -push_inst "-" “-“ "Administrator" "q1w2e3r4" "cmsys.company.com" 2 1

   -host "winsys2.company.com" -smisa A.10.10 -autodr A.10.10 -fra_ls A.10.10 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1

   -host "winsys3.company.com" -smisa A.10.10 -autodr A.10.10 -fra_ls A.10.10 -push_inst "-" "-" "Administrator" "w1q2e3r4" "cmsys.company.com" 2 1

   -host "winsys4.company.com" -smisa A.10.10 -autodr A.10.10 -fra_ls A.10.10 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1
   ```

   Since password is not provided for host winsys2.company.com, previous client credentials in which push installation was successful will be used. In the above example host credentials used for winsys1.company.com, will be used for host winsys2.company.com also. In case host winsys2.company.com has different credentials than winsys.company.com, user will be prompted to enter the new credentials. This newly entered credentials will be used for clients, for which credentials are not provided in input file.

   For host winsys4.company.com, credentials provided for winsys3.company.com will be used.

5. To start remote installation on Linux hosts, unsys1.company.com, unsys2.company.com, unsys3.company.com and unsys4.company.com, using the Installation Server "issys2.company.com" and import the client into the cell of the Cell Manager "cmsys.company.com", where the input file is named "infile.txt" and the specified components are P6000 / 3PAR SMI-S Agent, Automatic Disaster Recovery, and French Documentation (Guides, Help), execute the following command:

   ```
   ob2install -server issys2.company.com -input infile.txt
   ```

   The input file "infile.txt" must contain the following line:

   ```
   -host "unsys1.company.com" -smisa A.10.00 -autodr A.10.00 -fra A.10.00 -push_inst "-" “-“ "root" "q1w2e3r4" "cmsys.company.com" 2 1

   -host "unsys2.company.com" -smisa A.10.10 -autodr A.10.10 -fra A.10.10 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1

   -host "unsys3.company.com" -smisa A.10.00 -autodr A.10.00 -fra A.10.00 -push_inst "-" “-“ "-" "-" "cmsys.company.com" 2 1

   -host "unsys4.company.com" -smisa A.10.10 -autodr A.10.10 -fra A.10.10 -push_inst "-" "-" "-" "-" "cmsys.company.com" 2 1
   ```

   Since password is not provided for host uxsys2.company.com, previous client credentials in which push installation was successful will be used. In the above example host credentials used for uxsys1.company.com, will be used for host

uxsys2.company.com also. In case host uxsys2.company.com has different credentials than uxsys1.company.com, user will be prompted to enter the new credentials. This newly entered credentials will be used for clients, for which credentials are not provided in input file.

For host uxsys3.company.com and uxsys4.company.com, credentials provided for uxsys1.company.com will be used.

omnib2dinfo

omnib2dinfo - displays information about CatalystStore and StoreOnce Software stores
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

omnib2dinfo -help | -h

omnib2dinfo -version | -v

omnib2dinfo -store_info -b2ddevice *libraryname*

omnib2dinfo -list_stores -b2ddevice *libraryname*

omnib2dinfo -list_objects -b2ddevice *libraryname* [-metadata] [-tags] [-modified_since="dd.mm.yyyy hh:mm:ss" in UTC]

omnib2dinfo -get_server_properties -b2ddevice *libraryname*

omnib2dinfo -delete_object -b2ddevice *libraryname* -object_key *mediumID*

DESCRIPTION

This command displays information about an ObjectStore or StoreOnce Software store – store details, list of stores and associated team members (for teamed stores), objects within the store, and details about the store host.

OPTIONS

-version

Displays the version of the omnib2dinfo command.

-help

Displays the usage synopsis for the omnib2dinfo command.

-store_info

Displays detailed information about the store specified in the device configuration, such as the store name, description, and status, as well as size of the stored data, the actual size of the store, the deduplication ratio, and backup and store size quota (if set). Unlike -list_stores , this option lists only the store associated with the device, not other stores residing on the same system.

-list_stores

Lists all stores that reside on the same system as the store to which the specified device points to. For example, if store str1 is configured for device dev1 and store str2 for device dev2 and both reside on the same system, both stores are listed regardless if you specify device dev1 or dev2 . Store str3 which is configured for dev3 but resides on a different system is not listed.

Additional details are displayed for each store such as the store name, description, status (online, offline), whether encrypted (Yes, No), whether teamed (Yes, No), list of team members (for teamed stores) and their status (ON, OFF), the user data stored, the store data size, and the deduplication ratio.

-list_objects

Lists details about objects in the store specified in the device configuration, such as the object key, creation date, last modified date, and the size of the object on the disk.

In addition, it displays details such as:

- metadata : Includes common section, format version, the Catalyst library version, name of the backup product, version of the backup product, OS information (Gateway OS), product-specific section, host name of Cell Manager, gateway name, and the deduplication mode (server/target).
- tags : Includes specification list, session type, backup type, and session ID.
- modified since : Retrieves objects modified on or after the specified date, which is defined in UTC.

-get_server_properties

Displays the server properties such as the hostname, B2D version, the B2D serial number, disk size, and the free space on the disk.

-b2ddevice *DeviceName*

Specifies the B2D device for which the information is displayed.

-delete_object

Deletes the specified object from the specified store.

EXAMPLES

1. To list all StoreOnce Software stores that reside on the same system as the store to which the device “StoreDev8” points to, execute:

   omnib2dinfo -list_stores -b2ddevice StoreDev8

2. To list only the StoreOnce Software stores for the device “StoreDev8”, execute:

   omnib2dinfo -store_info -b2ddevice StoreDev8

3. To list details about all objects in the store for the device “StoreDev45”, execute:

   omnib2dinfo -list_objects -b2device StoreDev45

SEE ALSO

omniamo(1), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnicellnamechange.pl

The omnicellnamechange.pl utility is developed as a script and gets installed along with the Cell Manager installation kit.

The omnicellnamechange.pl script exists in the following location:

Windows: %DP_HOME_DIR%\bin Unix: /opt/omni/sbin

If required, the Data Protector administrators can run this utility when required to change the Cell Manager name.

> **Note** The omnicellnamechange.pl utility can be run only by the user with administrative privileges.

Synopsis

You can run the omnicellnamechange.pl utility using the following syntax and options:

The omnicellnamechange.pl script exists in the following location:

Windows: %DP_HOME_DIR%\bin

UNIX: /opt/omni/sbin

You can run the omnicellnamechange.pl utility using the following syntax and options:

- omnicellnamechange.pl --help | -h
- omnicellnamechange.pl --newcmhost <*new_cm_name*>

Description

The omnicellnamechange.pl utility helps in the following tasks:

- Replace new Cell Manager name in Data Protector configuration files
- Regenerate certificates
- Configure Cell Manager name in IDB
- Run user migration

Options

The omnicellnamechange.pl utility supports the following option:

- --newcmhost

Specifies the name of the new Cell Manager.

Examples

The following section lists sample commands for running the omnicellnamechange.pl utility on Windows and UNIX.

- **Windows**: %Data_Protector_home%\bin\perl.exe omnicellnamechange.pl --newcmhost <*new_cm_name*>
- **UNIX**: /opt/omni/bin/perl omnicellnamechange.pl --newcmhost <*new_cm_name*>

omnicheck

omnicheck - performs a DNS connections check within a Data Protector cell and lists Data Protector patches installed on Data Protector clients
(this command is available on systems with any Data Protector component installed)

SYNOPSIS

omnicheck -version | -help

omnicheck -dns [-host *Client* | -full] [-verbose]

omnicheck -patches -host *Client*

omnicheck -ssphf -host *Client*

DESCRIPTION

The following tasks can be performed using the omnicheck command:

CHECKING DNS CONNECTIONS WITHIN A Data Protector CELL

To check DNS connections within a Data Protector cell, use the -dns option with the omnicheck command.

The omnicheck command does not verify DNS connections in general. It verifies that DNS information matches over all communications relevant for Data Protector among Data Protector cell members. The command reports only failed checks and the total number of failed checks unless the -verbose option is specified.

It is possible to verify the following DNS connections in the Data Protector cell, using the omnicheck command:

- To check that the Cell Manager and every Media Agent resolve DNS connections to every Data Protector client in the same cell properly and the other way round, use the -dns option.
- To check that a particular Data Protector client resolves DNS connections to every Data Protector client in the same cell properly and the other way round, use the -host option.
- To check all possible DNS connections in the cell, when every client resolves DNS connections to all other clients in the same cell, use the -full option.

LISTING PATCHES INSTALLED ON Data Protector CLIENTS

The omnicheck command can be used to list Data Protector patches installed on a particular client. The omnicheck option used to list Data Protector patches installed on a particular client is -patches.

LISTING SITE SPECIFIC PATCHES OR HOT FIXES INSTALLED ON Data Protector CLIENTS

The omnicheck command can be used to list Data Protector Site Specific Patches (SSPs) or Hot Fixes (HFs) installed on a particular client. The omnicheck option used to list Data Protector SSPs or HFs installed on a particular client is -ssphf.

OPTIONS

-version

Displays the version of the omnicheck command.

-help

Displays the usage synopsis for the omnicheck command.

-dns

Checks that the Cell Manager and every Media Agent resolve DNS connections to every Data Protector client in the same cell properly and the other way round. This option performs the same as running the omnicheck -dns -host CellManager and omnicheck -dns-host MediaAgent1... omnicheck -dns -host MediaAgentN commands.

-dns -host *Client*

Checks that a Data Protector client specified by the -host option resolves DNS connections to every Data Protector client in the same cell properly and the other way round.

-dns -full

Checks all possible DNS connections in the cell. Every client in the cell tries to resolve all other clients in the same cell.

-verbose

Returns all the messages when using the -dns option. If this option is not set (default), only the messages that are the result of failed checks are returned.

-patches -host *Client*

Returns Data Protector patches (patch level, patch description and number of all patches installed) installed on a Data Protector client specified by the -host option. To use this option, you need the Client configuration user right (by default only users in the admin user group).

-ssphf -host *Client*

Returns Data Protector Site Specific Patches or Hot Fixes (Site Specific Patch (SSP) or Hot Fixes (HF) name, status, and number of SSPs or HFs installed) installed on a Data Protector client specified by the -host option. To use this option, you need the Client configuration user right (by default only users in the admin user group).

RETURN VALUES

See the man page omniintro for return values.

Additional return values of the omnicheck command used to check the DNS connections are:

client_1 cannot connect to *client_2*

client_1 connects to *client_2*, but connected system presents itself as *client_3*

client_1 failed to connect to *client_2*

checking connection between client_1 and *client_2*

all checks completed successfully.

number_of_failed_checks checks failed.

client is not a member of the cell.

client contacted, but is apparently an older version. Hostname is not checked.

Additional return values of the omnicheck command used to list the Data Protector patches are:

List of patches found on host client

Patch level Patch description

Number of patches found: number_of_patches

List of patches on host client is not available.

Host client is not a member of this cell.

Host client is unreachable.

Additional return values of the omnicheck command used to list the Data Protector SSPs or HFs are:

List of SSPs/HFs found on host client

Site Specific Patch or Hot Fix status

Number of SSPs and HFs found: number_of_patches

List of SSPs/HFs on host client is not available.

Host client is not a member of this cell.

Host client is unreachable.

NOTES

The omnicheck command can be used only within one Data Protector cell.

EXAMPLES

1. To check DNS connections needed for normal Data Protector operating (the Cell Manager and every Media Agent in the cell resolve DNS connections to every Data Protector client in the cell properly and the other way round), execute:

   omnicheck -dns

2. To check if the client with the hostname backup.system.com resolves DNS connections to every Data Protector client in the same cell properly and the other way round, and to get all relevant messages, execute:

   omnicheck -dns -host backup.system.com -verbose

3. To list the patches installed on client with the hostname backup.system.com, execute:

   omnicheck -patches -host backup.system.com

4. To list the SSPs/HFs installed on client with the hostname backup1.system.com, execute:

   omnicheck -ssphf -host backup1.system.com

SEE ALSO

omnicc(1), omnicellinfo(1), omnidlc(1M), omnisv(1M)

omnicjutil

omnicjutil - starts, stops, and queries the Windows Change Journal on Windows clients
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnicjutil -help

omnicjutil -version

omnicjutil -file *filename*

omnicjutil -host *hostname* -volume *vol* { -start [-maxsize *max* -delta *del*] | -stop [-wait] | -query }

DESCRIPTION

The omnicjutil command is used to remotely control and administer the Change Journal on Windows clients.

OPTIONS

-help

Displays the usage synopsis of the omnicjutil command.

-version

Displays the version for the omnicjutil command

-file *filename*

Defines the file containing multiple single line entries of this command. Each line must conform to the usage of the omnicjutil command. Note that no tabs are allowed. If a syntax error is found, none of the commands is executed.

-host *hostname*

Defines the name of the system hosting the Change Journal.

-volume *vol*

Defines the volume name in the form /C or /C:\mounted_folder.

-start [-maxsize *max* -delta *del*]

Starts the Change Journal on the specified volume.

The -maxsize max option sets the maximum size of the Change Journal in bytes. The highest possible value is 4 GB (4 294 967 296 bytes). Any specified value greater than 4 GB will be rounded down to 4 GB. Note that a reasonable size for a 100 GB drive is an 85 MB Change Journal.

The -delta *del* option specifies the size in bytes to be purged from the Change Journal when it reaches its maximum size. recommends the value be approximately one-eighth to one-quarter the value of the maximum size but not greater than one quarter the size of the maximum size. This value may be automatically adjusted to better correspond to the volume cluster size.

-stop

Stops the Change Journal asynchronously.

The -wait specifies that the Change Journal will be stopped synchronously. The call returns only after the Change Journal has been deleted.

-query

Queries the status of the Change Journal.

NOTES

If the -start option is specified and the Change Journal is already active, the Change Journal is adjusted to the value of the maximum size and delta. Note that these values can only be adjusted to increase.

When starting the Change Journal, if you not specify -maxsize and -delta, or specify 0 for these parameters, the system chooses a default value based on the volume size.

The command line tool gets the input either directly from the command line or from a file. Using input directly from the command line allows only one operation at a time. To perform more than one operation, create a file using the -file *filename* option and use it as an input. Note that the commands in the file are executed from top to bottom.

As an alternative to the Data Protector omnicjutil command, you can also use the Windows fsutil command for administering the Change Journal.

EXAMPLES

To start the Change Journal with the maximum size of 8 MB (in bytes) and specify the size of 1 MB (in bytes) to be purged from the Change Journal when it reaches the specified maximum size, execute:

```
cjutil -start -maxsize 8388608 -delta 1048576
```

SEE ALSO

cjutil(1M)

omnidbcheck

omnidbcheck - checks the consistency of the Data Protector Internal Database (IDB)
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnidbcheck -version | -help

omnidbcheck [-quick | -extended]

omnidbcheck -sibf [-detail | -dumpmedia] [-summary]

omnidbcheck -smbf [-detail | -dumpmessages] [-summary]

omnidbcheck -keystore [-summary]

omnidbcheck -verify_db_files [-detail]

omnidbcheck -connection [-detail]

omnidbcheck -media_consistency [-detail]

omnidbcheck -schema_consistency [-detail]

omnidbcheck -database_consistency [-detail]

omnidbcheck -bf [-summary]

omnidbcheck -dc [-quick] [-media <list>] [-detail [-detail]] [-summary]

DESCRIPTION

The Data Protector Internal Database (IDB) consists of Media Management Database (MMDB), Catalog Database (CDB), Detail Catalog Binary Files (DCBF), and Session Messages Binary Files (SMBF). The MMDB and CDB objects, object versions and media positions form the core part of the IDB. The DCBF and SMBF form the detail part of the IDB.

The omnidbcheck command checks the status of the IDB or parts of the IDB and sends a report to the standard output.

Note that errors found during the database connection check and encryption keystore check are Critical, errors found during the schema check, database check, media check, and datafiles check are Major, errors found during the Detail Catalog check or binary files check are Minor, and errors found during the SMBF check are Warning.

Data Protector creates a log file for each part of the check on the Cell Manager in the default server log files directory:

Check_smbf.txt

Check_bf.txt

Check_dc.txt

There is a timestamp at the beginning of each log file stating when the check was performed.

OPTIONS

-version

Displays the version of the omnidbcheck command.

-help

Displays the usage synopsis for the omnidbcheck command.

-quick

Checks the database connection, schema consistency, data files consistency, presence and size of the DCBF part of the IDB, and displays the summary of the check.

-extended

Checks the entire IDB with the exception of the SMBF and displays the summary of the check.

-sibf

This option relates to the functionality that is no longer supported in the installed Data Protector version.

If the -detail option is specified, it lists all SIBF and their status (OK or corrupted/missing). If the -detail option is not specified (default), only the corrupted SIBF and their status (corrupted or missing) are listed.

If the -dumpmedia option is specified with the -sibf option, it sends the SIBF filenames, object versions information, offset of the data in the SIBF file belonging to an object version as well as size of the data in the SIBF file belonging to an object version to the standard output.

If the -summary option is specified, the command sums up the data and displays the status of the SIBF.

-summary

Displays only the summary of the check (OK or failed/missing). The option does not impact the thoroughness of the check except for omnidbcheck -dc, where -summary implies a -dc -quick check.

-smbf

Checks the presence of the SMBF.

Note that if you have removed a SMBF in any way (for example, using Data Protector GUI or CLI or deleted the file manually), then this option reports the removed session message as missing. This does not mean that IDB is corrupted-it only indicates that a session has been removed.

If the -detail option is specified, it lists all SMBF and their status (OK or corrupted/missing). If the -detail option is not specified (default), only the SMBF and their status (corrupted or missing) are listed.

If the -dumpmessages option is specified with the -smbf option, it sends the session messages in the SMBF to the standard output.

If the -summary option is specified, the command sums up the data and displays the SMBF.

-keystore

Performs a consistency check of the Data Protector's keymap index file and the encryption keys in the keystore. The following information is listed for each encryption key in the cell: key ID, store ID, KeyStore name, KeyFile name, and a result of the check (OK or corrupted).

If the -summary option is specified, the command sums up the data and displays the status of the keystore.

-verify_db_files

Checks for the existence of database datafiles.

If the -detail option is specified, the command lists missing datafiles in case of a datafiles consistency failure.

-connection

Checks the status of Data Protector database connectivity.

If the -detail option is specified, the command lists errors in case of a connection failure.

-media_consistency

Checks the consistency of media.

If the -detail option is specified, the command lists inconsistent media names in case of a media consistency failure.

-schema_consistency

Checks the consistency of schema and detects changes in the schema since its first creation during the Data Protector installation.

If the -detail option is specified, the command lists the difference between the original and current schema in case of a schema consistency failure.

-database_consistency

Checks the database consistency.

If the -force option is specified, it overrides the default safety check. With this option, there is no confirmation request for the check of database consistency. If the -force option is not specified, the command displays a confirmation request for the check of database consistency.

If the -detail option is specified, the command lists errors in case of a database consistency failure.

-bf

Performs a presence and size check of the DCBF.

If the -summary option is specified, the command sums up the data and displays the binary files.

-dc

Checks consistency between the core and DC part of the database.

If -detail option is specified once, the check lists all encountered errors. Without -detail option, it only displays the summarized error information. With -detail option specified twice, the check lists statuses of all checked items regardless of error (maximum verbosity).

If -quick option is specified, the check only checks the most recently completed segments for each DC binary file.

If -media <list> is specified, the check only checks DCBFs corresponding to the media matching the specified IDs in the list.

If -summary mode is specified, only summary is written to the console in -extended format, while the full output (depending on the specified options) is still written to the Check_dc.txt . In -summary mode, -quick option is implied.

EXAMPLES

1. To perform an extended check of the IDB, execute:

   omnidbcheck -extended

2. To perform a consistency check of the Data Protector's keymap index file and the encryption keys in the keystore, execute:

   omnidbcheck -keystore

3. To list all missing datafiles in case of a consistency failure, execute:

   omnidbcheck -verify_db_files -detail

4. To list all media with inconsistent names in case of a media consistency failure, execute:

   omnidbcheck -media_consistency -detail

SEE ALSO

omnidb(1), omnidbinit(1M), omnidbp4000(1), omnidbsmis(1), omnidbutil(1M), omnidbvss(1), omnidbxp(1), omnidbzdb(1),

omniofflr(1M)

omnidbinit

omnidbinit - initializes the Data Protector Internal Database (IDB)
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnidbinit -version | -help

omnidbinit [-force]

DESCRIPTION

The omnidbinit command initializes the Data Protector Internal Database (IDB). All information about sessions, media, and objects is lost after the initialization. The command does not delete the IDB archived log files but creates a gap in the sequence of them; when a rollforward operation is performed using the omnioffl r command, the operation applies only the archived log files logs created before the initialization of the IDB.

In order to initialize the IDB successfully, the underlying structure of the embedded database has to exist at the Data Protector Internal Database location in the pg directory. Note that the actual location of the pg directory may not be the default one, if you have restored the IDB to some other location and registered the restored instance as the new IDB.

Make sure that the Data Protector Internal Database Service (hpdp-idb) is running and the connection to the current IDB is available. Verify it with the omnisv -status command. Any error found during omnidbinit execution is reported.

OPTIONS

-version

Displays the version of the omnidbinit command

-help

Displays the usage synopsis for the omnidbinit command

-force

Overrides the default safety check for the initialization. By default, the command displays a confirmation request. With this option, there is no confirmation request.

Note This command also deletes templates from the IDB. To get the templates on Web based scheduler, execute the following command: omnidbutil -migrate_schedules -only_advsch

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbp4000(1), omnidbsmis(1), omnidbutil(1M), omnidbvss(1), omnidbxp(1), omnidbzdb(1), omnioffl r(1M)

omnidbutil

omnidbutil - handles various Data Protector Internal Database (IDB) maintenance tasks.
(This command is available on the Data Protector Cell Manager.)

SYNOPSIS

omnidbutil -version | -help

omnidbutil -readdb *Directory* [-jce] [-detail]

omnidbutil -writedb *Directory* [-jce]

omnidbutil -show_locked_devs [-all]

omnidbutil -free_locked_devs

[-all | *DevName* | *MediumID* | *CartName* *PhyLocation* | *Serial_LDEV* | *WWW_LUN*]

omnidbutil -changebdev *FromDev ToDev* [-session *SessionID*]

omnidbutil -purge { -sessions [*NumberOfDays*] | -days

[*NumberOfDays*] | -messages [*NumberOfDays*] | -daily | -dcbf }

omnidbutil -purge_failed_copies

omnidbutil -clear

omnidbutil -change_cell_name [*OldHost*]

omnidbutil -show_cell_name

omnidbutil -set_session_counter *NewSessionID*

omnidbutil -show_db_files

omnidbutil -free_pool_update

omnidbutil -list_large_mpos *MinNumberOfMpos* [-top *NumOfTopMedia*]

[-detail] [-csv *CSVFile*]

omnidbutil -free_cell_resources

omnidbutil -mergemmdb *CellManagerHostname*

omnidbutil -cdbsync *CellManagerHostname*

omnidbutil -info

omnidbutil -autovacuum { -set -table *TableName* [-to_default]

[-on_n_rows *NRows*] [-on_percentage *Percent*]

[-freeze_max_age *FreezeMax*] | -get

[-table *TableName* | -enabled | -disabled | -all]}

omnidbutil -list_dcdirs

omnidbutil -add_dcdir *PathName* [-maxsize *MaxSizeInMB*]

[-maxfiles *NumberOfFiles*] [-spacelow *SpaceLowInMB*] [-seq *SeqNumber*]

omnidbutil -modify_dcdir *PathName* [-maxsize *MaxSizeInMB*]

[-maxfiles *NumberOfFiles*] [-spacelow *SpaceLowInMB*] [-seq *SeqNumber*]

omnidbutil -remove_dcdir *PathName*

omnidbutil -remap_dcdir

omnidbutil -fixmpos

omnidbutil -cp { -set *ParamName ParamValue* | -get [-param *ParamName*]}

omnidbutil -set_passwd *UserName*

omnidbutil -set_passwd java -pass *PreferredPassword*

omnidbutil -sync_srv

omnidbutil -config_cell_name *NewCellManagerHostname*

omnidbutil -delete_obsolete_resumed_versions [-session *SessionID*]

omnidbutil -export_schedules {-all [–location <path>] | -spectype *SpecificationType* }

-apptype [ApplicationType] -specname *SpecificationName* [–location <path>]

omnidbutil -import_schedules {-all [–location <path>] | -spectype SpecificationType}

-apptype [ApplicationType] -specname *SpecificationName* [–location <path>]

omnidbutil -create_schedule {-spectype *SpecificationType*

-apptype [ApplicationType] -specname *SpecificationName*

-dpName <DpName> -dpType <*DpType*>

-recurrenceType <*RecurrenceType*> -startDate <*YYYY-MM-DD*>

-startTime <StartTime> -everyNth <EveryNth> [-endDate <*YYYY-MM-DD*>]

[-endTime <*EndTime*>] [-fromTime <*FromTime*>] [-toTime <*ToTime*>]

[-dayOfMonth <*DayOfMonth*>] [-daysOfWeek <*DaysOfWeek*>]

[-nthDayOfWeekInMonth <*NthDayOfWeekInMonth*>]

[-disabled <*true|false*>] [-dpLoad <*low|medium|high*>] [-dpPriority <*dpPriority*>]

[-pauseLowerPriorityJobDisabled <*true|false*>]

[-holidaysEnabled <*true|false*>] [-dpProtection <*Default|None|Until|Days|Weeks|Permanent*>]

[-dpProtectionParam <*DpProtectionParam*>]

[-enabled_debug <enabled_debug>] [-filename <filename>] [-range <range>]}

omnidbutil -list_schedules {-spectype *SpecificationType*}

-apptype [ApplicationType] -specname *SpecificationName*

omnidbutil -modify_schedule { -scheduleId <*ScheduleId*> [-dpName <*DpName*>]

[-dpType <*DpType*>] [-recurrenceType <*RecurrenceType*>]

[-startDate <*StartDate*>] [-startTime <*StartTime*>] [-everyNth <*EveryNth*>]

[-endDate <*EndDate*>] [-endTime <*EndTime*>] [-fromTime <*FromTime*>] [-toTime <*ToTime*>]

[-dayOfMonth <*DayOfMonth*>] [-daysOfWeek <*DaysOfWeek*>]

[-nthDayOfWeekInMonth <*NthDayOfWeekInMonth*>]

[-disabled <*Disabled*>] [-dpLoad <*DpLoad*>] [-dpPriority <*DpPriority*>]

[-pauseLowerPriorityJobDisabled <*PauseLowerPriorityJobDisabled*>]

[-holidaysEnabled <*HolidaysEnabled*>] [-dpProtection <*DpProtection*>]

[-dpProtectionParam <*DpProtectionParam*>] [-debug_filename <*FileName*>

[-enabled_debug <enabled_debug>] [-filename <filename>] [-range <range>]}

omnidbutil -delete_schedule <*ScheduleId*>

omnidbutil -migrate_schedules

omnidbutil -reinstate_legacy_schedules { [-force] }

omnidbutil - encrypt_array_cred

omnidbutil - encrypt_idb_pass

omnidbutil - encrypt_user_pass

omnidbutil - encrypt_dedupe_pass

omnidbutil - encrypt_integ_files

omnidbutil - app_client_pass

OTHER OPTIONS

spectype = { backup | copy | consolidation | reporting, mediacopy | verification }

apptype = { Lotus | Oracle8 | Mailbox | MSSQL | SAPDB | MSVSSW | Sybase | SAP | MSESE | VMware | E2010 | mssharepoint| VEAgent | IDB | db2 | hana | Informix | Stream | MySQL| PostgreSQL}

recurrenceType = { ONCE | EVERYMINUTE | HOURLY | DAILY | WEEKLY | MONTHLY }

DESCRIPTION

The omnidbutil command is used for Data Protector Internal Database (IDB) maintenance tasks. These tasks involve:

OPERATIONS ON DETAIL CATALOG BINARY FILES (DCBF)

The Detail Catalog part of the IDB is composed of two parts: 1) The Detail Catalog (DC) binary files, which stores pathnames of the backed up files and directories, together with client system names, and version information (size, modification time, attributes/protection, exact position on a medium (segment and block offset within a segment) of a backed up file or directory, and so on). 2) DC directories: registered directories that contain DC binary files. A DC directory is allocated when creating a new DC binary file using one of three possible allocation algorithms, specified by the DCDirAllocation global option.

Operations on DCBF include: 1) Registering, removing, and updating DC directories. 2) Locating DCBF across DC directories if they had been manually moved. 3) Removing invalid references to DC binary files. Invalid references may occur after an IDB recovery during which the replay of the archived logs is executed. In that case, CDB is newer than DCBF.

The omnidbutil options used for operations on DC are: -list_dcdirs , -add_dcdir , -modify_dcdir , -remove_dcdir , -remap_dcdir , and -fixmpos .

EXPORTING AND RE-CREATING THE CONTENTS OF THE MEDIA MANAGEMENT DATABASE (MMDB) AND CATALOG DATABASE (CDB)

The contents of MMDB and CDB can be exported and imported back. Data Protector uses the PostgreSQL pg_dump command to create files in the UTF-8 format for this purpose.

The omnidbutil options used for exporting and recreating the contents of MMDB and CDB are: -readdb and -writedb .

LISTING AND UNLOCKING BACKUP DEVICES, TARGET VOLUMES, MEDIA, AND LIBRARY SLOTS

Backup devices, target volumes, backup media, and library slots in use are locked during Data Protector sessions. In certain situations (backup or restore sessions end abnormally) devices remain locked, even though the Data Protector Media Agent or a Data Protector disk array integration agent is no longer running. By default, such devices are automatically unlocked after 60 minutes.

The omnidbutil options used for listing and unlocking backup devices, target volumes, backup media, and library slots are: -show_locked_devs and -free_locked_devs .

MERGING LOCAL MMDBS INTO A CENTRALIZED MMDB (CMMDB)

In large multicell environments with high-end backup devices, you may want to share these devices and media among several cells. This can be achieved by having one centralized MMDB (CMMDB) for all the cells and keeping an individual CDB for each cell. This allows backup media and backup device sharing while preserving the security capabilities of the multicell structure. To achieve this, merge the local MMDBs into the CMMDB.

The omnidbutil option used for merging MMDB into CMMDB is -mergemmdb .

SYNCHRONIZING CDB AND MMDB

In certain situations, the CDB and MMDB may be out of sync (the CDB and MMDB were imported from files generated in separate export sessions, the CMMDB was restored while leaving local CDB intact, and so on). In such cases, synchronize both databases.

The omnidbutil option used for synchronizing CDB and MMDB is -cdbsync .

MISCELLANEOUS TASKS

These tasks involve operations such as displaying the information about the IDB and the IDB upgrade process, updating backup device references in object versions, changing ownership of the CDB to the current Cell Manager, displaying the actual CDB ownership, reclaiming free disk space, setting parameters for the connection pool configuration file, changing the password for a configured user account, changing the password for Data Protector Web reporting, and more.

The omnidbutil options used for this group of tasks are: -changebdev , -purge , -clear , -change_cell_name , -show_cell_name , -set_session_counter , -show_db_files , -free_pool_update , -list_large_mpos , -top , -csv , -free_cell_resources , -info , -autovacuum , -cp , -set_pasw , -set_passwd java -pass , and -sync_srv .

The -purge_failed_copies option needs exclusive access to the IDB. Before you use it, make sure that no backup, restore, or

media management sessions are in progress and that no graphical user interfaces are launched in the cell.

The omnidbutil -telemetry option is scheduled daily to collect the telemetry data at 02:00 (HH:MM) as a part of theData Protector check mechanism. The schedule value can be changed by changing the DailyTelemetryTime global option file.

OPTIONS

-version

Displays the version of the omnidbutil command.

-help

Displays the usage synopsis for the omnidbutil command.

-readdb *Directory* [-jce] [-detail]

Reads and restores the IDB data from the Directory previously written using the omnidbutil -writedb command. Note that the -readdb command does not restore DCBFs or SMBFs but leaves the old files in place. You may need to backup and restore these manually using the paths listed by the -writedb command.

-writedb *Directory* [-jce]

Writes the IDB data (without the DCBF and SMBF directories) to the specified Directory . The command lists all the DCBF and SMBF directory paths that need to be manually backed up, if needed for a restore later on. Note that the commands -writedb and -readdb are not a substitute for the IDB backup.

-jce is an optional parameter that is used to import and export the JCE database from the IDB.

-show_locked_devs [-all]

Lists all locked devices, target volumes, media, and slots in the Data Protector cell.

The -all option applies only when you execute the command on the MoM system, in which case locked devices, target volumes, media, and slots from all cells are listed.

-free_locked_devs [-all | *DevName* | *MediumID* | *CartName* *PhyLocation* | *Serial_LDEV* | *WWN_LUN*]

Unlocks a specified device, target volume, medium, or slot, where *DevName* is the device, *MediumID* is the medium, *CartName* is the library name, *PhyLocation* is the number of the slot to be unlocked, *Serial_LDEV* is the target volume where *Serial* is the serial number of a disk array of the P9000 XP Disk Array Family and *LDEV* is the P9000 XP Disk Array Family volume number, *WWN_LUN* is the target volume where *WWN* is the world-wide-name of a disk array and *LUN* is the logical unit number (LUN). If none of the above is specified, all devices, target volumes, media, and slots in the Data Protector cell are unlocked.

The -all option applies only when you execute the command on the MoM system, in which case all devices, target volumes, media, and slots from all cells are unlocked.

-changebdev *FromDev* *ToDev* [-session *SessionID*]

Changes all references in object versions from device *FromDev* to device *ToDev*. You can change the device name only for a single session by using the -session option.

-purge { -sessions [*NumberOfDays*] | -days [*NumberOfDays*] | -messages [*NumberOfDays*] | -daily | -dcbf }

This option allows you to remove obsolete backup, restore, and media management sessions, session messages, and obsolete DC binary files from the IDB.

The -sessions option removes media management sessions, restore sessions, and obsolete backup sessions (backup sessions without backed up data) older than *NumberOfDays*.

The -days option removes media management sessions, restore sessions, obsolete backup sessions (backup sessions without backed up data), and session messages for all sessions older than *NumberOfDays*.

The -messages option removes session messages for all sessions older than *NumberOfDays*.

The -daily option starts the same purge session as started every day at 12:00 (depending on the Data Protector global option setting) and is a part of Data Protector daily maintenance tasks. This purge session deletes DCBF based on the

catalog protection and removes obsolete sessions and their messages, by running the omnidbutil -purge -sessions KeepObsoletSessions -messages KeepMessages -dcbf command, where *KeepObsoleteSessions* and *KeepMessages* are specified in the Data Protector global options. Default values for these two parameters are 30 and 0, respectively.

The scheduled time at which the -daily option is started every day is defined by the DailyMaintenanceTime global option.

The -dcbf option removes the DC binary file of each media with expired catalog protection.

Specify at least one of these options. You can change or disable the global option DailyMaintenanceTime for the -daily option.

-purge_failed_copies

In certain circumstances the Data Protector IDB may hold multiple copies of objects made during a backup. Use this option to remove all unrequired copies that may overload an IDB. This option requires exclusive access to the database.

-clear

Sets the status of all sessions that are actually not running but are marked *In Progress/Failed*, to *Failed*. It requires exclusive database access to ensure that no session is running.

-change_cell_name [*OldHost*]

This option changes the owner of the CDB to the current Cell Manager. It also changes all references in the CMMDB from *OldHost* to the current Cell Manager. It modifies all media entries within the MMDB or CMMDB associated with the original Cell Manager (old host).

If the *OldHost* parameter is not specified, omnidbutil determines the previous owner of the CDB (old host) from the database itself.

If you want to associate all media in a CMMDB with the current Cell Manager, it is necessary to execute the command once for each Cell Manager that has media associated with it, using the *OldHost* parameter.

Specify the *OldHost* parameter exactly the same as the owner of the media. If the system's Fully Qualified Domain Name (FQDN) is associated with the media, also use the FQDN with this command. If the *OldHost* parameter is not specified correctly, the operation will not be performed.

This command is used after moving databases from one Cell Manager to another or after using -readdb on files that were created on another Cell Manager.

-show_cell_name

Queries the CDB for its owner. If there is no information available, use the -change_cell_name option to update the information.

-set_session_counter *NewSessionID*

Sets a new value for the counter that is used for generating the sessionID. This option is used after the restore and recovery of the IDB to enable the import of tapes that were created on the same day. Suggested value is 100.

-show_db_files

Lists all directories and files that are backed up during an IDB backup, such as the IDB datafiles, IDB write-ahead logs, DCBF and SMBF . In effect they contain all components of IDB.

-free_pool_update

Finds any free (unprotected) media in pools with the free pool and move free media to free pool options set and by default deallocates the found free media to a free pool every day at 00:00.

-list_large_mpos *MinNumberOfMpos* [-top *NumOfTopMedia*] [-detail] [-csv *CSVFile*]

Lists top *NumOfTopMedia* media that has more than *MinNumberOfMpos* media positions. By default, positions used and medium are displayed. With the -detail option, additional fields are displayed: the total object versions, the data protected object versions, the catalog protected object versions, and the last-write time for medium. Every report is logged to the list_large_media.log file. Optionally, the report can be written to a comma separated values (CSV) file specified with the -csv option.

-free_cell_resources

Frees all resources that were allocated during backup and restore sessions. The option is used if a session ends abnormally or a process is terminated unexpectedly.

-mergemmdb *CellManagerHostname*

Merges the local MMDB from the remote Cell Manager *CellManagerHostname* to the CMMDB. A MoM cell and a remote cell with a local MMDBF must exist for this action. All duplicated items (stores, media pools, devices) will have "_N" appended to their name, where N represents the number of the duplicate (starting with 1). Once the database is merged you cannot revert the operation. The merge operation preserves the local MMDB, which is no longer in use but must remain stored on the local system for the local IDB backup sessions to succeed.

-cdbsync *CellManagerHostname*

Synchronizes the centralized MMDB (CMMDB) and local CDB on the specified Cell Manager. In a MoM environment, the MMDB and CDB may be out of sync as a result of the centralized IDB restore.

Execute the command on the system where the CMMDB is installed.

If the CMMDB was changed, execute the command for each Cell Manager in this MoM cell that you want to use the central media managements by specifying each Cell Manager in the cell as the *CellManagerHostname* argument.

-info

Displays information about the IDB, such as MMDB, CDB, archived log files, datafiles, diskspace, DCBF, SMBF, and SIMBF usage.

-autovacuum { -set -table *TableName* [-to_default] [-on_n_rows *NRows*] [-on_percentage *Percent*] [-freeze_max_age *FreezeMax*] | -get [-table *TableName* | -enabled | -disabled | -all]}

Recovers or reuses disk space occupied by updated or deleted rows. The vacuum operation (periodic maintenance) is done automatically. By default, the option is enabled.

The -table option specifies the table to set or displays its autovacuum properties. You can provide the exact table name or use the asterisk (*) at the end to define a group of tables (for example, -table "dp_catalog_*"). Make sure that you quote the string if you use an asterisk. If a table was not yet customized with the -autovacuum option, Default is displayed as the value for all table properties.

If the -to_default option is specified together with -set and -table , the command resets autovacuum parameters for the selected table to default values.

If the -on_n_rows option is specified together with -set and -table , the command initiates the vacuum operation when the specified number of table rows is updated or deleted. By default, the value is set to 50 .

If the -on_percentage option is specified together with -set and -table , the command initiates the vacuum operation when the specified percentage of table rows is updated or deleted. By default, the value is set to 20 .

If the -freeze_max_age option is specified together with -set and -table , the command specifies the maximum age (in number of transactions) before autovacuum operation is forcibly invoked on the table. This happens even if autovacuum operation is disabled. Valid values for the option are between 100 million and 2 billion, by default it is set to 200000000 transactions.

If the -get option is specified, the command lists all table names:

-enabled lists all tables that are included in the autovacuum operation

-disabled lists all tables that are excluded from the autovacuum operation

-all lists all tables and their properties

-list_dcdirs

Lists all registered DC directories.

-add_dcdir *PathName* [-maxsize *MaxSizeInMB*] [-maxfiles *NumberOfFiles*] [-spacelow *SpaceLowInMB*] [-seq *SeqNumber*]

Creates a new directory at the specified path and registers it in the IDB as a new DC directory. If the specified directory path is not a physical path, then it is resolved and added as full physical directory path.

The -maxsize option specifies the maximum amount of disk space that can be used for DC binary files in this directory. When the specified size is reached, Data Protector stops creating new DC binary files here, and starts using the next DC directory defined by the effective allocation policy.

The -maxfiles option specifies the maximum number of DC binary files that can reside in the directory. When the specified number is reached, Data Protector stops creating new DC binary files here, and starts using the next DC directory defined by the effective allocation policy.

The -spacelow option defines the conditions under which the DC directory is considered to be full. It actually defines the minimum allowed difference between the actual size and the configured maximum size of the DC directory. When this threshold is reached, Data Protector starts using the next DC directory defined by the effective allocation policy. Additionally, this option defines the minimum amount of free space needed on the volume where the DC directory resides. Data Protector requires this space to log names of the backed up files and directories to the IDB. When free space for the last writable DC directory drops under this amount (meaning all other DC directories are considered to be full already), Data Protector automatically switches to the logging level No Log. recommends to use 10% to 15% of the currently configured maximum DC directory size as a suitable value for this option.

If argument to any of the options -maxsize, -maxfiles, and -spacelow is omitted, the default value is used for the respective amount.

The -seq option specifies the consecutive number that defines the order in which Data Protector chooses this DC directory to write new data to, provided that the effective DC directory allocation policy is fill in sequence (the DCDirAllocation global option is set to 0). The first DC directory to be used has the lowest allocation sequence number. If argument to this option is omitted, the value 0 is used.

-modify_dcdir *PathName* [-maxsize *MaxSizeInMB*]

[-maxfiles *NumberOfFiles*] [-spacelow *SpaceLowInMB*] [-seq *SeqNumber*]

Modifies properties of a DC directory that is registered with the specified path. The path itself cannot be changed.

The -maxsize option modifies the maximum amount of disk space that can be used for DC binary files in this directory. When the specified size is reached, Data Protector stops creating new DC binary files here, and starts using the next DC directory defined by the effective allocation policy. When you increase the maximum size for a specific DC directory, you should also adjust its minimum free disk space property by using the -spacelow option.

The -maxfiles option modifies the maximum number of DC binary files that can reside in the directory. When the specified number is reached, Data Protector stops creating new DC binary files here, and starts using the next DC directory defined by the effective allocation policy.

The -spacelow option modifies the conditions under which the DC directory is considered to be full. It actually defines the minimum allowed difference between the actual size and the configured maximum size of the DC directory. When this threshold is reached, Data Protector starts using the next DC directory defined by the effective allocation policy. Additionally, this option defines the minimum amount of free space needed on the volume where the DC directory resides. Data Protector requires this space to log names of the backed up files and directories to the IDB. When free space for the last writable DC directory drops under this amount (meaning all other DC directories are considered to be full already), Data Protector automatically switches to the logging level No Log. recommends to use 10% to 15% of the currently configured maximum DC directory size as a suitable value for this option.

If argument to any of the options -maxsize, -maxfiles, and -spacelow is omitted, the respective default value is used.

The -seq option modifies the consecutive number that defines the order in which Data Protector chooses this DC directory to write new data to, provided that the effective DC directory allocation policy is fill in sequence (the DCDirAllocation global option is set to 0). The first DC directory to be used should have the lowest allocation sequence number. If argument to this option is omitted, the value 0 is used.

-remove_dcdir *PathName*

Withdraws registration of the specified DC directory in the IDB without removing the directory itself. The directory must not contain DC binary files in order to become unregistered.

-remap_dcdir

Locates DCBF across all DC directories and updates DCBF locations in the IDB if they had been moved manually (using the mv command or similar) between DC directories. This makes the IDB aware of the locations of each DCBF. This option requires exclusive access to the database.

-fixmpos

Removes invalid references to DCBF. This option should be used in the case of IDB recovery (after the dbreplay phase of the IDB restore process or -import_logs) or after a DCBF has been manually removed. This option requires exclusive access to the database.

-cp { -set *ParamName ParamValue* | -get [-param *ParamName*]}

Lists and sets parameters for the connection pool configuration file. The idbhpdp-idb-cp.cfg file is located in the Data Protector server configuration directory.

Certain parameters are predefined during the Data Protector installation and cannot be changed, such as hpdpidb, service_

name , auth_type , auth_file , admin_users , and stats_users .

-set_passwd *UserName*

Changes the password for the configured Internal Database Service and Application Server user account.

-set_passwd java -pass *PreferredPassword*

Change the password for configuring the Data Protector Web reporting.

-sync_srv

Synchronizes the location of the IDB data files for all nodes in a cluster environment. Execute it on the active cluster node.

Use this option only when restoring the IDB to a different location in an Serviceguard environment on UNIX systems.

-config_cell_name NewCellManagerHostname

This option is used to set a new FQDN hostname. Internally, the services are configured with the existing credentials for the new cell name -config_cell_name cellHostName .

-delete_obsolete_resumed_versions [-session SessionID]

This option is used to delete failed objects if they were successfully backed up during resumed session.

session SessionID – This option removes only failed objects from the given SessionID.

-export_schedules {-all [–location <path>] | -spectype SpecificationType -apptype [ApplicationType] -specname SpecificationName [-location <path>]}

Exports the schedules.

all – This option specifies to export all the schedules to scheduler database. When you specify -all option, you can only specify -location option.

location - This option allows the user to select a location where the schedules of all backup specifications can be exported. If the -location option is not specified, by default the schedules will be imported to the <*OmniBack_Data*>\Config\Server path in Windows and /etc/opt/omni path in Linux.

apptype [*ApplicationType*] – This specifies the application type used while creating the schedule. The value for *ApplicationType* is dependent on the value specified for spectype [*SpecificationType*] . If the *SpecificationType* is **backup**, the *ApplicationType* can be any of the integration types. For example:

- db2
- E2010
- hana
- IDB
- Informix
- Lotus
- Mailbox
- MSESE
- mssharepoint
- MSSQL
- MSVSSW
- Oracle8
- SAP
- SAPDB
- Stream
- Sybase
- VEAGent
- VMware

If the *SpecificationType* is **copy**, **consolidation**, **verification**, **report**, or **mediacopy**, the *ApplicationType* is either **filesystem** or **datatype**.

spectype [*SpecificationType*] – This specifies the specification type used while creating the schedule. The *SpecificationType* can be any of the following values:

- Backup
- Copy
- Consolidation
- Verification
- Report

- Mediacopy

specname *SpecificationName* – This specifies the specification name used while creating the schedule.

-import_schedules {-all [–location <path>] | -spectype SpecificationType -apptype [ApplicationType] -specname SpecificationName [–location <path>]}

Imports the schedules.

all – This option specifies to import all the schedules from scheduler database. When you specify -all option, you can only specify -location option.

location - This option allows the user to select the location where the schedules of all backup specifications can be imported back to the Scheduler database. If the -location option is not specified, by default the schedules will be imported to the *<OmniBack_Data>*\Config\Server path in Windows and /etc/opt/omni path in Linux.

apptype [*ApplicationType*] – This specifies the application type used while creating the schedule. The value for *ApplicationType* is dependent on the value specified for spectype [*SpecificationType*] . If the *SpecificationType* is **backup**, the *ApplicationType* can be any of the integration types. For example:

- db2
- E2010
- hana
- IDB
- Informix
- Lotus
- Mailbox
- MSESE
- mssharepoint
- MSSQL
- MSVSSW
- Oracle8
- SAP
- SAPDB
- Stream
- Sybase
- VEAgent
- VMware

If the *SpecificationType* is **copy**, **consolidation**, **verification**, **report**, or **mediacopy**, the *ApplicationType* is either **filesystem** or **datalist**.

spectype [*SpecificationType*] – This specifies the specification type used while creating the schedule.

specname *SpecificationName* – This specifies the specification name used while creating the schedule. The *SpecificationType* can be any of the following values:

- Backup
- Copy
- Consolidation
- Verification
- Report
- Mediacopy

-create_schedule -spectype SpecificationType -apptype [ApplicationType] -specname SpecificationName -dpName <DpName> -dpType <*DpType*> -recurrenceType <RecurrenceType> -startDate <StartDate> -startTime <StartTime> -everyNth <EveryNth> [-endDate <*EndDate*>] [-endTime <EndTime>] [-fromTime <FromTime>] [-toTime <ToTime>] [-dayOfMonth <DayOfMonth>] [-daysOfWeek <DaysOfWeek>] [-nthDayOfWeekInMonth <NthDayOfWeekInMonth>]

This option is used to create schedule.

apptype [*ApplicationType*] – This specifies the application type used while creating the schedule. The value for *ApplicationType* is dependent on the value specified for spectype [*SpecificationType*] . If the *SpecificationType* is **backup**, the *ApplicationType* can be any of the integration types. For example:

- db2
- E2010
- hana
- IDB
- Informix
- Lotus
- Mailbox
- MSESE
- mssharepoint
- MSSQL
- MSVSSW
- Oracle8
- SAP
- SAPDB
- Stream
- Sybase

- VEAgent
- VMware

If the *SpecificationType* is **copy**, **consolidation**, **verification**, **report**, or **mediacopy**, the *ApplicationType* is either **filesystem** or **datalist**.

spectype [*SpecificationType*] – This specifies the specification type used while creating the schedule. The *SpecificationType* can be any of the following values:

- Backup
- Copy
- Consolidation
- Verification
- Report
- Mediacopy

specname *SpecificationName* – This specifies the specification name to be used for creating the schedule.

-dpName <DpName> – This specifies the name of the schedule.

-dpType <DpType> – This specifies the backup type as full or incremental

-recurrenceType <RecurrenceType>, -startDate <StartDate>, -startTime <StartTime>, everyNth <EveryNth>, [-endDate <EndDate>], [-endTime <EndTime>], -[-fromTime <FromTime>], [-toTime <ToTime>], [-dayOfMonth <DayOfMonth>], [-daysOfWeek <DaysOfWeek>], and [-nthDayOfWeekInMonth <NthDayOfWeekInMonth>] – These specify the options for recurrence of the schedule.

When a schedule is created, the following parameters take the below default values. If you want to change the default values, use the -modify_schedule option.

Parameter	Default value
disabled	false
dpLoad	high
dpPriority	3000
pauseLowerPriorityJobDisabled	true
expectedDurationMillis	60000
holidaysEnabled	false
dpProtection	Default

Note If you create a schedule that conflicts with an existing schedule of the same backup specification, the scenario of conflicting schedules arises. The schedules will then be created in a conflicting state by default. The conflicting schedule will be listed in the CLI, however, it will not be listed in the Web-based Scheduler and will not be triggered. For more information about schedule conflicts, see Handling schedule conflicts.

-list_schedules {-all [-specType <specificationType>][-detail] | -spectype SpecificationType -apptype [ApplicationType] -specname SpecificationName [-detail]}

Lists all the available schedules.

The detail option gives more information about the schedules that are listed.

apptype [*ApplicationType*] – This specifies the application type used while creating the schedule.

spectype *SpecificationType* – This specifies the specification type used while creating the schedule.

specname *SpecificationName* – This specifies the specification name used while creating the schedule.

-modify_schedule { -scheduleId <ScheduleId> [-dpName <DpName>] [-dpType <DpType>] [-recurrenceType <RecurrenceType>] [-startDate <StartDate>] [-startTime <StartTime>] [-everyNth <EveryNth>] [-endDate <*EndDate*>] [-endTime <EndTime>] [-fromTime <FromTime>] [-toTime <ToTime>] [-dayOfMonth <DayOfMonth>] [-daysOfWeek <DaysOfWeek>] [-nthDayOfWeekInMonth <NthDayOfWeekInMonth>] [-disabled <Disabled>] [-dpLoad <DpLoad>] [-dpPriority <DpPriority>] [-pauseLowerPriorityJobDisabled <PauseLowerPriorityJobDisabled>] [-holidaysEnabled <HolidaysEnabled>] [-dpProtection <DpProtection>] [-dpProtectionParam <DpProtectionParam> -debug_filename <FileName> -debug_range <StartRange>-<EndRange> -debug_enabled <true | false>] }

This option is used to modify a schedule.

[-dpName <DpName>] – This specifies the name of the schedule.

[-dpType <DpType>] – This specifies the backup type as full or incremental

[-recurrenceType <RecurrenceType>], [-startDate <StartDate>], [-startTime <StartTime>], [-everyNth <EveryNth>], [-endDate

<*EndDate*>], [-endTime <*EndTime*>], [-fromTime <FromTime>], [-toTime <ToTime>], [-dayOfMonth <DayOfMonth>], [-daysOfWeek <DaysOfWeek>], and [-nthDayOfWeekInMonth <NthDayOfWeekInMonth>] – These specify the options for recurrence of the schedule.

[-disabled <Disabled>] – This specifies if the schedule is disabled or enabled. Values are true or false . Default is false.

[-dpLoad <DpLoad>] – This determines how much load a schedule lays. Values are high, medium, and low. Default is high.

[-dpPriority <DpPriority>] – This specifies the priority level for the schedule in the range between 1 and 6000. Higher the number, lower the priority. Default is 3000.

[-pauseLowerPriorityJobDisabled <PauseLowerPriorityJobDisabled>] – This specifies to pause the low priority jobs. Values are true and false . Default is true.

[-holidaysEnabled <HolidaysEnabled>] – If enabled, the schedule does not run on holidays. Values are true and false . Default is false.

[-dpProtection <DpProtection>] – This specifies the time the backed up data is protected. Values are Until, None, Permanent, and Default. Default value is Default.

[-dpProtectionParam <DpProtectionParam> -debug <StartRange>-<EndRange> -debug_enabled <true | false>] – This specifies the time the backed up data is saved. If the -dpProtection parameter is defined in days, the -dpProtectionParam parameter is defined in days. Similarly, if the protection is defined in weeks, the protection parameter is defined in weeks. If protection value is Until, the protection parameter defines until what date the backed up data is protected or saved. The debug option creates a log file to help you debug.

-delete_schedule [ScheduleId]

Deletes a backup schedule.

{ ScheduleId } – This specifies the schedule to be deleted.

-migrate_schedules

Migrates schedules from Basic Scheduler to Web-based Scheduler.

-reinstate_legacy_schedules { [-force] }

-reinstate_legacy_schedules - Reinstates all schedules to the Basic Scheduler and retains the schedules created using the Web-based Scheduler in the Web-based Scheduler. Only the schedules created using the Basic Scheduler will be reinstated.

-reinstate_legacy_schedules -force - Deletes all schedules created using the Web-based Scheduler and recreates these schedules in the Basic Scheduler from the .migrate files.

Note It is recommended to use the { [-force] } option to reinstate schedules from the Web-based Scheduler to the Basic Scheduler, when you have upgraded from Data Protector 8x or 9x to 10x to the latest version. If this option is not used, the schedules created using the Web-based Scheduler will remain and be triggered in the Web-based Scheduler and will also be recreated in the Basic Scheduler. This will cause duplication of schedules in both the Schedulers.

-encrypt_array_cred

Encrypts files that contain storage array credentials in the Cell Manager system.

- encrypt_idb_pass

Encrypts Internal Database access credentials stored in the Cell Manager system.

- encrypt_user_pass

Encrypts Data Protector user credentials stored in the Internal Database.

-encrypt_dedupe_pass

Encrypts the deduplication target credentials stored in the Internal Database.

-encrypt_integ_files

Encrypts files that contain application credentials in the Cell Manager system.

- encrypt_app_client_pass

Encrypts application credentials stored in the Cell Manager system.

EXAMPLES

The following examples illustrate how the omnidbutil command works.

All schedules listed successfully.

All details of scheduled are successfully listed.

All CONSOLIDATION schedules listed successfully.

1. To create a new DC directory in the "/var/opt/test" directory with maximum size 1000 MB, execute:

   omnidbutil -add_dcdir /var/opt/test -maxsize 1000

2. To list all locked devices, target volumes, media, and slots, execute:

   omnidbutil -show_locked_devs

3. To unlock a device, a medium, or library slot, respectively, execute:

   omnidbutil -free_locked_devs machine

   omnidbutil -free_locked_devs 0a1106452:5a45add9:2548:0007

   omnidbutil -free_locked_devs libraryName phyLocation

4. To unlock the target volume whose volume number is "288" and which resides on the P9000 XP Disk Array Family storage system with the serial number "30658", execute:

   omnidbutil -free_locked_devs 30658_288

5. To manually change the maximum size for DC directory "dcbf13" in the "C:\Program Files\OmniBack\db46" directory to 48 GB and modify the free disk space needed for a DC binary file, execute:

   omnidbutil -modify_dcdir C:\Program Files\OmniBack\db46\dcbf13 -maxsize 49152 -spacelow 7372

6. To manually remove expired sessions and session messages older than 30 days, obsoleted data from the DCBF part of the IDB, and all the object versions for the overwritten tapes if the daily maintenance is disabled, respectively, execute:

   omnidbutil -purge –sessions 30

   omnidbutil -purge –messages 30

   omnidbutil -purge –dcbf

7. To remove all unrequired copies of objects that were made during a backup and may overload the IDB, execute:

   omnidbutil –purge_failed_copies

8. To export the IDB schema and its data into the dpidb.dat file and store it in the directory named "C:\dump_location", execute:

   omnidbutil –writedb C:\dump_location

9. To initiate a cleanup (vacuuming) of the table named "dp_catalog13" when 30% of table rows are updated or deleted, execute:

   omnidbutil –autovacuum -table dp_catalog13 -set -on-percentage 30

10. To display information about autovacuum properties for all catalog tables named "dp_catalog*", execute:

    omnidbutil –autovacuum -get -table "dp_catalog*"

11. To specify the maximum age in number of transactions (for example, 5000000000) before autovacuum operation is forcibly invoked on the specified table, execute:

    omnidbutil –autovacuum -set -table dp_catalog_object_type -freeze_max_age 5000000000

12. To get the connection pool configuration, execute:

    omnidbutil –cp -get

13. To set the connection pool parameter "max_client_conn" to "200", execute:

    omnidbutil –cp -set -max_client_conn 200

14. To set a new password for the user named "hpdpidb_app", execute:

    omnidbutil –set_passwd hpdpidb_app

15. To set a password for the Web reporting named "Pa55word", execute:

    omnidbutil -set_passwd java –pass Pa55word

16. The generated telemetry files are stored in the following location:

    telemetry_data – <Omniback-Home>/Config/Server/telemetry/

17. The generated dashboard files are stored in the following location:

    dashboard_data – <Omniback-Home>/Config/Server/telemetry/

18. To create a backup schedule occurring once at a specified time, execute:

    omnidbutil -create_schedule -spectype backup -apptype filesystem -specname New1 -dpName dp1 -dpType full -recurrencetype ONCE -startda te 2018-02-19 -startTime 15:00

    ```
    Schedule created successfully with Id: 9c2a81f7-b5a8-40ba-af7c-00abcb0b6bcd
    ```

19. To create a backup schedule to run every minute between the given time, execute:

    omnidbutil -create_schedule -spectype backup -apptype DATALIST -specname New1 -dpName Schxyz_Bkp11 -dpType FULL -recurrenceType e veryminute -startDate 2019-11-19 -startTime 22:00:00.254+05:30 -everyNth 2 -fromTime 18:00:00 -toTime 06:00:00 -daysOfWeek mon,tue,we d -endTime 23:00:00.254+05:30

    ```
    Schedule created successfully with Id: fab02a09-7e88-4977-ab12-4de33bf3c0ea
    ```

20. To create a backup schedule to run every day on a specified time, execute:

    omnidbutil -create_schedule -spectype backup -apptype filesystem -specname New1 -dpName dp3 -dpType full -recurrencetype DAILY -startda te 2018-02-27 -startTime 15:15 -everyNth 1 -endDate 2018-03-26 -endTime 01:00

    ```
    Schedule created successfully with Id: ad437dd6-5e1d-48d1-838c-d41a4fd65abc
    ```

21. To create a backup schedule to run every week on a specified date and time, execute:

    omnidbutil -create_schedule -spectype backup -apptype filesystem -specname New1 -dpName dp4 -dpType full -recurrencetype WEEKLY -start date 2018-02-28 -startTime 15:20 -everyNth 1 -endDate 2018-03-26 -endTime 01:00 -daysOfWeek MON

    ```
    Schedule created successfully with Id: fd5c7411-06e9-48d0-b652-b20b0416953f
    ```

22. To create a backup schedule to run every hour between specified dates, execute:

    omnidbutil -create_schedule -spectype backup -apptype filesystem -specname New1 -dpName dp5 -dpType full -recurrencetype HOURLY -start date 2018-03-01 -startTime 15:33 -everyNth 2 -endDate 2018-03-13 -endTime 01:00

    ```
    Schedule created successfully with Id: 42611145-2d2a-47b7-ace0-44e3e6bb3460
    ```

23. To create a backup schedule to run monthly at specified date and time, execute:

    omnidbutil -create_schedule -spectype backup -apptype filesystem -specname New1 -dpName dp5 -dpType full -recurrencetype MONTHLY -da yOfMonth 15 -startdate 2018-03-02 -startTime 15:45 -everyNth 1 -endDate 2018-10-13 -endTime 01:00

    ```
    Schedule created successfully with Id: 2ced6439-7630-49bc-b510-e5aa644a3a1e
    ```

24. To list all the schedules, execute:

    omnidbutil -list_schedules -spectype backup -apptype filesystem -specname New1

    ```
    ID: Mode: Recurrence: Status: Name: h6ßlW?4-f?dø-4ldd-a9S6-a?cfRif33d2S full MONTHLY Enabled monthly_schedl d241aa8-cøc2--46b?-9Sce-608f19422b62 full HOURLY Enabled sadasd b9?øcSø-9?c9-4686-aabø-d20?132c4e1c full ONCE Enabled dpi 3ec4b'?a-4e6d-4ab4-8ec3-cbf94aW?ibfd full MONTHLY Enabled monthly_sched2
    ```

25. To list all schedules configured in the system, execute:

    omnidbutil -list_schedules -all

    ```
    ID: Mode: Recurrence: Status: Name: 0aa47b97-9d58-416e-9e09-384656c890b4 full EVERYMINUTE Disabled Backup-filesystem-Spec1_1 41785d3-5999-41eb-a545-b3f7a8926a90 full DAILY Enabled Backup-filesystem-Spec2_1
    ```

26. To list details of all the schedules listed, execute:

    omnidbutil -list_schedules -all -detail

```
Specification Name : Spec1 | Application Type : DATALIST | Specification Type : BACKUP ID : 0aa47b97-9d58-416e-9e09-384656c890b4 Schedule Name : Backup-filesystem-Spec1_1 Status : Disabled Protection Type : Default Protection Parameter : Default Network Load : High Holidays : Disabled Priority : 3000 Debug : 0-200 debug.txt Backup Type : Full Recurrence Type : EVERYMINUTE Start Date : 2018-06-21 11:48 End Date : 2018-06-22 23:59 Specification Name : Spec2 | Application Type : DATALIST | Specification Type : BACKUP ID : b41785d3-5999-41eb-a545-b3f7a8926a90 Schedule Name : Backup-filesystem-Spec2_1 Status : Enabled Protection Type : Default Protection Parameter : Default Network Load : High Holidays : Disabled Priority : 3000 Debug : 0-200 debug.txt Backup Type : Full Recurrence Type : DAILY Start Date : 2018-06-21 11:49 End Date : No End Date
```

27. To list schedules of a particular specification type, execute:

    ```
    omnidbutil -list_schedules -all -specType consolidation
    ```

    ```
    ID: Mode: Recurrence: Status: Name: 960bc05a-ecf6-4a4e-a283-4d84c298dea2 full DAILY Enabled Consol1-DAILY-full 48746284-4ced-4265-8923-fcfeaff606e9 full DAILY Enabled Consol1-DAILY-full
    ```

28. To modify a schedule to run on holidays, execute:

    ```
    omnidbutil -modify_schedule -scheduleId c0425d3b-7b8d-43f0-8033-1e304df864a4 -holidaysEnabled false
    ```

    ```
    Successfully modified schedule c0425d3b-7b8d-43f0-8033-1e304df864a4. New Schedule ID : c0425d3b-7b8d-43f0-8033-1e304df864a4
    ```

29. To modify a schedule to pause the low priority jobs, execute:

    ```
    omnidbutil -modify_schedule -scheduleId c0425d3b-7b8d-43f0-8033-1e304df864a4 -pauseLowerPriorityJobDisabled true
    ```

    ```
    Successfully modified schedule c0425d3b-7b8d-43f0-8033-1e304df864a4.
    ```

30. To modify a schedule to enable the protection of backed up data untill a certain date, execute:

    ```
    omnidbutil -modify_schedule -scheduleId c0425d3b-7b8d-43f0-8033-1e304df864a4 -dpProtection Until -dpProtectionParam “2018-02-13”
    ```

    ```
    Successfully modified schedule c0425d3b-7b8d-43f0-8033-1e304df864a4
    ```

31. To modify a schedule to protect the backed up data for a specific duration (in days), execute:

    ```
    omnidbutil -modify_schedule -scheduleId c0425d3b-7b8d-43f0-8033-1e304df864a4 -dpProtection Days -dpProtectionParam 13
    ```

    ```
    Successfully modified schedule c0425d3b-7b8d-43f0-8033-1e304df864a4
    ```

32. To modify a schedule to protect the backed up data for a specific duration (in weeks), execute:

    ```
    omnidbutil -modify_schedule -scheduleId c0425d3b-7b8d-43f0-8033-1e304df864a4 -dpProtection Weeks -dpProtectionParam 4
    ```

    ```
    Successfully modified schedule c0425d3b-7b8d-43f0-8033-1e304df864a4
    ```

33. To delete a schedule, execute:

    ```
    omnidbutil -delete_schedule 9c2a81f7-b5a8-40ba-af7c-00abcb0b6bcd
    ```

    ```
    Schedule deleted successfully: 9c2a81f7-b5a8-40ba-af7c-00abcb0b6bcd
    ```

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbp4000(1), omnidbsmis(1), omnidbvss(1), omnidbxp(1), omnidbzdb(1), omniofflr(1M)

omnidlc

omnidlc - gathers or deletes Data Protector debug, log, and getinfo files from the Data Protector cell or from a MoM environment
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnidlc -version | -help

omnidlc { -session *sessionID* | -did *debugID* | -postfix *string* | -no_filter } [-hosts *list*] [-pack *filename* | -depot [*directory*] | -space | -delete_dbg | [-no_logs] [-no_getinfo] [-no_compress] [-no_config] [-no_debugs | -debug_loc *dir1* [*dir2* ...]] [-no_verbose] [-add_info [-any | *host*] *path*]

omnidlc -localpack [*filename*]

omnidlc -unpack [*filename*]

omnidlc -uncompress *filename*

omnidlc [-hosts *list*] -del_ctracelog

omnidlc [-module] -module 1, module 2

DESCRIPTION

The omnidlc command collects Data Protector debug, log, and getinfo files from the Data Protector cell (by default, from every client).

The Data Protector debug files are created during a Data Protector debug session. By default, the command collects debug files from the Data Protector default debug files directory. To collect debugs also from other directories, use the -debug_loc option.

Using the command, it is possible to collect Data Protector debug, log and getinfo files from selected clients in the Data Protector cell. In a MoM environment, you can only collect data for each Data Protector cell separately by running the command from the respective Cell Manager. On OpenVMS systems, getinfo files are not collected because the get_info utility is not available.

You can specify multiple filters for gathering the debug logs, for instance, Session ID, Postfix and Debug ID. A sample command may be –session <SessID> –postifx <string> . You can also specify multiple modules, for which you need the debug files. A sample command may be omnidlc –session <SessID> -module BSM,VBDA,DBSM .

Additionally, the Data Protector debug files to be collected can be limited to debugs that were generated within the specified Data Protector session or to debugs identified by a debugID or by a debug filename (debug postfix).

Typically, the Session Manager debugs and other non-session related executables do not have a sessionID along with the debug name. The debug collector also collects debugs that do not have a sessionID. While investigating the defects the IDB, MMD and other non-session related debugs are also required. If you require debugs that belong only to specific sessions, then ensure the target debug folder is empty, before you run the session.

By default, every collected debug, log and getinfo file is then compressed and sent over the network to the Cell Manager. The final extension .gz is added on the Cell Manager, where all collected files with the .gz extension are, by default (if the -depot option is not specified), packed and saved in the current directory as the dlc.pck file. The file includes a generated directory structure that includes the hostnames, paths and the (compressed) collected files of the clients involved. This directory structure is described further on in this man page.

Optionally, files can be sent over the network to the Cell Manager uncompressed (if the -no_compress option is specified). Besides that (if the -depot option is specified), the transferred files can be left unpacked in the specified directory on theCell Manager, in which the directory structure that includes the hostnames, paths and the collected files of the clients involved is generated as follows:

UNIX systems:

./dlc/ *system_1* /tmp/ *debug_files*

./dlc/ *system_1* /log/ *log_files*

./dlc/ *system_1* /getinfo/get_info.txt

./dlc/ *system_2* /tmp/ *debug_files*

./dlc/ *system_2* /log/ *log_files*

./dlc/ *system_2* /getinfo/get_info.txt

...

Windows systems:

.\dlc\ *system_1* \tmp\ *debug_files*

.\dlc\ *system_1* \log\ *log_files*

.\dlc\ *system_1* \getinfo\get_info.txt

.\dlc\ *system_2* \tmp\ *debug_files*

.\dlc\ *system_2* \log\ *log_files*

.\dlc\ *system_2* \getinfo\get_info.txt

...

If the file to be sent over the network is larger than 2 GB, the file is split in 2 GB chunks before it is compressed (it can be left uncompressed) and sent to the Cell Manager. Every chunk retains the file name and is added the first extension ranging from `s001` to `s999`. The second extension (`.gz`) is not added if the files are not compressed. Additionally, on the Cell Manager side, if the size of all collected compressed or uncompressed files exceeds 2 GB, the collected files are packed in 2 GB sized (original size) packages and added an extension ranging from `s001` to `s999`.

The collected debug files can also be deleted (if the `-delete_dbg` option is specified), or the disk space required on the Cell Manager for the collected files can be displayed (if the `-space` option is specified). In these two cases, the selected files are neither transferred from the clients to the Cell Manager nor packed on the Cell Manager.

When collecting or deleting files or when displaying the required disk space, additional criteria can be defined to limit the files selection. Thus, it is possible to exclude the getinfo file, the log files, the debug files or any combination of the three groups of files from the selection.

Using the command, the collected files can then be additionally packed to be sent to the support center. The command provides also a means of unpacking the packed collected files.

OPTIONS

-version

Displays the version of the `omnidlc` command.

-help

Displays the usage synopsis for the omnidlc command.

-session *sessionID*

Limits the collected debug files to those that were produced during the Data Protector session identified by the *sessionID*. Note that on OpenVMS, the omnidlc command run with the -session parameter does not collect the debug files produced during specified session, because session names are not part of the OpenVMS debug filename. Instead, all available logs are collected.

-did *debugID*

Limits the collected debug files to those identified by the *debugID*.

-postfix *string*

Limits the collected debug files to the specified debug postfix.

-no_filter

Does not limit (select) the collected debug files.

-module

Allows you to specify multiple modules, for which you need the debug files. You can use comma (,) to separate the modules specified.

-hosts *list*

Limits the files to be collected to the clients specified in the *list*. The hostnames must be separated by spaces. The debug files collected are still subject to -session, -did or -postfix options.

-pack *filename*

All collected files are, by default (if this option is not specified), packed and saved in the current directory as the dlc.pck file. If this option is specified, the collected files are packed and saved in the specified file in the current directory on the Cell Manager. If the full path name is specified, the files are packed and saved in the specified file in the specified directory.

To add files other than the collected files to the package, copy the files to one of the following directories before running the command: dlc/ *client* /getinfo, dlc/ *client* /log, or dlc/ *client* /tmp (on UNIX), or .\dlc\ *client* \getinfo, .\dlc\ *client* \log, or .\dlc\ *client* \tmp (on Windows). You cannot add directories, but only files. If the files are not copied to one of the specified directories, the package cannot be unpacked during the unpack phase.

-depot [*Directory*]

If the *Directory* is specified, the collected files are not packed and are saved to the dlc directory of the specified directory. If the *Directory* is not specified, the files are saved on the Cell Manager in the default debug files directory.

-space

Displays the disk space required on the Cell Manager for the collected files.

-delete_dbg

Deletes the selected files on clients. On OpenVMS, if run together with the -session parameter, the command does not delete any debugs from the debug files directory.

-no_getinfo

Excludes the getinfo file from the selection. For OpenVMS, this parameter is not applicable as OpenVMS systems do not have the get_info utility.

-no_config

Excludes the configuration information from the selection.

-no_logs

Excludes the log files from the selection.

-no_debugs

Excludes the debug files from the selection.

-no_compress

Disables the compression of the collected files on clients. By default, the compression is enabled.

-debug_loc *dir1* [*dir2*]...

Includes debugs not only from the default debug files directory but also from other directories, dir1 , dir2 ,.... Note that the subdirectories are excluded from the search. If a specified directory does not exist on a particular client, the directory is ignored.

This option is valid only if the -no_debugs option is not specified.

-no_verbose

Disables verbose output. By default, verbose output is enabled.

-add_info *path*

Includes the additional information (for example, screenshots, pictures and the like) from a directory on client identified by *path* .

The -any option is used when the directory path is the same for all clients. It is important to make sure the path is not host-specific before using this option.

-localpack [*filename*]

Packs the directory structure from the current directory (must be the directory containing the dlc directory generated by the -depot option) to the *filename* . If the *filename* is not specified, the dlc.pck file is created in the current directory.

This option is equivalent to the -pack option, but is to be used only if the data is collected using the -depot option.

To add files other than the collected files to the package, copy the files to one of the following directories before running the command: dlc/ *client* /getinfo , dlc/ *client* /log , or dlc/ *client* /tmp (on UNIX), or .\dlc\ *client* \getinfo , .\dlc\ *client* \log , or .\dlc\ *client* \tmp (on Windows). You cannot add directories, but only files. If the files are not copied to one of the specified directories, the package cannot be unpacked during the unpack phase.

-unpack [*filename*]

Creates the dlc directory in the current directory, and unpacks the contents of the *filename* to the dlc directory. If the *filename* is not specified, the dlc.pck file in the current directory is unpacked.

Use this option when the collected (compressed or uncompressed) data was packed on theCell Manager either using the -pack option or the -localpack option.

-uncompress *filename*

Uncompresses the unpacked compressed single file in the current directory.

Use this option after the packed data is unpacked using the -unpack option.

[-hosts *list*] -del_ctracelog

Deletes ctrace.log files containing the information where (on which clients) debug logs are generated and which debug prefixes are used. If the -hosts *list* option is specified, the command deletes ctrace.log files on specified clients only. Otherwise, ctrace.log files on all clients in a cell are deleted.

NOTES

The omnidlc command cannot be used to collect the Data Protector installation execution traces.

The Data Protector GUI debug files for systems other than Cell Manager can only be gathered using the -hosts option.

To collect debug files in a cluster, the command must be run using the -hosts option; the cluster nodes hostnames must be specified as the argument for the option. In a cluster, if the -hosts option is not specified, the data is collected from the active node.

Paths specified in postfix are not allowed.

EXAMPLES

1. To collect and compress all debug, log and getinfo files from the cell, and pack them in the "dlc.pck" file in the current directory on Cell Manager, using the verbose output, execute:

   ```
   omnidlc -no_filter
   ```

2. To collect only the log and debug files (without the getinfo files) from the clients "client1.company.com" and "client2.company.com" to the directory "c:\depot" on the Cell Manager, without compressing and packing the files, execute:

   ```
   omnidlc -no_filter -hosts client1.company.com client2.company.com -depot c:\depot -no_getinfo -no_compress
   ```

3. To collect log, debug, and getinfo files from the client "client1.company.com", compress and pack them to the "c:\pack\pack.pck" file on the Cell Manager, execute:

   ```
   omnidlc -hosts client1.company.com -pack c:\pack\pack.pck
   ```

4. To collect log, debug, and getinfo files from the default location and debugs from the additional directories, "C:\tmp" and "/temp/debugs", from the clients "client1.company.com" and "client2.company.com", and to compress and pack the files on the Cell Manager, execute:

   ```
   omnidlc -hosts client1.company.com client2.company.com -debug_loc C:\tmp /tmp/debugs
   ```

5. To delete all debug log files for the session with the ID "2013/04/27-9", execute:

   ```
   omnidlc -session 2013/04/27-9 -delete_dbg
   ```

6. To display disk space needed on the Cell Manager for the uncompressed debug files with the debugID "2351" from the client "client.company.com", execute:

   ```
   omnidlc -did 2351 -hosts client.company.com -space -no_getinfo -no_logs -no_compress
   ```

7. To pack the additional file located in the "C:\debug" directory on the client client1.company.com together with debug log files for the session with the ID 2013/05/17-24, execute:

   ```
   omnidlc -session 2013/05/17-24 -add_info -host client1.company.com C:\debug
   ```

8. To pack the directory structure in the current directory (must be the directory containing the dlc directory generated by the -depot option) to the "dlc.pck" file in the same directory, execute:

   ```
   omnidlc -localpack
   ```

9. To unpack the "dlc.pck" file to the "dlc" directory of the current directory, execute:

   ```
   omnidlc -unpack
   ```

10. To specify multiple modules, execute:

    ```
    omnidlc bsm,vbda,dbsm
    ```

SEE ALSO

omnicc(1), omnicellinfo(1), omnicheck(1M), omnisv(1M)

omnidr

omnidr - a general purpose Data Protector disaster recovery command. Based on its input, it decides on what type of restore to perform (online restore using omnir or offline restore using omnioffl r), as well as how to perform the restore (whether or not to use live operating system features).
(this command is available on systems with any Data Protector component installed)

SYNOPSIS

omnidr -version | -help

omnidr [-srd *FileName*] [-temp [os]] [-drimini *P1S*] [-map *OrgMnt_1 TrgMnt_1* [-map *OrgMnt_2 TrgMnt_2* ...]] [- [no_] cleanup] [-msclusdb] [-omit_deleted_files] [*GeneralOptions*]

GeneralOptions

-target *ClientName*

-local

-report *Level*

-omit_deleted_files

DESCRIPTION

The omnidr command is a general purpose Data Protector disaster recovery command that can be used in all recovery scenarios. Based on its input, omnidr decides what type of restore is going to be performed: online restore using omnir or offline restore using omnioffl r, as well as how the restore is going to be performed (using or avoiding live operating system features).

OPTIONS

-version

Displays the version of the omnidr command.

-help

Displays the usage synopsis for the omnidr command.

-srd *FileName*

Specifies the path to System Recovery Data (SRD) file that contains all required backup and restore object information to perform the restore.

Note that omnidr always requires a valid SRD file with updated object information. By default the command searches the working directory for recovery.srd file. If it is not found, an error is reported. The -srd option overrides the default name recovery.srd .

-temp [os]

Specifies a temporary operating system used for disaster recovery. This way, the omnidr command can determine how to restore CONFIGURATION data. If this option is not specified, the active operating system is used.

-drimini *P1S*

Specifies the path to Phase 1 Startup (P1S) file if you have interrupted the drstart command during the 30 second pause and selected the install only option when performing EADR. In this case, the drstart command only installs disaster recovery files and exits. You have to start the omnidr command manually and provide the path to the P1S file using the -drimini option. The default path is C:\$DRIM$.OB2\OBRecovery.ini (Windows) or /opt/omni/bin/drim/drecovery.ini (Linux).

-map *OrgMnt TrgMnt*

Specifies mapping of original volumes to current volumes.

-[no_]cleanup

When the -cleanup option (default) is specified during disaster recovery of an active operating system, the omnidr command prepares a cleanup script and stores it into the %ALLUSERSPROFILE%\Start Menu\Programs\Startup folder. At first logon after the boot, the Data Protector disaster recovery installation is removed.

When this option is specified during disaster recovery of a temporary operating system, a cleanup command is written into restored software hive in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce. The cleanup command is executed at first logon after the boot and it removes the temporary operating system installation together with Data Protector disaster recovery installation.

The cleanup script/command is not generated in the following cases:

- If Data Protector installation was found on the system during the omnidr command initialization.
- If the -no_cleanup option has been specified.
- If Data Protector disaster recovery installation does not reside in the *%SystemRoot%* folder (in this case it was most likely not installed during Data Protector disaster recovery).
- If the -debug option has been specified, the cleanup is not performed, because you would loose the debug information at next logon.
- if the Minimal Recovery option has been selected during EADR or OBDR, meaning that only boot and system disks would be recovered.

When the omnidr command is used on a dual-boot machine, it is strongly recommended to use the -no_cleanup option.

-msclusdb

If this option is specified, the omnidr command restores the Microsoft Cluster Service database.

GeneralOptions

-target *ClientName*

Specifies the target client system name. All objects will be restored to a computer specified by the -target parameter. If this parameter is not specified, the data will be restored to the system specified in the SRD file.

This option is used in two cases:

- During Disk Delivery disaster recovery the disks being restored can be installed into a client with a different hostname as original, therefore the name of the client must be specified.
- During Manual Disaster Recovery, it is possible, that DHCP protocol is installed. In this case, the hostname can be generated automatically by the DHCP server and is different from the original system hostname.

-local

Forces offline recovery from a local device. The devbra command is used to automatically scan for and configure attached devices. A list of detected devices is displayed if more than one is found and you must select one of them. If this option is not specified, the device used for the restore is going to be the same as the device used during backup.

-report *Level*

Specifies the error reporting level. This is useful if you want to reduce the number of messages written during recovery. For example, since practically all operating system files are overwritten during the active operating system recovery, this means that innumerable warnings bringing no useful information will be displayed, thus slowing down the recovery. Messages are classified (in ascending order) as: 1 (warning), 2 (minor), 3 (major) and 4 (critical). For example, if 3 is selected, only major and critical messages are reported. By default, all messages are reported.

-omit_deleted_files

Specifies that the files that were deleted between incremental backups or between a full and incremental backup are not restored. Note that this may slow down the recovery process.

NOTES

The omnidr command is available on Windows and Linux systems only.

EXAMPLES

The following examples illustrate how the omnidr command works.

1. To use the SRD file stored on a floppy drive for the restore, execute:

   omnidr -srd "A:\recovery.srd"

2. To use the local backup device, execute:

   omnidr -local

SEE ALSO

omniiso(1), omniofflr(1M), omnisrdupdate(1M)

omnigencert.pl

As a part of the Cell Manager installation, the omnigencert.pl utility script runs to generate and store certificates in predefined locations.

Location of the omnigencert.pl :

- **Windows**: %Data_Protector_home%\bin
- **Linux**: /opt/omni/sbin

If required, the Data Protector administrators can run this utility any time after the installation to regenerate certificates using the new keys pair or the new CA setup. However, it's not mandatory to use the certificates generated by this utility for the certificate-based authentication. Instead, you can use an existing CA setup for generating the necessary certificates.

Note: To run the omnigencert.pl utility, log in as an Administrator user on Windows or the root user on Linux.

Synopsis

The Data Protector installer executes this utility as a part of Cell Manager installation and generates and stores the necessary certificates in predefined locations. However, Data Protector administrators can run this utility any time after the installation to regenerate certificates.

Use the following command to run the omnigencert.pl utility:

omnigencert.pl [-no_ca_setup] [-server_id ServerIdentityName] [-keystore_password keystorePassword] [-truststore_password truststorePassword] [-cert_expire CertifcateExpireInDays] [-ca_dn CertifcateAuthorityDistinguishedName] [-server_dn ServerDistinguishedName] [-server_san SubjectAlternativeNamesList] [-server_san_type Santype] [-recreate] [-get_ssl_csr] [-import_ssl_certs -server_crt <server_pem_file> -cacert <ca_crt_file>] [-import_ssl_key_certs -server_private_key <server_private_key> -server_crt <server_pem_file> -cacert <ca_crt_file>] [-import_ssl_rs_certs -server_crt <server_pem_file>] [-debug_level <DebugLevel>]

where:

- ServerIdentityName = { Host FQDN | IP Address}
- CertificateAuthorityDistinguishedName = { CN=<Value>,O=<value>, ST=<value>, C=<value>}
- ServerDistinguishedName = { CN=<Value>,O=<value>, ST=<value>, C=<value>}
- SubjectAlternativeNamesList = { Santype:<value>,Santype:<value>....}
- Santype = { dns | ip}
- DebugLevel = { -2 (error), -1 (warning), 0 (main functionality) 6 (verbose), 7 (debug) }

Description

omnigencert.pl- The X.509 certificate generation utility that generates the Certificate Authority (CA) and server certificates does the following:

- Sets up a single-level root CA
- Generates CA and server certificates
- Creates the necessary directory structure for storing keys, certificates, configuration, and keystore files
- Stores the generated certificates in predefined locations on the CM
- Generates the properties files of web service roles
- Generates CSR for signing custom certificates via external CA.
- Imports custom certificates signed by external CA.
- Imports keys and certificates generated outside Data Protector for using in DP Cell Manager.
- Imports server certificate for reporting server.

Options

The omnigencert.pl utility supports multiple options, which provide flexibility while generating certificates. If no options are specified, the utility uses default values for generating the certificates.

- no_ca_setup

Generates the server certificates for an existing CA setup. This option is invalid if a CA setup does not exist.

-server_id

Specifies the value for the Common Name (CN) entity in the Distinguished Name (DN) section of the server certificate. The default value for this option is the CM Fully Qualified Domain Name (FQDN).

-keystore_password

Defines the password for the keystore, where the server certificate, including the key, is stored. If this option is not provided, a random password is generated and used for keystore password.

-truststore_password

Defines the password for the truststore, where the CA certificate is stored. If this option is not provided, a random password is generated and used fo

r truststore password.

-cert_expire

Defines the expiry of the generated certificate in days. The default value for this option is 8760 days (24 years).

-ca_dn

Defines the DN string for the CA. The DN format is as follows: “CN=<value>, O=<value>, ST=<value>, C=<value>” CN = Common Name, O=Organization Name, ST=Sate Name, C=Country Name. The default values for the O, ST, and C parameters are as follows: CN = CA <FDQN name of CM server> O = HEWLETT-PACKARD ST = CA C= US

-server_dn

Defines the DN string for the server certificate. The DN format is as follows: “CN=<value>, O=<value>, ST=<value>, C=<value>” CN = Common Name, O=Organization Name, ST=Sate Name, C=Country Name. The default values for the O, ST, and C parameters are as follows: CN = <FDQN name of CM server> O = HEWLETT-PACKARD ST = CA C= US

-server_san

Specifies the Subject Alternative Names (SAN) in the server certificate. However, the generated server certificate, during the installation of a Cell Manager, has entries of type DNS in the SAN section. These SAN entries are generated automatically based on the available IP numbers in the Cell Manager. To override default auto-generation of SAN entries in the server certificate, specify this option while generating certificates using the certificate generation utility.

The DNS and IP types of SAN entries are supported.

The format for this option value is as follows. Each SAN entry is separated by comma (‘,’) and it contains 2 parts; 1) SAN type, 2) value of the SAN type:
santype:value,santype:value

-server_san_type
Specifies the type of the Subject Alternate Name entry. It can be either “dns” or “ip”. “dns” is the default option used when this parameter is not specified.

-recreate
Re-generates the server certificate and key and overwrites the existing certificate and key.

-get_ssl_csr
Generates the server CSR that can be used to get a server certificate signed from external CA.

-import_ssl_certs
Imports the custom certificate for the server that is specified using -server_crt option signed by external CA that is specified using the –cacert option.

-import_ssl_key_certs
Imports the private key for the server that is specified using -server_private_key option, custom certificate for the server that is specified using -server_crt option signed by external CA that is specified using the –cacert option.

-import_ssl_rs_certs
Imports the certificate

-debug_level
Generate debug logs according to the level specified.

Examples:

dns:hostname, dns:hostname

ip:15.218.1.100, ip:15.218.1.200, ip:15.218.1.155

dns:hostname, ip:15.218.1.100

Important: The utility does not support the following combinations for options: -server_id and -server_dn and -no_ca_setup and -ca_dn.

Examples

The following sections list sample commands for running the omnigencert.pl utility on Windows and Linux.

1. To set up CA and to generate CA and server certificates using default values.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl

   Linux: /opt/omni/bin/perl omnigencert.pl

2. To set up CA and to generate CA and server certificates using specified common name values.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id <value>

   Linux: /opt/omni/bin/perl omnigencert.pl -server_id <value>

3. To set up CA and to generate CA and server certificates using specified store password.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -store_password <value>

Linux: /opt/omni/bin/perl omnigencert.pl -store_password <value>

4. To set up CA and to generate CA and server certificates using specified certificate expiry days.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -cert_expire <value>

   Linux: /opt/omni/bin/perl omnigencert.pl -cert_expire <value>

5. To generate the server certificate using an existing CA setup (which is created as part of the installation) using default values.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup

   Linux: /opt/omni/bin/perl omnigencert.pl –no_ca_setup

6. To set up CA and to generate CA and server certificates using specified DNS.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -ca_dn <value> -server_dn <value>

   Linux: /opt/omni/bin/perl omnigencert.pl -ca_dn <value> -server_dn <value>

7. To generate the server certificate using an existing CA setup using specified DNS.

   Windows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn <value>

   Linux: /opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn <value>

8. To generate server certificate using an existing CA certificate in the SG-CLUSTER environment.

   Windows:

   1. Retrieve the existing password from the attribute keystore-password in the file <DP_DATA_DIR>\Config\Server\AppServer\standalone.xml.
   2. Retrieve the **PGOSUSER** value from <DP_SDATA_DIR>\server\idb\idb.config.
   3. Run the omnigencert.pl utility with the cluster virtual system name as follows: %Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -store_password existing_keystor_passwd

   Linux:

   1. Retrieve the existing password from the attribute keystore-password in the file /etc/opt/omni/server/AppServer/standalone.xml.
   2. Retrieve the **PGOSUSER** value from /etc/opt/omni/server/idb/idb.config.
   3. Run the omnigencert.pl utility with the cluster virtual system name as follows: /opt/omni/bin/perl omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -store_password existing_keystor_passwd

9. To generate CA and server certificates in the SG-CLUSTER environment.

   Windows:

   1. Retrieve the existing password from the attribute keystore-password in the file <DP_DATA_DIR>\Config\Server\AppServer\standalone.xml.
   2. Retrieve the **PGOSUSER** value from <DP_SDATA_DIR>\server\idb\idb.config.
   3. Run the omnigencert.pl utility with the cluster virtual system name as follows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id cm_virtual_name.domain.com -store_password existing_keystor_passwd

   Linux:

   1. Retrieve the existing password from the attribute keystore-password in the file /etc/opt/omni/server/AppServer/standalone.xml.
   2. Retrieve the **PGOSUSER** value from /etc/opt/omni/server/idb/idb.config.
   3. Run the omnigencert.pl utility with the cluster virtual system name as follows: /opt/omni/bin/perl omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd

10. To generate a server certificate with SAN entries of type DNS for a specific Cell Manager server.

    Windows:

    %Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn hostname -server_san "dns:hostname,dns:hostname"

    Linux:

    /opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn hostname -server_san "dns:hostname,dns:hostname"

11. To generate a server certificate with SAN entries of type IP for a specific Cell Manager server.

    Windows:

    %Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn 15.218.1.100 -server_san “ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125,ip:15.218.1.116”

    Linux:

    /opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn 15.218.1.100 -server_san "ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125,ip:15.218.1.116"

12. To generate a server certificate with SAN entries of types DNS and IP for a specific Cell Manager server.

    Windows:

    %Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn hostname -server_san "dns:hostname, hostname,ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125,ip:15.218.1.116"

    Linux:

    /opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn hostname -server_san "dns:hostname, hostname,ip:15.218.1.100,ip:15.218.1.101,ip:15.218.1.125,ip:15.218.1.116"

13. To generate a CSR that can be provided to external CA for custom certificate.

    Windows:

    <Install_Folder>\OmniBack\bin\perl.exe" "<Install_Folder>\OmniBack\bin\omnigencert.pl" -get_ssl_csr -server_id <CellManagerHostName>

    Linux:

    /opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -get_ssl_csr -server_id <CellManagerHostName>

    The above command generates the CSR files and private key files in the directory <DP_CONFIG_PATH>\server\certificates_thirdparty. >

14. To import custom certificate signed by an external CA:

    Windows:

    <Install_Folder>\OmniBack\bin\perl.exe" "<Install_Folder>\OmniBack\bin\omnigencert.pl" -import_ssl_certs -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHostName>

    Linux:

    /opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -import_ssl_certs -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHostName>

15. To import the server key and certificate that were generated outside of Data Protector:

    Windows:

    <Install_Folder>\OmniBack\bin\perl.exe" "<Install_Folder>\OmniBack\bin\omnigencert.pl" -import_ssl_key_certs -server_private_key <Full_path_to_server_private_key.pem> -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

    Linux:

    /opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -import_ssl_key_certs -server_private_key <Full_path_to_server_private_key.pem> -server_crt <Full_path_to_server.pem> -cacert <Full_path_to_cacert.crt> -server_id <CellManagerHost>

Omnigencertss.pl

As a part of the Cell Manager or Client installation, the omnigencertss.pl utility script runs to generate and store INET secure communication certificates in predefined locations.

Location of the omnigencertss.pl :

- **Windows**: %Data_Protector_home%\bin
- **Unix**: /opt/omni/sbin

If required, the Data Protector administrators can run this utility any time after the installation to regenerate INET certificates and keys pair. However, it's not mandatory to use the certificates generated by this utility for the secure communication over INET. Instead, you can use an existing CA setup for generating the necessary certificates. Use this utility to generate a CSR for custom certificate signing.

Note: To run the omnigencertss.pl utility, log in as an Administrator user on Windows or the root user on Unix.

Synopsis

Use the following command to run the omnigencertss.pl utility:

omnigencertss.pl [-hostname <HostName>] [-expirydays <Number of Days>] [-force] [-fingerprint] [-renew] [-get_ssl_csr] [-debug_level <DebugLevel>]

where DebugLevel= { -2 (error), -1 (warning), 0 (main functionality) 6 (verbose), 7 (Debug) }

Description

The omnigencertss.pl utility does the following:

- Generates generate self-signed certificate for the INET secure communication
- Renews the INET certificate that is expired or about to expire
- Generates CSR for signing custom certificate from external CA to use for INET communication.

Options

The omnigencertss.pl utility supports multiple options, which provide flexibility while generating certificates. If no options are specified, the utility uses default values for generating the certificates.

- hostname

Provides the hostname for which the certificate will be generated. When you do not specify this option the current hostname in FQDN format will be used.

-expirydays

Provides the validity of the generated certificate in number of days. The default value is 3650 days (Approximately 10 years).

-force

Forces the generation(recreation) of certificate and key even if it exists already. This option is not required to be used with renew option as the certificate must exist for its renewal.

-fingerprint

Prints the fingerprint of the generated certificate in the log file during the generation of a new certificate.

-renew

Renews the certificate when it is about to expire or already expired.

-get_ssl_csr

Generates the Certificate Signing Request(CSR) to provide to external CA for custom certificate generation

-debug_level

Generates the debug logs from this script execution at the specified level.

Examples

The following sections list sample commands for running the omnigencertss.pl utility on Windows and Unix.

1. To re-generate certificate for a given hostname:

   Windows: %Data_Protector_home%\bin\perl.exe %Data_Protector_home%\bin\omnigencertss.pl -hostname <host name value> -force

Unix: /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl –hostname <host name value> -force

2. To re-generate certificate valid for a year (365 days):

   Windows: %Data_Protector_home%\bin\perl.exe %Data_Protector_home%\bin\omnigencertss.pl -expirydays 365 -force

   Unix: /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl –expirydays 365 -force

3. To renew certificate for a year (365 days):

   Windows: %Data_Protector_home%\bin\perl.exe %Data_Protector_home%\bin\omnigencertss.pl -renew -expirydays 365

   Unix: /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl -renew -expirydays 365

4. To generate Certificate Signing Request(CSR) to provide to external CA for custom certificate signing:

   Windows: %Data_Protector_home%\bin\perl.exe %Data_Protector_home%\bin\omnigencertss.pl -get_ssl_csr

   Unix: /opt/omni/bin/perl /opt/omni/lbin/omnigencertss.pl -get_ssl_csr

omnihealthcheck

omnihealthcheck - checks the status of Data Protector services, the consistency of the Data Protector Internal Database (IDB), and if at least one backup of the IDB exists
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnihealthcheck -version | -help

omnihealthcheck [-config *ConfigFile*]

DESCRIPTION

The omnihealthcheck command reads the specified configuration file where each line of the file is treated as a separate command and is executed. The commands must be listed with full paths except if they reside in the Data Protector default commands directory. With the Windows Cell Manager, the configuration file must be in the Unicode format. If the configuration file is not specified, the default HealthCheckConfig file located in the server configuration directory on the Cell Manager is used.

If the default file is used, omnihealthcheck checks if Data Protector services (CRS , MMD , hpdp-idb , hpdp-idb-cp , hpdp-as , KMS , omnitrig , and omniinet) are active, if the Data Protector MMDB is consistent, and if at least one backup of the Data Protector Internal Database (IDB) exists.

Exit codes of individual commands are inspected at the end.

There are 3 different exit codes for the omnihealthcheck command:

0 - All listed commands and their exit codes have been executed
1 - At least one of the commands in the configuration file could not be executed or has completed with an exit code other than 0 .
2 - The configuration file could not be read.

The final health check exit code is 0 (OK) only if all executed commands from the configuration file completed successfully (exit codes of all executed individual commands from the configuration file are 0).

Output of the omnihealthcheck command is saved on the Cell Manager in the HealthCheck.log file located in the default server log files directory.

If a timeout occurs, omnihealthcheck fails.

omnihealthcheck is by default scheduled to run daily at 12:00 (noon) as a part of the Data Protector check mechanism. The default schedule value can be changed by changing the DailyCheckTime global option.

OPTIONS

-version - Displays the version of the omnihealthcheck command.
-help - Displays the usage synopsis for the omnihealthcheck command.
-config *ConfigFile* - Specifies an alternative configuration file for the omnihealthcheck command. Note that you can define the commands to be executed in the health check.

SEE ALSO

omnirpt(1), omnitrig(1M)

omniinetpasswd

omniinetpasswd - manages the local Data Protector Inet configuration on Windows systems where the Inet process must be run under a specific user account, and sets a user account to be used by the Installation Server during remote installation (this command is available on systems with any Data Protector component installed)

SYNOPSIS

omniinetpasswd -version | -help

omniinetpasswd -add { *User*@*Domain* | *Domain**User* ...} [*Password*]

omniinetpasswd -delete { *User*@*Domain* | *Domain**User* ...}

omniinetpasswd -modify { *User*@*Domain* | *Domain**User* ...} [*Password*]

omniinetpasswd -list [*Domain*]

omniinetpasswd -clean

omniinetpasswd -[no_]inst_srv_user { *User*@*Domain* | *Domain**User* ...}

DESCRIPTION

On specific Windows operating systems, the Data Protector Inet process must be run under a specific operating system user account rather than under the local user account SYSTEM. Additionally, the Data Protector Installation Server must use a specific operating system user account for remote installation. The omniinetpasswd command provides functionality for management of Inet configuration on the local system, and functionality for setting a user account that will be used by the Installation Server during remote installation. Use command options -add , -delete , -modify , -list , and -clean for local Inet configuration management, and options -inst_srv_user and -no_inst_srv_user for setting a user account to be used for remote installation.

Note that omniinetpasswd does not add, remove, or change user accounts in the operating system configuration.

OPTIONS

-version

Displays the version of the omniinetpasswd command.

-help

Displays the usage synopsis for the omniinetpasswd command.

-add { *User*@*Domain* | *Domain**User* } [*Password*]

Adds the specified user account from the local Inet configuration. omniinetpasswd prompts for the password if not specified in the command line.

-delete { *User*@*Domain* | *Domain**User* }

Removes the specified user account from the local Inet configuration. omniinetpasswd prompts for the password if not specified in the command line.

-list *Domain*

Lists user accounts from the local Inet configuration: either all or only the accounts belonging to the specified domain.

-modify { *User*@*Domain* | *Domain**User* } [*Password*]

Changes the password for a configured user account. omniinetpasswd prompts for the password if not specified in the

command line.

-clean Domain

Removes all operating system user accounts from the local Inet configuration.

-inst_srv_user { *User*@*Domain* | *Domain**User* }

Sets the specified user in the local Inet configuration to be used by the Installation Server during remote installation.

This option can only be used on supported Windows systems.

-no_inst_srv_user { *User*@*Domain* | *Domain**User* }

Marks the specified user in the local Inet configuration not to be used by the Installation Server during remote installation.

This option can only be used on supported Windows systems.

NOTES

The omniinetpasswd command is available on supported Windows systems only.

EXAMPLES

1. To remove the user "User1" from the Inet configuration, execute:

   omniinetpasswd -delete CompanyDomain\User1

2. To delete all operating system accounts from the local Inet configuration, execute:

   omniinetpasswd -clean

3. To set the user "User1" from the domain "CompanyDomain" to be used by Installation Server, execute:

   omniinetpasswd -inst_srv_user User1@CompanyDomain

omniintconfig.pl

omniintconfig.pl - configures and checks the configuration of one or multiple Oracle databases (this command is available on systems with the Data Protector User Interface component installed).

SYNOPSIS

omniintconfig.pl -version | -help

omniintconfig.pl [-encode] [-chkconf] [-force] { -passwordfile *FileName* | *Param* = *Value* [*Param* = *Value* ...]}

Param

MoM

CellManager

Client

Instance

OSUSER

OSGROUP

TGTUser

TGTPasswd

TGTService

RCUser

RCPasswd

RCService

ORACLE_HOME

ClusterNodes

DESCRIPTION

Use the omniintconfig.pl command to configure and check the configuration of one or multiple Oracle databases at the same time. If configuration already exists then script does not perform the Oracle integration reconfiguration instead it changes only the specified configuration parameters directly in the existing configuration file.

On Windows systems, you must use the perl command to run omniintconfig.pl . An example of the command line is perl omniintconfig.pl -help .

OPTIONS

-version

Displays the version of the omniintconfig.pl command.

-help

Displays the usage synopsis for the omniintconfig.pl command.

-encode

Encodes passwords before they are saved to Data Protector Oracle database specific configuration files. Omit this option if the provided passwords are already encoded.

-chkconf

Performs a configuration check for specified Oracle databases. Provided parameter values are saved to corresponding Data Protector Oracle database configuration files, regardless of whether the check succeeds or not. By default, the session ends if a configuration check for a database fails. However, if you specify the -force option, Data Protector continues configuring other Oracle databases.

-passwordfile FileName

Specifies that configuration parameters should be read from a file. The file must be in XLS or CSV file format.

Alternatively, parameters can be specified at run time, however, only for one Oracle database at a time. See the parameters description below.

PARAMETERS

MoM

Manager of Managers (optional).

CellManager

Data Protector Cell Manager. Default: Cell Manager of the local client.

Client

Client with Oracle Server installed. In cluster environments, specify the virtual server or, in RAC, one of the cluster nodes. Default: local client.

Instance

Oracle database name (mandatory).

OSUSER , OSGROUP

(Applicable for UNIX clients.) The UNIX user account under which you want the configuration and browsing of Oracle databases to start. This user will be automatically added to the Data Protector admin user group for the client specified in Client .

TGTUser , TGTPasswd

Login information for the target database (username and password).

TGTService

Target database service(s). If there is more than one service, separate them with a semicolon (service1;service2...).

RCUser , RCPasswd

Login information for the recovery catalog database (username and password).

RCService

Recovery catalog database service.

ORACLE_HOME

Oracle Server home directory.

ClusterNodes

Cluster nodes (applicable in cluster environments). The user OSUSER , OSGROUP will be automatically added to the Data Protector admin user group for each cluster node listed here. Separate cluster nodes with a semicolon (node1;node2...).

If you do not specify this parameter, you need to add these users manually.

EXAMPLES

1. Suppose the file "C:\My_documents\Oracle_instances.csv" contains configuration parameters for the Oracle databases "IN1" and " IN2". The passwords in the file are encoded.

   To configure the Oracle databases "IN1" and "IN2" using the file "C:\My_documents\Oracle_instances.csv", log in to the Windows client on which the file is saved and execute:

   ```
   perl omniintconfig.pl -passwordfile C:\My_documents\Oracle_instances.csv
   ```

2. Suppose you are logged in to a UNIX client. To configure the Oracle database "IN2" by specifying parameters at run time, execute:

   ```
   omniintconfig.pl -encode CellManager=galaxy Client=star Instance=IN2 ORACLE_HOME=C:\oracle\product\10.2.0\db_1 TGTUser=system TGTPasswd=BlueMoon TGTService=IN2_1;IN2_2
   ```

   Note that the password "BlueMoon" is not encoded. Therefore, you must specify the "-encode" option.

3. Suppose you are logged in to a Windows client. To configure and check the configuration of all Oracle databases specified in "C:\My_documents\Oracle_instances.xls", execute:

   ```
   perl omniintconfig.pl -chkconf -force -passwordfile C:\My_documents\Oracle_instances.xls
   ```

4. Suppose you are logged in to a UNIX client. To check the configuration of the Oracle database "IN2", execute:

   ```
   omniintconfig.pl -chkconf CellManager=galaxy Client=star Instance=IN2
   ```

SEE ALSO

util_cmd(1M), util_oracle8.pl(1M), vepa_util.exe(1M)

omnikeytool

omnikeytool - manages keys used to encrypt backup data
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnikeytool -version | -help

omnikeytool -create *EntityName* [-description *Description*]

omnikeytool -activate *EntityName* -keyid *KeyID* *StoreID*

omnikeytool -deactivate *EntityName*

omnikeytool -export *keyFileName* *ExportOptions* [-password *Password*]

omnikeytool -import *keyFileName* [-password *Password*]

omnikeytool -modify -keyid *KeyID* *StoreID* -description *Description*

omnikeytool -list [-active | -unused]

omnikeytool -delete -keyid *KeyID* *StoreID*

ExportOptions

-keyid *KeyID* *StoreID*

-active

-entity *EntityName*

-time *Day Hour Day Hour*

-all

Date = *[YY]YY/MM/DD (1969 < [YY]YY < 2038)*

Hour = *HH:MM*

DESCRIPTION

The omnikeytool command manages keys used for encryption. You must create the key by using the omnikeytool command prior to performing an encrypted backup.

OPTIONS

-version

Displays the version of the omnikeytool command.

-help

Displays the usage synopsis for the omnikeytool command.

-create *EntityName* [-description *Description*]

EntityName can be:

- A ClientName value for the specified filesystem, disk image, or the IDB
- An AppType : *DatabaseID* pair or an AppType : *ClientName* : *AppName* trinity for the specified application integration
- A MediumID value, if you use drive-based encryption

Ensure that the value of ClientName matches the name that was specified for the client system in the correspondent backup specification.

If the -description option is specified, you can provide a description string for the new encryption key.

-activate *EntityName* -keyid *KeyID* *StoreID*

Associates the specified encryption key with the specified entity name string and activates the key.

-deactivate *EntityName*

Disassociates the specified entity name string from the current active backup encryption key.

The password encryption is done by AES keys with entity name “Data Protector Passwords”. Do not delete or deactivate this key, as Data Protector will not be able to decrypt encrypted strings. Deactivating the password key affects backup only; it does not affect restore, nor does it disable the key or act as a key revocation. For Cloud devices, deactivating or deleting the password key renders the Cloud device unusable.

-export *keyFileName* *ExportOptions* [-password *Password*]

Exports encryption key records into a binary file. The file is exported to the Data Protector encryption keys directory. Exporting does not delete encryption keys from the keystore. The file is encrypted with the password specified.

- Data protector will not store the password internally; it just uses the password to generate the encryption key. When importing the key file, enter the password that was specified when exporting the key file.
- When keys are exported to an existing file, the password should be the same as that was given in the previous exports.
- Import from the old plain text format is supported. In this case, use the -import option without password . For example: omnikeytool -import oldkey.csv .
- Starting with version 2019.08, the keys are exported in encrypted format only. Appending to plain text keyfile is not allowed.

The password you specify must meet the following requirements:

- Includes at least one upper case letter.
- Includes at least one of these special characters: an asterisk (*), a dot (.), an hyphen (-), or an underscore (_).
- Includes at least one numeric character.
- Does not include spaces.
- Must be of minimum 8 characters and maximum length 64 characters.

-import *keyFileName* [-password *Password*]

Imports encryption key record matching the key number from the specified keystore file. The file is decrypted only after entering the password specified when exporting the file. The file is imported to the Data Protector encryption keys directory.

- Data protector will not store the password internally; it just uses the password to generate the encryption key. When importing the key file, enter the password that was specified when exporting the key file.
- Import from the old plain text format is supported. In this case, use the -import option without password . For example: omnikeytool -import oldkey.csv .
- Starting with version 2019.08, the keys are exported in encrypted format only. Appending to plain text keyfile is not allowed.

-modify [-description *Description*]

Modifies the description for the specified encryption key.

-list [-active | -unused]

Lists encryption keys related information from the cell.

The command lists the following information for each encryption key in the keystore file: key status (active, inactive, migrated), key ID, date and time of creation, type of encryption, and the key description. For greater scrutiny, the above-mentioned information is listed for each client in the cell separately.

If the -active option is specified, the command just lists currently active keys and the entity names associated with them.

If the -unused option is specified, the command lists all encryption keys which are present in the keystore file on theCell Manager, but have never been used for encryption.

-delete

Deletes the record of an inactive encryption key identified by key ID.

Ensure that the key you intend to delete is not in use. If the encryption key is not available, restore of encrypted data is not possible.

ExportOptions

-keyid *KeyID StoreID*

Exports all encryption key records with the specified key ID.

-active

Exports all currently active encryption keys.

-entity *EntityName*

Exports only the active key record identified by the *EntityName* string.

-time *Day Hour Day Hour*

Exports all encryption key records in the specified time frame.

-all

Exports all encryption key records.

EXAMPLES

The following examples illustrate how the omnikeytool command works.

1. To activate the encryption key "10B536738F8831478408000000000000 5B9381955B9381955B9381955B938195" for the client system "proxima", execute:

   omnikeytool -activate proxima -keyid 10B536738F8831478408000000000000 5B9381955B9381955B9381955B938195

2. To deactivate an encryption key for the client system "stella", execute:

   omnikeytool -deactivate stella

3. To modify your description of the encryption key "10B53673B8232747A806000001000000 5B9381955B 9381955B9381955B938987", execute:

   omnikeytool -modify -keyid 10B53673B8232747A806000001000000 5B9381955B 9381955B9381955B938987 -description key_number_1

4. To export the active encryption key "10B53673B8232747A806000001000000 5B9381955B 9381955B9381955B938321" to a comma-separated values (CSV) file "a.csv", execute:

   omnikeytool -export a.csv -keyid 10B53673B8232747A806000001000000 5B9381955B 9381955B9381955B938321

5. To list all encryption keys which are present in the keystore file on theCell Manager, but have never been used for encryption, execute:

   omnikeytool -list -unused

6. To export a key file, encrypted using a password, execute:

   omnikeytool -export keyfilename ExportOptions -password Pass_word2

7. To import a key file, encrypted using a password, execute:

   omnikeytool -import keyfilename -password Pass_word2

SEE ALSO

omnib(1), omniobjconsolidate(1), omniobjcopy(1), omniobjverify(1), omnir(1)

omnimigrate.pl

omnimigrate.pl - migrates the Data Protector Internal Database (IDB) from the format used in earlier versions to the PostgreSQL relational database format used in Data Protector 8.00 and later.
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnimigrate.pl -help -version

omnimigrate.pl -cleanup

omnimigrate.pl -export [-new_cm *NewCmHostName*] [-output_dir *OutputDirectoryPath*]

omnimigrate.pl -import [-input_dir *InputDirectoryPath*]

omnimigrate.pl -export_critical_part [-output_dir *OutputDirectoryPath*]

omnimigrate.pl -import_critical_part [-input_dir *InputDirectoryPath*]

omnimigrate.pl -start_catalog_migration

omnimigrate.pl -report_catalog_migration_progress

omnimigrate.pl -stop_catalog_migration

omnimigrate.pl -report_old_catalog [media | sessions | objects]

omnimigrate.pl -remove_old_catalog

DESCRIPTION

The omnimigrate.pl command helps you migrate the Data Protector Internal Database (IDB) from the format used in earlier versions to the PostgreSQL relational database format used in Data Protector 8.00 and later.

After the upgrade, all objects whose catalogs are still protected and were backed up prior to the migration, have their catalogs stored in the old format. When catalogs expire, the old DC binary files are automatically deleted (through daily maintenance tasks).

Old database files are however kept as long as there are filenames which are protected.

A warning is displayed in the Event Log which lists the protected media, object, and sessions that still need the old DC binary files and IDB files, and the amount of space they occupy.

Use this command after an upgrade from earlier versions of Data Protector to:

- list the protected media, objects, and sessions that still need the old DC binary files and IDB files, and the amount of space they occupy
- migrate the Detail Catalog Binary Files (DCBF) to the new format.

Tip recommends that you wait until most of your old media expire and you trigger the migration only for permanently protected media.

OPTIONS

-help

Displays the usage synopsis for the omnimigrate.pl command.

-version

Displays the version of the omnimigrate.pl command.

-cleanup

Removes all export and import files from the specified directory. Use this command if the IDB export fails.

-export [-new_cm *NewCmHostName*] [-output_dir *Directory*]

The command exports the database, prepares it for import, and converts the IDB backup filesystem specification to IDB backup application integration specification. If no output directory is specified, the database is exported to the default Data_Protector_home\tmp (Windows systems) or /var/opt/omni/tmp (UNIX systems) directory.

If the -new_cm option is not specified, the command assumes that the system is being upgraded.

Use this command to export the database of Data Protector versions prior to 8.00.

For Data Protector versions 8.00 and later, there is no need to use this command because the database format is already in the PostgreSQL relational database format.

-import [-input_dir *Directory*] [-force]

Imports the data exported by the –export option into the new database. If no directory is specified, data is searched in the default Data_Protector_home\tmp (Windows systems) or /var/opt/omni/tmp (UNIX systems) directory, in the cdb and mmdb subdirectories. To force an import after a failure during the upgrade process, specify –force .

-export_critical_part [-output_dir *OutputDirectoryPath*]

This option is used during the upgrade process. It exports only the critical part of the old IDB without the catalog. If -output_dir is not specified, the files will be by default exported to the Data_Protector_home\tmp (Windows systems) or /var/opt/omni/tmp (UNIX systems) directory.

-import_critical_part [-input_dir *InputDirectoryPath*]

Imports only the critical part of the old IDB without the catalog (exported with the –export_critical_part option) into the PostgreSQL relational database. If -input_dir is not specified, the command searches by default in the Data_Protector_home\tmp (Windows systems) or /var/opt/omni/tmp (UNIX systems) directory.

-start_catalog_migration

Starts the catalog migration.

-report_catalog_migration

Displays the progress of the catalog migration.

-stop_catalog_migration

Stops the catalog migration process. The current DCBF upgrade is finished and logged. If you run the omnimigrate command with the -start_catalog_migration the migration continues from where it stopped.

-report_old_catalog [media | sessions | objects] [-shared_dir]

Displays the usage and statistics of the old catalog. The media option displays the list of media whose catalog is still in

the old format and their expiration date. The sessions option displays the sessions and their expiration date. The objects option displays the objects and their expiration date.

-remove_old_catalog

Removes all of the old DC binary files and all of the old database data files.

RETURN VALUES

0 - Successfully finished.
(1-4) - An error occurred.

ERRORS

1 - A generic error occurred.
2 - Migration of IDB catalogs failed.
3 - Configuration error (Cell Manager configuration error or an error during the import of clients) occurred.
4 - Error parsing options.

NOTES

The omnimgrate.pl command *cannot* be used to migrate the Cell Manager from obsolete platforms to supported ones. You need to migrate a Cell Manager to Data Protector 9.00 before you upgrade to Data Protector 2018.09(10.10).

EXAMPLES

1. To list all media, whose catalog is still in the old format and their expiration date, execute:

   omnimigrate.pl -report_old_catalog -media

2. To start the catalog migration on the Cell Manager after upgrade, execute the following command:

   omnimigrate.pl -start_catalog_migration

> **Note** Once the full catalog migration is done (after there are no old catalogs), change the global variable SupportOldDCBF to 0 .

SEE ALSO

ob2install(1M), omnigui(5), omniintro(9), omnisetup.sh(1M), omniusers(1), upgrade_cm_from_evaa(1M)

omnioffl r

omnioffl r - enables restore of any type of Data Protector backup objects in the absence of operable Data Protector Internal Database (IDB), including the IDB itself
(this command is available on systems with any Data Protector component installed)

SYNOPSIS

omnioffl r -version | -help

omnioffl r *DeviceOptions* *MediaOptions1* [*MediaOptions2* ...] *ObjectOptions1* [*ObjectOptions2* ...] [*GeneralOptions*]

omnioffl r -idb -autorecover [*AutorecoverOptions*] [[-changedevhost *MAClientName* | -changedevhost *MAClientName*]] [*GeneralOptions*]

omnioffl r -idb -read *OptionFile* [*GeneralOptions*]

omnioffl r -idb *DeviceOptions* *MediaOptions1* [*MediaOptions2* ...] *ObjectOptions1* [*ObjectOptions2* ...] [*GeneralOptions*]

AutorecoverOptions

[-force]

[-session *SessionID*]

[-save *OptionFile*]

[-skiprestore]

[-logview]

[-optview]

DeviceOptions

-name *DeviceName*

-dev *PhysicalDevice1* [*PhysicalDevice2* ...]

-mahost *DeviceHostName*

-policy *LogicalDevicePolicy*

-type *LogicalDeviceType*

[-ioctl *RoboticsSCSIAddress*]

[-description *DeviceDescription*]

[-blksize *BlockSize*]

MediaOptions

-maid *MediumID1* [*MediumID2* ...]

[-slot *Slot1[:Flip1]* [*Slot2[:Flip2]* ...]]

[-position *Segment1:Offset1* [*Segment2:Offset2* ...]]

ObjectOptions

FILESYSTEM RESTORE

{ -filesystem | -winfs } *Client:MountPoint Label*

-daid *DAID*

-tree *TreeName1* [*TreeOptions1*] [-tree *TreeName2* [*TreeOptions2* ...]]

[-merge]

[-[no_]overwrite]

[-move_busy]

[-omit_deleted_files [-time ObjectBackupStartTime]]

[-var *OptName* *OptValue*]

DISK IMAGE RESTORE (WINDOWS SYSTEMS)

-rawdisk *Client Label*

-section [*ToSection1=*] *Section1*

[-section [[*ToSection2=* | *ToSection2=*]] *Section* 2...]

-daid *DAID*

TreeOptions

-exclude *TreeName1* [*TreeName2...*] { -as | -into } *NewTreeName*

GeneralOptions

-keyfile *CSVFilePath*

-verbose

-preview

-report

-target *TargetHostName*

-[no]ok[mediumlist]

DESCRIPTION

The omnioffIr command is a standalone command. On Windows and Linux systems, it can also be used indirectly by the higher-level omnidr command, which automatically generates appropriate omnioffIr command-line options, based on the information retrieved from the SRD file.

The omnioffIr command enables you to restore any type of Data Protector backup objects in the absence of operable Data Protector Internal Database (IDB), including the IDB itself. The IDB may not be functioning as a result of a disaster, loss of connectivity with the Cell Manager, or other undesirable circumstances.

To execute the omnioffIr command, you need to specify the details about the backup (restore) device and the backup media, including backup object positions on the media. You can obtain these details automatically from the SRD files location, or supply them manually in the omnioffIr command line. Query the IDB using the omnidb command after the backup session, and write down the results. You can also prepare a script that queries the IDB and generates another script within which the omnioffIr command is invoked with appropriate options.

Prerequisites

From Data Protector version 2018.09 (10.10), a secure connection is enabled between the clients. The omnioffl r command can only be used if secure connections are enabled between the hosts. The omnicc command is used to enable the secure connection. For more information on how to use omnicc command options, see omnicc command.

Complete the steps listed in the following scenarios to configure the certificates to enable the secure communication between the communicating clients.

If certificates do not exist or are expired, generate new certificates and key. Run the following command on the hosts before running the omnicc command:

```
perl omnigencertss.pl
```

Scenario 1: The omnioffl r host computer1.company.com has to restore data securely on target host computer2.company.com with media agent host mediaHost.company.com . In this case, enable secure communication between omnioffl r host and target host, and between omnioffl r host and media agent host.

1. Run the following command on the omnioffl r host, computer1.company.com :

   - omnicc -secure_comm -configure_peer mediaHost.company.com

   - omnicc -secure_comm -configure_peer computer2.company.com

2. Run the following command on the target host, computer2.company.com :

   - omnicc -secure_comm -configure_peer computer1.company.com

3. Run the following command on media agent host, mediaHost.company.com :

   - omnicc -secure_comm -configure_peer computer1.company.com

Scenario 2: The omnioffl r host is same as the target host. In this case, enable secure communication between target host and media agent host.

1. Run the following command on the target host:

   - omnicc -secure_comm -configure_peer mediaHost.company.com

2. Run the following command on the media agent host:

   - omnicc -secure_comm -configure_peer targetHost.company.com

Offline restore of the IDB

OFFLINE RESTORE OF THE IDB

The IDB restore process, when invoked by omnioffl r , consists of four phases:

1) Stopping the Data Protector services/daemons (with the exception of the Data Protector Inet service on Windows system).

2) Restoring the IDB.

3) Performing a rollforward operation on the IDB using transactions from the available archived log files.

4) Starting the Data Protector services/daemons.

A new archived log file is created every time an IDB backup session is started, the IDB is initialized or checked for consistency, or an existing archived log file reaches its maximum size. Archived log files reside on the Cell Manager in the directory Data_Protector_program_data \server\db80\pg\pg_xlog_archive (Windows systems) or /var/opt/omni/server/db80/pg/pg_xlog_archive (UNIX systems).

For restoring the IDB, omnioffl r can operate in three modes: autorecovery mode, read mode, and manual mode.

AUTORECOVERY MODE

In this mode, the omnioffl r operation is fully automated. The command retrieves all required IDB restore parameters from the IDB recovery file named obrindex.dat , residing on the Cell Manager in the rlog directory on the IDB recovery files location. It is updated during each IDB backup session and contains all required IDB restore parameters, including filenames of the archived log files created during the IDB backup session. You can create and maintain a duplicate of this file by configuring the RecoveryIndexDir global option. omnioffl r can use the duplicate if the original is missing or corrupted. also recommends to place the IDB recovery file on a physical disk separate from the core part of the IDB.

READ MODE

You can use this mode to direct omnioffl r to obtain the parameters from the file *OptionFile* that has been created either manually or using the omnioffl r options -idb -autorecover -save . Use this mode when, for example, the restore devices differ from the backup devices (or they are attached to a different system). In such a case, you have to manually update the file *OptionFile* appropriately before invoking the restore session.

MANUAL MODE

You can use this mode when neither the obrindex.dat file nor the file *OptionFile* are available, and you need to manually specify all required parameters in the omnioffl r command line.

OPTIONS

-version

Displays the version of the omnioffl r command.

-help

Displays the usage synopsis for the omnioffl r command.

-idb

Selects the Data Protector Internal Database (IDB) for restore. If no additional options as -autorecover or -read are specified, the -idb option starts the IDB restore in the manual mode.

-autorecover

This option can be only used in combination with the -idb option.

Starts the IDB restore in the autorecovery mode. To use this mode, the IDB recovery file obdrindex.dat (the original or its duplicate) should exist on the Cell Manager.

-changedevhost *MAClientName*

This option can be only used in combination with the -idb and -autorecover options.

Specifies the hostname of the Data Protector Media Agent system to be used for the IDB restore instead of the Media Agent system specified in the IDB recovery file.

-read *OptionFile*

This option can be only used in combination with the -idb option.

Starts the IDB restore in the read mode using IDB restore parameters from the specified file. To use this mode, the IDB restore parameter file should be available on the local system. The file should reflect the current configuration of the Data Protector cell with regards to the Media Agent system, the backup (restore) device, and the backup media on which IDB backup image is stored.

AutorecoverOptions

-force

> ⚠ **Caution** This option removes archive log files.

Forces Data Protector to overwrite existing Internal Database files that reside at their original location. If you omit this option, only the missing files are recreated with data from the IDB backup images.

-session *SessionID*

This option can be only used in combination with the -idb and -autorecover options.

Omits selecting the last valid IDB backup session for the restore process, and instead selects the specified IDB backup session (full or incremental). Make sure the specified session is referenced in the IDB recovery file.

-save *OptionFile*

This option can be only used in combination with the -idb and -autorecover options.

Saves the IDB restore parameters retrieved in the autorecovery mode to the specified parameter file in order to enable starting the IDB restore with omnioffl r in the read mode later. Note that unless you specify the option -skiprestore , the IDB restore is also performed.

-skiprestore

This option can be only used in combination with the -idb and -autorecover options.

Skips starting the actual IDB restore process. Usually, you may want to specify this option together with the -save option.

-logview

This option can be only used in combination with the -idb and -autorecover options.

Displays the contents of the IDB recovery file.

-optview

This option can be only used in combination with the -idb and -autorecover options.

Displays the parameters used for the IDB restore session.

DeviceOptions

-name *LogicalDeviceName*

Parameter that specifies the logical device name.

-dev *PhysicalDevice*

Specifies the pathname of the device file. For example, c:\temp\dev1 , scsi1:0:0:0 , or /dev/tape0 .

> **Note** The Drive index number must be specified when restoring the IDB without an IDB recovery file, if the drive index is not 1. For more details, see Example 5.

-mahost *DeviceHostName*

Specifies the name of the client, where the restore device is attached and a Media Agent started.

-policy *LogicalDevicePolicy*

Specifies the policy ID for the device specified by the -dev option. Policy can be defined as:

1 (Standalone)

3 (Stacker)

5 (6300 magneto-optical jukebox)

6 (Exchange through cmd execution)

8 (GRAU DAS exchanger library)

9 (Silo medium library)

10 (SCSI exchanger)

11 (RSM exchanger)

-type *LogicalDeviceType*

Specifies the media type for the media in the device specified by the -device option. Media type numbers are defined as media class in the scsitab file. For location, see the help index “support of new devices”.

-ioctl *RoboticsSCSIAddress*

Specifies the pathname of the robotics control device file for library device. For example, c:\temp\roboticsdev , scsi1:2:0:0 , or /dev/dlt_robotics

-description *DeviceDescription*

This is an optional parameter that specifies the logical device description.

-blksize *BlockSize*

This is an optional parameter that specifies the block size the device is going to use when accessing media.

MediaOptions

-maid *MediumID*

Specifies the medium identification number of the medium that contains the object data; for example 8c04110a:3b0e118b:041c:0001 . If unknown is specified, each medium will be accepted as valid and restore will be attempted. Whole medium will be scanned for the requested object and it may take a very long time, if the object is not on the medium. Mount prompt in such case will request the next medium, without specifying the medium label.

-slot Slot [: *Flip*]

Specifies the slot identifier of the slot, where the required media is located, thus enabling Data Protector to automatically load media from the exchanger slots. Note that the sequence has to match the sequence in the list created using the -maid option.

-position *Segment* : *Offset*

Specifies the segment and offset position of the restore object data on the medium; for example 67:20 . If the position is not specified, the position 1:0 is assumed, thus prolonging the restore time. Note that the sequence has to match the sequence in the list created using the -maid option.

ObjectOptions

-filesystem *Client* : *MountPoint Label*

Selects the filesystem identified with *Client:MountPoint Label* for restore. Client determines the name of the system where the object was backed up. *MountPoint* specifies the mount point name of the volume to be restored (for example /C , /tmp , / , and so on). It must be in the same format as stored in the IDB. *Label* specifies the backup/restore objects description that uniquely defines an object (-filesystem computer.domain.net:/mount label)

-winfs *Client* : *MountPoint Label*

Selects the Windows filesystem identified with *Client:MountPoint Label* for restore. Client determines the name of the system where the object was backed up. *MountPoint* specifies the mount point name of the volume to be restored (for example /C , /tmp , / , and so on). It must be in the same format as stored in the IDB. Therefore, for example, on Windows systems C: translates into /C . Label specifies the backup/restore object's description that uniquely defines an object (-winfs computer.domain.net:/C: , and so on)

-rawdisk *Client Label* -section [*ToSection* =] *Section*

Selects the disk image identified by *Host* and *Label* for restore. Specifies the disk image section to be restored. To restore the section to a new section, include both the source and destination sections.

This option is available only for supported Windows systems.

-daid *DAID*

Specifies the identification number of the Disk Agent process that backed up an object. The identification number must be in the POSIX time format. You can obtain it by invoking the omnidb -session SessionID -detail command while the Data Protector Internal Database is available.

-merge

This option merges files from the backup medium to the target directory and replaces older versions that exist in the directory with newer (if they exist on the medium) files. Existing files are overwritten if the version on the medium is newer than the version on disk. No existing directory is deleted. If a directory or file doesn't exist on disk (but is on the backup medium) it is restored (created).

-overwrite

By default, or if the -overwrite option is specified, the already existent files on the disk are overwritten by the restored files.

-no_overwrite

If the -no_overwrite option is specified, only the files that do not exist on the disk are restored.

-move_busy

This option is used with the -omit_deleted_files or -overwrite option. A problem can occur if, for example, a file to be overwritten cannot be deleted because it is currently in use. If this option is specified, Data Protector moves busy file *filename* to *#filename* on UNIX systems (adding a hash- mark in front of the filename), or to *filename.001* on Windows system. On UNIX systems the original file can thus be deleted as the lock is transferred to the corresponding file starting with the #sign. For example, /tmp/DIR1/DIR2/FILE would be moved to /tmp/DIR1/DIR2/omniofflr#FILE. On Windows system the application only uses the newly-restored file after the file is restored and the system is restarted.

-omit_deleted_files

This option can only be used in combination with the -overwrite and -time options. For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

If this option is specified, Data Protector recreates the state of the backed up directory tree at the time of the last incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are not restored.

If this option is not specified, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

If you use this option in combination with the -as or -into option, carefully choose the restore location to prevent accidental removal of existing files.

-time *ObjectBackupStartTime*

This option should be used in combination with the -omit_deleted_files option.

Specifies the backup start time for the backup object you are restoring. *ObjectBackupStartTime* must be a value in the POSIX time format. You should obtain it by invoking the omnidb -session SessionID -detail command while the Data Protector Internal Database is available, where *SessionID* is implicitly defined by the -daid DAID option.

-var *OptName OptValue*

This option lets you specify a variable name and its value for proper operation of some platforms and integrations. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

-tree *TreeName TreeOptions*

Specifies the starting root directory of data restore. Note that this starting directory is also restored.

TreeOptions

-exclude *TreeName*

Specifies trees excluded from the restore.

-as *NewTreeName*

This is an optional parameter that restores the selected fileset as the specified tree. This parameter is of vital importance for the Disk Delivery disaster recovery, since without it the restore to the original location would be performed.

-into *NewTreeName*

This is an optional parameter that restores the selected fileset into the given directory. This parameter is of vital importance for the Disk Delivery disaster recovery, since without it the restore to the original location would be performed.

GeneralOptions

-keyfile *CSVFilePath*

This option can only be used in combination with the -idb option for offline restore of encrypted IDB backups. It specifies full path to the CSV file that stores the encryption key.
Example (Windows)
omnioffl.exe -idb -autorecover -force -keyfile ProgramData\OmniBack\Config\Server\export\keys\IDB-myserver.net-keys.csv
Example (Linux)
omnioffl.exe -idb -autorecover -force -keyfile /var/opt/omni/server/export/keys/IDB-myserver.net-keys.csv
For more information about the CSV file, refer omnikeytool.

-verbose

Specifies the verbose level of progress reporting.

-preview

Specifies that the preview mode of the restore is entered.

-report

Displays a report of the disaster recovery using the omnioffl command.

-target

Specifies the target system name which is different than the original.

-[no]ok[mediumlist]

By default the options are parsed and displayed so that the user can check them and confirm the start of restore. This means that the omnioffl command used from a script could not be executed because it would wait for the confirmation before starting the restore. This option has to be used to skip confirmation, thus enabling the execution of the omnioffl command from a script.

NOTES

The omnioffl command is available on Windows systems and Linux systems.

The omnioffl command does not support robotic loaders of backup media. You need to ensure the appropriate media is loaded into the specified backup devices. For this purpose, you can use the uma command on the system to which robotics is attached.

In computer clusters, execute the omnioffl command on the active cluster node.

EXAMPLES

The following examples illustrate how the omnioffl command works.

1. To restore the "c:/temp" directory of the system "computer.company.com" without the "c:/temp/vnc" directory, which was backed up using an Ultrium standalone backup device on a STK Ultrium backup medium, attached to the Cell Manager "cm.company.com", into the "c:/test/temp" directory, execute:

   omnioffl -verbose -name HP:Ultrium -dev scsi2:0:4:0C -mahost cm.company.com -policy 1 -type 13 -maid 9e03110a:3b5ee669:05ac:0001 -computer.company.com:/C C: -daid 996144004 -tree /temp -exclude /temp/vnc -into c:/test/temp

To get the logical device name and its SCSI address, execute:

```
devbra -dev
```

The output of the command looks something like this:

```
HP:Ultriumscsi2:0:4:0cLTO : HP LTO drive
```

"HP:Ultrium" is the logical device name of the backup device while "scsi2:0:4:0c" specifies the SCSI address of the device.

To obtain the medium ID (MAID), execute the omnidb command with the appropriate backup session ID:

```
omnidb -session 2013/05/06-1 -media
```

To obtain all backup session IDs for the winfs computer.domain.com:/C computer.domain.com [/C], execute:

```
omnidb -winfs computer.domain.com:/C "computer.domain.com [/C]"
```

To obtain the Disk Agent ID (DAID) and the object name, execute the omnimm command with the relative MAID:

```
omnimm -catalog 9e03110a:3b5ee669:05ac:0001
```

2. To perform a disaster recovery, using the Enhanced Automated Disaster Recovery (EADR) method, of the system "computer.company.com" (including its disk image sections E: and F:) using the standalone file device "E:\Devices\file_FR_EADR2.fd" and the Media Agent residing on the system "device.company.com", execute:

```
omniofflr -name "file_FR_EADR2" -dev "E:\Devices\file_FR_EADR2.fd" -policy 1 -type 7 -mahost rdevice.company.com -blksize 1024 -maid f178b
09b:4d6a83ce:0dd8:0001 -position 9:0 -winfs computer.company.com:"/C" "C:" -daid 1302093850 -tree / -overwrite -move_busy -rawdisk comp
uter.company.com "[Disk Image E, F]: computer.company.com" -section \\.\D:=\\.\e: -section \\.\E:=\\.\f: -daid 1302093851 -report 1 -debug 1-2
00 dr.txt
```

3. To restore the Data Protector Internal Database with omniofflr in the autorecovery mode, using the backup image created in the backup session "2013/04/12-44", using a different backup device attached to the Media Agent system "newmasys.company.com", to save the IDB restore parameters to the file "new_ma_option_file.dat", and to display the IDB recovery file contents, execute:

```
omniofflr -idb -autorecover -changedevhost newmasys.company.com -session 2013/04/12-44 -save new_ma_option_file.dat -logview
```

4. To restore the Data Protector Internal Database with omniofflr in the read mode to a different system "newcmsys.company.com", using the IDB restore parameters from the file "new_ma_option_file.dat", and to monitor restore progress details, execute:

```
omniofflr -idb -read new_ma_option_file.dat -verbose -target newcmsys.company.com
```

5. Consider a device configuration with two drives: drive 1 with path dev/rtape/tape37_BESTn and drive 2 with path dev/rtape/tape_74_BESTn. If we use drive 1 to restore the IDB by following the "Restoring the IDB Without IDB Recovery File", everything works fine. But if we use drive 2, the restore fails with "Cannot unload exchanger medium" error. So, if you use drive 2, you need to use the following:

```
-dev /dev/rtape/tape74_BESTn 2
```

Here, 2 represents the drive_index. The drive_index can be 2 or more depending on the number of drives.

6. To restore the Data Protector Internal Database with omniofflr in the read mode with saved archived log files for rollforward, using the IDB restore parameters from the file "idb_restore_parameter.dat", execute:
   1. Save the IDB restore parameters retrieved in the autorecovery mode to the specified parameter file (**idb_restore_parameter.dat**) in order to enable starting the IDB restore with omniofflr in the read mode later:
      ```
      omniofflr -idb -autorecover [-session YYYY/MM/DD-NN] -skiprestore -save idb_restore_parameter.dat
      ```
   2. Copy saved archive log files to server\db80\pg\pg_xlog
   3. Autorecover IDB from the saved parameter file:
      ```
      omniofflr -idb -read idb_restore_parameter.dat
      ```

SEE ALSO

omnidr(1M), omniiso(1), omnisrdupdate(1M), omniusb(1)

omniresolve

omniresolve - resolves a filesystem object or a list of filesystem objects and writes the results to the standard output or to a Unicode file
(this command is available on systems with any Data Protector integration component installed)

SYNOPSIS

omniresolve -version | -help

omniresolve { -files *filename* [*filename2* ...] | -inputfile *datafile* } [-verbose] [-unicodefile *outfile*]

DESCRIPTION

The omniresolve command reads the filesystem structures locating the physical disks (on Windows) or volumes (on UNIX) on which a filesystem object resides. If the files reside on a logical volume which is a part of a volume group (disk group), all volumes in a volume group are displayed.

You can list the filesystem objects to be resolved either in the CLI (on UNIX and Windows systems) or using a Unicode file (on Windows systems only). The results are written to standard output (on UNIX and Windows systems) or to a Unicode file (on Windows systems only).

OPTIONS

-version

Displays the version of the omniresolve command.

-help

Displays the usage synopsis for the omniresolve command.

-files *filename* [*filename2* ...]

Resolves a list of files separated by spaces and writes the results to the standard output.

-inputfile *datafile*

Resolves all objects listed in *datafile* in and writes the results to the standard output.

Note that on Windows systems, if *datafile* is in the Unicode format, the output is by default written to the file uniout.dat . You can redirect the output to a different file by using the -unicode option.

-verbose

Provides a more detailed report (displaying details such as WWNs, LUNs, or LDEVs) using SCSI inquiry on physical disks.

-unicodefile *outfile*

Defines the file to which the output is redirected if the input file is a Unicode file.

NOTES

The resolve process requires root permissions on UNIX systems to get access to the disk device files. Therefore, the SUID flag is set on for omniresolve .

EXAMPLES

1. To resolve a list of three files ("system01.dbf", "redo01.log", and "control01.ctl") located in "/opt/orahome/oradata/dbname", execute:

   omniresolve -f '/opt/orahome/oradata/dbname/system01.dbf' '/opt/orahome/oradata/dbname/redo01.log' '/opt/orahome/oradata/dbname/control01.ctl' -v

omnirsh

omnirsh - returns the hostnames of the physical and virtual nodes for the specified cluster hostname, or returns the cell information stored in the cell_info file on the specified cluster
(this command is available on the Data Protector Cell Manager)

SYNOPSIS

omnirsh -version | -help

omnirsh *cluster_hostname* { INFO_CLUS | INFO }

DESCRIPTION

The omnirsh command returns the hostnames of the physical and virtual nodes for the specified cluster hostname, together with the flag indicating whether a specific node is a physical node or virtual node. The command can also be used to list the contents of the cluster cell_info file.

OPTIONS

-version

Displays the version of the omnirsh command.

-help

Displays the usage synopsis for the omnirsh command.

cluster_hostname

Sets the hostname of the cluster for this command.

INFO_CLUS

Lists the hostnames of the physical and virtual nodes for the specified cluster hostname, together with the flag indicating whether a specific node is a physical node or virtual node. Flag value 1 indicates a physical node, whereas flag value 8 indicates a virtual node.

INFO

Displays the contents of the cell_info file for the system specified by the *cluster_hostname* parameter. The file resides on the Cell Manager on server configuration files location in the cell directory.

SEE ALSO

omniclus(1M)

omnisetup.sh

omnisetup.sh - installs or upgrades a Data Protector Cell Managers, Installation Servers, and UNIX client systems locally; installs and removes patch bundles.
(this command is available on the Data Protector installer bundle or is provided together with a patch bundle)

SYNOPSIS

omnisetup.sh -version | -help

omnisetup.sh [-source *directory*] [-server *name*] [-install *Component_list*] [-CM] [-IS] [-bundleadd *BundleTag* | -bundlerem *BundleTag*] [-inetport inetPort]

[-accept_obsolescence] [-no_telemetry]

[-compname compName] [-proxyhost ProxyAddress/ProxyURL] [-proxyport proxyPort] [-proxyuser proxyUserName] [-proxypasswd proxyPassword]

[-secure_data_comm *secureDataComm*] [-auditlog *auditLog* [-retention_months auditlogRetention]]

omnisetup.sh [-bundleadd BundleTag] [-installpatch] [-extractpacket] [-os osname] [-platform platformname] [-install Component_list] [-targetfolder / directory]

Component_list

cc = User Interface

da = Disk Agent

ndmp = NDMP Media Agent

ma = General Media Agent

sap = SAP R/3 Integration

sapdb = SAP MaxDB Integration

oracle8 = Oracle Integration

sybase = Sybase Integration

ssea = P9000 XP Agent

informix = Informix Integration

lotus = Lotus Integration

db2 = DB2 Integration

smisa = 3PAR SMI-S Agent

netapp = NetApp Storage Provider

vepa = Virtual Environment Integration

StoreOnceSoftware = StoreOnce software deduplication

autodr = Automatic Disaster Recovery

docs = English Documentation (Guides, Help)

jpn_ls = Japanese Documentation (Guides, Help)

fra_ls = French Documentation (Guides, Help)

chs_ls = Simplified Chinese Documentation (Guides, Help)

osname platformname

osname	platformname
linux-oes-x86-64	x86_64
linux-x86-64	x86_64
hp-ux-113x	sia64
aix-51	rs6000
solaris-10	sparc
solaris-9	sparc
solaris-8	sparc
solaris-10	x86_64

Note that the osname and platformname specified in the command should match from the above list.

DESCRIPTION

The command first checks if Data Protector is already installed on the system.

New Installation or Re-installation of the same version of Data Protector

If Data Protector is not installed, then the command, depending on the selected options, installs the Cell Manager, Installation Server, or every Data Protector software component specified with the -install option. If none of these options are specified, the command issues a prompt for every Data Protector software component supported on the current system OS. Using this prompt, software components supported on the current system OS can be confirmed or rejected for installation, or the execution of the command can be canceled. There is no such prompt if the -install option is specified.

Upgrade from an earlier version of Data Protector

To upgrade your cell from the earlier versions of Data Protector, proceed as follows:

- Upgrade the Cell Manager
- Upgrade the Installation Server
- Upgrade the clients

To upgrade all Data Protector components on the system, run omnisetup.sh without options. If the Installation Server is installed together with the Cell Manager, or if it is installed without client components, it is upgraded automatically during the Cell Manager upgrade.

If the Installation Server is installed with the client components, it is removed during the Cell Manager upgrade. In this case, a new Installation Server must be installed using the -IS option, after the upgrade finishes.

To add a client to the Cell Manager, specify the -install option. If the client not residing on the Cell Manager is to be upgraded, the -install option does not need to be specified. In this case, the setup selects the same components as were installed on the system before the upgrade without issuing a prompt.

In all cases (new installation, re-installation, or upgrade), the following applies when using this command:

- When using the -install option, the software components not supported on the current system OS and mistyped software components are skipped.
- After the client (re-)installation or upgrade is finished, the system is imported to a Data Protector cell if the -server option was set, or if the /etc/opt/omni/client/cell_server (HP-UX, Solaris, and Linux clients) or the /usr/omni/config/cell/cell_server (other UNIX clients) file exists on the system.
- The first time any software component is selected for installation or re-installation, the core component is automatically installed (or re-installed). Similarly, the first time any integration software component is selected for installation or re-installation, the core-integ component is automatically installed (or re-installed).

Installation and removal of Data Protector Patch Bundles

If Data Protector is already installed on your system, you can also install a Data Protector patch bundle (a set of Data Protector patches) on this system by using the -bundleadd option. It is not possible to install individual patches from the patch bundle.

You can install a Data Protector patch bundle only on the Installation Server and the Cell Manager. If the installation fails or you stopped it, you can continue with the installation and install the rest of the patches (on Linux systems only), roll installed patches back to the previous patch level, or exit the installation without completing it.

You can remove the Data Protector patch bundle using the `-bundlerem` option. After removing the patch bundle, the base Data Protector release version remains on the system.

In all cases (new installation, re-installation, or upgrade), the following applies when using this command:

- option `-bundleadd` and `-installpatch` on client hosts will upgrade the components installed on the client
- option `-extractpacket` can be used to extract the `packet.Z` files for components that can be installed on client hosts.

OPTIONS

-version

Displays the version of the `omnisetup.sh` command.

-help

Displays the usage synopsis for the `omnisetup.sh` command.

-source *directory*

Sets the location of the Data Protector installation files (DVD-ROM mountpoint). If this option is not specified, the current directory is set as the location of Data Protector installation files.

-server *name*

Sets the hostname of the Cell Manager of the cell to which the installed or upgraded client is to be imported after the installation or upgrade.

If this option is not specified, and the `/etc/opt/omni/client/cell_server` (HP-UX, Solaris, and Linux clients) or the `/usr/omni/config/cell_server` (other UNIX clients) file does not exist on the system, the installed or upgraded client is not imported to any cell and has to be imported manually.

-install *Component_list*

Sets Data Protector software components that you want to install or upgrade on the current system. If more than one software component is to be installed or upgraded, a listing of software components, delimited by comma (without spaces) must be entered as the argument. If this option is not specified (except for the case when the client not residing on the Cell Manager needs to be upgraded), the command issues a prompt for every Data Protector software component supported on the current system OS; prompting whether to install or upgrade certain Data Protector software component or not.

If the client is to be upgraded, this option does not need to be specified. In this case, the setup selects the same components as were installed on the system before the upgrade without issuing a prompt.

-CM

Installs/upgrades the Data Protector Cell Manager.

-IS

Installs/upgrades the Data Protector Installation Server with *all* remote installation packages.

Use `-IS` if you install from the DVD-ROM.

Use `-IS1` when installing from the *first* Installation Server CD-ROM and `-IS2` when installing from the *second* Installation Server installation CD-ROM.

If you have copied the `DP_DEPOT` directory from *both CD-ROMs to one directory* on your local disk, use `-IS1 -IS2` .

Note that the Installation Server can be upgraded only after the Cell Manager in the Data Protector cell is upgraded.

-bundleadd *BundleTag*

Installs the Data Protector patch bundle (a set of Data Protector patches) on the Cell Manager, the Installation Server, and the client.

-bundlerem *BundleTag*

Removes the Data Protector patch bundle (a set of Data Protector patches) from the Cell Manager and the Installation Server.

After removing the patch bundle, the base Data Protector release version remains on the system.

-inetport inetPort

This option is used to specify Inet port value during new or fresh installation only. The value mentioned as a part of command line argument will override the socket.dat file. The Inet port value cannot be changed during bundle installation or upgrade. The default Inet port value is 5565 .

[-installpatch]

Installs the Data Protector patches on the Cell Manager, Installation Server, and client (only the components installed in the client are upgraded).

[-extractpacket]

Extracts the packet from Data Protector installation package.

[-os osname]

Extract packet for specific operating system.

[-platform platformname]

Extract packet for specific platform.

[-targetfolder]

Extracts the packets specified in install option to the the targetfolder . If targetfolder is not specified, packets will be extracted under packets folder under current directory.

[-accept_obsolescence]

With this option the user can accept the obsolescence information as understood and agreed.

[-no telemetry]

By default, this option opts out the user from the telemetry subscription.

-telemetry : This option is used to configure the telemetry registration.

- -compname : This option is used to specify the company name.
- -proxyhost : This option is used to specify the proxy host URL or IP address to access network.
- -proxyport : The option is used to specify the port of the proxy server.
- -proxyuser : This option is used to specify the user name to connect to the proxy server.
- -proxypasswd : This option is used to specify the password for the given user name.
- -no_telemetry : This option can be used to skip the telemetry data entry.

> **Note** Telemetry options are only valid for Cell Manager installation.

-secure_data_comm<*secureDataComm*>

This option enables secure data communication. The <*secureDataComm*> is either 0 or 1. Default is 0.

- <*secureDataComm*> of 0 disables secure data communication and sets the global variable "EnableSecureDataCommunication" to 0.
- <*secureDataComm*> of 1 enables secure data communication and sets the global variable "EnableSecureDataCommunication" to 1.

-auditlog <*auditLog*> [-retention_months <*auditLogRetention*>]

This option enables audit log. The <*auditLog*> is either 0 or 1. Default is 0. You can also specify how long (number of months) audit log files are kept before being purged. Audit logs are purged on a monthly basis, meaning that the session information for an entire month is removed after the specified number of months. By default, the audit log is retained for 7.5 years (90 months). If the value is set to 0, audit log purging is disabled. If the -retention_months option is not used, then a default value of 90 months is set. There is no limit to specify maximum value for audit log retention, however, Micro Focus recommends to limit the value to 99 years (1188 months).

- <*auditLog*> of 0 disables audit log and sets the global variable "AuditLogEnable" to 0.
- <*auditLog*> of 1 enables audit log and sets the global variable "AuditLogEnable" to 1.
- <*auditLogRetention*> specifies how long (number of months) audit log files are kept before being purged. Audit logs are purged on a monthly basis, meaning that the session information for an entire month is removed after the specified number of months. By default, the audit log is retained for 90 months. If the value is set to 0, audit log purging is disabled. There is no limit to specify maximum value for audit log retention, however, Micro Focus recommends to limit the value to 99 years (1188 months). The <*auditLogRetention*> sets the global variable "AuditLogRetention" value to the number of months specified.

NOTES

This command requires that the

- DP_DEPOT and LOCAL_INSTALL folders are copied to the disk.

Before running the command make sure that no Data Protector backups or restores are running on the system. The command must be executed using the default POSIX ksh or pdksh shell.

EXAMPLES

1. To upgrade a system, execute:

   ```
   omnisetup.sh
   ```

2. To install or re-install the General Media Agent, Disk Agent, 3PAR SMI-S Agent, and SAP R/3 Integration software components, execute:

   ```
   omnisetup.sh -install ma,da,smisa,sap
   ```

3. To install the Cell Manager and Installation Server, mount the DVD-ROM and execute the following command from the LOCAL_INSTALL directory:

   ```
   omnisetup.sh -CM -IS
   ```

4. To install the Data Protector patch bundle b701 on the Cell Manager, execute:

   ```
   omnisetup.sh -bundleadd -CM
   ```

5. To upgrade to the release bundle 1003, execute:

   ```
   ./omnisetup.sh -bundleadd b1003
   ```

   This command installs the release bundle 1003 in Cell Manager, Installation Server, and client hosts.

6. To perform a patch upgrade, execute

   ```
   /omnisetup.sh -installpatch
   ```

   The command installs the patch on Cell Manager, Installation Server, and client hosts.

7. To extracts the packet.Z files of da and ma components for linux operating system and x86-64 platform, execute:

   ```
   ./omnisetup.sh -extractpacket -os linux-x86-64 -platform x86_64 -install da,ma
   ```

8. To extract the packet.Z files of da and ma components for solaris-10 operating system and sparc platform, execute:

   ```
   ./omnisetup.sh -extractpacket -os solaris-10 -platform sparc -install da,ma
   ```

9. To register telemetry, run the following commands:

   ```
   omnisetup.sh [-compname xyz] [-proxyhost server.domain.com] [-port 8080] [-user root] [-passwd MyPassword]
   ```

SEE ALSO

ob2install(1M), omnigui(5), omniintro(9), omnimigrate.pl(1M), omniusers(1), upgrade_cm_from_evaa(1M)

omnisrdupdate

omnisrdupdate - updates the System Recovery Data (SRD) file

SYNOPSIS

omnisrdupdate -version | -help

omnisrdupdate [-session *FSSessionID* [*IDBSessionID*]] [-cell *CMName*]

[-host *ClientName*] [-location *Path_1* [-location *Path_2* ...]]

[-asr] [-use_raw_object] [-anyobj]

DESCRIPTION

The omnisrdupdate command is used to update System Recovery Data (SRD) file. An SRD file, which is a text file in the Unicode (UTF-16) format, is generated during CONFIGURATION backup, and saved to the Cell Manager to the SRD files directory.

The SRD filename is identical to the name of the system where it was generated, for example computer.company.com . After the CONFIGURATION backup, the SRD contains only the system information required for system configuration and installation of the operating system needed for disaster recovery. To be able to perform a disaster recovery without a functioning Data Protector Internal Database (IDB), additional information about backup objects and corresponding media must be added to the SRD by running this command. The name of the updated SRD file is recovery.srd .

OPTIONS

-version

Displays the version of the omnisrdupdate command.

-help

Displays the usage synopsis for the omnisrdupdate command.

-session *FSSessionID* [*IDBSessionID*]

Specifies IDs of the backup sessions that serve as the basis for updating the SRD file. All object backed up in the specified sessions and included in the SRD file are used for the update. This option must be specified when the omnisrdupdate command is run interactively, and must be omitted when the omnisrdupdate command is run from a post-exec script. In the latter case, Data Protector automatically obtains the required information from the environment.

If you are updating the SRD file for a Data Protector client, specify the *FSSessionID* argument for the most recent full or incremental filesystem backup session that involves the entire client. If you are updating the ISO image file for the Data Protector Cell Manager, additionally specify the *IDBSessionID* argument for an appropriate full or incremental Data Protector Internal Database backup session.

CAUTION: The specified Data Protector Internal Database backup session must be a session that was run after the specified filesystem backup session had completed. To ensure the highest consistency of the included data, the time frame between both sessions' start times should be minimal.

Updating the SRD file succeeds only when all critical backup objects (as specified in the SRD file) were actually backed up in the specified sessions. To view which objects are marked as critical for the SRD update, open the SRD file in a text editor. All critical objects are listed under the -section objects section. Note that the database is represented as "/".

-cell *CMName*

Specifies the Cell Manager to connect to in order to obtain the required information about backup objects and the corresponding media from the IDB.

If this option is omitted, Data Protector automatically obtains the required information from the current environment.

-host *ClientName*

Specifies the system for which the SRD file is to be updated.

If this option is omitted, Data Protector automatically obtains the required information from the current environment.

-location *Path*

Specifies the location where the updated SRD file is saved. A local directory or a network share can be specified. To create several copies of the updated SRD file on different locations, use multiple -location Path argument pairs. It is recommended that, in addition to the Cell Manager, the updated SRD file is copied to several safe storage locations as a part of disaster recovery preparation policy. For example, assuming that this storage location is considered safe, you can copy the updated file to the SRD files directory on the Cell Manager.

When the omnisrdupdate command is run from a pre-exec or post-exec script, this option can be omitted. In this case, the omnisrdupdate command updates System Recovery Data internally in the Data Protector session, but does not save it to any SRD file. System Recovery Data updated in such a way can only be used for subsequent processing within the same session.

If you are running the omnisrdupdate command in a pre-exec or post-exec script, do not add a backslash at the end of the path.

-asr

If specified, the ASR archive file (a collection of files required for proper reconfiguration of the replacement disk packed in a single archive file) is downloaded from the Cell Manager and ASR files are extracted and stored to all destinations, specified by the -location option. At least one -location option must be specified otherwise the -asr option is ignored. If the ASR archive file on the Cell Manager does not exist, the omnisrdupdate command fails and the SRD file is not updated.

-use_raw_object

If the specified backup session contains both filesystem and disk image backup objects for the same volume, this option specifies that a disk image backup object should be used. If this option is not specified, filesystem backup objects have a priority. If only one backup object for the same volume is present in the specified backup session, this option is ignored.

-anyobj

Enables you to create a recovery image even if the specified backup session does not contain all client volumes. Note that all host critical volumes must be part of the specified backup session:

- the boot and system volumes
- the Data Protector installation volume
- the volume where the CONFIGURATION object is located
- the Active Directory database volume (in case of an Active Directory controller)
- the quorum volume (in case of a Microsoft Cluster)

NOTES

- The omnisrdupdate command is available on Windows and Linux systems only.
- If the BTRFS volume is detected, you get the following **Warning** message:

  Warning: BTRFS volume detected. Make sure that you have included all the BTRFS sub volumes in the specified version.

EXAMPLES

1. To update the SRD file for the Data Protector Cell Manager with the backup object information belonging to the sessions "2013/05/02-5" and "2013/05/02-6", execute:

   ```
   omnisrdupdate -session 2013/05/02-5 2013/05/02-6
   ```

   To obtain the sessions IDs, execute the omnidb command with the -session option. To obtain the latest session ID, execute:

```
omnidb -session -latest
```

2. To update the SRD file for a Data Protector client with the backup object information which belongs to the session "2013/05/02-5" and save the updated SRD file on a diskette as well as to the network share "srdfiles" on the system with the hostname "computer", execute:

```
omnisrdupdate -session 2013/05/02-5 -location A: -location //computer/srdfiles
```

3. To update the first diskette from the ASR set for a Data Protector client with the backup object information and ASR files which belong to the session "2013/05/02-5", ensure the first diskette is not write-protected, insert it into the floppy disk drive, and execute:

```
omnisrdupdate -session 2013/05/02-5 -location A: -asr
```

SEE ALSO

omnidr(1M), omniiso(1), omniofflr(1M), omniusb(1)

omnisv

omnisv - starts or stops the Data Protector services or daemons, displays their status, or turns the maintenance mode on or off (this command is available on the Data Protector Cell Manager)

Synopsis

omnisv -version | -help

omnisv -status

omnisv { -start | -stop | -start_mon }

omnisv -maintenance [*GracefulTime* | -mom | -stop | -mom_stop | -cmmdb_force]

omnisv -restart

Description

The omnisv command enables you to start or stop the Data Protector services or daemons, display their status, or turn the maintenance mode on and off.

omnisv can start or stop the CRS, MMD, KMS, hpdp-idb, hpdp-idb-cp, hpdp-as, and omniinet services on the Cell Manager. Note that the MMD service can only be started or stopped locally on the Cell Manager with the MMDB.

On Linux Cell Managers, the omnisv command also adds the omnitrig process to the cron table and schedules it (on Windows systems, the omnitrig command is started by the CRS service). You can modify the scheduler granularity by changing the SchedulerGranularity global option. By default, the granularity is 15 minutes, but it can be modified to 1 minute.

On Windows Cell Managers, omnisv also starts he Inet service (the Data Protector Inet program (/opt/omni/lbin/inet), which is on Linux systems started by the system inet daemon when an application tries to connect to the Data Protector port; normally, these daemons are started automatically during the system startup).

The omnisv command can also initiate maintenance mode, which prepares your environment for maintenance tasks on Cell Manager that require preventing changes to the Internal Database. The JCE database is now a part of this maintenance. The Quartz scheduler remains paused during the maintenance and the scheduled jobs do not get triggered.

Options

-version

Displays the version of the omnisv command.

-help

Displays the usage synopsis for the omnisv command.

-status

Displays the status and PID of the services.

-start

Starts the Data Protector services or daemons. On Linux systems, it also adds the omnitrig command to the cron table, thus configuring it as a cron job.

-stop

Stops the Data Protector services or daemons. On Linux systems, it also removes the omnitrig command from the cron table.

> **Note** Do not run this command to stop services while the Home Context is opened. Home Context prevents omnisv from stopping the application server.

When used with the -maintenance option, -stop exits the maintenance mode.

-start_mon

Waits in loop until the CRS, MMD, KMS, hpdp-idb, hpdp-idb-cp, and hpdp-as services are up and running. If any daemon or service stops, omnisv exits with an exit code 1. Exit code 0 means that all relevant Data Protector daemons/services are up and running, whereas the exit code 1 means that at least one of the relevant Data Protector daemons or services is not running.

-maintenance

Initiates the maintenance mode. The optional *GracefulTime* parameter overrides the MaintenanceModeGracefulTime global option and specifies the seconds given to the Data Protector services to abort the running sessions. The JCE database is now a part of this maintenance. The Quartz scheduler remains paused during the maintenance and the scheduled jobs do not get triggered.

-mom

Initiates the maintenance mode in the entire MoM environment.

-mom_stop

Exits the maintenance mode in the MoM environment.

-restart

Restart option starts and stops all Data Protector services.

-cmmdb_force

This option puts IDB in maintenance mode in a Centralised Media Management Database (CMMDB) environment.

Notes

On Windows systems, only the users in the Data Protector admin group can execute this command. On Linux systems, only the root user can execute this command. It is not possible to start or stop services in clusters using this command.

Examples

Put IDB in maintenance mode

Run one of the following commands:

- omnisv -maintenance <GracefulTime> -cmmdb_force
  The optional GracefulTime parameter overrides the global option (MaintenanceModeGracefulTime) and specifies the seconds given to the Data Protector services to abort the running sessions.
- omnisv -maintenance -cmmdb_force
  In this command, the GracefulTime parameter is not used. Therefore, the Data Protector services abort the running sessions based on the value of global option (MaintenanceModeGracefulTime). By default, the time is set to 300 seconds.

Exit the maintenance mode

Run the following command:

omnisv -maintenance -stop

omnitrig

omnitrig - Triggers daily maintenance jobs and manages the Quartz scheduler. (This command is available on the Data Protector Cell Manager.)

SYNOPSIS

omnitrig -version | -help

omnitrig [-start] [-log]

omnitrig -stop

omnitrig -run_checks

DESCRIPTION

The omnitrig command triggers daily maintenance jobs and manages the Quartz scheduler.

OPTIONS

-version

Displays the version of the omnitrig command.

-help

Displays the usage synopsis for the omnitrig command.

-start

Adds the omnitrig command to the cron table and triggers it. This option also starts the Quartz scheduler.

The daily maintenance jobs will be run.

-log

If this option is specified, the omnitrig will save information about each start of the omnitrig command and the maintenance jobs started by the omnitrig command into the Data Protector log files directory to the omnitrig.log file.

-stop

Removes the omnitrig command from the cron table. This option pauses triggering of jobs from the Quartz scheduler.

The daily maintenance jobs will not be run.

-run_checks

Starts checks for the following Data Protector notifications: IDB Space Low, Not Enough Free Media, Unexpected Events, Health Check Failed, IDB Limits, IDB Backup Needed, License Will Expire, License Warning, and User Check Failed (if configured) every day at 12:30 P.M.

Starts the check for the IDB Reorganization Needed notification every Monday at 12:30 P.M.

You can change the time of these checks or disable them by changing the DailyCheckTime global option.

SEE ALSO

omnihealthcheck(1M), omnirpt(1)

omniwl.pl

omniwl.pl - can be used for bulk modification of filesystem backup specifications (datalists). The input data for modifying specifications must be present in a CSV file, with semicolon (;) as the delimiter and double quotes (") as text separator.

This command is available only on the Data Protector Cell Manager.

SYNOPSIS

omniwl.pl –file <filename> {-datadir <directory_name>| -replace}

DESCRIPTION

The omniwl.pl command allows you to modify multiple backup specifications. The input for modifying specifications must be present in a CSV file, with semicolon (;) as the delimiter. It is recommended that you use a spreadsheet application to create the input document, and subsequently export the document as a CSV file with semicolon as the delimiter.

When you execute the omniwl.pl command the specifications that need to be modified and operations that need to be performed on them are read from the CSV input file. The modified specifications can be saved in the original location (-replace) or to alternative one (-datadir). In case of -replace option the original specifications are overwritten.

The input document must be accurate for the correct execution of the command. Ensure that you read and understand the Creating the input document section before you create the input document.

> **Note**: Perl is installed with Data Protector. You do not need to install it separately. Only Perl that is available with Data Protector is supported.

OPTIONS

-file <file_path_name>

This option points to the CSV file.

-datadir <directory_name>

The directory where the modified specifications are saved. If you use -datadir in a MoM environment while editing datalists from multiple Cell Managers in a single input document, then ensure that all of the datalists have unique names.

-replace

The original specifications are overwritten.

INPUT DOCUMENT

This section describes the format and rules for creating the input document.

- **Input document format**: This section describes the columns that must be present in the input document.
- **UTF-8 support**: This section describes the supported encoding formats for the CSV file.
- **Usage of wildcard characters and multiple values**: This section describes the columns that support the usage of wildcard characters and multiple values.
- **Rules for the usage of quotes**: This section describes the rules for the usage of quotes in the input document.

Input document format

The input document may contain multiple rows. Each row contains details of one client. Ensure that the column headings are capitalized. Here is a sample input document format from a spreadsheet editor:

CELL MANAGER	SPECIFICATION	CLIENT	MOUNTPOINT	DESCRIPTION	OPTION	VALUE
computer1.company.com	new_backup_1	MOD computer1.company.com	/		tree	(/data1/file1)
computer2.company.com	new_backup_2	MOD computer2.company.com	/	*	exclude	(/data1/file2)

View the CSV format of the above document in the CSV format section.

The input document column description is listed below:

- **Cell Manager**: This column should provide the Cell Manager host name. A single value can be specified. By default,Data Protector uses fully qualified domain names for Cell Manager and clients in the backup specifications. If you specify an IP address or an alias name, the `omniwl.pl` command will not resolve it, and the specified client may not be found.

Example: computer.company.com

- **Specification**: This column should provide the filesystem backup specification name.

Example: new_backup_1

- **Client**: This column should provide the operation, followed by the host name of the target client. If a valid operation is not present before the host name, an error is displayed. The operation and host names must be separated by single space. The supported operations are DEL, ADD, and MOD. Note that the operator names must be capitalized. The description of each operation is listed here:
  - If the operation is DEL, the complete client section (mountpoint or full host) is deleted. If the specification remains without a single object, a warning is displayed.
  - If the operation is ADD, then the client section will be created if it does not exist. If the client section is present, an error message is displayed.
  - If the operation is MOD, you can specify the Option that needs to be modified. Ensure that you specify the Value.
  - Unless the default value is used for the description field (empty description field) MOD and DEL operations do not require the target client to be a part of the Cell Manager. The ADD operation always requires a valid Cell Manager client.

Example: MOD `computer1.company.com`

- **Mountpoint**: This column should provide the mountpoint name. For full host backups, you must leave this column blank.

Examples: `C:\<mountpoint>` and `/C:\<mountpoint>`

- **Description**: For full host backups, the default description is a full client name. If the field is empty, the default value is taken. For file system backups, the default value for Windows is *mountpoint, and the volume label enclosed in brackets*. The default value for Linux or Unix is the *mountpoint*.

Windows example: /I: [New Volume]

Unix/Linux example: /tmp

- **Option**: This column should provide the option to be modified. The option and value fields must be specified in JSON format. If DEL is specified at the beginning, the value is ignored, and the option is deleted from the specification. The following options are supported:

JSON format	Data Protector specification format
tree	-trees
exclude	-exclude

- **Value**: This column should provide the values that need to be modified. Multiple values can be specified by enclosing them in parentheses, and separating them using a comma (,). For overwriting the list value, specify the equal sign (=) at the beginning. Duplicate values are not allowed.

An example of the Option-Value pair is shown below:

OPTION	VALUE	OPTION	VALUE
tree	(/tmp,/home/file1,DEL/home/work)	exclude	=(/var/opt)

When the omniwl.pl command is executed with the above Option-Value pair, /tmp and /home/file1 is added, and /home/work is deleted from the tree section. The exclude section is overwritten with the new value, /var/opt .

CSV format

The CSV format of the sample input document is shown here:

```
CELL MANAGER;SPECIFICATION;CLIENT;MOUNTPOINT;DESCRIPTION;OPTION;VALUE
computer1.company.com;new_backup_1;MOD computer1.company.com;/;;tree;(/data1/file1)
computer2.company.com;new_backup_2;MOD computer2.company.com;/;*;exclude;(/data1/file2)
```

UTF-8 support

UTF-8 and plain ASCII encoding formats are supported for the input document. If Microsoft Excel is used for editing the input document, exporting the document to the CSV format with UTF-8 format may not work as expected. Therefore, Excel is not recommended. Plain text editors are also not recommended, since using and editing CSV files from text editors may result in errors. But, OpenOffice Calc can handle UTF-8 documents correctly. Therefore, it is recommended that you use this tool to convert the input document into the CSV format.

Wildcard and multiple value support

- The Specification, Client, Mountpoint, and Description fields support wildcard characters.
- The Value field supports multiple values.
- If the asterisk symbol (*) is specified, any sequence of characters is matched. For

Example: If ***p*** is specified in the Client field, all the clients that have "p" in their names are considered for the operation.

- If the question mark symbol (?) is specified, any single character will be matched.

Example: If **backup?** is specified in the Specification field, all the specification names that have "backup followed by any character" are considered for the operation.

- In the Specification field, wildcard patterns are matched against the specifications present on the Cell Manager.
- In the Client field,
  - If MOD or DEL is specified, wildcard patterns are matched against the client section in the specification, even if host names and mountpoints are not present in the Cell Manager. Exception to this rule is when the Description field is blank. Then, the default value is extracted from the existing host and mountpoint. Therefore, wildcard patterns in the Mountpoint and Client fields are matched only against existing clients on the Cell Manager and the respective mountpoints. For more details, see the example Deleting the client section using wildcards.
  - If ADD is specified, wildcard patterns are not allowed in the Description field. Wildcard patterns in the Client field are matched against the existing clients on the Cell Manager. Wildcard patterns in the Mountpoint field are matched against the existing mountpoints from clients that belong to the Cell Manager. For more details, see the example Adding the client section using wildcards.

Input document rules

- The comma (,) is used as the separator for list values.
- List values are supported only in the Value field. The list values must be specified in a parentheses. Even if there is only one list value, it must be enclosed in parentheses.
- The DEL command is supported in the Option and Client fields. It must be used before the list values.
- Option and Value fields must not be empty. The only exception is when ADD or DEL is specified before the client name or the option name, or when DEL is specified before the option name.

Rules for the usage of quotes in field values

- For the Specification, Client , Mountpoint, and Description fields, the asterisk and the question mark symbols are reserved symbols. Therefore, these symbols must be enclosed in quotes if they are part of the string.
- In the Value field, strings that contain comma (,) must be double quoted.
- The list values have to be quoted for each list element separately.
- In the Client field, ADD, MOD and DEL followed by a space at beginning are reserved keywords. But, they don't have to be quoted if they are part of the host name, because host names cannot have spaces.

  Examples: ADD host1.company.com , MOD DEL* , DEL DEL.company.com .

- In the Value field, DEL followed by a space at the beginning is a reserved keyword. Therefore, if DEL followed by a space is part of a string, the content has to be double quoted. The same rule applies for the usage of comma in the string.

  Example: If the file name is *DEL File*, the file name should be *"DEL File"* in the CSV file.

Rules for the usage of quotes in CSV

- If a column delimiter or a double quote character is included in the fields, the entire field content has to be double quoted. For instance, *abc;* must be changed to *"abc;"*.
- If any string has double quotes, the double quotes also have to be doubled. For instance,*abc"test"* must be changed to *"abc""test"""*. After doubling all double quotes, the resulting string must be enclosed in double quotes.

In the Value field, list elements have to be quoted according to the CSV rules with comma as the separator. List elements that have characters like comma have to be quoted first.

Example: If the list elements are:

/tmp

/tmp,coma

/file"quotes"

The list elements must be represented as /tmp,"/tmp,coma","/file""quotes""" .

EXAMPLES

This section has a sample specification, an input document to modify the specification, and a modified specification after the command is executed.

Executing the command with the input document

Consider that you have named the input document as *Modifications.csv*. To update backup specifications with the changes specified in this file, and to save the new specifications to the directory named *ModifiedSpecifications*, execute the following command:

For Windows

```
cd <Data_Protector_home>/bin
```

```
perl omniwl.pl –file C:\Modifications.csv –datadir C:\ModifiedSpecifications
```

For UNIX

```
cd /opt/omni/lbin
```

```
omniwl.pl –file /tmp/Modifications.csv –datadir /tmp/ModifiedSpecifications
```

Modifying the `tree` and `exclude` sections of the specification

In this example, the tree and exclude sections of the specification "new_backup_1" are modified.

Original specification

```
FILESYSTEM "/" comp.company.com:"/"
{
-trees
"/e"
"/var"
"/home/work"
-exclude
"/e/restore"
"/e/target"
}
```

Input document

CELL MANAGER	SPECIFICATION	CLIENT	MOUNTPOINT	DESCRIPTION	OPTION	VALUE

comp.company.com	new_backup_1	MOD comp.company.com	/		tree	(/tmp,/home/file1,DEL/home/wor

When the omniwl.pl command is executed with the above input document, /tmp and /home/file1 is added, and /home/work is deleted from the tree section. Also, /var/opt is added in the exclude section, and the old values are deleted.

Modified specification

```
FILESYSTEM "/" c3po.hermes.si:"/"
{
-trees
"/e"
"/var"
"/tmp"
"/home/file1"
-exclude
"/var/opt"
}
```

Deleting the client section using wildcards

In this example, wildcards are used in the input document to delete client sections in the specification.

Consider a Cell Manager computer1.company.com that has 2 clients: computer2.company.com , and computer3.company.com .

Original specification

This specification has one client section in which the host name does not belong to the Cell Manager.

```
FILESYSTEM "/" server1.company.com:"/"
{
-trees
"/e"
"/var"
"/home/work"
-exclude
```

```
"/e/restore"

"/e/target"

}
```

Input document

CELL MANAGER	SPECIFICATION	CLIENT	MOUNTPOINT	DESCRIPTION	OPTION	VALUE
computer1.company.com	new_backup_1	DEL server*	/	/		

When the omniwl.pl command is executed with the above input document, client sections with host names starting with "server", and having “/” in the mountpoint and description sections, are deleted. The omniwl.pl code searches all the host names in the client sections in specified backup specifications, and matches and deletes the client section specified above.

The client needs to be member of the Cell Manager in order to add it to a backup specification. If it is not found in the*cell_info* file, then the following error message is displayed:

```
Can not add object: there is no client hostname matching <hostname from input document> pattern
```

Adding the client section using wildcards

In this example, wildcards are used in the input document to add new client sections to the specification.

Consider a Cell Manager computer1.company.com that has 2 clients: computer2.company.com , and computer3.company.com .

Input document

CELL MANAGER	SPECIFICATION	CLIENT	MOUNTPOINT	DESCRIPTION	OPTION	VALUE
computer1.company.com	new_backup_1	ADD computer*				

When the omniwl.pl command is executed with the above input document, all host names from theCell Manager clients list that have " computer" are matched, and full host backup client sections are created in the specification. Note that only the host names that belong to the Cell Manager are matched.

Modified specification

```
HOST " computer1.company.com " computer1.company.com

{

}

HOST " computer2.company.com " computer2.company.com

{
```

```
}
```

sanconf

sanconf - auto-configures a library, modifies an existing library or drive configuration, or removes drives from a library configuration within a SAN environment
(this command is available on systems with the Data Protector User Interface component installed)

SYNOPSIS

sanconf -version | -help

sanconf [-mom] -list[_devices] [*ListFileName*] [-hosts *host_1* [*host_2...*] | -hostsfile *HostsFileName*]

sanconf [-mom] -configure [*ListFileName*] -library *LibrarySerialNumber* *LibraryName* [*RoboticControlHostName*] [*DeviceTypeNumber* | "DeviceTypeExtension "] [-hosts *host_1* [*host_2...*] | -hostsfile *HostsFileName*] [-drive_template *DriveTemplateFileName*] [-library_template *LibraryTemplateFileName*] [-[no_]multipath] [-sanstableaddressing]

sanconf [-mom] -remove_drives *LibraryName* [-hosts *host_1* [*host_2...*] | -hostsfile *HostsFileName*]

sanconf [-mom] -remove_hosts *host_1* [*host_2 host_3 ...*] -library *LibSerNo* [-[no_]multipath]

DESCRIPTION

The sanconf command is a utility that provides easier configuration of libraries in SAN environments. It can automatically configure a library within a SAN environment by gathering information on drives from multiple clients and configuring them into a single library. In MoM environments, sanconf can also configure any library in any Data Protector cell that uses CMMDB, provided that the cell in which sanconf is run uses CMMDB as well.

The sanconf command can be run on the Data Protector Cell Manager or on Data Protector clients.

You can perform the following tasks using the sanconf command:

- Scan the specified Data Protector clients, gathering the information on SCSI addresses of drives and robotic controls connected to the clients in the SAN environment.
- Configure or modify settings of a library or drive for given clients using the information gathered during the scan of Data Protector clients.
- Remove drives on all or the specified clients from a library.

All sanconf sessions are logged to the sanconf.log file in the Data Protector log files directory.

OPTIONS

-version

Displays the version of the sanconf command.

-help

Displays the usage synopsis for the sanconf command.

-mom

Switches sanconf to operate in the MoM mode. This allows listing all devices connected to a MoM environment (see -list) and to configure devices in cells utilizing CMMDB (see - configure , -remove_hosts , -remove).

[-mom] -list[_devices] [*ListFileName*]

This option scans Data Protector clients to gather information on SCSI addresses of drives and robotic controls connected to the clients in the SAN environment and lists the gathered information. The information is uploaded to the Media Management Database on the Cell Manager. When *ListFileName* parameter is specified, the information acquired during the scan of clients is saved to the configuration file, which will be then used for configuring the library.

It is recommended to scan all clients that you want to configure, those that can see the robotics and those that can see the drives.

Note: When the option -mom is specified, sanconf lists clients and devices of all Data Protector cells in the MoM environment, even if they do not use CMMDB.

-hosts *host_1* [*host_2...*]

Specify the -hosts option if you want to limit the sanconf actions only to specified clients. Other clients in the Data Protector cell are skipped.

-hostsfile *HostsFileName*

Specify the -hostsfile option if you want to limit the sanconf actions only to clients specified in the *HostsFileName*. Other clients in the Data Protector cell are skipped. The *HostsFileName* is comprised of an ASCII list of clients, one client per line. It is recommended that all clients are specified in the clients list before you save the scan information to the configuration file.

For multipath devices, the path order is determined by the order in the given list or file.

[-mom] -configure [*ListFileName*]

This option scans, lists, configures, or reconfigures the specified library. Only one library can be configured with each invocation of the command line. If the *ListFileName* option is not specified, the sanconf command will dynamically scan, list, and configure the library. If this option is specified, the scan and data information that was saved to a file during the scan of the specified clients is used to configure the library and scan is not performed. If a client is not scanned, the library will not be configured.

Important: [*RoboticControlHostName*] and -hosts or -hostfile information must be specified during configuration.

Note: When reconfiguring a library, it is recommended that configuration information is first stored in the configuration file in case of configuration failure. It is also recommended that a different filename is used so that the initial configuration can be restored without any complications. sanconf reuses the custom settings when reconfiguring a library.

-library *LibrarySerialNumber LibraryName*

[RoboticControlHostName]

[DeviceTypeNumber | " *DeviceTypeExtension* "]

Specify the -library parameter to configure or reconfigure the specified library. Only one library can be configured with each invocation of the command line. sanconf creates only one logical library per physical library in the system and all devices on all specified clients. If the *RoboticControlHostName* parameter is specified, the specified client, which is connected to the specified library, will control the robotics for the library being configured. If this parameter is not specified, the library will be created with robotics on all clients, which are connected to the specified library, within the Data Protector cell, the Cell Manager will be used as a control host. If no library is installed on theCell Manager in a multipath library, another client will be used as a control host.

If the *ListFileName* parameter is used together with the *RoboticControlHost* but without the -hosts or -hostsfile option specified, the *RoboticControlHost* parameter will be ignored and a library will be created on all clients which are connected to the library.

When the RoboticControlHostName is used with the -hosts or -hostsfile parameter (option) it limits a library configuration on a specified client. Robotics will be configured on the host which is specified with the *RoboticControlHostName* and on the drives on the host specified with the -hosts or -hostsfile option. The configuration will be successful only in case that the *RoboticControlHostName* and the *Hosts* have the specified library installed.

In case that you try to configure a library with a robotic control host on a client which does not have a library installed, the configuration will not be successful (parameter -hosts is used).

In a MoM environment and with the -mom option specified, if the *RoboticControlHostName* parameter is specified without the -hosts or -hostsfile options, the sanconf command will configure a library on all hosts which are connected to it. For example, we have two hosts using the same CMMDB, but they can be on a different Cell Manager. If the hosts are both connected to the same library and only one of them is specified in the *RoboticControlHostName*, sanconf will configure two libraries with a robotic control on each host. The same happens in case of a host name which does not have the specified library installed.

If the *ListFileName* parameter is used together with the *RoboticControlHost* but without the -hosts or -hostsfile option, the *RoboticControlHost* parameter will be ignored and a library will be created on all clients which are listed in the file.

When the *RoboticControlHostName* is used with the -hosts or -hostsfile parameter it limits a library configuration on a specified client. Robotics will be configured on the host which is specified with the *RoboticControlHostName* and on the drives

on the host specified with the -hosts or -hostsfile option. The configuration will be successful only in case that the *RoboticControlHostName* and the *Hosts* have the specified library installed.

In case that you try to configure a library with a robotic control host on a client which does not have the library installed, the configuration will not be successful.

Additionally, if you try to configure a library on a host which does not use the CMMDB, but its own (local) MMDB, the configuration will fail, whether you try to configure a library which is also installed on clients in the same CMMDB or not.

When the *DeviceTypeNumber* parameter is used, the drives of that type will be configured in the library. When the *DeviceTypeNumber* is not specified, the LTO drive types are used as the default. Only one type number may be specified per library. If you use the ".DeviceTypeExtension" parameter instead of the *DeviceTypeNumber* parameter, you can specify the device type extension of the tape device to be configured in the library.

In the following table, *DTN* stands for *DeviceTypeNumber*, and *DTE* stands for *DeviceTypeExtension*.

DTN	*DTE*
1	DDT
2	QIC
3	EXA
4	AIT
5	3480
6	RDSK
7	REGFILE
8	9840
9	TAPE
10	DLT
11	D3
12	3590
13	LTO
14	SDLT
15	VXA
16	DTF
17	9940
18	SAIT
19	3592

When drives in the library are not of the same type as specified, an error is reported.

-drive_template *DriveTemplateFileName*

This option alters the default configuration of each tape device added to the library. You can alter the default configuration of the library only at the initial configuration. After the library is configured, you can no longer change the configuration of the library using the sanconf command.

The *DriveTemplateFileName* must be an ASCII file with one parameter specified per line.

Drive template supports the following parameters:

VERIFY

This parameter corresponds to the CRC Check option in the Data Protector GUI.

CLEANME

This parameter corresponds to the Detect dirty drive option in the Data Protector GUI.

RESCAN

This parameter corresponds to the Rescan option in the Data Protector GUI.

SANSTABLEADDRESSING

This parameter corresponds to the Automatically discover changed SCSI address option in the Data Protector GUI.

-library_template *LibraryTemplateFileName*

This option alters the default configuration of the library. You can alter the default configuration of the library only at the initial configuration. After the library is configured, you can no longer change the configuration of the library using the san conf command.

The *LibraryTemplateFileName* must be an ASCII file with one parameter specified per line.

Library template supports the following parameters:

BARCODEREADER

This parameter corresponds to the Barcode reader support option in the Data Protector GUI.

BUSYDRIVETOSLOT

This parameter corresponds to the Busy drive handling: Eject medium option in the Data Protector GUI.

BUSYDRIVETOMAILSLOT

This parameter corresponds to the Busy drive handling: Eject medium to mail slot option in the Data Protector GUI.

SANSTABLEADDRESSING

This parameter corresponds to the Automatically discover changed SCSI address option in the Data Protector GUI.

-[no_]multipath

By default or if the -no_multipath option is given, sanconf does *not* configure multipath devices – a separate logical device will be configured for *each* path.

When reconfiguring a multipath library as a non-multipath library, only one path is created. Multipath drives contained inside a multipath library are not changed, while new drives are created. Only non-multipath drives are modified.

If the -multipath option is used, sanconf configures all paths pointing to a single physical device as a *single* multipath device.

When reconfiguring a non-multipath library as a multipath library, the library control host is used as the first path. Non-multipath drives are not changed or removed. Instead, new multipath drives are created. Only multipath drives are modified.

-sanstableaddressing

Enables automatic discovery of changed SCSI addresses for the devices being configured.

[-mom] -remove_drives *LibraryName*

This option removes all tape devices in the specified library. If you want to remove drives on specific clients, you can use the -hosts host_1 [*host_2...*] or the -hostsfile HostsFileName option. This command cannot be used together with the -multipath option. Drives that are configured as multipath drives are not removed.

Note: No rescanning is required for this operation.

[-mom] -remove_hosts

All paths containing the specified hosts are removed. However, if the specified hosts cover all paths of the library, no paths are not removed from this library, instead a warning is displayed.

To remove paths only from *multipath* devices, add the -multipath option.

To remove paths only from *non-multipath* devices, add the -no_multipath option.

To remove paths from *both*, multipath *and* non-multipath devices, execute the command *without* the -no_multipath and -multipath options.

NOTE: No rescanning is required for this operation.

NOTES

The sanconf command is available on Windows and Linux systems only.

All drives created with the sanconf command are named automatically. Drive names must not be changed manually because the reconfiguration will not work. You must follow the drive naming convention.

- For *non-multipath* devices:

libname_index_host

libname_index_busindex_host

The busindex number is used only if there is more than one path for the drive.

- For *multipath* devices:

  libname_index

EXAMPLES

The following examples illustrate how the sanconf command works.

1. To scan host(s) for robotic control(s) and tape device(s) and create a file that will be used by sanconf -configure, execute:

   sanconf -list device.list

   This will display the serial number for any library discovered in the SUMMARY REPORT.

2. To scan and configure a library using the library serial number and the library name, on all clients on which the library is installed and which use CMMDB, execute:

   sanconf -mom -configure -library US9LS01033 SAN_STORE

   Clients on which the library is installed and which use a local MMDB are skipped.

3. To scan the specified clients and then create a logical library named "SAN_STORE" with robotics configured on client "host33" and drives for that library configured on clients "host01", "host02" and "host03", execute:

   sanconf -configure -library MPC0100013 SAN_STORE host33 -hosts host01 host02 host03

   A device type is .lto. An extension parameter does not need to be added.

4. To scan the SAN environment for the configuration information on the specified clients "host01", "host02", "host03", and "host33" which use CMMDB, and save this information is into the mySAN.cfg file, execute:

   sanconf -mom -list_devices mySAN.cfg -hosts host01 host02 host03 host33

5. To use information stored in the mySAN.cfg file and create a logical library named "SAN_STORE" with robotics configured on client host33 and drives for the library configured on clients "host01", "host02", and "host03", execute:

   sanconf -configure mySAN.cfg -library MPC0100013 SAN_STORE host33 -hosts host01 host02 host03

6. To scan all clients in the cell and then create a logical library named "SAN_STORE" on client "host33" with the parameters specified in the files DriveTemplate.txt and LibraryTemplate.txt, execute:

   sanconf -configure -library MPC0100013 SAN_STORE host33 -hosts host33 -drive_template DriveTemplate.txt -library_template LibraryTemplate.txt

7. To configure a tape library with the default tape device and library settings using the "device.list" file created by the example above, execute:

   sanconf -configure device.list -library MPC0220423 myLib1

8. To configure a library with a specific drive type, execute:

   sanconf -configure -library MPC0100013 SAN_STORE host33 ".9840" -hosts host01 host02

   This command creates a library named "SAN_STORE" with robotics configured on client "host33" and STK drives configured on clients "host01" and "host02". The drives are named as follows:

   SAN_STORE_1_host01

   SAN_STORE_1_host02

   SAN_STORE_2_host01

   SAN_STORE_2_host02

9. To configure three libraries using the configuration options contained in the library template "myway", execute:

   sanconf -configure -library US9LS02033 mylib5 -library_template myway

   sanconf -configure -library US9LS02034 mylib6 -library_template myway

   sanconf -configure -library US9LS02035 mylib7 -library_template myway

10. To configure a multipath LTO library with the serial number "LLL1", named "Library1", and connected to client "host1", execute:

    sanconf -configure -library LLL1 Library1 host1 ".LTO" -multipath

11. To configure a multipath LTO library with the serial number "LLL1", named "Library1", and connected to client "host1" and "host2", execute:

    ```
    sanconf -configure -library LLL1 Library1 host1 ".LTO" -hosts "host1" "host2" -multipath
    ```

    This will configure a library and drives with multipath option checked and configured paths on host1 and host2.

12. To update an already configured library with the configuration information for new hosts or tape devices, execute:

    ```
    sanconf -configure -library US9LS01023 mylib2
    ```

13. To reconfigure an already configured library after adding a new host "myhost" to a Data Protector cell, execute:

    ```
    sanconf -configure -library US9LS01033 mylib2 -hosts myhost
    ```

    This will scan and configure only the new host.

14. In a MoM environment, to reconfigure an already configured library on "host02" after adding a new host "myhost" to a Data Protector cell, execute:

    ```
    sanconf -mom -configure -library US9LS01033 mylib2 host02 -hosts myhost
    ```

    This will add drives from the host "myhost" to the library "mylib2" which is configured on the host "host2".

15. To configure only LTO Ultrium tape drives and add them into the library "myLTOlib", execute:

    ```
    sanconf -list device.list
    ```

    ```
    sanconf -configure device.list -library MPC0230031 myLTOlib "libraryhost" ".LTO"
    ```

16. To reconfigure a non-multipath library named "SAN_STORE" with serial number "MPC0100013" to a multipath library using the `-hosts` option, when new clients "host04" and "host05" are added to the cell, execute:

    ```
    sanconf -configure -library MPC0100013 SAN_STORE host33 -hosts host04 host05 -multipath
    ```

17. To delete all tape drives configured in the library "mylib2" related to the clients "host04" and "host05", execute:

    ```
    sanconf -remove_drives mylib2 -hosts host04 host05
    ```

18. To delete all tape drives configured in the library "mylib2", execute:

    ```
    sanconf -remove_drives mylib2
    ```

19. To remove all paths in the multipath library named "SAN_STORE" with serial MPC0230031 that are configured on clients "host04" and "host05", execute:

    ```
    sanconf -remove_hosts -hosts host04 host05 -library MPC0230031 -multipath
    ```

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), uma(1M)

uma

uma - controls the robotics of SCSI compliant autochangers
(this command is available on systems with the Data Protector General Media Agent or NDMP Media Agent component installed)

SYNOPSIS

uma -version | -help

uma [-policy *LogicalDevicePolicy*] -ioctl *deviceFile* [-interface { 0 | 1 }] [-tty] [-barcode] [-device *deviceFile_1* [*deviceFile_n*] -type *DeviceType*] [-ddt *NDMP_server_name NDMP_port_number backup_type username password*]

uma command line-interface commands:

help

inq

init

addr

offl *driveID*

sense

pos *slot*

move *source_slot destination_slot* [0 | 1]

stat [{ *slot* | *drive* | *transport_element* | *mail_slot* }]

modesense [*page*]

test

bye | exit | quit

doorlock [0 | 1]

enter *slot*

eject *slot*

DESCRIPTION

The uma program is a standalone utility program which can be used to control the robotics of most SCSI compliant autochangers, also those which are not directly supported by Data Protector. It implements a shell-like user command interface and can be used both interactively and in batch mode.

uma is packaged and installed as part of a Data Protector Media Agent fileset. If you have received uma as a standalone program or if you run it on a system where Data Protector has not been installed, the uma command is fully functional and behave as documented, but it is probably not able to locate and use Data Protector NLS message catalog.

On Linux and Solaris systems, the NLS message catalog is located in the /opt/omni/lib/nls/C/ directory.

On Windows systems, the NLS message catalog is located in the Data_Protector_home\bin directory.

uma can be started both interactively or in batch mode. The only obligatory option is the pathname of the device file (UNIX systems) or the SCSI address (Windows systems) that controls the robotics of the target autochanger (the -ioclt option). For backup devices with library robotics connected to an NDMP Server (to a supported NAS device), the -interface and the -ddt options must also be specified.

For your convenience, the uma command allows you to specify symbolic instead of physical element addresses (slot IDs). Whenever you need to refer to the 1st drive of the autochanger, you can specify either the physical address '128' or the more convenient, symbolic 'D1'. The output of the addr command reflects this addressing convention.

OPTIONS

-version

Displays the version of the uma command.

-help

Displays the usage synopsis for the uma command.

-policy *LogicalDevicePolicy*

Specifies the backup device policy ID. Policy can be defined as 6 (external control), 8 (Grau DAS exchanger library), 9 (STK Silo medium library), or 10 (SCSI Library).

The default value for the -policy option is 10 .

-ioctl *deviceFile*

Specifies the pathname of the device file (UNIX systems) or the robotics SCSI address (Windows systems) that controls the robotics of the target autochanger.

-interface { 0 | 1 }

Sets the type of SCSI interface used to access library robotics. This option is to be used only with backup devices with library robotics connected to an NDMP Server. 0 sets the standard SCSI interface (the default value). 1 sets the NDMP protocol interface and must be specified for backup devices with library robotics connected to an NDMP Server. The default value is 0 .

-tty

Forces the uma command to enter the command line interface mode or to read from script. This option is obligatory on UNIX systems. On Windows systems, this option is not to be used; the command line interface mode is invoked automatically.

-barcode

If this variable is set, the uma command's stat command displays also the barcode information for each medium.

-device *deviceFile_1* [*deviceFile_n* ...]

Specifies the device file (UNIX systems) or the SCSI address (Windows systems) of one or more autochanger drives. For a multi-drive autochanger, you must specify a list of device files/SCSI addresses which correspond to the autochanger's drives in ascending order. The drives have to be known to uma in order for the offl command to work. This option is only to be used together with -type option.

-type *DeviceType*

Specifies the media type for the media in the device specified by the -device option. Media type numbers are defined as media class in the scsitab file.

-ddt *NDMP_server_name NDMP_port_number backup_type username password*

This option is mandatory for backup devices with library robotics connected to an NDMP Server (to a supported NAS device). It specifies the NDMP Server name, port number used by Data Protector to connect to the NDMP Server and username and password used by Data Protector to connect to the NDMP server. The *backup_type* parameter has to be set to dump .

uma command-line interface commands:

help

Displays the usage synopsis for the uma command.

inq

Performs a SCSI Inquiry operation on the device file/SCSI address specified with the -ioctl option. It returns the device's type, vendor ID, product ID and firmware revision number.

init

Performs a SCSI 'initialize element status' operation, which (if applied to an autochanger robotic device) forces the autochanger to reset its internal state and perform an inventory of its repository. This command should not be used if another process is accessing the autochanger at the same time, as the effects are unpredictable.

addr

Queries and displays the autochanger's element assignment page. Each addressable item inside the autochanger mechanism (drive, repository slot, robotic arm, import/export slot) has a unique integer number (slot ID) which can be used to address this specific item.

As the element assignment differs among different autochangers, the software, which is to control the movement of media inside the autochanger, must find out and use these numbers to perform move, pos and stat operations.

offl *driveID*

This command can be used only if at least one drive was specified using the -device option. If a medium is loaded in the specified drive, it will eject the medium just as if an UNIX mt offl command was specified. The mandatory argument is a symbolic drive ID (that is, D3 for the 3rd drive == the 3rd device file specified with the -dev option). If the drive specified is not defined by the -device option, then the last drive defined by the -device option will be used.

The offl command can fail with a message: "No such device or address" if it is issued immediately after the move command since it takes a certain time after the move command for the drive to be online. For more information, see the move command.

sense

Read the device's sense data and dump them in a hex- dump format.

pos *slot*

Positions the autochanger transport mechanism in front of the specified slot. This operation is only meaningful if the specified slot refers to an import/export, data drive or repository element. The actual meaning of this operation may differ among different autochanger models. This command is generally not required, but is provided for testing purposes and convenience. Both physical as well as symbolic slot addressing may be used.

move *source_slot* *destination_slot* [0 | 1]

Moves a medium from a source slot into a destination slot. This command has two mandatory arguments, the source and destination slot IDs (address numbers, as reported by the addr command described above) and an optional numeric Boolean argument which can be used to instruct the robotics to flip the medium before inserting it into the destination slot. By default (if no flipping argument is specified), flipping is disabled.

Note that when move command is issued to move a tape into a drive, it takes a certain time (around 30 seconds) for the drive to become online, because tape load and calibration/selftest have to be performed. The command prompt however, returns immediately after the command is issued.

Note: Flipping is supported only for double-sided optical media. For tapes, the effect of the flip command is not defined.

NOTE: Most autochanger do not allow you to move a tape from a drive to a repository location if the tape has not been dismounted and ejected by the drive. You might want to use the offl command on the drive device file/SCSI address to put the drive offline before executing the move command.

stat [{ *slot* | *drive* | *transport_element* | *mail_slot* }]

Queries the device for information about the state of each of its addressable elements. The output of this command is a table of physical and symbolic element IDs and their states, indicating which elements are free (Empty) and occupied (Full).

Additionally, if barcode support is available and enabled, the barcode for each medium is displayed.

The uma command recognizes one specific environment variable which can be used to enable barcode support for autochangers which are equipped with barcode reading hardware. By default, uma barcode support is disabled. It can be enabled by exporting/setting the OB2BARCODE=1 environment variable before starting the command or by using the -barcode option.

The stat command can be used to query the status of a specific slot (that is, 'stat 290' or 'stat S35') or a related group of slots (that is, 'stat D' will query all drives, 'stat S' will query all repository slots, and so on).

If no additional arguments are specified, the stat command will query and print the status information for all slot IDs it can address.

modesense [page]

Reads the vendor specific data and unit settings from the unit and displays them. You can limit the display only to certain pages by using the page parameter. If the page parameter is not specified, all pages are displayed.

test

Checks if the unit is ready. If the unit is not used by any process, then the unit is ready. If it is, however, used either by the robotics, backup or restore processes then it is not ready.

exit | bye | quit

Exits the command mode.

doorlock [0 | 1]

If the input parameter is 1 , this command locks the library mail slot door; if it is 0 , it unlocks it.

-enter *slot*

Enters media into a specified library slot.

-eject *slot*

Ejects media from a specified library slot.

NOTES

Do not use the uma utility while Data Protector backup or restore is running. On UNIX systems the -tty option is obligatory. On Windows systems it is not used.

EXAMPLES

1. uma can be started both interactively or in batch mode. The only option which needs to be specified (except for backup devices with library robotics connected to an NDMP Server) is the pathname of the device file which controls the robotics of the target autochthons:

   UMA -ioctl /dev/spt/sctl0

   *** PROGRAM: UMA VERSION: Data Protector 10.03

```
*** Copyright (C) 1999 Hewlett Packard Enterprise Company

*** License is restricted for use with licensed

*** Data Protector products.

/dev/spt/sctl0> exit
```

2. To start `uma` for a backup device with the library robotics connected to the NDMP Server with the robotics SCSI address "mc2", the NDMP Server hostname "ndmpserver", the port number used by Data Protector to connect to the NDMP Server "10000", and username and password of the user used by Data Protector to connect to the NDMP Server "user password", enter the following command:

   ```
   UMA -ioctl mc2 -interface 1 -ddt ndmpserver 10000 dump user password
   ```

3. To let `uma` execute a batch script of its own commands, simply redirect its stdin to a file containing a list of uma commands separated with newlines:

   ```
   cat >/tmp/cmdFile

   inq

   addrstat

   < ctrl-D>

   uma -ioctl /dev/spt/sctl0 < /tmp/cmdFile >/tmp/outFile
   ```

4. The following output is obtained by executing the `addr` command on the UNIX device file referring to an ACL 4/52 DLT autochanger:

   ```
   /dev/spt/sctl0>addr Element Addresses (T=Transport, X=Im/Export, D=Drive, S=Storage):

   Transport: 1 .. 1 (T1 .. T1)

   Im/Export: 64 .. 67 (X1 .. X4)

   Data Drive(s): 128 .. 131 (D1 .. D4)

   Repository: 256 .. 303 (S1 .. S48)
   ```

   The numbers returned by the `addr` command are the physical element addresses of different elements within the autochanger - that is, element address "256" would correspond to the first repository slot, element address "65" would correspond to the location of the second data drive, and so on.

5. To start `uma` for the Grau DAS exchanger library with the robotics device file "grauamu", execute:

   ```
   uma -pol 8 -ioctl grauamu
   ```

SEE ALSO

omniamo(1), omnib2dinfo(1M), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M)

util_cmd

This feature is available in the Premium Edition

util_cmd - sets, retrieves, or lists the parameters stored in the Data Protector Oracle, MySQL, SAP R/3, SAP MaxDB, Microsoft Exchange Server 2010/2013, Informix, and Sybase configuration files. In addition, it encodes passwords.
(this command is available on systems with any Data Protector component installed)

SYNOPSIS

util_cmd -version | -help

util_cmd -getconf[ig] { Oracle8 | MySQL | SAP | SAPDB | Informix | Sybase } *instance* [-local *filename*]

util_cmd -getopt[ion] [{ Oracle8 | MySQL | SAP | SAPDB | Informix | Sybase } *instance*] *option_name* [-sub[list] *sublist_name*] [-local *filename*]

util_cmd -putopt[ion] [{ Oracle8 | MySQL | SAP | SAPDB | Informix | Sybase } *instance*] *option_name* [*option_value*] [-sub[list] *sublist_name*] [-local *filename*]

util_cmd -encode *Password*

util_cmd -setomnirc *hostname* *name* [*value*]

util_cmd -getomnirc *hostname* *name*

util_cmd -delomnirc *hostname* *name*

DESCRIPTION

The util_cmd command is used to set, retrieve, or list the parameters stored in the Data Protector Oracle, SAP R/3, SAP MaxDB, Microsoft Exchange Server 2010/2013, Informix, and Sybase configuration files. In addition, it can be used to encode passwords.

Data Protector stores the integration parameters on the Cell Manager in the directory Data_Protector_program_data\Config\Server\Integ\Config\ *integration_name* (Windows systems) or /etc/opt/omni/server/integ/config/integration_name (UNIX systems).

ORACLE

For each configured Oracle database, the following configuration files are created:

- Target database configuration file: client_name%[*DB_NAME* | *INSTANCE_NAME*]

  For Oracle Data Guard, client_name is primary_hostname or secondary_hostname

  The parameters stored in the target database configuration file are:

  - Oracle home directory

  - encoded connection strings to the target database, recovery catalog, and standby database

  - variables, which are exported when you start a session using the Data Protector GUI or CLI

  OB2_RMAN_COMMAND_TIMEOUT (environment variable)

  This variable is applicable when Data Protector tries to connect to a target or catalog database. It specifies how long (in seconds) Data Protector waits for RMAN to respond that the connection succeeded. If RMAN does not respond within the specified time, Data Protector aborts the session. Default: 300 s.

  OB2_SQLP_SCRIPT_TIMEOUT (environment variable)

  This variable is applicable when Data Protector issues an SQL*Plus query. It specifies how long Data Protector waits for SQL*Plus to respond that the query completed successfully. If SQL*Plus does not respond within the specified time, Data Protector aborts the session. Default: 300 s.

SBT_LIBRARY

Specifies which Data Protector MML should be used by RMAN, in case you want to override the default Data Protector selection.

- Global database configuration file: client_name%_OB2_GLOBAL

  The parameters stored in the global configuration file are:

  - instance list (all Oracle instances on the Oracle server)

  - variables that need to be exported prior to starting a backup and which affect every Oracle instance on the Oracle server.

- In case of zero downtime backup, backup method configuration file: zdb_methodORACLE_DBID
- In case of zero downtime backup, for backup set method, the file: client_name%init *DB_NAME* _bckp.ora

SAP R/3

The SAP R/3 parameters stored are:

- Oracle home directory
- encoded connection string to the target database
- BRTOOLS home directory
- variables, which are exported when you start a session using the Data Protector GUI or CLI:

ORA_NLS_CHARACTERSET

- After upgrading a Data Protector __DP_V55 __ SAP R/3 client to the latest version of Data Protector, set this variable to the encoding used by the Oracle database.

OB2_MIRROR_COMP

- This variable is applicable for ZDB sessions that use the SPLITINT functionality (-t { online_mirror | offline_mirror }). Set this variable to 1 if you want BRBACKUP to be started on the backup system and not on the application system. By default, BRBACKUP is started on the application system.

SBT_LIBRARY

- Specifies which Data Protector MML should be used by RMAN, in case you want to override the default Data Protector selection.

- concurrency number and balancing (for each backup specification) and number of channels for RMAN backup
- speed parameters (time needed for a specific file to back up - in seconds)
- manual balancing parameters

SAP MaxDB

The SAP MaxDB parameters stored are:

- Username of the SAP MaxDB database user
- Password of the SAP MaxDB database user
- SAP MaxDB version
- SAP MaxDB independent program path parameter that was specified during the installation of SAP MaxDB Server
- Data Protector SAP MaxDB integration related environment variables

INFORMIX SERVER

The Informix parameters stored are:

- Informix Server home directory
- pathname of the sqlhosts file
- name of the Informix instance ONCONFIG file

SYBASE

The Sybase parameters stored are:

- Sybase home directory
- pathname for the isql command
- Sybase backup operator username and password
- name of the Sybase *SYBASE_ASE* directory (Sybase 12.x only)

- name of the Sybase *SYBASE_OCS* directory (Sybase 12.x only)
- environment variables

RETURN VALUES

The util_cmd command displays a short status message after each operation (written to the standard error):

- Configuration read/write operation successful.

  This message is displayed when all the requested operations have been completed successfully.

- Configuration option/file not found.

  This message appears when either an option with the specified name does not exist in the configuration, or the file specified as the -local parameter does not exist.

- Configuration read/write operation failed.

  This message is displayed if any fatal errors occurred, for example: the Cell Manager is unavailable, the Data Protector configuration file for a specific integration is missing on the Cell Manager, and so on.

OPTIONS

-version

Displays the version of the util_cmd command.

-help

Displays the usage synopsis for the util_cmd command.

-getconf[ig] *integration instance*

Lists the Data Protector configuration files parameters for the specified integration and instance to the standard output, unless the -local option is specified.

-getopt[ion] [*integration instance*] *option_name*

Retrieves the parameter (specified by the option_name) and its value from one of Data Protector configuration files and writes it to the standard output, unless the -local option is specified.

-putopt[ion] [*integration instance*] *option_name* [*option_value]*

Sets the specified parameter (specified by the option_name) and (optionally) its value to the Data Protector configuration files, unless the -local option is used.

To remove a value of a parameter, specify the *option_name*, without the *option_value*. However, if the option is in a sublist, you must specify an empty ("") *option_value* to remove a value.

-sublist *SublistName*

Specifies the sublist in the configuration file in which a parameter is written to or taken from.

-local *FileName*

If the -local option is used with the -getconf option, the command output is written to the file with the filename specified by the -local option. If the -local option is used with the -getopt option, the parameter and its value is taken from the file with the filename specified by the -local option. If the -local option is used with the -putopt option, the parameter and its value is written to the file with the filename specified by the -local option.

-encode *Password*

Returns the encoded form of the specified password.

-setomnirc *hostname name* [*value*]

This option sets the environment variable name with a value in the omnirc file on the host specified as hostname. If the environment variable is present in the omnirc file, its values gets updated, otherwise it gets created.

The following parameters are passed in the -setomnirc command:

- hostname - Specifies the place where the omnirc file is located.
- name - Specifies the environment variable name.
- value - Specifies the value of the environment variable.

The access to remote omnirc may fail due to the following reason:

- When strict security is enabled. In this case, you need to start the util_cmd on the cell server.

Note The omnirc file does not support multiple occurrences of the same variables as it leads to errors. All these limitations apply to getomnirc and delomnirc commands too.

-getomnirc *hostname name*

This option reads the value of the environment variable from the omnirc file on the hostname.

-delomnirc *hostname name*

This option deletes the environment variable from the omnirc file on the hostname.

EXAMPLES

The following examples illustrate how the util_cmd command works.

> The command util_cmd must be executed on the Cell Manager. To use it, the environmental variable OB2BARHOSTNAME must be defined before running the command.
>
> Set OB2BARHOSTNAME=client_name (Windows) or OB2BARHOSTNAME=client_name (Linux)

1. To set the Data Protector "OB2OPTS" parameter for the Oracle instance "ICE", execute:

   util_cmd -putopt Oracle8 ICE OB2OPTS "-debug 1-200 INSTANCE.txt" -sublist Environment

2. To set the Data Protector "OB2OPTS" parameter for the SAP R/3 instance "ICE", execute the following command on the Data Protector SAP R/3 client:

   util_cmd -putopt SAP ICE OB2OPTS '-debug 1-200 INSTANCE.txt' -sublist Environment

3. To set the "BR_TRACE" parameter for the SAP R/3 instance "ICE" to value "10" in the "Environment" sublist, execute the following commands on the Data Protector SAP R/3 client:

   util_cmd -putopt SAP ICE BR_TRACE "'10'" -sublist Environment

4. To list the Data Protector configuration file parameters for the Oracle instance "ICE", execute:

   util_cmd -getconf Oracle8 ICE

5. To retrieve the value of the "OB2OPTS" parameter for the Oracle instance "ICE", execute:

   util_cmd -getopt Oracle8 ICE OB2OPTS -sublist Environment

6. To remove the value of the "OB2OPTS" parameter for the SAP R/3 instance "ICE", execute the following command on the Data Protector SAP R/3 client:

   util_cmd -putopt SAP ICE OB2PTS "" -sublist Environment

7. To get the encoded form of the password "BlueMoon", execute:

   util_cmd -encode BlueMoon

8. To set the environment variable "OB2_RMAN_COMMAND_TIMEOUT" to "100" seconds for the Oracle database "INST2", execute:

   util_cmd -putopt Oracle8 INST2 OB2_RMAN_COMMAND_TIMEOUT 100 -sublist Environment

9. To set the environment variable "TEST1" with value "10" to omnirc file on the hostname "Win9", execute:

   util_cmd -setomnirc Win9 TEST1 10

10. To get the value of the environment variable "TEST1" from omnirc file on hostname "Win9", execute:

    util_cmd -getomnirc Win9 TEST1

11. To delete the environment variable "TEST1" from omnirc file on hostname "Win9", execute:

    util_cmd -delomnirc Win9 TEST1

SEE ALSO

omnib(1), omniintconfig.pl(1M), util_oracle8.pl(1M), vepa_util.exe(1M)

util_hana.pl

util_oracle8.pl

This feature is available in the Premium Edition

util_oracle8.pl - configures an Oracle database and prepares the environment for backup, and checks the configuration of an Oracle database
(this command is available on systems with the Data Protector Oracle Integration component installed)

SYNOPSIS

util_oracle8.pl -version | -help

util_oracle8.pl -chkconf -dbname *DB_NAME* [-client *CLIENT_NAME*]

util_oracle8.pl -chkconf_smb -dbname *DB_NAME* [-bkphost *BACKUP_SYSTEM*] [-client *CLIENT_NAME*]

util_oracle8.pl -chkconf_ir -dbname *DB_NAME* [-client *CLIENT_NAME*]

util_oracle8.pl -config -dbname *DB_NAME* -orahome *ORACLE_HOME* *PRIMARY_DB_LOGIN* | *USEOSAUTHENTICATION* [*CATALOG_DB_LOGIN*] [*STANDBY_DB_LOGIN*] [*ZDB_OPTIONS*] [*ASM_OPTIONS*] [-client *CLIENT_NAME*]

PRIMARY_DB_LOGIN

-prmuser PRIMARY_USERNAME

-prmpasswd PRIMARY_PASSWORD

USEOSAUTHENTICATION

-useosauth USE_OS_AUT

-racdbname RAC_DB_NAME

CATALOG_DB_LOGIN

-rcuser *CATALOG_USERNAME*

-rcpasswd *CATALOG_PASSWORD*

-rcservice *CATALOG_NET_SERVICE_NAME*

STANDBY_DB_LOGIN

-stbuser *STANDBY_USERNAME*

-stbpasswd *STANDBY_PASSWORD*

-stbservice *STANDBY_NET_SERVICE_NAME_1* [, *STANDBY_NET_SERVICE_NAME_2* ...]

ZDB_OPTIONS

-zdb_method { *PROXY* | *BACKUP_SET* }

[-ctlcp_location *BACKUP_CONTROL_FILE_COPY_LOCATION*]

[-pfile *PARAMETER_FILE*]

[-bkphost *BACKUP_SYSTEM*]

ASM_OPTIONS

[-asmhome *ASM_HOME*]

[-asmuser *ASM_USERNAME* -asmpasswd *ASM_PASSWORD* -asmservice *ASM_NET_SERVICE_NAME_1* [, *ASM_NET_SERVICE_NAME_2* ...]]

DESCRIPTION

Use the util_oracle8.pl command to configure an Oracle database and prepare the environment for backup, and to check the configuration of the database.

To back up a standby database, you must provide the *STANDBY_DB_LOGIN* information. For standby database backup, a recovery catalog must be used. Therefore, you must also provide the *CATALOG_DB_LOGIN* information.

To configure an Oracle database for ZDB, you must provide the *ZDB_OPTIONS* information. If your ZDB method is backup set, you must also provide the *BACKUP_SYSTEM* information.

The *ASM_OPTIONS* options are needed for instant recovery in Oracle Server configurations that use Automatic Storage Management (ASM).

On Windows systems, you must use the perl command to execute util_oracle8.pl . An example of the command line is perl util_oracle8.pl -help .

On OpenVMS systems, you must omit the command's file extension to execute the command. An example of the command line is util_oracle8 -help .

OPTIONS

-version

Displays the version of the util_oracle8.pl command.

-help

Displays the usage synopsis for the util_oracle8.pl command.

-client *CLIENT_NAME*

Name of the Oracle Server system with the database to be configured. It must be specified in a cluster environment or if the ZDB configuration is run on the backup system.

In an RAC environment: Name of the node or the virtual server of the Oracle resource group. The latter can only be used on HP-UX systems: Name of the database to be configured.

In an Oracle Data Guard environment: Name of either a primary system or secondary (standby) system.

-dbname *DB_NAME*

Name of the database to be configured.

-orahome *ORACLE_HOME*

Pathname of the Oracle Server home directory.

-config

Configures an Oracle database.

-chkconf

Checks the configuration of an Oracle database.

-chkconf_smb

Checks if an Oracle database is properly configured for ZDB.

-chkconf_ir

Checks if an Oracle configuration is suitable for instant recovery.

-bkphost *BACKUP_SYSTEM*

Name of the backup system. It must be specified for a ZDB backup set configuration.

-prmuser *PRIMARY_USERNAME*

Username for login to the target or primary database. Note that the user must have been granted the SYSDBA privilege. The user must have been granted the SYSBACKUP privilege. You can also use the user with SYSDBA privilege, but first you must set omnirc variable OB2_ORACLE_USE_SYSDBA to 1.

-prmpasswd *PRIMARY_PASSWORD*

Password for login to the target or primary database. Note that the user must have been granted the SYSDBA privilege. The user must have been granted the SYSBACKUP privilege. You can also use the user with SYSDBA privilege, but first you must set omnirc variable OB2_ORACLE_USE_SYSDBA to 1.

-prmservice *PRIMARY_NET_SERVICE_NAME_1* [*,PRIMARY_NET_SERVICE_NAME_2 ...*]

Net services names for the primary database.

In an RAC environment: Each net service name must resolve into a specific database instance.

-useosauth USE_OS_AUT

This parameter is used to communicate to the configuration script to use Oracle OS authentication instead of username and pass authentication. Value should be 1.

-racdbname RAC_DB_NAME

This parameter is used in Oracle RAC environments in order to find Oracle SID for current Oracle RAC node. This parameter represent Oracle global database name and this is mandatory on Oracle RAC platforms.

-rcuser *CATALOG_USERNAME*

Username for login to the recovery catalog. This is optional and is used only if you use the recovery catalog database catalog as an RMAN repository for backup history.

-rcpasswd *CATALOG_PASSWORD*

Password for login to the recovery catalog. This is optional and is used only if you use the recovery catalog database catalog as an RMAN repository for backup history.

-rcservice *CATALOG_NET_SERVICE_NAME*

Net services name for the recovery catalog.

-stbuser *STANDBY_USERNAME*

Used in the Oracle Data Guard environment for backing up a standby database. Username for login to the standby database.

-stbpasswd *STANDBY_PASSWORD*

Used in the Oracle Data Guard environment for backing up a standby database. Password for login to the standby database.

-stbservice *STANDBY_NET_SERVICE_NAME_1* [*,STANDBY_NET_SERVICE_NAME_2 ...*]

Net services names for the standby database.

-zdb_method { PROXY | BACKUP_SET }

Configures the Oracle database for ZDB environment and sets the ZDB method to Oracle proxy-copy or Oracle backup set.

-ctlcp_location *BACKUP_CONTROL_FILE_COPY_LOCATION*

The location on the source volumes where a copy of the current control file is made during ZDB to disk. This is optional and if not specified, ob2rman.pl will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

If you use a raw logical volume as the *BACKUP_CONTROL_FILE_COPY_LOCATION*, the logical volume must reside on a volume group that will be replicated. If there is no such raw logical volume available, create a new shared disk (volume group) residing on the disk that will be replicated and configure a raw logical volume on it. If you use a raw logical volume, in case of an ZDB to disk, you need to ensure enough free space in the /var/opt/omni/tmp directory on the backup host to hold the copy of the raw logical volume.

-pfile *PARAMETER_FILE*

Full name of the PFILE residing on the application system. This is optional and used if backup method is backup set and the database instance uses PFILE (and not SPFILE).

-asmhome *ASM_HOME*

Specifies the home directory of the ASM instance in an Oracle ASM configuration. Specify this option if the value differs from the home directory of the Oracle database instance.

-asmuser *ASM_USERNAME*

This option can be used only in combination with the -asmpasswd and -asmservice options.

Specifies the user name used by the Data Protector Oracle integration agent to connect to the ASM database. Note that the user must have been granted the SYSDBA privilege.

-asmpasswd *ASM_PASSWORD*

This option can be used only in combination with the -asmuser and -asmservice options.

Specifies the password used by the Data Protector Oracle integration agent to connect to the ASM database.

-asmservice *ASM_NET_SERVICE_NAME_1* [*,ASM_NET_SERVICE_NAME_2 ...*]

This option can be used only in combination with the -asmuser and -asmpasswd options.

Specifies the name of the net service to be used to access the ASM database. For Oracle environments involving multiple net services, multiple names can be specified.

NOTES

- On OpenVMS, to invoke the Data Protector CLI, execute:

  $@OMNI$ROOT: [BIN] OMNI$CLI_SETUP.COM

- BACKUP_CONTROL_FILE_COPY_LOCATION:

  This parameter is optional and if not specified, ob2rman.pl will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

  If you use a raw logical volume as the *BACKUP_CONTROL_FILE_COPY_LOCATION*, the raw logical volume must reside on a volume group that will be replicated. If there is no such raw logical volume available, create a new shared disk (volume group) residing on the disk that will be replicated and configure a raw logical volume on it. If you use a raw logical volume,

in case of an ZDB to disk, you need to ensure enough free space in the /var/opt/omni/tmp directory on the backup host to hold the copy of the raw logical volume.

- PARAMETER_FILE:

  This parameter is optional and used if backup method is backup set and the database instance uses PFILE (and not SPFILE).

EXAMPLES

The following names are used in the examples below:

- database name: oracl
- Oracle Server home directory: /app12/oracle12/product/12.0
- primary user name: system
- primary password: manager
- primary net service name 1: netservice1
- primary net service name 2: netservice2
- recovery catalog user name: rman
- recovery catalog password: manager
- recovery catalog net service name: catservice
- standby user name (Oracle Dataguard only): system
- standby password (Oracle Dataguard only): manager
- standby net service name 1 (Oracle Dataguard only): netservicesb1
- standby net service name 2 (Oracle Dataguard only): netservicesb2
- parameter file: /app12/oracle12/product/12.0/dbs/pfile.ora
- backup system name: bcksys
- ASM home directory: /oracle/crshome/crshome/crs/app/12.0/grid
- ASM user name: sys
- ASM password: oracle
- ASM net service name: ASMSRV

1. The following example illustrates the configuration of an Oracle database and its recovery catalog in an Oracle Data Guard environment and using the Oracle backup set ZDB method:

   ```
   util_oracle8.pl -config -dbname oracl -orahome app12/oracle12/product/12.0 -prmuser system -prmpasswd manager -prmservice netservice1,netservice2 -stbuser system -stbpasswd manager -stbservice netservicesb1,netservicesb2 -rcuser rman -rcpasswd manager -rcservice catservice -zdb_method BACKUP_SET -pfile /app12/oracle12/product/12.0/dbs/pfile.ora
   ```

2. The following example illustrates the configuration of an Oracle database and its recovery catalog in an Oracle backup set ZDB environment:

   ```
   util_oracle8.pl -config -dbname oracl -orahome app12/oracle12/product/12.0 -prmuser system -prmpasswd manager -prmservice netservice1,netservice2 -rcuser rman -rcpasswd manager -rcservice catservice -zdb_method BACKUP_SET -pfile /app12/oracle12/product/12.0/dbs/pfile.ora -bkphost bcksys
   ```

3. The following example illustrates the configuration of an Oracle database and its recovery catalog in an Oracle backup set ZDB environment which uses Automatic Storage Management (ASM):

   ```
   util_oracle8.pl -config -dbname oracl -orahome app12/oracle12/product/12.0 -prmuser system -prmpasswd manager -prmservice netservice1,netservice2 -rcuser rman -rcpasswd manager -rcservice catservice -zdb_method BACKUP_SET -pfile /app12/oracle12/product/12.0/dbs/pfile.ora -bkphost bcksys -asmhome /oracle/crshome/crshome/crs/app/12.0/grid -asmuser sys -asmpasswd oracle -asmservice ASMSRV
   ```

SEE ALSO

omniintconfig.pl(1M), util_cmd(1M), vepa_util.exe(1M)

vepa_util.exe

vepa_util.exe - configures a VMware ESX(i) Server system, VMware vCenter Server system, H3C CAS, Microsoft Hyper-V system, checks the configuration, configures virtual machines, browses and lists VMware datacenters
(this command is available on Windows and Linux systems with the Data Protector Virtual Environment Integration component installed)

SYNOPSIS

vepa_util.exe --version | --help | --details { command_opt | query_opt | browse_opt }

vepa_util.exe { command *COMMAND_OPTIONS* | query *QUERY_OPTIONS* | browse *BROWSE_OPTIONS* } *ENVIRONMENT_OPTIONS*

vepa_util.exe command --upgrade-cell_info

COMMAND_OPTIONS

--add-standalone-host *ESX_CONFIG_OPTIONS* [--ssl-thumbprint *ThumbPrint*]

--remove-standalone-host --esx-server *EsxName* [*EsxName* ...]

--update-staging-details [--host *HostName* --staging-username *UserName* --staging-password *Password*]

--check-config

--config *CONFIG_OPTIONS*

--configvm *VM_CONFIG_OPTIONS*

--unlock-vmotion { --vm *VmPath* | --uuid *VmUUID* }

--show-incremental-flag [--uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID* ...]"]

--enable-incremental { --uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID* ...]"}

--disable-incremental { --uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID* ...]"}

--clear-vm-lock --vm-uuid

QUERY_OPTIONS

--list-organizations

--list-datacenters

--list-datastores

--list-esx-servers [--cluster *ClusterName*]

--list-resource-pools [--hypervisor *ClusterOrESXName*]

--list-clusters [--instance *DatacenterName*]

--list-vms

--list-sockets [--hypervisor ESXNameOrHypervNode]

--list-hostpools

--list-hostsClusters

--list-specificHosts

--list-storagePools

--list-category

--list-tags [-category_id *CategoryId*]

--list-barlist-vms

BROWSE_OPTIONS

--root-node *NodePath*

--inventory-view { hosts_and_clusters | vms_and_templates | tags_and_categories | storage}

ENVIRONMENT_OPTIONS

--virtual-environment { VMWare | vCD | HyperV | H3CCAS }

--host *HostName*

CONFIG_OPTIONS

--port *PortNumber*

--username *UserName*

--password *Password*

--encoded-password *EncodedPassword*

--webroot *Webroot*

--security-model { 0 | 1 }

ESX_CONFIG_OPTIONS (VMWare only)

--esx-username *EsxUsername*

--esx-password *EsxPassword*

--esx-server *EsxName* [*EsxName* ...]

--datacenter *DatacenterName*

--ssl-thumbprint *SslThumbprint*

VM_CONFIG_OPTIONS

--instance { *DatacenterName* | *HostpoolName* }

--vm *VmPath*

--transportation-mode { san | nbd | nbdssl | hotadd }

--quiescence

--quiescenceErrLvl { 0 | 1 }

--uuid *VmUuid*

--default

DESCRIPTION

Use the vepa_util.exe command to configure a VMware ESX(i) Server system, VMware vCenter Server system, and Microsoft Hyper-V system, check the configuration, configure virtual machines, browse and list VMware datacenters.

OPTIONS

--version

Displays the version of the vepa_util.exe command.

--help

Displays the usage synopsis for the vepa_util.exe command.

--details { command_opt | query_opt | browse_opt }

Displays short descriptions for the specified vepa_util.exe options.

--upgrade-cell_info

Upgrades the cell_info file after upgrading Data Protector 6.20 to the latest product version.

The cell_info file upgrade is mandatory.

COMMAND_OPTIONS

--add-standalone-host *ESX_CONFIG_OPTIONS* [--ssl-thumbprint *ThumbPrint*]

This is a VMware specific option.

Adds the specified standalone ESX Server system to the datacenter.

--remove-standalone-host --esx-server *EsxName* [*EsxName*]...

This is a VMware specific option.

Removes the specified ESX Server system from a datacenter.

--update-staging-details [--host *HostName* --staging-username *UserName* --staging-password *Password*]

Updates the staging details in case of a non-cached backup.

--check-config

Checks whether the specified application client is configured right.

--config *CONFIG_OPTIONS*

Configures the specified application client.

--configvm *VM_CONFIG_OPTIONS*

This is a VMware and Hyper-V specific option.

Configures the backup options for virtual machines.

Note that this option does not check the environment. If you mistype a virtual machine name or a virtual machine UUID the configuration reports success but it is useless.

--unlock-vmotion { --vm *VmPath* | --uuid *VmUUID* }

This is a VMware specific option.

Unlocks vMotion for the specified VMware virtual machine.

--show-incremental-flag [--uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID*]..."]

This is a Microsoft Hyper-V specific option.

Displays states of the specified virtual machines (GUIDs) with regard to their readiness for incremental backup. If the option --uuid is not specified, the states of all virtual machines residing on the specified Hyper-V system or in the specified Hyper-V cluster are listed.

--enable-incremental { --uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID*]..."}

This is a Microsoft Hyper-V specific option.

Prepares specified virtual machines (GUIDs) for Data Protector incremental backup sessions by enabling them for incremental backup in the Hyper-V environment. To complete the preparation process, you need to further run a full backup session for them.

--disable-incremental { --uuid *VmGUID* | --uuid " *VmGUID* , *VmGUID* [, *VmGUID*]..."}

This is a Microsoft Hyper-V specific option.

Makes specified virtual machines (GUIDs) incremental backup-disabled in the Hyper-V environment. You cannot perform incremental backup on these virtual machines until you prepare them for incremental backup sessions again. Executing the vepa_util.exe command with this option specified is the only way to prevent the specified virtual machines from being backed up incrementally.

--clear-vm-lock --vm-uuid

This is a H3C CAS specific option.

It is used to clear the Virtual Machine lock of the specified H3C CAS virtual machine.

QUERY_OPTIONS

--list-organizations

This is a VMware specific option.

Lists all organizations in the vCloud Director.

--list-datacenters

This is a VMware specific option.

Lists all datacenters.

--list-datastores

This is a VMware specific option.

Lists all datastores.

--list-esx-servers [--cluster *ClusterName*]

This is a VMware specific option.

Lists all ESX Server systems.

--list-resource-pools [--hypervisor *ClusterOrESXName*]

This is a VMware specific option.

Lists all resource pools (including vApps).

The --hypervisor is a cluster or an ESX Server system. If specified as a cluster it lists all resource pools on the specified cluster. If specified as an ESX Server system it lists all resource pools on the specified ESX Server system. If the --hypervisor is not specified the --list-resource-pools option lists all datastores of the specified client.

--list-clusters [--instance *DatacenterName*]

This is a VMware specific option.

Lists all clusters on the specified client.

If the --instance option is specified, it lists all clusters on the specified datacenter.

--list-vms

This is a Microsoft Hyper-V specific option.

Lists names and GUIDs of all virtual machines configured on the specified Hyper-V system or in the specified Hyper-V cluster.

--list-sockets [--hypervisor *ESXNameOrHypervNode*]

This lists the sockets available for the hypervisor.

If the hypervisor is not specified, socket details of all hypervisors in vCenter/HyperVCluster/H3C CAS Server are listed.

--list-hostpools

This is a H3C CAS specific option. It lists all hostpools.

--list-hostsClusters

This is a H3C CAS specific option. It lists all the clusters and hosts for the specified hostpool.

--list-specificHosts

This is a H3C CAS specific option. It lists the hosts in a specific cluster.

--list-storagePools

This is a H3C CAS specific option. It lists the active storage pools in the specified host.

--list-category

This is a VMware specific option. It lists all the categories configured in a VMware vCenter server.

--list-tags [--category_id *CategoryId*]

This is a VMware specific option. It lists all the tags for the specified category in a VMware vCenter server.

--list-barlist-vms

This is a VMware specific option. It lists all the virtual machines in the barlist which contains datastores.

BROWSE_OPTIONS

--root-node *NodePath*

This option is specific to VMWare and H3C CAS Server.

Specifies a root node to start the browsing.

--inventory-view { hosts_and_clusters | vms_and_templates | tags_and_categories |storage }

This option is applicable to VMware and H3C CAS virtual environments.

The hosts_and_clusters option displays all available objects grouped by hosts and clusters.

The vms_and_templates option displays all available objects grouped by virtual machines.

The tags_and_categories option displays all available objects grouped by tags and their categories. It is a VMware specific option.

The storage option displays all available objects grouped by datacenters and datastores.

For H3C CAS, the vms_and_templates option displays only the virtual machine list.

ENVIRONMENT_OPTIONS

--virtual-environment { vmware | vCD | hyperv | H3CCAS }

Specifies the virtual environment type. Either VMWare, vCD, HyperV or H3CCAS.

--host *HostName*

Specifies the application host (for example, a vCenter Server system, ESX(i) Server system, vCloud Director, Microsoft Hyper-V system, or H3C CAS system).

CONFIG_OPTIONS

--port *PortNumber*

This option is specific to VMWare and H3C CAS Server.

Specifies the port to connect to (for example, 443).

--username *UserName*

Specifies an operating system user account for the connection.

--password *Password*

Specifies the user's password.

--encoded-password *EncodedPassword*

Specifies the user's encoded password.

--webroot *WebRoot*

This is a VMware specific option.

Specifies the web service entry point URI (for example, /sdk).

--security-model { 0 | 1 }

This option is specific to VMWare and H3C CAS Server.

Specifies the security model.

If the `0` option is specified, you have to specify all login credentials manually (standard security). H3C CAS Server supports only this option.

If the `1` option is specified, Data Protector connects to the VMware vCenter Server system with the user account under which the Data Protector Inet service on the backup host is running (integrated security). Ensure this user account has appropriate rights to connect to the VMware vCenter Server system.

ESX_CONFIG_OPTIONS

--esx-username *EsxUserName*

This is a VMware specific option.

Adds a username for the ESX Server system.

--esx-password *EsxPassword*

This is a VMware specific option.

Adds a password for the ESX Server system.

--esx-server *EsxName* [*EsxName*]...

This is a VMware specific option.

Specifies ESX Server system(s) on which to execute a command.

--datacenter *DatacenterName*

This is a VMware specific option.

Adds a datacenter to the backup client.

--ssl-thumbprint *SslThumbPrint*

This is a VMware specific option.

Specifies the thumbprint of a SSL certificate.

VM_CONFIG_OPTIONS

--instance { *DatacenterName* | *HostpoolName* }

This is a VMware and H3C CAS specific option.

Specifies the datacenter or the hostpool to which a virtual machine belongs to.

--vm *VmPath*

This is a VMware specific option.

Specifies the virtual machine (for example, /vm/myTestVM).

--transportation-mode { san | nbd | nbdssl | hotadd }

This is a VMware specific option.

Specifies the transportation mode to be used for backup. If this option is not specified, the fastest available transportation mode is used.

--quiescence

This is a VMware specific option.

Specifies whether to use Microsoft Volume Shadow Copy Service (VSS) functionality to quiesce all applications with VSS writers before performing the backup.

--quiescenceErrLvl { 0 | 1 }

This is a VMware specific option.

Specifies the level of error message to be generated if the quiescence snapshot fails: 0 (warning), 1 (fatal). Default: 0.

--uuid *VmUuid*

This is a VMware and H3C CAS specific option.

Specifies the UUID of the virtual machine.

--default

This is a VMware specific option.

Uses default virtual machine settings for all virtual machines.

--forceNonCBTFull

This option is used to disable CBT backups and force only non-CBT backups.

--allowNonCBTFull

This option is used to prevent failed CBT backup and allow fallback to non-CBT.

EXAMPLES

The following examples illustrate how the vepa_util.exe command works.

1. To configure the vCenter Server system "vc.company.com", execute:

   vepa_util command --config --virtual-environment vmware --host vc.company.com --security-model 0 --username Administrator --password XYZ --webroot /sdk --port 443

2. To check the configuration of the vCenter Server system "vc.company.com", execute:

   vepa_util command --check-config --virtual-environment vmware --host vc.company.com

3. To unlock the Virtual Machine with UUID "501bc598-e04f-449c-fd84-baacd8cb48c7" of vCenter Server system "vc.company.com", execute:

   vepa_util command --unlock-vmotion --uuid 501bc598-e04f-449c-fd84-baacd8cb48c7 --virtual-environment VMWare --host vc.company.com

4. To list all datacenters registered in the vCenter Server system "vc.company.com", execute:

   vepa_util query --virtual-environment vmware --host vc.company.com --list-datacenters

5. To browse the datacenter "PRODUCTION" registered in the vCenter Server system "vc.company.com", execute:

   vepa_util browse --virtual-environment vmware --host vc.company.com --root-node "PRODUCTION"

6. To list all vCloud Director organizations, execute:

   vepa_util query --virtual-environment vcd --host vcd.vepa.company.com --list-organizations

7. To check whether the configuration of the vCloud Director client "vcd.vepa.company.com" was successful, execute:

   vepa_util command --virtual-environment vcd --host vcd.vepa.company.com --username admin --encoded-password xaF3r3af

8. To list names and GUIDs of the virtual machines configured on the Microsoft Hyper-V virtual server "hyperclus3.company.com", execute:

   vepa_util query --list-vms --virtual-environment HyperV --host hyperclus3.company.com

9. To prepare virtual machine with the GUID "741FF564-DA19-45E5-B273-D72FA2D91998" on the Microsoft Hyper-V system "hypersysB.company.com" for incremental backup, execute:

   vepa_util command --enable-incremental --uuid 741FF564-DA19-45E5-B273-D72FA2D91998 --virtual-environment HyperV --host hyperclus3.company.com

10. To configure the virtual machine to use the "forceNonCBTFull" option, execute:

    vepa_util command –configvm –virtual-environment vmware –host peh –instance /DP DEV SA –vm /DP DEV SA/klaster/VM1_test1 –uuid '503eff1

b-9bc8-eea5-a417-7678da09d529'-quiescence 1 quiescenceErrLvl 0 –transportation-mode fastest --forceNonCBTFull

11. To configure the virtual machine to use the "allowNonCBTFull" option, execute:

    vepa_util command –configvm –virtual-environment vmware –host peh –instance /DP DEV SA –vm /DP DEV SA/klaster/VM1_test1 –uuid '503eff1 b-9bc8-eea5-a417-7678da09d529'-quiescence 1 quiescenceErrLvl 0 –transportation-mode fastest --allowNonCBTFull

12. To list all ESX names, bios UUID, and sockets for a given vCenter "vc.company.com", execute:

    vepa_util query --virtual-environment vmware --host vc.company.com --list-sockets

13. To list ESX names, bios UUID, and sockets for a given hypervisor "es1.company.com", execute:

    vepa_util query --virtual-environment vmware --host esx1.company.com --list-sockets

14. To list ESX names, bios UUID, and socket for a given hypervisor "esx1.company.com" of vCenter "vc.company.com" ,execute:

    vepa_util query --virtual-environment vmware --host vc.company.com --list-sockets --hypervisor esx1.company.com

15. To list the hyper-v node name, bios UUID, and socket for a given Hyper-V cluster "hyperclus3.company.com", execute:

    vepa_util query --virtual-environment HyperV --host hyperclus3.company.com --list-sockets

16. To list the hyper-v node name, bios UUID, and socket for a given Hyper-V node "hypernode1.company.com", execute:

    vepa_util query --virtual-environment HyperV --host hypernode1.company.com --list-sockets

17. To list the hyper-v node name, bios UUID, and socket for a given hypervisor "hypernode1.company.com" of Hyper-V cluster "hyperclus3.company.com", execute:

    vepa_util query --virtual-environment HyperV --host hyperclus3.company.com --list-sockets –hypervisor "hyperclus3.company.com"

18. To list all hostpools registered in the H3C CAS Server system "cas.company.com",execute:

    vepa_util query --virtual-environment h3ccas --host cas.company.com --list-hostpools

19. To list the clusters and hosts (not in clusters) in the H3C CAS server system cas.company.com , execute:

    vepa_util.exe query --virtual-environment h3ccas --host cas.company.com --instance /Hostpool1 --list-hostsClusters

20. To list hosts in a specific cluster in the H3C CAS server system cas.company.com" , execute:

    vepa_util.exe query --virtual-environment h3ccas --host cas.company.com --instance /Hostpool1 --cluster /Cluster1 --list-specificHosts

21. To list all the active storage pools in a H3C CAS server system cas.company.com , execute:

    vepa_util.exe query --virtual-environment h3ccas --host cas.company.com --instance /Hostpool1 --hypervisor /Hypervisor1--list-storagePools

22. To list all categories in the VMware VCenter server host, execute the following:

    vepa_util.exe query --virtual-environment vmware --host vc.company.com --list-category

23. To list all tags of a specified category for a given VMware vCenter server, execute the following:"

    vepa_util.exe query --virtual-environment vmware --host vc.company.com --list-tags --category_id *Category_id*

24. To list all virtual machines in a barlist which contains datastores, execute the following:

    vepa_util.exe query --virtual-environment vmware --host vm.company.com --barlist *BarlistName*--list-barlist-vms

25. To browse for VMs by tags and categories for a datacenter "DP" in VMware Infrastructure, execute the following:

    vepa_util.exe browse --virtual-environment VMWare --host vc.company.com --root-node DP --inventory-view tags_and_categories

26. To configure virtual machine hyperv.company.com , execute:

    vepa_util.exe command --configvm --host host.company.com --virtual-environment hyperv --instance HyperV --vm hyperv.company.com --uuid <VM_UUID> --quiescence quiescenceErrLvl1

27. To browse for VMs by datastores and storage for a datacenter "DP" in VMware Infrastructure, execute the following:

    vepa_util browse --virtual-environment VMWare --host vm.company.com --root-node DP --inventory-view storage

SEE ALSO

omniintconfig.pl(1M), util_cmd(1M), util_oracle8.pl(1M)

StoreOnceSoftware utility

The StoreOnceSoftware utility is a service/daemon and maintenance tool for performing general administration tasks on the StoreOnce library (the deduplication store).

Note On Windows systems, the term utility refers to the StoreOnceSoftware.exe service. On Linux systems, StoreOnceSoftwared is a script which utilizes the StoreOnceSoftware CLI (the options are: {start | stop | status}).

Synopsis

```
StoreOnceSoftware --help | -h

StoreOnceSoftware --version

StoreOnceSoftware --configure_store_root --path=RootDirectory [--force] [LOG_OPTIONS]

StoreOnceSoftware --create_store --name=StoreName

[--store_description=StoreDescription] [LOG_OPTIONS]

StoreOnceSoftware --modify_store --name=StoreName

[--store_description=StoreDescription] [LOG_OPTIONS]

StoreOnceSoftware --delete_store --name=StoreName [LOG_OPTIONS]

StoreOnceSoftware --start_store --name=StoreName [--set_readonly=ON | OFF] [LOG_OPTIONS]

StoreOnceSoftware --stop_store --name=StoreName [--force] [LOG_OPTIONS]

StoreOnceSoftware --set_autostart=ON | OFF --name=StoreName [LOG_OPTIONS]

StoreOnceSoftware --list_stores [--name=StoreName] [LOG_OPTIONS]

StoreOnceSoftware --get_server_properties [LOG_OPTIONS]

StoreOnceSoftware --set_readonly=ON | OFF [--name=StoreName] [--force] [LOG_OPTIONS]

LOG_OPTIONS

[--log_path=LogPath]

[--log_level=no_log | fatal | critical | error | warning |

notice | information | debug | tracing]
```

Note The same format is used for options on both, Windows and Linux platforms:

- --option or --option=Value
- The short notation only works for the help option: --help or -h

Note the following:

- Before any administrative store commands can be used, the StoreOnceSoftware utility must be running, otherwise, an error message is displayed.

If the StoreOnceSoftware utility is not running and you do not specify a parameter, the following message is displayed: The daemon is stopped .

- When starting the utility, you can define a path for logs and a logging-level with the options

--log_path and --log_level .

- If the command-line option is not recognized (for example, the option is specified without the leading characters '-- '), the following message is displayed:

Unknown option specified: unknown_option.

- You can use the omnirc command OB2DBGDIR for debugging purposes. Ensure that the path is in the correct format. For instance, OB2DBGDIR=/SOSLogs/.

- If you specify --log_path for logging, you must specify the path in the correct format. For instance, --log_path=/SOSLogs/postfix.txt.

Description

--help | -h

Displays a list of CLI options with descriptions.

--configure_store_root --path=RootDirectory [--force]

Configures the root directory of the store(s). The root directory must be configured before you can create a store. When StoreOnce software deduplication is first installed, it is running in a non-configured mode and cannot be used until the root directory of the store has been set. The option --path specifies the path to the root directory. The path must not be empty, must be a valid directory which already exists on the system, and not previously used as a store-root path. If successful, Data Protector displays the path in the CLI. If the root directory cannot be configured (there may be several reasons), you are prompted to stop/start the utility (daemon). Use the stop/start commands given below.

When the root directory is configured, Data Protector automatically creates the subdirectory StoreOncelibrary below the root directory.

Use the --force option to reconfigure the location of the root directory in cases where the actual data has been moved to another location. Make sure the data is already at the specified location before using the --force option (see below for details).

Once the root directory is configured, it cannot be reconfigured through the GUI. To move the store to a new, never previously used, location (in case of a disaster recovery or being unable to use the existing mount point), proceed as follows:

1. Stop the StoreOnceSoftware utility.

   Windows systems: Use net stop StoreOnceSoftware or use the Service Manager

   Linux systems: Use /opt/omni/lbin/StoreOnceSoftwared stop)

2. Manually move the data from the *Old_Path* to the *New_Path*. This means the subdirectory StoreOncelibrary and all its contents.

3. Run the command:
   StoreOnceSoftware --configure_store_root --path=New_Path --force
   (make sure New_Path includes the full path, for example, --path=C:\Volumes\ NewRoot)

4. Start the StoreOnceSoftware utility.

   Windows systems: Use net start StoreOnceSoftware or use the Service Manager

   Linux systems: Use /opt/omni/lbin/StoreOnceSoftwared start)

--log_path=LogPath

Defines a path where logs are to be stored.

--log_level={no_log | fatal | critical | error | warning | notice | information | debug | tracing}

Defines the logging detail as defined by:

no_log	Logging is disabled (default value).
fatal	A fatal error. The application will most likely terminate. This is the highest severity.
critical	A critical error. The application might not be able to continue running successfully
error	A non-critical error. An operation did not complete successfully, but the application continues.
warning	A warning. An operation completed with an unexpected result.
notice	A notice, which is information with a higher severity.
information	An informational message, usually denoting the successful completion of an operation.
debug	A debugging message.
tracing	A tracing message. This is the lowest severity.

--create_store --name=StoreName [--description=StoreDescription]

Creates a deduplication store with the specified name. Depending on the success of the operation, one of the following messages is displayed:

- If successful: The store: StoreName has been created successfully.
- If the store exists: The store StoreName has already been created.
- If an error occurs: Failed to create the store: StoreName
- If a name is not specified:

  The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart, require the name option.

--modify_store --name=StoreName [--description=StoreDescription]

Modifies the store with the specified name.

--delete_store --name=StoreName [--force]

Deletes the store with the given store name. The store is stopped before it is deleted.
If the –-force option is used, the operation will try to close all the current activities, stop the store and then delete the store.
One of the following messages is displayed:

- If successful: The store: StoreName has been deleted successfully.
- If an error occurs: Failed to delete the store: StoreName.
- If name of the store is not specified:

The options --start_store, --stop_store, --create_store, --delete_store and --set_autostart require the --name option.

--start_store --name=StoreName [--set_readonly=ON|OFF]

Starts the store specified by the store name. Depending on the success of the operation, one of the following messages is displayed:

- If successful: The Store StoreName has been successfully started.
- If already started: The store: StoreName has already been started.
- If an error occurs: Failed to start the store: StoreName
- If a name is not specified:

The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart require the name option.

--stop_store --name=StoreName [--force]

Stops the store specified by the store name. If the –-force option is used, the store attempts to close all current connections and then stops the store. Depending on the success of the operation, one of the following messages is displayed:

- If successful: The store: StoreName has been stopped successfully.
- If already stopped: The store: StoreName has already been stopped.
- If an error occurs: Failed to stop the store: StoreName
- If a name is not specified: The options --start_store, --stop_store, --create_store, --delete_store, and --set_autostart require the --name option.

--set_autostart=ON|OFF --name=StoreName

Sets a store to be started automatically (ON) or not automatically started (OFF). Depending on the success of the operation, one of the following messages is displayed:

- If successful: Autostart option for the store StoreName successfully set to ON/OFF.
- If an error occurs: Failed to set Autostart option for store: StoreName
- If a name is not specified: The options --start_store, --stop_store, --create_store, and --set_autostart require the name option.

--list_stores

Displays a list of stores that are configured on the StoreOnce Software deduplication system. It includes the following information:

- Store Name
- Store ID
- Store Description
- Store Status
- Store Autostart status
- User Data Stored (original, not deduplicated data)
- Store Size on Disk (resulting, deduplicated data)
- Deduplication Ratio

Depending on the success of the operation, one of the following messages is displayed:

- If successful: Listing of the stores succeeded.
- If an error occurs: Failed to list the stores.
- If no stores can be identified: There are no stores in database.

--list_stores supports the use of the --name option, which lists only the information about the store specified with the --name option. The following is a typical output showing three stores:

```
C:\Users\Administrator>StoreOnceSoftware --list_stores

Store Name:             StoreOnceLibrary
Store Id:               1
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       1305 MB
Store Size on Disk:     770 MB
Deduplication Ratio:    1.7 : 1

Store Name:             Berlin_Store
Store Id:               2
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       20 MB
Store Size on Disk:     1530 KB
Deduplication Ratio:    13.7 : 1

Store Name:             Lisbon_Store
Store Id:               5
Store Description:      Data protector store
Store Status:           started
Store Autostartable:    ON
User Data Stored:       4549 MB
Store Size on Disk:     1174 MB
Deduplication Ratio:    3.9 : 1

Listing of the stores succeeded.
```

--get_server_properties

Displays a list of server/store related properties:

- Path and name of the root directory (Store Root:)
- Existing stores
- Available stores
- Space capacity

- Disk space free

```
C:\Users\Administrator>StoreOnceSoftware --get_server_properties
Store Root:             c:\StoreOnceRoot

Existing Stores:        3
Available Stores:       29
Disk Capacity:          49 GB
Disk Space Free:        29 GB

Listing of the daemon properties succeeded.
```

--daemon

Applies to Linux systems only. Run StoreOnceSoftware as a daemon for debugging purposes.

If the option --name is used in combination with non-valid options, the following message is displayed:

The option --name can only be specified with the --start_store, --stop_store, --create_store, --delete_store, --set_autostart or the --list_stores command.

The option --description can only be used when creating a store (--create_store).

Section 5: Miscellaneous

omnigui - describes usage of the commands that launch the Data Protector GUI.

SYNOPSIS

GUICommand [-help]

GUICommand

manager [*ContextOptions*] [-server *HostName*]

mom [*ContextOptions*] [-server *HostName*]

ContextOptions

-admin

-backup

-clients

-copy

-db

-instrec

-monitor

-report

-restore

-users

DESCRIPTION

These commands are used to launch the Data Protector GUI and activate all or any combination of the Data Protector GUI contexts.

To use the Data Protector GUI functionality with Linux Cell Manager systems, on which the Data Protector GUI is not available, use the omniusers command to remotely add a new Data Protector user to a Cell Manager on which the Data Protector GUI is not installed. It is **mandatory** that the **user added has a password defined** or the connection will fail. You can then use the user account of the newly added Data Protector user to launch the Data Protector GUI on another system with the Data Protector GUI installed, and connect to the Cell Manager. For details, see the omniusers reference page.

COMMANDS

manager

Launches the Data Protector GUI with all Data Protector contexts activated, or, when additional options are specified, with the specified Data Protector contexts activated.

mom

Launches the Data Protector Manager-of-Managers GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts) or, when additional context options are specified, with the specified Data Protector contexts activated.

OPTIONS

-help

Displays the usage synopsis for the specified command.

-server *HostName*

Connects to the specified Cell Manager.

-display *HostName:0*

Redirects the output to the display on the specified system.

-admin

Launches the Data Protector GUI with the Devices & Media contexts activated.

-backup

Launches the Data Protector GUI with the Backup context activated.

-clients

Launches the Data Protector GUI with the Clients context activated.

-copy

Launches the Data Protector GUI with the Object Operations context activated.

-db

Launches the Data Protector GUI with the Internal Database context activated.

-instrec

Launches the Data Protector GUI with the Instant Recovery context activated.

-monitor

Launches the Data Protector GUI with the Monitor context activated.

-report

Launches the Data Protector GUI with the Reporting context activated.

-restore

Launches the Data Protector GUI with the Restore context activated.

-users

Launches the Data Protector GUI with the Users context activated.

EXAMPLES

1. manager

   This command launches the Data Protector GUI with all contexts activated.

2. manager -admin -monitor -report -server host3

   This command launches the Data Protector GUI with the Devices & Media, Monitor, and Reporting contexts activated and connects to the Cell Manager with the hostname "host3".

SEE ALSO

ob2install(1M), omniintro(9), omnimigrate.pl(1M), omnisetup.sh(1M), omniusers(1), upgrade_cm_from_evaa(1M)

GUI Descriptions

Provides description of fields in Data Protector GUI.

SAP HANA Configuration

This page explains the configuration details that you need to enter during the creation of an SAP HANA backup specification.

Login information for System Database

Username

Enter your SYSTEM DB username in this text box.

Password

Enter your SYSTEM DB password in this text box.

Instance number

Enter the instance number in this text box. You can only enter numeric values. The value must be between 0-99.

Port (Optional)

Enter the Instance SQL port number in this text box. This is an optional field. Based on the instance number you enter, the port gets updated automatically.

Instance base path

Enter the Instance base path. It is a path to a directory which contains files for the operation of a local instance as well as links to the data for one system. For example, /usr/sap/*<SID>*.

Application specific options - SAP HANA

This page explains the Advanced SAP HANA integration specific options.

General Information

Pre-exec

You can specify a pre-exec script in this dialog box, if any.

Post-exec

You can specify a post-exec script in this dialog box, if any.

Parallelism

This specifies the number of streams per database which can be backed up in parallel. The parallelism option is by default set to 3. The maximum value is 32 and the minimum value is 1. It is determined by the volume of the data backup.

Backup Prefix

Enter the backup prefix. The default backup prefix value is `DATA_<sid>` .

Browse Drives

In this page you specify the location of your device.

You cannot browse network drives in this dialog. Enter the path to them directly.

Important Network disks have to be mapped to a drive. The notation `\\Hostname\ShareName` is not supported, use the notation `DriveLetter:\DataStore\FileLibraryShare` instead.

Note In a Manager-of-Managers environment, you cannot browse drives if the file library resides on a client from another cell.

Related topic

- Configure a file library device

Directories

Summarizes the file library device properties.

Directory Name

The full path to the file library device on the disk where it resides.

Total Size (GB)

The total amount of space the file library device occupies on disk.

Max. File Depot Size (GB)

The maximum amount of size a file depot can reach.

Available Disk Space (GB)

The total amount of space available on the disk where the file library device resides.

Min. Space

The minimum amount of free disk space the file library device requires to function.

Tasks

- Setting File Library Device Properties

Properties - File Library Device

The options in this page set the file library device sizing properties and apply to each file depot in the file library device.

Maximum size of file depot (GB)

Enter the maximum amount of space you want to allocate to each file depot in the file library.

Minimum free disk space to create new file depot (MB)

Enter the minimum amount of space that needs to be available on the disk for creating another file depot in the file library device.

Amount of disk space which should be free on disk (MB)

Enter the minimum amount of space which must be kept free on the disk where the file library device resides.

Event if the free disk space drops below (%)

Enter a percentage of free disk space used by the file library device at which will send a message to the Event Log.

Tasks

- Setting File Library Device Properties

File Library Devices

In the Results Area, you can choose between directories and drives of the selected file library.

The following may be helpful:

- To display the properties of a library, right-click the library and click **Properties**.
- To display the configured drives of the library, double-click **Drives** in the Results Area.
- To display the directories of the library, double-click **Directories** in the Results Area.

Related topics

- File library devices

Related tasks

- Configure a file library device
- Set up file library device properties

File Library Device/ Smart Cache Device

In this page, specify a directory or a set of directories where you would like the file library/smart cache device to reside.

Add

Adds one or more directories where the file library/smart cache device is located.

Browse

Allows you to search for the directory/directories where you would like the file library/smart cache device to reside. In a MoM environment, you cannot browse drives if the file library resides on a client from another cell.

Properties

Set the sizing properties for file depots.

Delete

Removes the specified path(s) to the file library/smart cache device.

Number of writers

Specify the number of writers to the file library device. A writer is the equivalent of a tape drive. Note that you cannot specify more than 255 writers.

> **Note** This option is not applicable to Smart Cache device.

Related tasks

- Configure a file library device
- Configure backup to disk devices

Settings - File Library Device Properties

In this page, file library settings are specified.

Media Type

The file library's media type is File.

Distributed file media format

Use distributed file media format Select this option to enable the file library for virtual full backup. Backing up to a file library with distributed file media format is a prerequisite for virtual full backup. If you are not planning to use virtual full backup, do not select this option.

> **Note:** Media that uses distributed file media format cannot be exported or imported. To clean up a backed up distributed file library, see Unable to clean up a distributed file library.

Summary Tab - File Library Device/ Smart Cache Device

This tab is for information purposes and shows you details of the current file library device settings. It includes the following information:

Directory Name

The full path to where the file library/smart cache device is saved.

Total Size

The total amount of space allocated to the entire file library/smart cache device.

Used

The amount of space allocated to the file library device/smart cache which has already been used for backups.

Max Avail. for Backup

The total amount of space available to save data in the file library/smart cache device.

Max. File Depot Size

The maximum size of a single file depot.

Consolidation Tasks

In the Results Area, the following object consolidation tasks are available:

Objects

Double-click this item to consolidate objects interactively from the Objects starting point.

Sessions

Double-click this item to consolidate objects interactively from the Sessions starting point. Use this starting point to list sessions in which objects were written to media.

Automated post-backup consolidation

Double-click this item to configure a post-backup object consolidation specification. Post-backup object consolidation takes place after the completion of a backup session. It consolidates objects backed up in that particular backup session that match the specified criteria.

Automated scheduled consolidation

Double-click this item to configure a scheduled object consolidation specification. Scheduled object consolidation takes place at a user-defined time. Objects backed up during different backup sessions can be consolidated in a single scheduled object consolidation session.

Device Properties - General

In this page you can set options for the selected destination device.

Concurrency

Concurrency allows more than one Disk Agent to write to one backup device concurrently. This helps Data Protector keep the device streaming because it can accept data faster than a Disk Agent can send it. The data from these Disk Agents is interleaved on the media. The maximum concurrency value is 32. Data Protector provides default concurrencies for all supported devices. The maximum device concurrency for devices that are used for backing up Microsoft Exchange Server data is 2 for devices connected to the Exchange Server system directly and 1 for those connected to the Exchange Server system remotely. Specify the number of Disk Agents that can write concurrently to a device. This option can be specified for backup, object copy, and object consolidation operations.

CRC check

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during backup. The CRC checks allow you to verify the media after the backup. Dat Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying media or verifying objects. By default this option is not selected. This option can be specified for backup, object copy, and object consolidation operations.

Drive-based encryption

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media. For an up-to-date list of media that support drive-based encryption, see the latest Support Matrix.

Media pool

Prealloc list

Add

Click here to display a list of media that can be added to the prealloc list.

Delete

Removes the selected medium from the prealloc list.

Select New Device

In this page you select a new device to be used for reading the full backup in the object consolidation session.

Original device

The name of the selected device that was used for writing the full backup of the data.

New Device

To use a different device for the consolidation operation, select a device from the list and click**OK**.

Save or Start an Object Consolidation Session

You can save or start the object consolidation session you have configured.

Save As

Click the button to save the object consolidation specification.

Start Interactive Consolidation

Click the button to start the interactive object consolidation session.

Object Consolidation - Copies

In this page, a list of source objects that will participate in the session is displayed. In case of alternative restore chains, it may happen that not all the listed object versions will actually be used.

Object Name

The name of the object.

Version

The object version.

Copy selection

The selection of the copy of the object version to be used as a source (in case the object version has object copies) is automatic by default. You can disable automatic selection by specifying which copy to use in the object's properties dialog.

Properties

If the object version has object copies, click this button to manually select which copy will be used.

Object Consolidation - Backup Specifications

In this page, select backup specifications for the object consolidation operation.

All backup specifications

Select this option to include all backup specifications in the operation. If you configure new backup specifications at a later time, they will also be included.

Selected backup specifications

Select this option to include only specific backup specifications. Select the desired backup specifications.

Object Consolidation - Destination Devices

In this page, the devices that will write the consolidated objects are specified.

Show all

Select this option to display all configured devices.

Show selected

Select this option to display only selected devices.

Properties

To modify the properties of a device, select the device, highlight it, and then click this button.

Min devices

Specify the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be used) required for starting the session. If fewer devices are available than specified here, the session will queue. Default: 1.

Max devices

The maximum number of available devices that Data Protector will use in the session. Note that Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. Default: 5.

Object Consolidation - Time Frame

In this page, specify the time frame for the selection of objects to be consolidated. Only objects backed up in the specified time frame will be considered for object consolidation.

Include objects backed up in timeframe

This option defines the time frame within which Data Protector will search for sessions.

Relative time

Select this option to set a relative period of time, and then specify the time frame. The first number specifies the beginning of the time frame, and the second number the duration of the time frame. For example, if you specify 24 in the first field and 22 in the second field, and the operation is scheduled today at 22:00, Data Protector will consolidate objects from the sessions that took place between 22:00 yesterday and 20:00 today.

Absolute time

Select this option to set an absolute period of time. Specify the starting and the end date of the period. Click the drop-down arrows to display the calendar.

No time limit

Select this option to include all sessions, regardless of when they were performed.

Object Consolidation - General

In this page, specify the name of the object consolidation specification.

Consolidation specification name

Specify the name of the object consolidation specification.

Object Consolidation - Objects

Select the points in time of the desired objects to consolidate. You cannot select full backups, as they as such cannot be consolidated.

Selecting a point in time selects the entire restore chain. If several restore chains for the same point in time exist, all of them are selected, but only one will actually be used. Your selection is marked in blue, other incrementals that comprise the restore chain are marked in black, and the corresponding full backup in gray (shaded). The blue check mark indicates the point in time that will be consolidated.

You can select several points in time for consolidation, and the restore chains may overlap. If you select a point in time that already has a black check mark, the check mark will become blue.

To clear a selected restore chain, click the blue check mark. The entire restore chain is cleared, unless some object versions are part of another restore chain, in which case they remain selected with a black check mark.

Object Consolidation - Media

In this page, a list of media containing the selected objects is displayed. Media are listed for all object versions that will participate in the session. In case of alternative restore chains, all possible media are listed, although not all will actually be used in the session. If more than one copy of the same object version exists, you can influence the media selection by specifying the media location priority.

Change Priority

To change the media location priority for this session, select a media location and click this button.

Object Consolidation - Object Filter

In this page, select objects for the object consolidation operation.

All objects

Select this option to include all backed up objects in the operation. If you back up new objects at a later time, they will also be included.

Selected objects

Select this option to include only specific objects. Select the desired objects.

Include only protected versions of selected objects

Object Consolidation - Object Options

The options in this page apply only to the selected object. To change options for all objects, close this dialog and return to the Options property page.

Source object options

Recycle data and catalog protection after successful consolidation

Read device for incremental backups

You can select a specific file library or B2D device (except Smart Cache) drive to read the selected object.

Consolidation options

- Protection
- Catalog protection
- Logging
- Log All
- Log Directories
- Log Files
- No Log

Write device

By default, Data Protector automatically selects the most appropriate devices from those you specified in the Destination page, taking into account the device block size and the connection of a device. To use a specific device for the selected object, select it from the drop-down list.

Object Consolidation - Object Source

In this page you can select manually which copy of the object version to use if object copies exist.

Select source copy manually

Select this option to select the copy of the object version manually, and select a copy from the drop-down list.

Needed media

Depending on the selected copy, the needed media are listed.

Object Consolidation - Options

In this page, specify options for the object consolidation.

Source object options

Recycle data and catalog protection after successful consolidation

Filter source objects by owner

Select this option to consolidate only the objects belonging to the specified backup object owner. You can enter filter criteria in the User, Group, and System fields as desired. The specified Data Protector user needs no longer be configured in the cell.

User

(available when **Filter source objects by owner** is selected) The logon name of a Data Protector user.

Group

(available when **Filter source objects by owner** is selected) The Windows domain or UNIX user group of a Data Protector user.

System

(available when **Filter source objects by owner** is selected) The hostname or IP address of the Data Protector system where the original backup session was run.

Consolidation options

- Protection
- Catalog protection
- Logging
- Log All
- Log Directories
- Log Files
- No Log

The owner of the consolidated backup objects is the user who started the original backup sessions.

Object Consolidation - Source Devices

In this page, the devices that will read the backups are specified.

Read devices for incremental backups

The file libraries or B2D devices (except Smart Cache) where incremental backups reside are listed. Select the desired devices. Your selection of individual file libraries or B2D devices limits the operation to those object versions that have incremental backups in the selected devices.

Read devices for full backups

By default, the devices that were used for writing the full backup of the selected objects are used for reading this backup in the object consolidation operation. You can change these devices here if desired.

Original device

With interactive object consolidation, the devices that were used for writing the full backup of the selected objects are listed.With automated object consolidation, all devices configured in the Data Protector cell are listed.

New device

If you have changed the original device, the name of the new device to be used in the object consolidation operation appears here.

Change

After clicking the original device, click here to select a new device.

Object Consolidation - Summary

In this page, a summary of the selected objects is displayed.

Object Name

The name of the object.

Version

The object version.

Copy selection

The selection of the copy of the object version to be used as a source (in case the object version has object copies) is automatic by default. You can disable automatic selection by specifying which copy to use in the object's properties dialog in the Copies page.

Properties

To display an object's properties, select the object and click this button.

Delete

To remove an object from the list, select the object and click this button.

Start Consolidation

Select the session from the drop-down list.

Automated Object Consolidation

Data Protector provides the following methods of automated object consolidation:

Post Backup

Post-backup object consolidation takes place after the completion of a backup session. It consolidates objects backed up in that particular backup session that match the specified criteria.

Scheduled

Scheduled object consolidation takes place at a user-defined time. Objects backed up during different backup sessions can be consolidated in a single scheduled object consolidation session.

Automated Object Consolidation - Post-Backup

In the Results Area, a list of configured object consolidation specifications is displayed.

Name

The name of the object consolidation specification. The following may be helpful:

- To immediately start a configured post-backup object consolidation specification, right-click the specification and click **Start Consolidation**.
- To immediately copy a configured post-backup object consolidation specification, right-click the specification and click **Copy As**.

Automated Object Consolidation - Post-Backup

In the Results Area, a list of configured object consolidation specifications is displayed.

Name

The name of the object consolidation specification.

Scheduled

The date and time when the operation is scheduled to run. For recurring operations, the first scheduled occurrence is shown. The following may be helpful:

- To immediately start a scheduled object consolidation specification, right-click the specification and click **Start Consolidation**.
- To immediately copy a scheduled object consolidation specification, right-click the specification and click **Copy As**.

Consolidation

Data Protector provides the following methods of object consolidation:

Interactive

Expand this item to consolidate objects interactively.

Automated

Expand this item to configure automated object consolidation. Choose between post-backup and scheduled object consolidation.

Copy As

Enter a new name for the specification.

Name

You can use only alphanumeric and the following characters: **_ - ( )**.

Copy Tasks

In the Results Area, the following object copy tasks are available:

Objects

Double-click this item to copy objects interactively from the Objects starting point. Use this starting point to list types of backed up data, such as Filesystem, Database, and so on.

Sessions

Double-click this item to copy objects interactively from the Sessions starting point. Use this starting point to list sessions in which objects were written to media.

Media

Double-click this item to copy objects interactively from the Media starting point. Use this starting point to list media pools and media.

Automated post-backup copy

Double-click this item to configure a post-backup object copy specification. Post-backup object copying takes place after the completion of a backup session. It copies objects backed up in that particular backup session that match the specified criteria.

Automated scheduled copy

Double-click this item to configure a scheduled object copy specification. Scheduled object copying takes place at a user-defined time. Objects backed up during different backup sessions can be copied in a single scheduled object copy session.

Device Properties - General

In this page you can set options for the selected destination device.

Concurrency

Concurrency allows more than one Disk Agent to write to one backup device concurrently. This helps Data Protector keep the device streaming because it can accept data faster than a Disk Agent can send it. The data from these Disk Agents is interleaved on the media. The maximum concurrency value is 32. Data Protector provides default concurrencies for all supported devices. The maximum device concurrency for devices that are used for backing up Microsoft Exchange Server data is 2 for devices connected to the Exchange Server system directly and 1 for those connected to the Exchange Server system remotely. Specify the number of Disk Agents that can write concurrently to a device. This option can be specified for backup, object copy, and object consolidation operations.

CRC check

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during backup. The CRC checks allow you to verify the media after the backup. Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying media or verifying objects. By default this option is not selected. This option can be specified for backup, object copy, and object consolidation operations.

Drive-based encryption

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media. For an up-to-date list of media that support drive-based encryption, see the latest Support Matrix.

Media pool

Prealloc list

Add

Click here to display a list of media that can be added to the prealloc list.

Delete

Removes the selected medium from the prealloc list.

Select New Device

In this page you select a new device to be used as a source device for object copying.

Original Device

The name of the device that was used for writing the data, and is by default also used for copying objects.

New Device

To use a different device for the copy operation, select the device from the list and click**OK**. To revert to the original device, select (**original device**) and click **OK**.

Library

The name of the library in which the device resides.

Device Tag

Devices with the same device tag name can replace each other if needed. Such devices must be of the same media type and from the same library. Otherwise, automatic replacement is not successful.

Device Status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here. If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility.

Object Copy - Consolidation Specifications

In this page, select object consolidation specifications for the object copy operation.

Show

In the drop-down list, select one of the following:

All specifications

Select this option to include all object consolidation specifications in the operation. If you configure new specifications at a later time, they will also be included.

Selected specifications

Select this option to include only specific object consolidation specifications. Select the desired specifications.

Capable of replication

Lists all specifications that have a StoreOnce or DD Boost device selected as a destination device. Objects created in a such a session can then be replicated to a different device of the same type. Select this option to include only object consolidation specifications that can be replicated.

View by

In the drop-down list, select one of the following:

Name

Select this option to list selected object consolidation specifications by filename.

Type

Select this option to list selected object consolidation specifications by type.

> **Tip** To select or deselect all specifications in a directory, right-click on the chosen directory in the Results Area.

Object Copy - Copy Specifications

In this page, select object copy specifications for the object copy operation.

Show

In the drop-down list, select one of the following:

All specifications

Select this option to include all object copy specifications in the operation. If you configure new specifications at a later time, they will also be included.

Selected specifications

Select this option to include only specific object copy specifications. Select the desired specifications.

Capable of replication

Lists all specifications that have a StoreOnce or DD Boost device selected as a destination device. Objects created in a such a session can then be replicated to a different device of the same type. Select this option to include only object consolidation specifications that can be replicated.

View by

In the drop-down list, select one of the following:

Name

Select this option to list selected object copy specifications by filename.

Type

Select this option to list selected object copy specifications by type.

Tip To select or deselect all specifications in a directory, right-click on the chosen directory in the Results Area.

Save or Start an Object Copy Session

You can save or start the object copy session you have configured.

Save As

Click the button to save the object copy specification.

Start Interactive Copy

Click the button to start the interactive object copy session.

Object Copy - Backup Specifications

In this page, select backup specifications for the object copy operation.

Show

In the drop-down list, select one of the following:

All specifications

Select this option to include all backup specifications in the operation. If you configure new specifications at a later time, they will also be included.

Selected specifications

Select this option to include only specific backup specifications. Select the desired specifications.

Capable of replication

Lists all specifications that have a StoreOnce or DD Boost device selected as a destination device. Objects created in a such a session can then be replicated to a different device of the same type. Select this option to include only object consolidation specifications that can be replicated.

View by

In the drop-down list, select one of the following:

Group

Select this option to list selected backup specifications by backup groups.

Important If you change from group view to any other view, Data Protector issues a warning that changing the view will remove all current selections. If you continue, all previous selections are cleared.

Name

Select this option to list selected backup specifications by filename.

Type

Select this option to list selected backup specifications by type.

Tip To select or deselect all specifications in a directory, right-click on the chosen directory in the Results Area.

Object Copy - Destination Devices

In this page, the destination devices are specified.

> **Important** The minimum number of devices required for copying SAP MaxDB, DB2 UDB, or Microsoft SQL Server integration objects equals the number of devices used for backup. The concurrency of the devices used for backing up and copying these objects must be the same.

Show all

Select this option to display all configured devices.

Show Capable of replication

Select this option to include libraries that are able to replicate data.

Show selected

Select this option to display only selected devices.

Properties

To display the properties of a device, select the device, highlight it, and then click this button.

Min devices

Specify the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be used) required for starting the session. If fewer devices are available than specified here, the session will queue. Default: 1.

Max devices

The maximum number of available devices that Data Protector will use in the session. Note that Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. Default: 5.

Object Copy - Object Filter

In this page, specify the criteria for object selection. Only the objects matching the specified criteria will be copied.

Include only protected objects

Include only objects with number of copies less than

Include objects backed up in timeframe

(*available for scheduled object copying*) This option defines the time frame within which Data Protector will search for sessions.

Relative time

Select this option to set a relative period of time, and then specify the time frame. The first number specifies the beginning of the time frame, and the second number the duration of the time frame. For example, if you specify 24 in the first field and 22 in the second field, and the operation is scheduled today at 22:00, Data Protector will copy objects from the sessions that took place between 22:00 yesterday and 20:00 today.

Absolute time

Select this option to set an absolute period of time. Specify the starting and the end date of the period. Click the drop-down arrows to display the calendar.

No time limit

Select this option to include all sessions, regardless of when they were performed.

Automated Copy Operation - Foreign Cell Destination

In this page, the target device from the foreign Cell Manager is specified.

Foreign Cell Manager

Select the foreign cell server that you have imported. This lists the devices that are linked to the backup to disk store.

All the devices that are created from the target cell manager are displayed here. Therefore, ensure that you select the correct device for replication. If the Replicate to a foreign cell check box is not selected, the options in this page are disabled.

Object Copy - General

In this page, specify the name of the object copy specification.

Copy specification name

Specify the name of the object copy specification.

Object Copy - Library Filter

In this page, specify the library filter for object selection. Only objects residing on media in the specified libraries will be copied.

All libraries

Select this option to include all the listed libraries in the operation.

Libraries capable of replication

Select this option to include libraries that are able to replicate data.

Selected libraries

Select this option to include only specific libraries. Select the desired libraries.

Object Copy - Objects

Select the objects to copy.

> **Note** The GUI also shows backed up objects that cannot be copied.

> **Important** The Data Protector SAP MaxDB, DB2 UDB, and Microsoft SQL Server integrations have interdependent data streams. Hence the object copy operation must preserve the layout of objects on media to enable a restore. To ensure this, select all objects of these integrations with the same backup ID for copying. Otherwise, a restore from the copy will not be possible.

The content of the Results Area depends on the starting point you have selected:

- Objects

  Types of backed up data are listed, such as Filesystem, Internal Database, and so on. Expand a type of data, then a client and its logical disks or mount points to display the object versions.

  Object versions of certain types of backed up data, such as Microsoft Exchange Server 2010 or later, or Microsoft Hyper-V, are not listed in the Objects scope. Use the Session or the Media scope instead.

  To copy a restore chain (all backups that are necessary for a restore) of an object version, right-click the object version and click Select Restore Chain. The selection of a restore chain is not available for integration objects.

- Sessions

  Sessions are listed. Expand a session to display the object versions that were written in that session.

  To copy a restore chain (all backups that are necessary for a restore) of an object version, right-click the object version and click **Select Restore Chain**. The selection of a restore chain is not available for integration objects.

  To select all integration objects with the same backup ID, right-click an integration object and click**Select Backup Set**.

- Media

  Media pools are listed. Expand a media pool and then a medium to display the object versions residing on it.

  > **Note** For VMware backups, the virtual machine disks are considered as objects that run in parallel. The disk objects of the virtual machine are listed but disabled in the **Media** list to understand virtual machine disks backed to the media. The copy or verify operation is performed on the virtual machine objects and all its associated disk objects are considered internally. For VMware integration, the **Next** option is enabled only after selecting the virtual machine object in the **Media** list.

Enable selection of protected objects only

Object Copy - Media

In this page, a list of media containing the selected objects is displayed. If the Objects or Sessions starting point was used and more than one copy of the same object version exists, you can influence the media selection by specifying the media location priority.

Change Priority

(*available with Objects or Sessions as a starting point*) To change the media location priority for this session, select a media location and click this button.

Object Copy - Object Options

The options in this page apply only to the selected object. To change options for all objects, close this dialog and return to the Options property page.

Important If you select the **Change data and catalog protection after successful copy** option when you are copying objects from a ZDB to disk+tape session, be aware that after the period you specify, the source objects can be overwritten. After the media are overwritten, instant recovery from this backup using the GUI will no longer be possible.

Source object options

Change data and catalog protection after successful copy.

Target object options

- Protection
- Catalog protection
- Logging
- Log All
- Log Directories
- Log Files
- No Log

Write device

By default, Data Protector selects the most appropriate destination devices automatically, taking into account the device block size and the connection of a device. To use a specific device, select it from the drop-down list.

Object Copy - Copy Source

In this page you can select manually which copy of the object version to use if more than one copy exists.

Select source copy manually

Select this option to select the copy of the object version manually, and select a copy from the drop-down list.

Needed media

Depending on the selected copy, the needed media are listed.

Object Copy - Options

In this page, specify options for the object copy.

If you select the Change data and catalog protection after successful copy option when you are copying objects from a ZDB to disk+tape session, be aware that after the specified period expires, the source objects for object copy may be overwritten. After the backup media are overwritten, instant recovery from this backup using the GUI is no longer possible.

Device options

- Use replication
- Replicate to foreign cell

Source object options

- Change data and catalog protection after successful copy
- Recycle data and catalog protection of failed source objects after successful copy

(available with automated copy)

Filter source objects by owner

Select this option to copy only the objects belonging to the specified backup object owner. You can enter filter criteria in the User, Group, and System fields as desired. The specified Data Protector user needs no longer be configured in the cell.

User

(*available when Filter source objects by owner is selected*) The logon name of a Data Protector user.

Group

(*available when Filter source objects by owner is selected*) The Windows domain or UNIX user group of a Data Protector user.

System

(*available when Filter source objects by owner is selected*) The hostname or IP address of the Data Protector system where the original backup session was run.

Target object options

- Protection
- Catalog protection
- Logging
- Log All
- Log Directories
- Log Files
- No Log

Target media options

- Eject target media after successful copy

Location

(*available if Eject target media after successful copy is selected*)

The owner of the copied backup objects is the user who started the original backup session.

Object Copy - Source Devices

In this page, the source devices are specified. By default, the devices that were used for writing the objects that are selected for copying are used as source devices in the object copy operation. You can change the source devices here if desired.

Original device

The names of the devices that were used for writing the objects that are selected for copying.

Device Status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here. If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility.

Change

After clicking the original device, click here to select a new device.

Object Copy - Summary

In this page, a summary of the selected objects is displayed.

Object Name

The name of the object.

Version

The object version.

Copy selection

(*available with Objects or Sessions as a starting point*) The selection of the copy of the object version to be used as a source (in case the object version has more than one copy) is automatic by default.

> You can disable automatic selection by specifying which copy to use in the object's properties dialog.

Session

(*available with Media as a starting point*) The session in which the object was written.

Properties

To display an object's properties, select the object and click this button. You can change source object options, target object options, and the destination device. If the Objects or Sessions starting point was used, you can manually select which copy of the object version will be used if more than one copy exists.

Delete

To remove an object from the list, select the object and click this button.

Save As

Enter a name for the new object copy, object consolidation, or object verification specification.

Name

You can use only alphanumeric and the following characters: **_ - ( )**.

Start Copy

Select the session from the drop-down list.

Automated Object Copy

Data Protector provides the following methods of automated object copying:

Post Backup

Post-backup as well as post-copy and post-consolidation object copying, which are subsets of post-backup object copying, take place after the completion of a backup, object copy, or object consolidation session. They copy objects backed up, copied, or consolidated in sessions that match the specified criteria.

Scheduled

Scheduled object copying takes place at a user-defined time. Objects from different backup, object copy, or object consolidation sessions can be copied in a single scheduled object copy session.

Automated Object Copy - Post-Backup

In the Results Area, a list of configured object copy specifications is displayed.

Name

The name of the object copy specification. The following may be helpful:

- To immediately start a configured post-backup object copy specification, right-click the specification and click **Start Copy**.
- To immediately copy a configured post-backup object copy specification, right-click the specification and click **Copy As**.

Automated Object Copy - Scheduled

In the Results Area, a list of configured object copy specifications is displayed.

Name

The name of the object copy specification.

Scheduled

The date and time when the operation is scheduled to run. For recurring operations, the first scheduled occurrence is shown. The following may be helpful:

- To immediately start a scheduled object copy specification, right-click the specification and click **Start Copy**.
- To immediately copy a scheduled object copy specification, right-click the specification and click **Copy As**.

Copy

Data Protector provides the following methods of duplicating data after the backup:

Object copy

To use the object copy functionality, expand this item and choose between automated and interactive object copying.

Media copy

To use the media copy functionality, select **Devices & Media** in the context list.

Interactive Object Copy

You can select objects for interactive copying from the following starting points:

Media

Use this starting point to list media pools and media.

Objects

Use this starting point to list types of backed up data, such as Filesystem, Internal Database, and so on.

Sessions

Use this starting point to list sessions in which objects were written to media.

Note For VMware backups, the virtual machine disks are considered as objects that run in parallel. The disk objects of the virtual machine are listed but disabled in the Media list to understand virtual machine disks backed to the media. The copy or verify operation is performed on the virtual machine objects and all its associated disk objects are considered internally.

Media Copy

To use the media copy functionality, select Devices & Media in the context list.

Object Copy

Data Protector provides the following methods of object copying:

Interactive

Expand this item to copy objects interactively.

Automated

Expand this item to configure automated object copying. Choose between post-backup and scheduled object copying.

Application Associations

You can customize your Data Protector environment by associating particular applications with certain file types. The specified application is used when you access the file of the associated file type. For example, you can associate *.htm files with the Mozilla Firefox web browser.

Filename Extension

Type the extension representing the desired file type, for example, *.htm.

Associated application

Type the path to the application that w ill be used when you open files of the specified type, for example, /usr/bin/firefox . Click **Add/Set** to set the application association. To remove an application association, select it in the list and click **Remove**.

Authentication

Enter your login credentials according to the user management configuration for this cell (for example your LDAP account). This dialog box appears if the Cell Manager did not authorize your client computer and user access according to local account configuration.

Find

You can search for text in the currently displayed columns.

Search

Find what

Type the text you want to search for, or use the drop-down list to repeat a previous search.

Case sensitive search

Select this option to perform a case-sensitive search.Match whole word onlySelect this option to search only for whole word occurrences. For example, when searching for the word "system", longer words such as "filesystem" are ignored.

Search options

Search in all columns

Select this option to search in all columns that are currently displayed.

Search by

Select this option to search in a specific column displayed in the Results Area. Select the desired column from the drop-down list.

Next Step Wizard

This dialog box provides shortcuts to particular Data Protector wizards that you can use to perform most common operations in a Data Protector cell, such as adding clients, users, devices, and backup specifications, as well as running backups and restores. The dialog box pops up after each successful connection to a Data Protector Cell Manager unless set otherwise in general GUI preferences. When connected to a specific cell, you can disable it for this cell by selecting **Do not show wizard for this cell in future** at the bottom. Regardless of these settings, you can manually invoke the dialog box anytime from the **View** menu.

Advanced

Customize advanced options.

Localization options

Use system settings for number format

Select this option to display numbers in the format set in the system settings.

Use default number format

Select this option to display numbers in the default format. Application Associations (*available on UNIX systems*) You can associate certain applications with certain file types. The specified application is started when the file of the associated file type is accessed. Click **Edit** to set application associations.

Encoding

You can modify the displayed set of custom character encodings according to your needs.

Customize encoding values

You can change the description and the code of each character encoding that is displayed.

Encoding description

Type a description of the desired character encoding.

Value

Enter the character encoding code which will be used when the character encoding is selected. For the list of the character encoding codes for Windows systems, see http://msdn.microsoft.com/en-us/library/system.text.encoding.aspx.

Load defaults

Click here to replace the current encoding values with the defaults.

Note Close and relaunch the Data Protector GUI for the changes to take effect. To select a particular character encoding, the appropriate locale or code page conversion table must be installed on the local system.

Conect

The Data Protector Manager can connect to any Cell Manager in your environment. You can customize the behavior of the Data Protector Manager on startup.

Connect to default Cell Manager

By default, the Data Protector Manager connects to the Cell Manager to which the client you are using belongs. Connects to the Cell Manager to which the client you are working on belongs.

Connect to last used Cell Manager

Select this option to automatically connect to the Cell Manager you were connected to last.

Always connect to

Select this option to automatically connect to a specific Cell Manager, and specify its name in the text box.

Debug

Customize the debug settings as instructed by the support organization. You need to restart the Data Protector GUI for changes to take effect and to start the debugging.

When Data Protector is running in the debug mode, debug information is generated for every action. For example, if you start a backup session in the debug mode, Disk Agents deliver output on each client system backed up in this backup specification.

For Data Protector 10.30 and later, debugging is enabled during installation. It is normally disabled after successful installation. However, if the debugging is not disabled by default due to some reason, follow these steps to disable it:

Windows

1. Go to My Computer > Properties > Advanced System Settings > Environment Variables and edit the environment variables.
2. Remove entry with `OB2DBG` and restart Data Protector services (including Inet).

Linux

1. Unset the environment variable - `OB2DBG` .
2. Restart `xinetd` service and Data Protector services.

Debug options

Range specification

Specify the debug range. The range should always be specified as 1-200, unless instructed otherwise. Additional options might be required to limit the debug file size (C:n) and to set the timestamp resolution (T:s). The options must be separated by commas.

Compressing the log files

You can choose to compress the debug log files by specifying the gz option after the range, (1-200,gz). This will create logs in a compressed format and not in plain text format. The logs will be created with the .gz extension, and you can use any commercial tool to extract the log files.

Limitations

- This feature is supported only on CM platforms. Due to the build system specifics, HP UX version 11.23 will partially support compression.
- VEPA and Lotus will disable compression, and will produce pure text files.
- If you enable circular debugging, compression will be disabled.
- The debug log archive is not usable during an abnormal termination.

Debug file name

Specify the debug postfix.

Debug Module/s

Specify the modules for which you need to create the debug files.You can specify multiple modules, each separated by a comma. For example, BSM, VDBA, DBSM. You need to restart the Data Protector GUI for changes to take effect and to start the debugging.

Use these settings for the next restart only

Select this option to restart the Data Protector GUI in the debug mode only once. The debugging is automatically disabled for the following restarts of the GUI. This is the preferred option when you need to collect debug information.

Use these settings always

Select this option to always start the Data Protector GUI in the debug mode. When you no longer wish to debug, you need to disable the debug mode.

Do not use these settings in the future

Select this option to disable the Data Protector GUI debug mode.

Restart now

Click here to restart the Data Protector GUI and start the debugging.

General

Customize the behavior of the Data Protector Manager.

Next Step Wizard

Show Next Step Wizard at reconnect

By default, the Next Step Wizard is invoked each time you start the Data Protector Manager GUI or connect to a Cell Manager. You can change this setting here, or disable it in the Next Step Wizard dialog.

Help viewer

System default web browser

Select this option to use the web browser that is currently configured in the operating system as the default web browser for viewing the help topics and context-sensitive Help (in the HTML format).

Event Log Warning dialog

Show a dialog if a new event occurred in the last x day(s)

When you start the Data Protector GUI or connect to a Cell Manager, Data Protector issues a warning if the Data Protector Event Log contains new or unread messages. You can change the period in which this warning will be displayed.

Help Navigator

Enable context-sensitive Help Navigator

When the HTML Help viewer built in the operating system is selected to display context-sensitive Help, Help Navigator dynamically displays context-sensitive Help describing the current view by default. If you clear this option, the currently displayed Help Navigator window remains static until you refresh it.

Monitor

Customize the message text font and color settings and the monitor window refresh interval.

Message font and color

By default, message text uses the font Courier, 10pt. To use a different font, click **Change** and select the desired font. To set the system default font, click **Set system default font**.

Use color highlighting

By default, different colors are used for message level indicators, for example, green for Normal, red for Critical, and so on. To display all indicators in black, clear this option.

Refresh interval (seconds)

By default, the information in the monitor window is updated every 5 seconds.

Manager

The update interval (in seconds) for sessions running on the Cell Manager.

Manager-of-Managers

(**available on a MoM Manager**) The update interval (in seconds) for sessions running in the MoM environment.

Max data conversion unit

This field can be set to any value between **MB** to **TB**. It enables data unit conversion to be done automatically only up to the unit specified. It does not change the value to a higher data unit.

Restore

Customize the default time interval that will be used when browsing the IDB for object versions for restore. You can change the time interval in the Restore context when searching for a specific object version to restore.

Search interval

In the drop-down list, select the search interval. To set the search interval in months, select **Last ... months**. To set an absolute search interval, select **Interval** and specify the start and end dates in the **From** and **To** fields. To list all object versions, select **None**.

Settings

In this page, the default web browser for your system is configured. It is also possible to use other browsers, but in this case you need to enter the appropriate HTML viewer settings. For a list of supported web browsers for viewing Help on UNIX platforms, see the latest .

HTML Viewer Settings

Location of executable script or binary file (directory) The location of your browser (for example, /usr/bin). If you relocate the web browser, you must update the path specified in this option.

Command to start viewer

The command used to start the web browser (for example, firefox $HTML$).

Default Help Page

The Data Protector Help Navigator shows context-sensitive help for the currently selected context.

Properties - Advanced

Specify the advanced option for your Microsoft SQL Server database restore.

Restore database with new name

If the logical and destination file names are not listed, add them to the list. Type the names that were used in the ZDB session. Otherwise, the instant recovery fails.

Add/Set

After typing a destination file name, click here.

Remove

To cancel your selection, select the file and click here.

Properties - Version

In this page you can select the backup versions.

- Backup version
- Point in time restore
  (*available if a Trans backup version is selected*)
- Stop at

Instant Recovery Advanced Options - Microsoft Exchange Server Integration

In this page, specify the Data Protector Microsoft Exchange Server 2010 integration instant recovery options.

Startup client

Specify the client on which the integration agent (e2010_bar.exe) should be started. If the DAG virtual client (host) is selected, the integration agent is started on the currently active node. To find out which Microsoft Exchange Server node is currently active, connect to one of the nodes and run: cluster group.

Default: The same client that was specified for the backup session. If the DAG virtual client was specified, this client is now selected. However, note that the integration agent may not be started on the same physical node as during the backup session; it depends which node is currently active.

User and group/domain

User name

Group/domain name

Specify which Windows domain user account to use for the restore session. Ensure that the specified user has the appropriate Microsoft Exchange Server permissions to back up and restore databases.

If these options are not specified, the restore session is started under the user account under which the Data Protector Inet service is running.

Consistency check

- Perform consistency check
- Check log files only
  (*available if the Perform consistency check is selected*)
- Throttle check for 1 second every I/O operations
  (*available if the Perform consistency check is selected*)

Instant Recovery Source - Microsoft Exchange Server Integration

In this page, you select which Microsoft Exchange Server databases to restore.

Restore Objects

Select which Microsoft Exchange Server databases to restore. When you select a database, the Properties for Database dialog box is displayed. To change a restore method for a database, right-click the database and click **Properties**. For databases that are part of a DAG, the default restore method is Repair all passive copies with failed status. For standalone databases, the default is Restore to the latest state.

Restore Options

- Configuration check mode
- No recovery

Instant Recovery - Type of Backup Selection

In the Results Area, a list of backup specifications of the selected type of data is displayed. Expand the desired backup specification for a list of performed ZDB to disk+tape and ZDB to disk sessions, sorted by date.

Instant Recovery

In the Scoping Pane, you can search for sessions to restore under Restore Objects or Restore Sessions.

Restore Objects

Expand this item to list the types of data backed up (Filesystem, Disk Image, SAP R/3, and so on). Expand the desired type of data to display a list of backup specifications with ZDB to disk+tape or ZDB to disk sessions performed. Expand the desired backup specification for a list of performed backup sessions, sorted by date.

Restore Sessions

Expand this item to list ZDB-to-disk+tape or ZDB-to-disk sessions performed.

Instant Recovery - Backup Specification Information

In the Results Area, a list of performed ZDB to disk+tape and ZDB to disk sessions for the selected backup specification is displayed.

Note To use the filters available for the displayed list, click on Show filter settings and modify the parameters. On how to use the filter settings, see the Using the Filter Settings task topic below.

Name

The session ID.

Status

The overall status of the session.

Backup Specification

The name of the backup specification that was used for the session.

Backup Type

The backup type for the session.

Start Time

The time when the session started.

End Time

The time when the session ended.

Owner

The owner of the backup specification that was used for the session.

Instant Recovery - Options

In this page, you select the database recovery options.

User name

(*available for UNIX systems*) User group (*available for UNIX systems*) Specify the OSDBA user under which you want instant recovery to run (for example, user ora, group dba). This user must have Oracle rights to restore the database. Also, it must be added to the admin or operator user group.

Parallelism

(*not available for Oracle proxy-copy ZDB method*)

Recover until

Open database after recovery

Select this option to automatically open the database after a recovery.

Reset logs

Instant Recovery - Options

In this page, you select the SAP database recovery options.

User name

(*available for UNIX systems*) Enter the Oracle user name. When the user account has been specified, the Oracle restore process can start. The user needs to be a member of the DBA group.

User group

(*available for UNIX systems*) Enter the name of the user group to which the user specified in the User name field belongs. This has to be the Oracle DBA group. The User name and the User group must be the same as defined in the backup ownership.

Recovery

If this option is selected, a database recovery will be automatically performed after instant recovery.

Recover until

Open database after recovery

Select this option to automatically open the database after a recovery.

Reset logs

Instant Recovery - Source

In this page, you select the objects and specify options for the instant recovery, and then preview or start the instant recovery. Before restoring the data, it is recommended to preview the instant recovery. Click **Preview** to preview the instant recovery. Click **Restore** to start the actual instant recovery process.

Restore Objects

Select the object. Since an instant recovery session can only include all objects of the corresponding ZDB session, the subordinate objects cannot be selectively selected.

Restore Options

- Restore method
- Wait for the replica to complete
- Wait up to n minutes
- Retain source for forensics
- Check the data configuration consistency
- Force the removal of all replica presentations
- Keep the replica after the restore

Instant Recovery - Source

In this page, you select the objects for the instant recovery, specify the instant recovery options, and preview or start the instant recovery. In case of Oracle or SAP R/3 integrations, click **Options** to set also the database recovery options. Before restoring the data, it is recommended to preview the instant recovery. Click **Preview** to preview the instant recovery. Note that preview only checks if the replica can be restored. In case of Oracle and SAP R/3 integrations, it does not check if the database recovery will be successful. Click **Restore** to start the instant recovery.

Restore Objects

Select the object. Since an instant recovery session can only include all objects of the corresponding ZDB session, the subordinate objects cannot be selectively selected.

Restore Options

- Restore method
  (default: Copy replica data to the source location; disabled in case of 3PAR StoreServ Storage integration)
- Wait for data copy to complete
  (disabled in case of 3PAR StoreServ Storage integration)
- Wait up to n minutes
  (disabled in case of 3PAR StoreServ Storage integration)
- Retain source for forensics
  (disabled in case of 3PAR StoreServ Storage Integration)
- Check the data configuration consistency
- Force the removal of all replica presentations
- Force restore of 3PAR volume set

Instant Recovery - Source

In this page, you select the objects for the instant recovery, specify the instant recovery options, and preview or start the instant recovery. In case of Oracle or SAP R/3 integrations, click **Options** to set also the database recovery options. Before restoring the data, it is recommended to preview the instant recovery. Click **Preview** to preview the instant recovery. Note that preview only checks if the replica can be restored. In case of Oracle and SAP R/3 integrations, it does not check if the database recovery will be successful. Click **Restore** to start the instant recovery.

Restore Objects

Select the object. Since an instant recovery session can only include all objects of the corresponding ZDB session, the subordinate objects cannot be selectively selected.

Restore Options

- Restore method
- Wait for the replica to complete
- Wait up to n minutes
- Retain source for forensics
- Check the data configuration consistency
- Force the removal of all replica presentations

Instant Recovery - Source

In this page, you select the objects for the instant recovery, specify the instant recovery options, and preview or start the instant recovery. In case of Oracle or SAP R/3 integrations, click **Options** to set also the database recovery options. Before restoring the data, it is recommended to preview the instant recovery. Click **Preview** to preview the instant recovery. Note that preview only checks if the replica can be restored. In case of Oracle and SAP R/3 integrations, it does not check if the database recovery will be successful. Click **Restore** to start the instant recovery.

Restore Objects

Select the object. Since an instant recovery session can only include all objects of the corresponding ZDB session, the subordinate objects cannot be selectively selected.

Restore Options

- Check the data configuration consistency
- Keep the replica after the restore

Instant Recovery - Source

In this page, you select the objects to be restored and specify the VSS integration options for instant recovery, and then start the instant recovery. Click **Options** to specify the P4000 SAN Solutions, P9000 XP Array, or 3PAR StoreServ hardware provider options. Click **Restore** to start instant recovery.

Restore Objects

Specify writers and/or components for restore. For Exchange Server, in case you select a LCR or CCR copy for restore, note that restore will be performed to the production database (Exchange Information Store) and not to the database copy (Exchange Replication Service), because restore to a replicated storage group is not supported. The following may be helpful:

- To specify options for the consistency check of a Microsoft Exchange Writer, right-click the writer and click**Additional options**.
- To perform restore to a different location (in case of Exchange Server), right-click a storage group or a store or transaction logs and click **Restore as**.

Restore Options

- Configuration check mode
- No recovery

Instant Recovery - Options

In this page, you select the default VSS instant recovery options.

- Restore using Microsoft Virtual Disk Service
  (available if supported by the VDS hardware provider)
- Retain source for forensics
- Retain source for forensics
  (available if supported by the VSS hardware provider)
- Restore using Microsoft Volume Shadow Copy service LUN resync
- Retain source for forensics
  (available if supported by the VSS hardware provider)

Instant Recovery - Options

In this page, you select the VSS instant recovery options specific for P4000 SAN Solutions VSS hardware provider.

- Restore using Microsoft Virtual Disk Service
  - Retain source for forensics
  - Retain source for forensics
    (available if supported by the VSS hardware provider)
- Restore using Microsoft Volume Shadow Copy service LUN resync
  - Retain source for forensics
    (available if supported by the VSS hardware provider)
- Restore using P4000
- Restore snapshot data to the source volume

Instant Recovery - Options

In this page, you select the VSS instant recovery options specific for 3PAR VSS hardware provider.

- Restore using Microsoft Virtual Disk Service
  (not available)
- Retain source for forensics
  (not available)
- Restore using Microsoft Volume Shadow Copy service LUN resync
  (not available)
- Retain source for forensics
  (not available)
- Restore using P10000 3PAR
  (always selected)
- Restore snapshot data to the source volume

Instant Recovery - Options

In this page, you select the VSS instant recovery options specific for P9000 XP Array provider.

- Restore using Microsoft Virtual Disk Service
  (this type of restore can be performed if a backup is created with the P9000 XP Array provider in the VSS compliant mode)
- Retain source for forensics
  (available if supported by the VSS hardware provider)
- Restore using Microsoft Volume Shadow Copy service LUN resync
- Retain source for forensics
  (available if supported by the VSS hardware provider)
- Restore using P9000 XP
  (this type of restore can be performed if a backup is created with the P9000 XP Array provider in the resync mode)
  With this type of restore, the P9000 XP Agent (SSEA) synchronizes a source volume (P-VOL) with its target volume (S-VOL) and then splits the pair during the instant recovery session.
- Resync replica data to the source volume
- Quick-Resync replica data to the source volume (internal swap)

Microsoft Exchange Additional Options

In this page, you select the Microsoft Exchange Server specific options.

- Perform consistency check
- Throttle check for 1 second every n I/O operations

MS Exchange Additional Options - Restore to a Different Location

Specify options for restore to different location for Microsoft Exchange Server.

Target server name

Select the target system for restore if you want to restore to different system than original.

Target storage group

(available if Restore to a different store is selected) In the drop-down list, all available storage groups on the selected target system are listed. Select the storage group you want to restore into.

Reload

Click this button to refresh the current GUI page. If there were changes made to the storage group (for example, a database was mounted) on the selected target system while the GUI was opened, the changes are applied after the reload.

Restore to a different store

Restore to a non-Exchange location

Restore to a non-Exchange location and create RSG

Original

In the drop-down list, the log files and all stores that can be restored are listed. Select each store you want to restore from the Original drop-down list, then, in case of restore to a different store, select the target store for this original store from the Target drop-down list, and then click **Add**. If all stores are added to the list, the whole storage group will be restored, otherwise only stores that you add to the list will be restored. Note that if you want to restore individual stores, they must reside on different target volumes, otherwise restore will fail. Note also that logs are automatically added to the list due to the limitation that only stores without logs cannot be restored to a different location. When a component is added to the list, all other restore options are disabled. To enable again all restore options, clear the selected stores and logs from the list by selecting the components and clicking **Remove**. If you already selected components to be restored in the Source property page and if they are different from what you selected here, note that the selection in the source property page will be overwritten by the selection in this dialog box.

Target

(available if Restore to a different store is selected) In the drop-down list, all available stores of the selected storage group are listed. Each of these stores can be selected for restore of your original stores.

Mount backup volume to the path

(available if instant recovery is performed)

Restore into location

(available if standard restore is performed)

Start Instant Recovery

Select the operation you want to perform, and click **OK** to start the session.

Important Before restoring the data, it is recommended to preview the restore.

Start/Preview Session Options

Start Restore Session

Select this option to start the instant recovery session.

Start Preview Session

Select this option to start the preview of the instant recovery session.

Automated Media Operation - Devices

In this page, the source devices and the destination devices for the automated media operation are specified. For each media type, you must have at least one pair of devices (one source and one destination device).

Source drives

Select one or more drives for the source media.

Destination drives

Select one or more drives for the target media.

Automated Media Operation - General

In this page, the backup specification and the type of automated media operation are specified.

Backup specification

In the drop-down list, select the backup specification the media of which you want to copy after the backup finishes.

Media operation type

Select the media operation type.

Automated Media Operation - Options

In this page, you specify the number of copies, whether the media will be ejected automatically after the operation, as well as the location and protection for the target media.

Number of copies

Specify how many copies of the medium will be created. The maximum number of copies is 5. Default: 1.

Eject media

This option specifies whether any of the media will be ejected after the operation. You can select one of the following:

- **Do Not Eject Media**: None of the media will be ejected.
- **Eject Source Media**: Only the source media will be ejected.
- **Eject Target Media**: Only the target media will be ejected.
- **Eject All Media**: Both the source media and the target media will be ejected.

Location for target media

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Protection for target media

Specifies the protection period for the data on the target media. During this period the information cannot be overwritten. You can select one of the following:

- **Same as original**: The protection period will be the same as on the source medium.
- **Permanent**: The data will have permanent protection.
- **None**: The data will not be protected.
- **Days**: The protection period will last for the specified number of days.
- **Weeks**: The protection period will last for the specified number of weeks.

Drive-based encryption

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media. For an up-to-date list of media that support drive-based encryption, see the latest Support Matrix.

Automated Media Operation - Source Media

In this page, the condition and protection of the source media are defined. Only media matching the selected criteria will be considered for the automated media operation.

Media condition

Specify the required condition of the source media.

Media protection

Specify the protection of the source media.

Any

Select this option to consider media regardless of their protection.

Unprotected

Select this option to consider only unprotected media.

Protected

Select this option to consider only protected media, and specify how long the media to be considered are protected.

Automated Media Operation - General

In this page, the name and type of the automated media operation are specified.

Media operation name

Specify the name of the automated media copy operation.

Media operation type

The only media operation type currently available is Media Copy.

Automated Media Operation - Backup Specifications

In this page, backup specifications are selected for the automated media operation.

All backup specifications

Select this option if you would like to include all the listed backup specifications in the operation.

Selected backup specifications

Select this option if you would like to include only specific backup specifications. Select the desired backup specifications.

Automated Media Operation - Time Frame

In this page, the time frame within which Data Protector will search for sessions is defined.

Relative time

Select this option if you would like to set a relative period of time, and then specify the time frame. The first number specifies the beginning of the time frame, and the second number the duration of the time frame. For example, if you specify 24 in the first field and 22 in the second field, and the operation is scheduled today at 22:00, Data Protector will copy media from the sessions that took place between 22:00 yesterday and 20:00 today.

Absolute time

Select this option if you would like to set an absolute period of time. Specify the starting and the end date of the period. Click the drop-down arrows to display the calendar.

No time limit

Select this option if you would like to include all sessions, regardless of when they were performed.

Change Location Priority

If an object version to be restored, copied, consolidated, or verified exists on more than one media set, any of the media sets can be used for the operation. By default, Data Protector automatically selects the most appropriate media set. You can influence the media set selection by specifying the media location priority. Specifying the media location priority here overrides the general media location priority setting for this session.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Number of media

The number of media present in a location.

Copying Media

In this page you select the device where the target medium is located.

Device (Library's Drive)

Select the device or library drive that will be used for the target medium.

Library's Slot

(*available if a library device is used*) Select the library slot where the target medium is located.

Copying Media

Select a media pool for the target medium.

Media Pool

Select the media pool to which the medium copy will be added.

Copying Media

Specify the description and location of the medium.

Medium Description

A medium description helps you identify the media. You can specify it using one of the following options:

Automatically generate

If this option is selected, Data Protector automatically generates the medium description.

Specify

Specify the medium description. A description can have a maximum of 80 characters, including any keyboard character or space.

Use barcode

If this option is selected, Data Protector generates media descriptions based on the barcode and writes them to the medium header on tape. This option is available for library devices with barcode support. This option is enabled by default if you enabled the **Use barcode as medium label on initialization** option in the library properties.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Copying Media

Specify options for the operation.

Options

Eject medium after operation This option is available for standalone and stacker devices. If it is enabled, ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Medium Size

Default

Data Protector specifies the default medium size depending either on the device's information about the medium size (if the device can detect the size), or on the default size for the specific medium type. This size is recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. Note that the total medium size will be set for non-compressed media. Hardware compression of the device may double the space on the media. Available space calculation can only be based on estimates, due to unknown compression ratio.

Specify (MB)

You can specify the size for your medium. It will be recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. For a file device, you specify the size when you first format the medium. If you reformat the medium and specify a new size, the originally specified size will be used.

Protection

Specifies the period of protection for data stored on a medium copy. If objects on the medium have different protection, the protection of the medium is the same as the protection of the object with the longest period of protection. During this period the information cannot be overwritten. You can select one of the following:

- **Same as original**: The protection period will be the same as on the source medium. This is the default value.
- **Permanent**: The protection will be permanent.
- **Until**: Specify the date until which the medium will be protected.

Grouping as a Magazine

If media are grouped as a magazine, this enables you to manage the media as a single unit. Media management tasks can be performed on the magazine or on an individual medium.

Magazine Description

Specify the magazine description. A description can have a maximum of 80 characters, including any keyboard character or space. The following may be helpful:

- You can also import a single medium into a magazine.
- To ungroup a magazine, right-click it and click **Ungroup**.

Importing Catalog

Specify options for the operation.

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, Data Protector ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Logging

The logging level determines the volume of detail on files and directories written to the IDB during backup, object copy, or object consolidation sessions. Note that you can restore your data regardless of the logging level used. The different logging level settings influence the IDB growth, the speed of backup, object copy, or object consolidation, and the convenience of browsing data for restore. Data Protector provides four logging levels: **Log All**, **Log Files**, **Log Directories**, and **No Log**. Logging levels are not available for disk image backup. For B2D devices, No Log and Log All levels are only applicable.

No Log

When this logging level is selected, no information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

Log All

This is the default logging level. All detailed information about backed up files and directories (names, versions, and attributes) is logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

Log Directories

When this logging level is selected, all detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring. However, during the restore Data Protector still performs fast positioning because a file is located on the tape near the directory where it actually resides. This option is suitable for filesystems with many auto-generated files, such as news and mail systems.

Log Files

When this logging level is selected, detailed information about backed up files and directories (names and versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

Importing a Medium in a Magazine

Specify the device that will be used to import the medium.

Device (Library's Drive)

Select the library drive that will be used to import the medium.

Library's Slot

Select the library slot where the medium that you want to import is located.

Importing a Medium in a Magazine

Specify options for the operation.

Eject medium after operation

(*not available for library devices*)

Import Copy as Original

Use this option when the original medium is not available anymore, because it has been overwritten or lost, and you want to import a copy and make it the original. This option also applies for media-related catalog data copies in MCF files.

Logging

The logging level determines the volume of detail on files and directories written to the IDB during backup, object copy, or object consolidation sessions. Note that you can restore your data regardless of the logging level used. The different logging level settings influence the IDB growth, the speed of backup, object copy, or object consolidation, and the convenience of browsing data for restore. Data Protector provides four logging levels: **Log All**, **Log Files**, **Log Directories**, and **No Log**. Logging levels are not available for disk image backup. For B2D devices, No Log and Log All levels are only applicable.

No Log

When this logging level is selected, no information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

Log All

This is the default logging level. All detailed information about backed up files and directories (names, versions, and attributes) is logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

Log Directories

When this logging level is selected, all detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring. However, during the restore Data Protector still performs fast positioning because a file is located on the tape near the directory where it actually resides. This option is suitable for filesystems with many auto-generated files, such as news and mail systems.

Log Files

When this logging level is selected, detailed information about backed up files and directories (names and versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

Importing Magazine Media

Specify the device that will be used to import the media that are part of the magazine.

Device (Library's Drive)

Select the library drive that will be used to import the media.

Importing Magazine Media

Specify the description of the magazine. The description of each medium in the magazine consists of the magazine description and the slot ID.

Medium Description

A medium description helps you identify the media. You can specify it using one of the following options:

- **Automatically generate**: If this option is selected, Data Protector automatically generates the medium description.
- **Specify**: Specify the medium description. A description can have a maximum of 80 characters, including any keyboard character or space.
- **Use barcode**: If this option is selected, Data Protector generates media descriptions based on the barcode and writes them to the medium header on tape. This option is available for library devices with barcode support. This option is enabled by default if you enabled the Use barcode as medium label on initialization option in the library properties.

Importing Magazine Media

Specify options for the operation.

Eject medium after operation

(*not available for library devices*)

Import Copy as Original

Use this option when the original medium is not available anymore, because it has been overwritten or lost, and you want to import a copy and make it the original. This option also applies for media-related catalog data copies in MCF files.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Logging

The logging level determines the volume of detail on files and directories written to the IDB during backup, object copy, or object consolidation sessions. Note that you can restore your data regardless of the logging level used. The different logging level settings influence the IDB growth, the speed of backup, object copy, or object consolidation, and the convenience of browsing data for restore. Data Protector provides four logging levels: **Log All**, **Log Files**, **Log Directories**, and **No Log**. Logging levels are not available for disk image backup. For B2D devices, No Log and Log All levels are only applicable.

No Log

When this logging level is selected, no information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

Log All

This is the default logging level. All detailed information about backed up files and directories (names, versions, and attributes) is logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

Log Directories

When this logging level is selected, all detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring. However, during the restore Data Protector still performs fast positioning because a file is located on the tape near the directory where it actually resides. This option is suitable for filesystems with many auto-generated files, such as news and mail systems.

Log Files

When this logging level is selected, detailed information about backed up files and directories (names and versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

Importing Media

Specify the device that will be used to import the medium.

Device (Library's Drive)

Select the device or library drive that will be used to import the medium.

Library's Slot

(*available if a library device is used*) Select the library slot where the medium that you want to import is located.

Importing Media

Specify options for the operation.

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, Data Protector ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Import Copy as Original

Use this option when the original medium is not available anymore, because it has been overwritten or lost, and you want to import a copy and make it the original. This option also applies for media-related catalog data copies in MCF files.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Logging

The logging level determines the volume of detail on files and directories written to the IDB during backup, object copy, or object consolidation sessions. Note that you can restore your data regardless of the logging level used. The different logging level settings influence the IDB growth, the speed of backup, object copy, or object consolidation, and the convenience of browsing data for restore. Data Protector provides four logging levels: **Log All**, **Log Files**, **Log Directories**, and **No Log**. Logging levels are not available for disk image backup. For B2D devices, No Log and Log All levels are only applicable.

No Log

When this logging level is selected, no information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

Log All

This is the default logging level. All detailed information about backed up files and directories (names, versions, and attributes) is logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

Log Directories

When this logging level is selected, all detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring. However, during the restore Data Protector still performs fast positioning because a file is located on the tape near the directory where it actually resides. This option is suitable for filesystems with many auto-generated files, such as news and mail systems.

Log Files

When this logging level is selected, detailed information about backed up files and directories (names and versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

Magazines

In the Results Area, a list of magazines in the media pool is displayed.

Description

A description of the magazine.

Used Media (GB)

Data Protector calculates used space on the media in a magazine.

Total Media (GB)

The total space on the media in a magazine.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device. The following may be helpful:

- To display the properties of a magazine, right-click the magazine and click **Properties**.
- You can perform certain media operations on the entire magazine. You export all media in the magazine, recycle them, or move the magazine to another media pool.

Media in a Magazine

In the Results Area, a list of media in the selected magazine is displayed.

Description

A description of the medium.

Quality

The physical condition of the medium (good, fair, or poor), based on media condition factors.

Protection

The protection of the data on the medium.

Available Space (MB)

The amount of space on the medium that is still free. Data Protector calculates available space as the difference between the total media size, specified at media initialization, and used media space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Media

In the Results Area, a list of media in the selected media pool is displayed. To use the filters available for the displayed list, click on Show filter settings and modify the parameters.

Description

A description of the medium.

Quality

The physical condition of the medium (good, fair, or poor), based on media condition factors.

Protection

The protection of the data on the medium.

Available Space (MB)

The amount of space on the medium that is still free. Data Protector calculates available space as the difference between the total media size, specified at media initialization, and used media space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Media Locations

In the Results Area, a list of configured media locations is displayed. Before you transfer a medium to a vault, it is recommended to mark its location.

Name

The name of the vault.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Number of media

The number of media present in a location.

Media Pools

In the Results Area, a list of configured media pools is displayed. Data Protector provides a default media pool for each media type (for example, Default DDS). To use the filters available for the displayed list, click on **Show filter settings** and modify the parameters.

Pool Name

The name of the media pool. The icons in front of each pool name represent the following:

Icon	Description
	An empty media pool.
	A media pool in good condition.
	A media pool in fair condition.
	A media pool in poor condition (not usable for backup).

Media Type

The type of media in the media pool, such as DLT, DDS, and so on.

Used Media (GB)

The total used space on all the media in the media pool.

Total Media (GB)

The total space on all the media in the media pool.

Number of media

The number of media in the media pool.

Number of poor media

The number of media in poor condition in the media pool.

Description

A description of the media pool, if one was provided.

Tip To display the properties of a media pool, right-click the media pool and click**Properties**.

Media and Magazines

In the Results Area, you can choose between Media and Magazines of the selected media pool.

Media

In the Results Area, you can choose between media locations and media pools.

Formatting a Medium in a Magazine

Specify the device that will be used to format the medium.

Device (Library's Drive)

Select the library drive that will be used to format the medium.

Library's Slot

Select the library slot where the medium that you want to format is located.

Formatting a Medium in a Magazine

Specify options for the operation.

Options

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, Data Protector ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Medium Size

Default

Data Protector specifies the default medium size depending either on the device's information about the medium size (if the device can detect the size), or on the default size for the specific medium type. This size is recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. Note that the total medium size will be set for non-compressed media. Hardware compression of the device may double the space on the media. Available space calculation can only be based on estimates, due to unknown compression ratio.

Specify (MB)

You can specify the size for your medium. It will be recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. For a file device, you specify the size when you first format the medium. If you reformat the medium and specify a new size, the originally specified size will be used.

Formatting Magazine Media

Specify the device that will be used to format the media that are part of the magazine.

Device (Library's Drive)

Select the library drive that will be used to format the media.

Formatting Magazine Media

Specify the description and location of the magazine media. The description of each medium in the magazine consists of the magazine description and the slot ID.

Medium Description

A medium description helps you identify the media. You can specify it using one of the following options:

Automatically generate

If this option is selected, Data Protector automatically generates the medium description.

Specify

Specify the medium description. A description can have a maximum of 80 characters, including any keyboard character or space.

Use barcode

If this option is selected, Data Protector generates media descriptions based on the barcode and writes them to the medium header on tape. This option is available for library devices with barcode support. This option is enabled by default if you enabled the Use barcode as medium label on initialization option in the library properties.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for xample, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Formatting Magazine Media

Specify options for the operation.

Options

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, Data Protector ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by Data Protector (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format Data Protector media. Data Protector media with protected data will not be formatted until the protection is removed.

Medium Size

Default

Data Protector specifies the default medium size depending either on the device's information about the medium size (if the device can detect the size), or on the default size for the specific medium type. This size is recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. Note that the total medium size will be set for non-compressed media. Hardware compression of the device may double the space on the media. Available space calculation can only be based on estimates, due to unknown compression ratio.

Specify (MB)

You can specify the size for your medium. It will be recognized as the total medium size. After filling up the medium, Data Protector will update the information on the size. For a file device, you specify the size when you first format the medium. If you reformat the medium and specify a new size, the originally specified size will be used.

Media Location

In this page you can modify the media location priority of the location.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Number of media

The number of media present in a location.

New Location for Media

Specify the new media location. You can type it in the text box, or select one of the predefined locations from the drop-down list.

When you modify a media location, the new location is written in the IDB and not on the medium itself. Therefore, if you export a medium and import it again, the location information in the IDB is replaced with the location stored on the medium.

Tip To change the location information for multiple media, select the media using Ctrl or Shift, right-click them, and click **Change Location**.

Editing Locations

Create a list of locations that you use for vaulting media. The list will be available when you perform media management tasks, such as formatting, so that you can select a predefined location for the medium.

To add a location, type its name in the box and click **Add**. To remove a location, select it in the list and click**Delete**.

General

In this page, general properties of the magazine are specified.

Description

The additional descriptive text is optional, but recommended for easier identification. It can contain any characters and can be up to 80 characters long (including spaces).

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Quality

The quality of the media in a magazine determines the quality of the magazine. For example, as soon as one medium in a pool is poor, the whole magazine is marked as poor.

The following media conditions exist:

- **Good**: This media status means that less than 80% of the threshold for age or usage has been reached.
- **Fair**: This media status means that 95 to 100% of the threshold for age or usage has been reached.
- **Poor**: This media status means that the threshold for age or usage has been exceeded, or read/write errors have occurred on the medium. Data Protector will not use media in poor condition for backup.
  If a medium is marked as poor due to a device error, you can verify the medium to check and change its condition.

Tip You can change the media condition factors that are used to calculate the condition of a medium. To do this, click the **Condition** tab in the media pool properties. The new media condition factors are used to calculate the condition of all media in the media pool.

Usage

The pie chart displays estimated free space and used space on the media in the magazine.

Formatting Media

Specify the device that will be used to format the medium.

Device (Library's Drive)

Select the device or library drive that will be used to format the medium.

Library's Slot

(available if a library device is used)

Select the library slot where the medium that you want to format is located.

Formatting Media

Specify the description and location of the medium.

Medium Description

A medium description helps you identify the media. You can specify it using one of the following options:

Automatically generate

If this option is selected, automatically generates the medium description.

Specify

Specify the medium description. A description can have a maximum of 80 characters, including any keyboard character or space.

Use barcode

If this option is selected, generates media descriptions based on the barcode and writes them to the medium header on tape. This option is available for library devices with barcode support. This option is enabled by default if you enabled the Use barcode as medium label on initialization option in the library properties.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB.

Allows you to create a list of predefined locations to simplify vaulting and archiving.

Formatting Media

Specify options for the operation.

Options

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed.

If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

Use this option in order to format (initialize) media that are in other formats recognized by (such as tar, OmniBack I, and so on), or media that have been used by another application, or to re-format media.

Media with protected data will not be formatted until the protection is removed.

Medium Size

Default

Specifies the default medium size depending either on the device's information about the medium size (if the device can detect the size), or on the default size for the specific medium type. This size is recognized as the total medium size. After filling up the medium, will update the information on the size. Note that the total medium size will be set for non-compressed media. Hardware compression of the device may double the space on the media. Available space calculation can only be based on estimates, due to unknown compression ratio.

Specify (MB)

You can specify the size for your medium. It will be recognized as the total medium size. After filling up the medium, will update the information on the size.

For a file device, you specify the size when you first format the medium. If you reformat the medium and specify a new size, the originally specified size will be used.

Automated Operations List

In the Results Area, a list of configured automated operations is displayed.

Name

The name of the automated operation.

Scheduled

The absolute or relative (Post Backup) time of the automated operation.

Type

The type of the automated operation.

Copies

In this page, copies of the medium are listed.

Description

The description of the medium.

Quality

The physical condition of the medium. The media condition status can be good, fair, or poor.

Protection

The protection of the data on the medium.

Available Space (MB)

The amount of space on the medium that is still free. Data Protector calculates available space as the difference between the total media size, specified at media initialization, and used media space.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

General

In this page, general properties of the medium are specified.

Description

The additional descriptive text is optional, but recommended for easier identification. It can contain any characters and can be up to 80 characters long (including spaces).

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Media label

The barcode of the medium if it is available (in brackets), and the user-defined description of the medium.

Format

Media formats recognized by Data Protector, such as Data Protector, tar, cpio, and so on. Data Protector does not recognize blank media format. A medium that has been exported from the Data Protector cell or has been created on another Cell Manager has the Data Protector foreign media format. This means that information about backed up data on the medium is not in the IDB. You can import the medium in order to browse data on the medium. This simplifies the restore, as its format becomes the Data Protector media format.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Media Pool

The name of the media pool to which the medium belongs.

Cell

The name of the cell where the media pool has been configured.

Original

(*available for media copies*) Click this button to obtain information on the location, ID, and name of the original medium.

Info

In this page, the medium ID, quality, protection, and statistics of the medium are displayed.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Quality

The physical condition of the medium. The media condition status can be good, fair, or poor.

Protection

The protection of the data on the medium.

Statistics

Statistical information on the medium.

Objects

In this page, objects backed up on the medium are listed.

Status

The backup status of the object on the medium.

Object Type

The type of the object on the medium.

All Media Available

Whether or not all media necessary for a restore of the object are available.

Client System

The client system on which the backed up object resides.

Source

The location of the backed up object on the client system.

Description

The user-defined description of the backed up object.

Size (KB)

The size of the backed up object in kilobytes.

Backup Type

The type of the backup (full or incremental; some other backup types are available for specific integrations).

Start Time

The time when the backup started.

End Time

The time when the backup finished.

Data Protection

The protection of the data on the medium.

Catalog Protection

The catalog protection for the object.

Number of Warnings

The number of warnings issued during the session.

Number of Errors

The number of errors that occurred during the session.

Access Type

Private

Private objects can be seen and restored only by the user who created the backup, the system administrator, or users with the

See private objects user right.

Public

Public objects can be seen and restored by all users who have appropriate restore user rights.

Session

The session ID, consisting of the date of the session and a unique number.

Encryption KeyID-StoreID

The KeyID-StoreID combination of the encryption key, if the object is encrypted.

Usage

The pie chart displays estimated free space and used space on the medium. If the medium belongs to a media pool with the **Non-appendable** media usage policy, the indicated free space will always be 0%.

Moving a Magazine to a Pool

You can move a magazine from one media pool to another media pool of the same type, provided that the target pool has the **Magazine support** option enabled.

Media Pool

Select the media pool to which the magazine will be added.

Tip If you want to move a magazine to another cell, export the magazine from one cell and then import it to another cell.

Moving a Medium to a Media Pool

You can move a medium from one media pool to another media pool of the same type.

Media Pool

Select the media pool to which the medium will be added.

Tip If you want to move a medium to another cell, export the medium from one cell and then import it to another cell.

Media Pool - General

In this page, the name of the media pool and the media type are specified.

Pool Name

The user-defined name of a media pool. It can contain any characters and can be up to 32 characters long (including spaces).

Description

The additional descriptive text is optional, but recommended for easier identification. It can contain any characters and can be up to 80 characters long (including spaces).

Media Type

Data Protector supports various media types, such as tapes and magneto-optical, File, and LTO media. When you select the media type, Data Protector estimates the available space on the media for the target media pool.

Allocation

In this page, media options are specified.

Usage

The media usage policy controls how new backups are added to the already used media, and influences which media are selected for backup.

Appendable

If this option is selected, the first medium a backup session uses contains backed up data from a previous backup session, so that the remaining space on the medium is used. If additional media are needed during the same backup session, empty or unprotected media are used. If several appendable media are available in the pool, the medium that was written to the least recently is used. With this media usage policy, the type of backup (full or incremental backup) can be combined in any order on the media. Appending media conserves media space but reduces flexibility in manipulating media because one medium can contain data from several backup sessions. Appendable media usage policy is not recommended for file library. Furthermore, appendable policy is not supported if object copying or object consolidation is performed using the file library. Non-appendable media usage policy is required.

Non-Appendable

If this option is selected, you can only write data from one backup session to this particular medium. Attempting to append a backup session to this medium results in a mount request. You need to respond to the mount request.

Appendable on Incrementals Only

If this option is selected and an incremental backup is performed, the first medium a backup session uses contains backed up data from a previous backup session, so that the remaining space on the medium is used. If additional media are needed during the same backup session, empty or unprotected media are used. If several appendable media are available in the pool, the medium that was written to the least recently is used. This media usage policy will create media that contain a full backup followed by any number of incremental backups.

Allocation

The media allocation policy defines the order in which media are accessed within a media pool.

Loose

If this option is selected, Data Protector accepts any suitable medium in the pool (the medium must not be in poor condition or protected). This option can be combined with the **Allocate unformatted media first** option. If the global option **InitOnLoosePolicy** is set to 1 (default is 0), media that are unrecognized by Data Protector are automatically initialized (formatted). This policy is recommended for stacker devices, which load media in sequential order, or if you do not want an unattended backup to fail because the specified media are not available.

Strict

If this option is selected, Data Protector requires a specific medium. The medium must already be formatted (initialized) for use with Data Protector. Data Protector does not automatically format media during a backup session. This allocation policy should be adopted where an even usage of media has priority over ease of use, as well as with library devices that contain both Data Protector and non-Data Protector media in the library. Choosing a strict allocation policy prevents accidental overwrites of non-Data Protector media.

Allocate unformatted media first

This option is available if the Loose allocation policy is selected. If this option is selected, Data Protector will select unformatted media for backup before free Data Protector media and fair media, but still after pre-allocation order (if specified), and appendable (as set in usage policy). If this option is not selected, Data Protector will select unformatted media for backup after free Data Protector media, as well as after pre-allocation order (if specified), and appendable (as set in usage policy). Only fair media will be selected after unformatted media. This is recommended if Data Protector is the only application using the library and you want to have even usage of all media.

Use free pool

When this option is selected, the pool is linked to the free pool selected from the drop-down list in order to share free media. Condition factors are inherited from the free pool. By default, the option is cleared. To create a new free pool with default properties for the selected media type, enter a new name and a new free pool will be automatically created.

Move free media to free pool

(available if the **Use free pool** is selected) If this option is selected, a deallocation of free media from a regular to a free pool takes place automatically. Default selected.

Magazine support

(not available with all media types)

Condition

In this page, media condition factors of the media pool are specified. Media condition factors define how long media are reliable for backup. Based on these factors, Data Protector changes the condition of media from good to fair or poor. The condition factors are set for the entire media pool, not for each medium.

Valid for (Months)

The age of a medium is calculated as the number of months that have elapsed since you initialized the medium. Once a medium is older than the threshold number of months, it is marked as poor. The default threshold is 36 months.

Maximum overwrites

The usage of a medium is defined as the number of overwrites to the medium. Once the medium has more than the threshold number of overwrites, it is marked as poor. The default threshold for DDS media is 100 overwrites. For all other types of media, the default is 250 overwrites.

Set to Default

Sets the media condition factors to their default values. This means that the media will be valid for 36 months or 250 overwrites to the media (100 for DDS media type).

Quality

The quality of the media in a media pool determines the quality of the media pool. For example, as soon as one medium in a pool is poor, the whole media pool is marked as poor. The following media conditions exist:

- **Good**: This media status means that less than 80% of the threshold for age or usage has been reached.
- **Fair**: This media status means that 95 to 100% of the threshold for age or usage has been reached.
- **Poor**: This media status means that the threshold for age or usage has been exceeded, or read/write errors have occurred on the medium. Data Protector will not use media in poor condition for backup.
  If a medium is marked as poor due to a device error, you can verify the medium to check and change its condition.

You can change the media condition factors that are used to calculate the condition of a medium. To do this, click the **Condition** tab in the media pool properties. The new media condition factors are used to calculate the condition of all media in the media pool.

Usage

The pie chart displays estimated free space and used space in the media pool.

This pie chart does not show the free disk space available for media pools created for file library devices. To get this information, you need to use operating system tools on the system where the file library device was defined. For example, `df -k` (Linux systems), and `Explorer > Properties` (Windows systems). By default, the file library device media pool has a Non-appendable media usage policy. The media pool's free disk space will always be indicated as 0%.

Selecting Media

You can search for specific media without browsing the entire list of media. Specify the desired search criteria. The media matching the specified criteria will be highlighted in the Results Area.

Description

To select media with a specific description, specify the description.

Location

To select media with a specific location, specify the location. Predefined locations can be selected from the drop-down list.

Written in Session

To select media used in a specific session, specify the session. Sessions are listed by date and session ID.

Written in Timeframe

To select media that were written to in a specific time frame, specify the dates in the From and To fields.

Protection

To select media with specific protection, specify the appropriate options.

Combine Selections Using

(applicable if more than one search criterion is specified) Logical ANDSelect this option to select media that match all the specified criteria. Logical ORSelect this option to select media that match any of the specified criteria.

Verifying Media

Specify the device that will be used to verify the medium.

Library Drive

Select the library drive that will be used to verify the medium.

Gateway

(available for backup to disk (B2D) devices) Select the gateway that will be used to verify the medium. Depending on the backup device and media you use, verifying can take considerable time to complete.

Copying Media Catalog

Specify the path to the directory to which you want to copy media-related catalog data.

Path

By default, the media-related catalog data are copied into media container format (MCF) files into default MCF directory that resides on the Cell Manager.

Browse

You can specify a different directory. Click this button to browse for the path instead of typing it.

Selecting Media Files

Browse the directory tree on current Cell Manager and select the MCF files you want to import. Data Protector GUI only shows and allows selection of the files with mcf extension. Other files are omitted from the directory tree.

Selecting Options

Specify additional options for the destination media pool.

Options

Import to original pool if possible

This option specifies a media pool for import and it is selected by default. If the media pool does not exist yet, it will be created. The media class of a medium must match the media class of a media pool.

Prefix for new pools

Type an optional prefix for a media pool to which you want to import MCF files or use the default prefix**IMPORTED_**.

Import Copy as Original

Use this option when the original medium is not available anymore, because it has been overwritten or lost, and you want to import a copy and make it the original. This option also applies for media-related catalog data copies in MCF files.

Current Sessions

The currently running sessions are listed. Finished or aborted sessions are kept in the list until you clear them or close the Data Protector GUI. You can view the status of the sessions, their type, their owner, their session ID, the start time of the sessions, as well as the names of the backup, object copy, object consolidation, or object verification specifications. If no sessions appear in this context, there are no sessions running.

The following may be helpful:

- To remove finished or aborted sessions from the list, click **Clear sessions** in the Actions menu.
- To remove a particular session, right-click the session and click **Remove From List**.

Backup Session Details

In the Results Area, the backup objects, devices, and session messages are displayed. At the end of the session, a dialog box appears indicating the session status. For each backed up and mirrored object and each device used in the session, all relevant information is displayed. This can include the object status and type, the device status and name, and so on. The level of messages displayed depends on the Report level setting in the backup specification. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- To confirm a mount request, right-click the device and click **Confirm Mount Request**.
- To cancel a device, right-click the device and click **Cancel Device**.
- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Client Details - Messages

Messages for the selected client system are displayed. The following may be helpful:

- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Object Consolidation Session Details

In the Results Area, the object consolidation session objects, devices, and messages are displayed. At the end of the session, a dialog box appears indicating the session status. For each object and device in the session, all relevant information is displayed. This can include the object status and type, the device status and name, and so on. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- To confirm a mount request, right-click the device and click **Confirm Mount Request**.
- To cancel a device, right-click the device and click **Cancel Device**.
- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

IDB Upgrade Details

In the Results Area, details on the IDB filename conversion are displayed. At the end of the session, a dialog box appears indicating the session status. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Status

The session status (running/failed/aborted).

Start Time

The time when the session started.

Inactive Time

Total elapsed time when the session was idle.

Working Time

Total elapsed time that was actually used for the filename conversion.

Progress

The progress of the session is displayed as a percentage of completion.

Clients

The number of clients considered for the filename conversion: if the Cell Manager is a Windows system, the number of all non-Windows clients, and the other way round.

Clients Done

The number of clients processed (including those where the filename conversion was not performed).

Clients Skipped

The number of clients for which filename conversion is not needed (their filenames have already been converted, or they have no filenames in the IDB).

Installation

In the Results Area, the clients that have been selected for installation and the installation messages are displayed. At the end of the session, a dialog box appears indicating the session status. Each session message has a level indicator that shows its severity (Normal, Warning, and so on).

Status

The installation status of a specific client system.

Client

The name of the client system.

Progress

The progress of the installation process as a percentage of completion.

Description

A brief description of the installation status. The following may be helpful:

- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Media Details

In the Results Area, the media session messages are displayed. At the end of the session, a dialog box appears indicating the session status. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Object Copy Session Details

In the Results Area, the object copy session objects, devices, and messages are displayed. At the end of the session, a dialog box appears indicating the session status. For each object and device in the session, all relevant information is displayed. This can include the object status and type, the device status and name, and so on. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- To confirm a mount request, right-click the device and click **Confirm Mount Request**.
- To cancel a device, right-click the device and click **Cancel Device**.
- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Purge Details

In the Results Area, details on the purge session are displayed.

Purge Sessions

The purge statistics for the different parts of the Data Protector Catalog Database are displayed.

Status

The purge status of the specific part of Data Protector Catalog Database.

Type

Identifies the part of the Data Protector Catalog Database.

Deleted

The number of deleted records for the specific part of the Data Protector Catalog Database as a percentage of the total.

Done

The number of processed records for the specific part of the Data Protector Catalog Database as a percentage of completion.

Time Statistic

- Start Time: The time that the purge session started.
- Inactive Time: The total elapsed time that the purge session was idle.
- Working Time: The total elapsed time that was actually used for purging the database.

Restore Session Details

In the Results Area, the backup objects that are being restored, the devices used, and the session messages are displayed. At the end of the session,

a dialog box appears indicating the session status.

For each object and device in the session, all relevant information is displayed. This can include the object status and type, the device status and name, and so on. The level of messages displayed depends on the Report level setting selected in the Start Restore Session dialog. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- To confirm a mount request, right-click the device and click **Confirm Mount Request**.
- To cancel a device, right-click the device and click **Cancel Device**.
- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Verification Session Details

In the Results Area, the object verification session objects, devices, and messages are displayed. At the end of the session, a dialog box appears indicating the session status. For each object and device in the session, all relevant information is displayed. This can include the object status and type, the device status and name, and so on. Each session message has a level indicator that shows its severity (Normal, Warning, and so on). The following may be helpful:

- To confirm a mount request, right-click the device and click **Confirm Mount Request**.
- To cancel a device, right-click the device and click **Cancel Device**.
- Some messages have a link (blue message number). Click a link for a detailed description of the error and a list of possible actions.
- Right-click the message area to copy messages, search them, or perform other operations.

Enterprise Monitor

In the Results Area, the Cell Managers in the MoM cell are listed. For each Cell Manager, its status information and the number of currently running sessions is displayed. The following may be helpful:

- Double-click a Cell Manager to display the currently running sessions on that Cell Manager. Finished or aborted sessions are kept in the list until you clear them or close the Data Protector GUI.
- To view session details or abort a session, right-click the session and select the desired action.
- To remove finished or aborted sessions from the list, click **Clear sessions** in the Actions menu.
- To remove a particular session, right-click the session and click **Remove From List**.

Mount Request Information

Data Protector issues a mount request if either a specific medium to read data from or more media to write data to are needed, but are not available in the device.

Confirm Mount Request

Insert the needed medium into the device and click this button to continue the session.

Cancel Device

Click this button to cancel the device with the mount request. The data specified for that device will not be backed up, restored, or copied.

Close

Click this button to close the dialog. You can then confirm the mount request or cancel the device in the monitor window.

Enter Password

Provide the data required to access the specific client system and click **OK**. The following may be helpful:

- To abort the entire installation process, click **Abort**.
- To skip the selected client system and proceed with the installation of other clients, click **Skip**.

Username

Type the username that is used to access the client.

Password

Type the password to access the client.

Domain

(available for Windows clients) Select or type the domain for the user.

Select New Device

In this page you select a new device to be used as a source device for object verification.

Selected device

The name of the device that was used for the original backup of the data, and is by default also used as the source device for object verification

New Device

To use a different source device for the copy operation, select a device from the list and click**OK**.

Object Verification - Consolidation Specifications

In this page, select the object consolidation specifications required for post-backup or scheduled object verification. Specify the following view parameters to adjust the list of specifications displayed:

Show

Select which object consolidation specifications to display: Only the selected specifications or all available specifications.

View by

Select how the object consolidation specifications should be listed: By group, filename, or type.

Select the required specifications for the operation.

Object Verification - Copy Specifications

In this page, select the object copy specifications required for post-backup or scheduled object verification. The following view parameters modify the list of specifications displayed:

Show

Select which object copy specifications to display: Only the selected specifications, or all available specifications.

View by

Select how the object copy specifications should be listed: By group, filename, or type.

Select the required specifications for the operation.

Object Verification - Backup Specifications

In this page, select the backup specifications required for post-backup or scheduled object verification. The following view parameters modify the list of specifications displayed:

Show

Select which backup specifications to display: Only the selected specifications or all available specifications.

View by

Select how the backup specifications should be listed: By group, filename, or type.

Select the required specifications for the operation.

Object Verification - General

In this page, specify the name of the object verification specification.

Name

Specify the name of the object verification specification.

Object Verification - Library Filter

In this page, specify the library filter for object selection. Only objects residing on media in the specified libraries will be verified.

All libraries

Select this option to include all the listed libraries in the operation.

Selected libraries

Select this option to include only specific libraries. Select the required libraries.

Object Verification - Objects

Select the object versions to verify.

The GUI also shows backed up objects that cannot be verified.

> **Important** The Data Protector SAP MaxDB, DB2 UDB, and Microsoft SQL Server integrations have interdependent data streams. All objects of these integrations with the same backup ID should be selected for verification in order to provide effective verification for integration objects.

The content of the Results Area depends on the starting point you have selected:

- Objects

  Types of backed up data are listed, such as Filesystem, Database, and so on. Expand a type of data, then a client and its logical disks or mount points to display the object versions.

  > **Important** Object versions of certain types of backed up data, such as Microsoft Exchange Server 2010 or later, or Microsoft Hyper-V, are not listed in the Objects scope. Use the Session or the Media scope instead.

  To select a restore chain of an object version (all object versions necessary for a restore to that object version) right-click the object version and select **Select Restore Chain**. The selection of a restore chain is not available for integration objects.
- Sessions

  Sessions are listed. Expand a session to display the object versions that were written in that session.

  To select a restore chain of an object version (all object versions necessary for a restore to that object version) right-click the object version and select **Select Restore Chain**. The selection of a restore chain is not available for integration objects.

  To select all integration objects with the same backup ID, right-click an integration object and select**Select Backup Set**.
- Media

  Media pools are listed. Expand a media pool and then a medium to display the object versions residing on it.From Data Protector 9.05 onwards, for VMWare backups, the virtual machine disks are considered as objects that run in parallel. The disk objects of the virtual machine are visible but disabled. This is done to display the objects present in the media. Select only the virtual machine object for object operations.

Enable selection of protected objects only

If this option is selected, only objects that have data protection can be selected for copying. The check boxes of objects without data protection are shaded.

Schedule Verification

In this page you select the time of the object verification operation (for a date already selected), as well as the intervals at which you want the operation to be performed.

Recurring

Here you set the frequency of the operation. If you do not want recurring, select **None**. If you want the operation to recur, select one of the intervals and specify more precisely when you want the operation to be performed.

Time options

Time

Select the time for the operation to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting (for recurring operations)

Select this option if you want the operation to start on a specific date, and specify the starting date.

Object Verification - Media

In this page, a list of all media containing the selected objects is displayed. If the Objects or Sessions starting point was used and more than one copy of the same object version exists, you can influence the media selection by specifying the media location priority.

Change Priority

To change the media location priority for this session, select a media location and click this button.

Object Verification - Object Filter

In this page, specify the criteria for object version selection. Only the object versions matching the specified criteria will be verified.

Include only protected objects

Select this option to operate only on objects with data protection.

Include only objects with number of copies less than

Select this option to verify only objects that do not have more than a certain number of copies. Specify the number. The maximum is 10.

Include objects created in timeframe

(available for scheduled processing) These options can be used to define a time frame within which object versions must have been created (by backup, object copy, or object consolidation) to be included in the processing.

Relative time

Select this option to set a relative period of time, and then specify the time frame. The first number specifies the beginning of the time frame (the number of hours before the scheduled start of processing); the second number specifies the duration of the time frame.For example, if you specify 24 in the first field and 22 in the second field, and the operation is scheduled today at 22:00, object versions from sessions that took place between 22:00 yesterday and 20:00 today will be included in the processing.

Absolute time

Select this option to set an absolute period of time. Specify the start and end dates of the period. Click the drop-down arrows to display the calendar.

No time limit

Select this option to include all object versions, regardless of when they were created.

Object Verification - Object Version Source

In this page you can select manually which copy of the object version to use, if more than one copy exists.

Select source copy manually

Select this option to manually select the required copy of the object version, and select a copy from the drop-down list.

Needed media

Depending on the selected copy, the required media are listed.

Save, or Start an Object Verification Session

You can save the object verification specification you have configured, or start an interactive session using it.

Save As

Click the button to save the object verification specification.

Start Interactive Object Verification

Click the button to start the interactive object verification session.

Object Verification - Source Devices

In this page, the source devices are specified.

Automatic device selection (Recommended)

(Default selection) Data Protector selects devices automatically: Normally, the devices that were used for writing the selected objects are used as the source devices. If the original devices are not available, Data Protector selects other suitable devices for reading the source media, avoiding delays.

Original device selection

Select this option to force the use of the original device: If it is not available, Data Protector will wait until it is available. The device table at the bottom of the form displays:

Original Device

The name of a device used for writing objects selected for verification.

Device Status

Whether or not the device is available for use.

You can substitute devices for the original source devices, for instance if the original device is unavailable, using the entries in the device table. To change a device, right-click the relevant entry in the table and select **Change Device**.

Start Verification

Select the session from the drop-down list.

Object Verification - Summary

In this page, a summary of the selected object versions is displayed.

Object Name

The name of the object.

Version

The object version.

Copy selection

(available with Objects or Sessions as a starting point) The selection of the copy of the object version to be used as a source (when the object version has more than one copy) is automatic by default. You can disable automatic selection by specifying which copy to use in the Properties dialog.

Session

(available with Media as a starting point) The session in which the object version was written.

Properties

To display an object version's properties, select the object version and click this button. If there is more than one copy of the selected object version, you can manually select which copy to use for the verification operation in the Properties dialog.

Delete

To remove an object version from the list, select the relevant entry and click this button.

Object Verification - Target Host

In this page, select the host on which the verification process will be performed. Note that the host selected must have a Data Protector Disk Agent installed.

Verify on source host

Select this option to perform the verification process on the host on which the original backup was performed. The path to the host will also be verified.

Verify on media agent host

Select this option to perform the verification process on the media agent host (containing the source device) with no network involvement.

Verify on alternate host

Select this option to perform the verification process on an alternative host. Select the host from those available in the cell.

Object Verification Tasks

In the Results Area, the following object verification tasks are available:

Objects

Double-click this item to verify objects interactively from the Objects starting point. Use this starting point to list types of backed up data, such as Filesystem, Database, and so on.

Sessions

Double-click this item to verify objects interactively from the Sessions starting point. Use this starting point to list sessions in which objects were written to media.

Media

Double-click this item to verify objects interactively from the Media starting point. Use this starting point to list media pools and media.

Automated post-backup verification

Double-click this item to configure a post-backup object verification specification. Post-backup object verification takes place after the completion of a backup, object copy, or object consolidation session. It verifies objects created in that particular session that match the specified criteria.

Automated scheduled verification

Double-click this item to configure a scheduled object verification specification. Scheduled object verification takes place at a user-defined time. Objects created during different backup, object copy, and/or object consolidation sessions can be verified in a single scheduled object verification session.

Automated Object Verification

Data Protector provides the following methods of automated object verification:

Post Backup

Post-backup object verification takes place after the completion of a backup, object copy, or object consolidation session. It verifies objects created in that particular session that match specified criteria.

Scheduled

Scheduled object verification takes place at a user-defined time. Objects created during different backup, object copy, and/or object consolidation sessions can be verified in a single scheduled object verification session.

Interactive Object Verification

You can select objects for interactive verification from the following starting points:

Media

Use this starting point to list individual media pools and media.

Objects

Use this starting point to list backup object types, such as Filesystem or Database.

Sessions

Use this starting point to list sessions in which objects were written to media.

For VMware backups, the virtual machine disks are considered as objects that run in parallel. The disk objects of the virtual machine are listed but disabled in the Media list to understand virtual machine disks backed to the media. The copy or verify operation is performed on the virtual machine objects and all its associated disk objects are considered internally.

Media Verification

To use the media verification functionality, select **Devices & Media** in the context list.

Object Verification

Data Protector provides the following methods of object verification:

Interactive

Expand this item to verify objects interactively.

Automated

Expand this item to configure automated object verification. Choose between post-backup and scheduled object verification.

Automated Object Verification - Post-Backup

In the Results Area, a list of configured post-backup object verification specifications is displayed.

Name

The name of the object verification specification.

Automated Object Verification - Scheduled

In the Results Area, a list of configured scheduled object verification specifications is displayed.

Name

The name of the object verification specification.

Verification

Data Protector provides the following methods of verifying backup objects:

Media verification

To use the media verification functionality, select **Devices & Media** in the context list.

Object verification

To use the object verification functionality, expand this item and choose between automated and interactive object verification.

Add Detail Catalog Directory

Specify the properties of the DC directory and click **Finish**.

Allocation sequence

A consecutive number that defines the order in which Data Protector chooses a DC directory to write new data to, provided the effective DC directory allocation policy is Fill in sequence (the DCDirAllocation global option is set to 0). The first DC directory to be used should have the lowest allocation sequence number. Default: (value matching the number of already existing DC directories)

Path

Data Protector installation process creates five DC directories at the default DC directory. You can create additional DC directories at the same or another location.

Browse

Click this button to browse for the path instead of typing it in.

Maximum size

An amount that limits the total size of DC binary files in the DC directory. Default: 204 800 MB (200 GB).

Maximum files

A number that limits the number of DC binary files which can coexist in the DC directory. One DC binary file is created for each Data Protector medium used for backup. When a backup medium is overwritten, its corresponding DC binary file is removed and a new one is created. Default: 100 000.

Low space

An amount that defines the conditions under which the DC directory is considered to be full. It actually defines the minimum allowed difference between the actual size and the configured maximum size of the DC directory. When this threshold is reached, Data Protector starts using the next DC directory defined by the effective allocation policy. Additionally, this option defines the minimum amount of free space needed on the volume where the DC directory resides. Data Protector requires this space to log names of the backed up files and directories to the IDB. When free space for the last DC directory drops under this amount (meaning all other DC directories are considered to be full already), Data Protector automatically switches to the logging level No Log. It is recommended to use 10% to 15% of the current maximum DC directory size as a suitable value for this option. Default: 2048 MB (2 GB).

Auditing

This page displays auditing information about backup, restore, copy, and consolidation sessions for the specified time period.

Search interval

In the drop-down list, specify the period for which to display backup, restore, copy, or consolidation session information.

From

(available if Interval is selected) Specify the desired start date and time. You can type a start date or select it from the calendar.

To

(available if Interval is selected) Specify the desired start date and time. You can type a start date or select it from the calendar.

Update

Click this button to display a list of all backup, restore, copy, and consolidation sessions performed during the selected period. Selecting a specific session from the session list displays detailed information about media used, objects, and the object completion statuses.

Related topics

- For more information about enabling audit logs during Cell Manager installation, see Install Cell Manager in non-cluster mode and Install Cell Manager in cluster mode.
- For more information about enabling audit logs using command-line interface, see omnicc command-line interface.

Backup Object Version Properties - Copies

In the Results Area, all copies of the selected backup object version are listed, including the backup.

Tip To automatically open the backup object version properties for a selected object copy version in the Internal Database\Objects in the Scoping Pane, right-click the object copy version and click Properties.

The cross-link works for any type of object as long as the object is present in the Internal Database\Objects in the Scoping Pane. The Properties menu item is disabled if the object version does not exist in the above-mentioned folder.

Backup Object Version Properties - Media

In the Results Area, a list of media that were used to back up, mirror, or copy the selected backup object version is displayed.

Backup Object Version Properties - General

In the Results Area, details about the backup object version are listed.

Reporting level

This option sets the reporting level of messages displayed in the Messages tab. By default, the last selected reporting level is shown.

Backup Object Version Properties - Messages

In the Results Area, the messages for the selected backup object that were generated during the session are displayed. The level of messages depends on the Reporting level setting in the General tab.

Browse Drives

Select the desired location for the new DC directory. You can select an existing directory, or create a new one by typing its name in the text box.

Change Data Protection

In this page you can change the data protection of the selected backup object versions.

Protection

This option enables you to set periods of protection for the data you back up to prevent the data from being overwritten. The default value is **Permanent**. Others are:

- **None**: provides no protection. Media will be removed/deleted before the next write operation/backup to the file library is started.
- **Until**: means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Days**: means that the data on the medium cannot be overwritten for the specified number of days.
- **Weeks**: means that the data on the medium cannot be overwritten for the specified number of weeks.

Change Catalog Protection

In this page you can change the catalog protection of the selected backup object versions.

Protection

This option enables you to set periods of protection for the data you back up to prevent the data from being overwritten. The default value is **Permanent**. Others are:

- **None**: provides no protection. Media will be removed/deleted before the next write operation/backup to the file library is started.
- **Until**: means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Days**: means that the data on the medium cannot be overwritten for the specified number of days.
- **Weeks**: means that the data on the medium cannot be overwritten for the specified number of weeks.

Disk Usage

The pie chart shows the percentage of disk space used by specific parts of the IDB.

Records Statistics

The chart shows the number of used and free records in the selected part of the IDB.

Serverless Integrations Binary Files

The functionality this online help topic used to describe is no longer supported in the installed Data Protector version.

Session Messages Binary Files

In this page, the properties of the Session Messages Binary Files (SMBF) part of the IDB are displayed.

Size

The size of the SMBF part.

Number of Files

The number of files in the SMBF part.

Path

The location of the SMBF part.

Detail Catalog Directory Properties - Disk Usage

The pie chart shows the percentage of used disk space and free disk space for the DC directory.

Detail Catalog Directory Properties - General

In this page, general properties of the DC directory are displayed.

Records Statistics

The pie chart shows the percentage of used and free records in the selected part of the IDB. The pie chart is not displayed for items that have unlimited number of records specified in the Total records option.

Internal Database

In the Scoping Pane, you can choose among Objects, Sessions, Usage, and Auditing. Select or expand an item to access information in the IDB on the item. To display Help on a specific item, select the desired item in the Scoping Pane.

Detail Catalog Binary Files

In the Results Area, a list of DC directories is displayed.

Media Management Database

In the Results Area, types of entities that can be configured in the Media Management Database (MMDB) part of the IDB are listed.

Name

A group of entities of a particular type.

Disk Usage (MB)

The disk space used by the item (*.dat file).

Records Used

The number of records that are actually occupied. This number depends on the amount of information removed from the IDB and the amount of information stored in the IDB.

Total Records

The number of records that can be stored in the Internal Database.

Used

The percentage of used records. This figure is calculated as the current amount of records divided by the amount of records allocated in the IDB in percents. Thus, this figure may vary substantially, since Data Protector automatically allocates new records whenever this figure reaches 100% (whenever all currently allocated records are used).

Backup Object Versions

In the Results Area, a list of backup object versions recorded in the IDB is displayed. The following may be helpful:

- To use the filters available for the displayed list, click on **Show filter settings** and modify the parameters.
- To remove a backup object version from the IDB, right-click the backup object version and click **Remove Version**. File versions of the backup object will be removed in the next daily purge session.
- To modify data protection for a backup object version, right-click the backup object version and click **Change Data Protection**.
- To modify catalog protection for a backup object version, right-click the backup object version and click **Change Catalog Protection**.
- To display properties for a backup object version, double-click the backup object version or right-click the backup object version and click **Properties**.

The VEAgentDisk objects do not support the following operations:

- Remove Version
- Change Data Protection
- Change Catalog Protection

However, when the above operations are performed on the VEAgent object, these will be applied on the disk object as well.

Internal Database - Objects

In the Results Area, a list of backed up client systems is displayed. The following may be helpful:

- Double-click the name of a client system to list the backup objects.
- To remove all unprotected object versions, right-click **Objects** in the Scoping Pane and click **Remove Version**.

Session

The list in the Results Area displays details about each backup object that was backed up, mirrored, or copied in the session. The following may be helpful:

- To use the filters available for the displayed list, click on **Show filter settings** and modify the parameters.
- To remove a backup object version from the IDB, right-click the backup object version and click **Remove Version**. File versions of the backup object will be removed in the next daily purge session.
- To modify data protection for a backup object version, right-click the backup object version and click **Change Data Protection**.
- To modify catalog protection for a backup object version, right-click the backup object version and click **Change Catalog Protection**.
- To display properties for a backup object version, double-click the backup object version or right-click the backup object version and click **Properties**.

The VEAgentDisk objects do not support the following operations:

- Remove Version
- Change Data Protection
- Change Catalog Protection

Sessions

In the Results Area, a list of backup, restore, object copy, object consolidation, object verification, and media management sessions stored in the IDB is displayed. The following may be helpful:

- To display the backup objects that were written in the session, double-click a backup, copy, or consolidation session.
- To restart the backup or the copy of objects that were not completed, right-click the backup or the copy session and click **Restart Failed Objects**.
- To resume a failed backup or restore session, right-click the failed session and select**Resume Session**. This functionality is available for filesystem and Oracle Server integration backup and restore sessions.
  A paused session automatically resumes once the higher priority sessions scheduled in Scheduler have completed. The ability to pause and resume from where the session left off is available for filesystem, VMware and Oracle Server integration sessions. For other integrations, after being paused, the backup session restarts from the beginning.
- To modify data protection for backup objects written in a session, right-click the backup, copy, or consolidation session and click **Change Data Protection**.
- To modify catalog protection for backup objects written in a session, right-click the backup, copy, or consolidation session and click **Change Catalog Protection**.
- To remove backup object versions (backup, copy, or consolidation sessions), session messages, or a session from the IDB, right-click the session and select the desired action. File versions of backup objects will be removed in the next daily purge session.
- To list only sessions that match specific criteria, right-click**Sessions** in the Scoping Pane and click **Properties**.
- To display session properties, right-click a session and click **Properties**.

Name

Each session is identified by a session ID consisting of a date in a YY/MM/DD format and a unique number.

Status

The status of the session.

Type

The type of the session: backup, restore, copy, consolidation, verification, or media.

Specification

For backup, object copy, object consolidation, and object verification sessions, the name of the backup, object copy, object consolidation, or object verification specification used, respectively.

Backup Type

For backup sessions, the type of the backup: full or incremental; some other backup types are available for specific integrations.

Start Time

The time when the session started.

End Time

The time when the session ended.

Owner

The user who started the session and the system from which the session was started, for example: [username]@[system_name].

Client System

In the Results Area, a list of backup objects of the selected client system is displayed. The following may be helpful:

- Double-click a backup object to display the backup object versions.
- To remove a backup object version from the IDB, right-click the backup object version and click **Remove Version**. File versions of the backup object will be removed in the next daily purge session.
- To modify data protection for a backup object version, right-click the backup object version and click **Change Data Protection**.
- To modify catalog protection for a backup object version, right-click the backup object version and click **Change Catalog Protection**.
- To display properties for a backup object version, double-click the backup object version or right-click the backup object version and click **Properties**.

Usage

In the Results Area, the constituent parts of the IDB are displayed. Double-click an item to access information in the IDB on the item.

Catalog Database (CDB)

Media Management Database (MMDB)

Detail Catalog Binary Files (DCBF)

Session Messages Binary Files (SMBF)

Serverless Integrations Binary Files (SIBF)

The item Serverless Integrations Binary Files (SIBF) relates to the functionality that is no longer supported in the installed version.

Catalog Database

In the Results Area, a list of types of records stored in the Catalog Database (CDB) part of the IDB is displayed.

Name

A group of records of a particular type.

Disk Usage (MB)

The disk space used by the item (*.dat file).

Records Used

The number of records that are actually occupied. This number depends on the amount of information removed from the IDB and the amount of information stored in the IDB.

Total Records

The number of records that can be stored in the Internal Database.

Used

The percentage of used records. This figure is calculated as the current amount of records divided by the amount of records allocated in the IDB in percents. Thus, this figure may vary substantially, since Data Protector automatically allocates new records whenever this figure reaches 100% (whenever all currently allocated records are used).

Global Options

The Results Area displays a table of global options that allows you to change certain behaviors in your cell.

Group

Represents a contextual section the option belongs to.

Save

Click the **Save** icon save all changes.

Add

Click the **Add** icon to add a new option. The Add New Option dialog opens.

In use

Indicates the status of an option. Selected options are in use; empty checkboxes indicate options that are commented out in the global options file.

Name

Specifies name of the option.

Origin

Indicates the file which the option is loaded from. This column is hidden initially, but you can reveal it by clicking the arrow in Global Options header and performing a search.

Value

Represents the current option value.

Description

A description of the option and how it influences your Data Protector environment. To modify the table appearance or search for a specific option, use filters in the table headers.

Edit

Click the **Edit** icon to edit an existing option. The Description field becomes active. Click **Save** to save the selected option. For specific options, you may need to restart the Data Protector services to bring changes into effect. To save changes to more than one option, click the **Save** icon.

Session Properties - Failed Logical Objects

In the Results Area, details about failed logical objects are listed. The logical objects in the list are not protected yet. To prevent the data from being overwritten, restart the backup session.

Session Properties - General

In the Results Area, details about the selected session are listed.

Reporting level

This option sets the reporting level of messages displayed in the Messages tab. By default, the last selected reporting level is shown.

Session Properties - Messages

In the Results Area, the messages that were generated during the selected session are displayed. The level of messages depends on the Reporting level setting in the General tab.

Sessions - Filter Parameters

To display only sessions that match specific criteria, specify the criteria and click**Apply**.

Created in

In the drop-down list, select the time period for which you want to display sessions. To customize your own date and time, select **Interval**.

From

(available if Interval is selected) Specify the desired start date and time. You can select a start date from the calendar or type it.

To

(available if Interval is selected) Specify the desired end date and time. You can select an end date from the calendar or type it.

From Type

In the drop-down list, select the type of session to be displayed.

Backup Specification

(available if the Backup type is selected) In the drop-down list, select a backup specification to display only the backup sessions started with this backup specification.

Session Properties - Media

In the Results Area, a list of media that were used to back up, mirror, or copy the backup objects in the selected session is displayed.

Add Report

Select the type of report to add to the report group. Data Protector provides various types of reports:

- Reports on Data Protector configuration
- Reports on the Internal Database
- Reports on session specification usage
- Reports on media and media pools
- Reports on sessions in a timeframe
- Reports on a single session

Backup Specifications

In this page, backup specifications for which a report will be generated are selected. By default, the report is generated for all backup specifications.

Filter Backup Specifications

Backups from all groups

Select this option to generate a report for all backup specification groups.

Backup group

Select this option to generate a report for a specific backup specification group. Select the group from the drop-down list.

Select Backup Specifications

All

Select this option to generate a report for all backup specifications.

None

Select this option to exclude all backup specifications from the report.

Manual

Select this option to manually select backup specifications.

Time Frame

In this page, the time frame criterion is specified. The report will include all the sessions that were started in the specified time frame.

Relative time

Select this option to set a relative period of time, and then specify the time frame. The first number specifies the beginning of the time frame, and the second number the duration of the time frame. For example, if you specify 24 in both fields, the report will take into account the last 24 hours, calculated from its start time. This option is especially suitable for scheduled reports.

Absolute time

Select this option to set an absolute period of time. Specify the beginning and end of the period. Click the drop-down arrows to display the calendar.

Session ID

Specify the session ID of the backup, copy, or consolidation session for which you want to generate a report.

Session

Type the session ID or select it from the drop-down list.

Media

In this page, the criteria for the selection of media that will be included in the report are specified. By default, all media are included in the report.

Type

Select a media type to limit the report to media of that type.

Description

Type a description to limit the report to media with that description.

Media condition

Select a media condition to limit the report to media in that condition.

Protection

Select a period of data protection to limit the report to media with such a protection period.

Clients

In this page, the clients that will be included in the report are specified.

All clients

Select this option to include all clients in the report.

Selected clients

Select this option to limit the report to specific clients. Select the desired clients below.

Select All

Click here to select all listed clients.

Deselect All

Click here to deselect all listed clients.

Networks

In this page, you specify networks for which you want to configure a report. Valid IP address forms are: a.b.c.d – a complete IPv4 address (for example, 10.17.1.1) a.b.c – an IPv4 C-class network address (for example, 10.17.1) IPv6 addresses in any valid form (for example, ::1, td10::abba:1603, and so on)

Networks

Type IP address and click **Add** to add it to the list. To remove an IP address from the list, select it and click**Remove**.

Library

In this page, the criteria for the selection of media that will be included in the report are specified regarding whether the media reside in specific libraries. By default, all media are included in the report.

Do not care

Select this option to include all media in the report, regardless of where the media reside.

Media in selected libraries

Select this option to limit the report to media in specific libraries. Select the desired libraries below.

Media out of selected libraries

Select this option to limit the report to media not residing in specific libraries. Select the desired libraries below.

Select All

Click here to select all listed libraries.

Deselect All

Click here to deselect all listed libraries.

Media Pools

In this page, the criteria for the selection of media that will be included in the report are specified regarding whether the media belong to specific media pools. By default, all media are included in the report.

All media pools

Select this option to include all media in the report, regardless of the media pool they belong to.

Selected media pools

Select this option to limit the report to media belonging to specific media pools. Select the desired media pools below.

Select All

Click here to select all listed media pools.

Deselect All

Click here to deselect all listed media pools.

Locations

In this page, the criteria for the selection of media that will be included in the report are specified regarding the media location. By default, all media are included in the report.

All locations

Select this option to include all media in the report, regardless of their location.

Selected locations

Select this option to limit the report to media at specific locations. Select the desired locations below. By default, the list of locations includes only predefined locations. To select a location that was specified manually, type the location and click **Add**.

Select All

Click here to select all listed media locations.

Deselect All

Click here to deselect all listed media locations.

Time Frame

In this page, the criteria for the selection of media that will be included in the report are specified regarding the media type. By default, all media are included in the report.

Type

Select a media type to limit the report to media of that type.

Media Type

In this page, the criteria for the selection of media that will be included in the report are specified regarding the media type. By default, all media are included in the report.

Type

Select a media type to limit the report to media of that type.

Session ID

Specify the session ID of the backup, copy, or consolidation session for which you want to generate a report and the level of messages that will be displayed in the report output. (Session per Client Report includes only backup specifications.)

Session

Type the session ID or select it from the drop-down list.

Message level

Select the message level to filter the messages shown. Messages of the selected level and higher are displayed.

Time Frame

In this page, the time frame for the report is specified.

Number of days

The report will be generated for the specified period of time in days from the time the report is started.

Client System

In this page, the client for which the report is configured is specified.

Client

In the drop-down list, select the name of the client.

Consolidation Specifications

In this page, consolidation specifications for which a report will be generated are selected. By default, the report is generated for all consolidation specifications.

Select Consolidation Specifications

All

Select this option to generate a report for all consolidation specifications.

None

Select this option to exclude all consolidation specifications from the report.

Manual

Select this option to manually select consolidation specifications.

Copy Specifications

In this page, copy specifications for which a report will be generated are selected. By default, the report is generated for all copy specifications.

Select Copy Specifications

All

Select this option to generate a report for all copy specifications.

None

Select this option to exclude all copy specifications from the report.

Manual

Select this option to manually select copy specifications.

Reports on the Cell Manager

In the Results Area, the names of all Cell Managers that are part of the MoM environment are displayed. Double-click a Cell Manager to access the available report types.

Cell Manager

The name of the Cell Manager.

Status

The status of the Cell Manager (for example, Up and Running, No Permissions, and so on).

Reports on Enterprise

In the Results Area, types of reports that can be generated in the enterprise environment (multicell reports) are displayed. Double-click a report type to select a report.

Name

The following report types are available:

- Configuration
- Internal Database
- Pools and Media
- Session Specifications
- Sessions in Timeframe

Event

In the Results Area, the properties of the selected event are displayed.

Time

The time when the event occurred.

Level

The severity level of the event.

Module

The Data Protector module that reported the event.

Event

The name of the event.

Description

The message of the notification that was triggered by the event.

Event Log

In the Results Area, Data Protector events logged to the Data Protector Event Log are displayed. Double-click an event to display its details. The Event Log is not refreshed automatically. To refresh it, press **F5**.

Time

The time when the event occurred.

Level

The severity level of the event.

New

Events that occurred since the Event Log was last checked are marked as new.

Module

The Data Protector module that reported the event.

Event

The name of the event.

Description

The message of the notification that was triggered by the event.

Add Notification

In this page, configure a new notification.

Name

Type a name for the new notification.

Event

Select an event which will trigger the notification. You can choose among the following events:

- Alarm
- Check UNIX Media Agent
- Csa Start Session Failed
- Device Error
- End of Session
- File Library Disk Usage
- Health Check Failed
- IDB Backup Needed
- IDB Corrupted
- IDB Limits
- IDB Reorganization Needed
- IDB Space Low
- License Warning
- License Will Expire
- Mail Slots Full
- Mount Request
- Not Enough Free Media
- Session Error
- Start of Session
- Too Many Sessions
- Unexpected Events
- User Check Failed

Notify

Send method

Select a send method for the notification. You can choose among the following methods:

- Broadcast message
- Data Protector Event Log
- Email
- Email (SMTP)
- External script/command
- Log to file
- SNMP
- Use Report Group

Host/E-mail address/Script/Log to file/System/Report Group

(the field depends on the send method selection) Specify the recipient of the notification.

Parameters

Specify the options as desired. Except the Level option, these options depend on the event type. For more information on these options, see the event concerned.

Notifications List

In the Results Area, all configured notifications are displayed. Some notifications were configured automatically when Data Protector was installed.

Name

The name of the configured notification.

Event

The event at which the notification is triggered.

Parameters

The values of parameters set for the event.

Notify Method

The send method for the notification.

Destination

The recipient of the notification. For example, an e-mail address or the pathname of a log file. The following may provide additional information:

- To modify a configured notification, right-click it and click **Properties**.
- To configure a new notification, right-click Notifications and click **Add Notification**.

Reports List

In the Results Area, a list of configured reports in the selected report group is displayed.

Name

The name of the report.

Type

The type of the report.

Environment

The environment for which the report is configured: a single cell or a multicell environment (enterprise report). The following may provide additional information:

- To display properties of a report, right-click the report and click **Properties**.
- To preview a report, right-click it and click **Preview**.
- To delete a report, right-click it and click **Delete**.

Reporting

In the Results Area, you can choose among Reports, Notifications, and Event Log. Select or expand an item to access its contents. To display Help on a specific item, select the desired item in the Scoping Pane.

Enterprise Reporting

In the Scoping Pane, the names of all Cell Manager that are part of the MoM environment are displayed. Select a Cell Manager to access reports, notifications, and the Event Log for that Cell Manager.

Cell Manager

The name of the Cell Manager.

Status

The status of the Cell Manager (for example, Up and Running, No Permissions, and so on).

Reports

In the Results Area, a list of configured report groups is displayed.

Name

The name of the report group.

Next Start

If the report group is scheduled, the date and time of the next start is displayed. The following may provide additional information:

- To display properties of a report group, right-click the report group and click **Properties**.
- To delete a report group, right-click it and click **Delete**.

Session

In this page, the level of messages that will be displayed in the report output is specified.

Modify Notification

The properties of the configured notification are displayed.

Name

Type a name for the new notification.

Event

Select an event which will trigger the notification. You can choose among the following events:

- Alarm
- Check UNIX Media Agent
- Csa Start Session Failed
- Device Error
- End of Session
- File Library Disk Usage
- Health Check Failed
- IDB Backup Needed
- IDB Corrupted
- IDB Limits
- IDB Reorganization Needed
- IDB Space Low
- License Warning
- License Will Expire
- Mail Slots Full
- Mount Request
- Not Enough Free Media
- Session Error
- Start of Session
- Too Many Sessions
- Unexpected Events
- User Check Failed

Notify

Send method

Select a send method for the notification. You can choose among the following methods:

- Broadcast message
- Data Protector Event Log
- Email
- Email (SMTP)
- External script/command
- Log to file
- SNMP
- Use Report Group

Host/E-mail address/Script/Log to file/System/Report Group

(the field depends on the send method selection) Specify the recipient of the notification.

Parameters

Specify the options as desired. Except the Level option, these options depend on the event type. For more information on these options, see the event concerned.

Object Copies

Include object versions with number of copies

Specify how many valid copies the object versions should have in order to be listed in the report. A valid backup means that the backup completed successfully and its protection has not expired. The number of copies includes also the original object version.

Add Notification

Depending on your previous selection of session type, select backup, copy, or consolidation specifications. The notification will be triggered only if the event relates to any of the specifications selected here.

Backup/Copy/Consolidation Specifications

Any

If this option is selected, a single notification will be created for all session specifications.

Selected

If this option is selected, a separate notification will be created for every selected session specification.

Select All

Click here to select all listed session specifications.

Deselect All

Click here to clear the selection of all listed session specifications.

Add Notification

Select backup devices. The notification will be triggered only if the event relates to any of the backup devices selected here.

Devices

Any

If this option is selected, a single notification will be created for all backup devices.

Selected

If this option is selected, a separate notification will be created for every selected backup device.

Select All

Click here to select all listed backup devices.

Deselect All

Click here to deselect all listed backup devices.

Add Notification

Select media pools. The notification will be triggered only if the event relates to any of the media pools selected here.

Media Pools

Any

If this option is selected, a single notification will be created for all media pools.

Selected

If this option is selected, a separate notification will be created for every selected media pool.

Select All

Click here to select all listed media pools.

Deselect All

Click here to deselect all listed media pools.

Add Report Group

Type a name for the report group.

Name

The name of the report group.

Report Output

In the Results Area, the output of the report is displayed. If you selected the Show selection criteria in report option when configuring the report, the input parameter values are listed as well.

Configuration reports

- Cell Information
- Client Backup Report
- Clients not Configured for Data Protector
- Configured Clients not Used by Data Protector
- Configured Devices not Used by Data Protector
- Licensing Report
- Look up Schedule

Internal Database report

- IDB Size Report

Pools and media reports

- Extended List of Media
- List of Media
- List of Pools
- Media Statistics

Session specification reports

- Average Backup Object Sizes
- Filesystems Not Configured for Backup
- Object's Latest Backup
- Objects Without Backup
- Session Specification Information
- Session Specification Schedule
- Trees in Backup Specification

Sessions in timeframe reports

- Client Statistics
- Device Flow Report
- Extended Report on Used Media
- List of Sessions
- Object Copies Report
- Report on Used Media
- Session Errors
- Session Flow Report
- Session Statistics

Single session reports

- Session Devices Report
- Session Media Report
- Session Object Copies Report
- Session Objects Report
- Session per Client Report
- Single Session Report

Report - General

In this page, the name and type of report are specified.

Name

The user-defined name of the selected report.

Type

The type of report.

Show selection criteria in report

(available for reports with additional input parameters) If this option is selected, the output of the report also displays input parameter values.

Reports on enterprise

(available for Manager-of-Managers) If this option is selected, the report is generated for all Cell Managers configured in the MoM environment (multicell report).

Generate multiple reports

(available for the Session per Client report and for enterprise (multicell) reports) If this option is selected, the report is divided into sections: a Session per Client report by client, and enterprise reports by Cell Manager.

Report Group - General

In this page, the name of the report group is displayed.

Name

The name of the report group.

Send Method

In this page, the send method, recipient, and format of the report are specified. Specify the options as desired and click**Add**. You can add several recipients. To remove a recipient from the list, select the recipient and click **Remove**.

Send method

The following send methods are available:

- Broadcast
- E-mail
- E-mail (SMTP)
- External
- Log
- SNMP

System/E-mail address/Script/Log to file

(the field depends on the send method selection) Specify the recipient of the report. Enter a hostname for the broadcast method, an e-mail address for E-mail and E-mail (SMTP) methods, or a path to the script or log file for the External and Log methods.

Format

Select the desired format. The available formats depend on the send method selection.

Session Specifications Reports

In the Results Area, session specification reports are listed. Double-click a type of report to generate a report interactively.

Name

The following session specifications reports are available:

- Average Backup Object Sizes
- Filesystems Not Configured for Backup
- Object's Latest Backup
- Objects Without Backup
- Session Specification Information
- Session Specification Schedule
- Trees in Backup Specification

Configuration Reports

In the Results Area, configuration reports are listed. Double-click a type of report to generate a report interactively.

Name

The following configuration reports are available:

- Cell Information
- Configured Clients not Used by Data Protector
- Configured Devices not Used by Data Protector
- Look up Schedule
- Clients not Configured for Data Protector
- Licensing Report
- Client Backup Report

Internal Database Report

In the Results Area, the Internal Database report is listed. Double-click a report to generate it interactively.

Name

The following IDB report is available:

- IDB Size Report

Pools and Media Reports

In the Results Area, pool and media reports are listed. Double-click a type of report to generate a report interactively.

Name

The following pool and media reports are available:

- List of Media
- Extended List of Media
- List of Pools
- Media Statistics

Single Session Reports

In the Results Area, single session reports are listed. Double-click a type of report to generate a report interactively.

Name

The following single session reports are available:

- Session Devices Report
- Session Media Report
- Session Object Copies Report
- Session Objects Report
- Session per Client Report
- Single Session Report

Sessions in Timeframe Reports

In the Results Area, sessions in timeframe reports are listed. Double-click a type of report to generate a report interactively.

Name

The following sessions in timeframe reports are available: Client Statistics

- Device Flow Report
- Extended Report on Used Media
- List of Sessions
- Object Copies Report
- Report on Used Media
- Session Errors
- Session Flow Report
- Session Statistics

Reports on Cell Manager

In the Results Area, types of reports that can be generated for the selected Cell Manager are displayed. Double-click a report type to select a report.

Name

The following report types are available:

- Sessions in Timeframe
- Backup Specifications
- Internal Database
- Configuration
- Pools and Media
- Single Session

Verification Specifications

In this page, object verification specifications for which a report will be generated are selected. By default, the report is generated for all object verification specifications.

Select verification Specifications

All

Select this option to generate a report for all object verification specifications.

None

Select this option to exclude all object verification specifications from the report.

Manual

Select this option to manually select object verification specifications.

DB2 Restore Options

In this page, specify the DB2 integration restore options.

General Options

Restore to client

By default, DB2 objects are restored to the original client. To restore the objects to another client, select its name in the drop-down list. This option is valid only for restore of the whole database.User nameDB2 user of the target DB2 instance. This user must have appropriate authorities to perform DB2 backup and restore-related operations (either SYSADM, SYSCTRL, or SYSMAINT) and must be added to both the Data Protector and DB2 admin user groups.

User group

User group of the user.

Password

Password of the user.

Restore to instance

By default, DB2 objects are restored to the original DB2 instance. To restore the objects to another DB2 instance, type its name here. This instance must be configured for use with Data Protector. Before starting a restore of a database to another instance, define new table space containers for non-system table spaces.

Rollforward

Select this option to perform a rollforward recovery. The database/tablespace is restored to its state at a specific point in time. During a rollforward recovery, both databases/tablespaces and archived logs are restored, and then the changes recorded in the archived logs are applied to the database/tablespace. The latest backup version of log files is used for this purpose. If log files are included in the backup and the omnirc variable OB2_DB2INCLDLOGS is set to 1, the included logs are restored to the Data Protector temporary folder. Specify the rollforward by selecting **Rollforward to the end of the logs** or **Rollforward to date**. When specifying **Rollforward to date**, use the coordinated universal time (UTC). Rollforward recovery of the system catalog can only be performed to the end of the logs. You cannot restore other table spaces of the same database from the same session simultaneously. To perform a rollforward recovery in a physically partitioned environment, restore all the parts with **Rollforward** cleared, connect to the catalog node, and then start a rollforward using the DB2 Command Line Processor. To perform a version recovery, clear this option. The database/tablespace is restored to its state at the time of the backup. For a version recovery, you need a full offline database backup. When restoring from an online backup with **Rollforward** cleared, the database enters the rollforward pending state and becomes unavailable for use. To make it available, start a rollforward (in a partitioned environment, from the catalog node) using the DB2 Command Line Processor or Command Center. By default, this option is selected.

Microsoft Exchange Server Options

The following restore options are specific to Microsoft Exchange Server.

Restore to another client

(available when restoring the Information Store) Specify this option to restore a Microsoft Exchange Server database to a Data Protector client different from the one the database was backed up from. Select also the name of the target client.

The target client must be a member of the Data Protector cell and must have the same Microsoft Exchange Server configuration structure as the original backed up client. If the target client is cluster-aware, specify its virtual server name.

Directory for temporary log files

Specify a path of the temporary directory for Microsoft Exchange Server transaction log files. Data Protector first restores the transaction log files to this directory. Microsoft Exchange Server then uses the log files to recover the database. This operation is referred to as hard recovery.

Last restore set (start recovery)

Select this option to perform a hard recovery after the restore process. Select this option only for the last restore session in the sequence of sessions used for restoring a particular Microsoft Exchange Server database.

Mount databases after recovery

Select this option to automatically mount the restored database after the hard recovery.

Last consistent state

Select this option to restore the Microsoft Exchange Server database to its last consistent state. The latest log files, created after the backup, will be applied to the restored database during the recovery process.

Microsoft Exchange Server Options

The following restore options are specific to Microsoft Exchange Server.

Restore to another client

(available when restoring the Information Store) By default, you restore to the same client from which the application data was backed up. If this option is selected, you can restore to a different client in the cell.

Delete existing log files

Deletes all existing log files pertaining to the directory or information store that is being restored. Select this option when you restore data to a different system or when you want your restore to be consistent to a specific point in time. It is not recommended to delete log files when restoring the latest backup to the system on which the backup was made.

Stop services before restore

If this option is selected, Data Protector stops all Microsoft Exchange services, except the Exchange System Attendant. If you do not use this option, you must stop these services manually before the restore.

Start services after restore

If this option is selected, Data Protector starts the Microsoft Exchange services that were stopped using the Stop services before restore. If you do not use this option, you must start these services manually after the restore.

Restore actions

(available for the Information Store)

Restore both databases

Restores both the public Information Store and the private Information Store.

Restore private database only

Restores the private Information Store.

Restore public database only

Restores the public Information Store.

DB2 Restore Source

This page displays the DB2 objects that have been backed up. Select the data to be restored. To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

Restore

Select the object type to be restored.

> **Important** In a physically partitioned environment, select only one database or several table spaces of the same database.

By default, the latest backup version is restored.

The following may provide additional information:

- To restore a DB2 object from a specific backup version, right-click the object and click **Properties**.
- To restore a database to a new database, right-click the database, click **Properties**, and then click the **Options** tab.

Oracle Restore Source

In this page, you specify the type of restore action that you want to perform, and select the objects to be restored.

Restore action

Select one of the following restore actions:

Perform Restore

Select this option to only restore (but not recover) the database objects using the Data Protector GUI, After restore, you must recover the database manually using RMAN.

Perform Restore and Recovery

Select this option to perform both the restore and the recovery using the Data Protector GUI.

Perform Recovery Only

Select this option to only recover the database objects using the Data Protector GUI.This option is used in ZDB environment after instant recovery and can only be performed on the whole database.

Perform RMAN Repository Restore

Select this option to restore the recovery catalog or the control file when the database objects are not available in this page.

Perform Duplication

Select this option in Oracle Data Guard environment to perform duplication of a production database. This action can only be performed on the whole database.

Application Restore Devices

In this page, you select devices for restore.

Automatic device selection

This option is applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup. By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option **AutomaticDeviceSelectionOrder**. For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup. Default: selected.

Original device selection

This option is applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available. This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration. Default: not selected.

Original Device

The names of all configured devices are listed. By default, Data Protector restores selected data with the same devices that were used during backup.

Device status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here. If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility.

The following may be helpful:

- To replace the original device with an alternative device, select the device and click **Change**. The new device will be used only for this session.
- To save all the selections made in this window as the defaults for the specified backup object, click **Save device mapping**.
- For more information on a device, right-click the device and click **Info**.
- To edit data restore policies for AWS S3 Glacier and S3 Deep Archive Glacier, select the device and click **S3 Retrieval Policies**.

Lotus Notes

In this page, you select devices for the restore of Lotus Notes/Domino Server objects.

Automatic device selection

This option is applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup. By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option **AutomaticDeviceSelectionOrder**. For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup. Default: selected.

Original device selection

This option is applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available. This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration. Default: not selected.

Original Device

The names of all configured devices are listed. By default, Data Protector restores selected data with the same devices that were used during backup.

Device status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here. If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility. The following may be helpful:

- To replace the original device with an alternative device, select the device and click **Change**. The new device will be used only for this session.
- To save all the selections made in this window for the specified backup object, click **Save device mapping**.
- For more information on a device, right-click the device and click **Info**.

Application Restore Media

In this page, the media needed for the restore are displayed. If an object version that you want to restore exists on more than one medium, all media are listed, except those obtained using the media copy functionality.

For more information on a medium, right-click the medium and click **Info**.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Number of media

The number of media present in a location.

Change priority

To change the media location priority for this session, select a media location and click this button.

Application Restore Source

This page displays the objects that have been backed up. Select the objects to be restored. To specify further options for your restore, click other tabs and set the desired options. To view object properties, right-click an object and select **Properties**.

Important In an availability group configuration, restore to a different client and instance is mandatory. Before restoring such a database, make sure that you do not select an availability group listener for the target client and that the selected SQL Server instance exists on the target client. Also make sure that the database which you selected for the restore does not belong to any availability group. This requirement is not applicable for ZDB.

Restore Source - Informix

This page displays dbobjects that have been backed up. Select the objects to be restored. To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

Restore complete database

Select this option to restore the complete database or for a whole-system restore.

Name

The names of dbobjects.

Application name

The name of the database server.

Lotus Notes/Domino Server Restore Source

This page displays the objects that have been backed up. Select the data to be restored. To specify further options for your restore, click other tabs and set the desired options in the appropriate pages. Before you can start a restore, you must specify the path to the notes.ini file in the Options page.

Includes/Excludes

Click here to specify the Lotus Notes/Domino Server data directories that you want to include in or exclude from the restore.

Restore Source - SAP MaxDB Integration

This page displays the objects of the selected SAP MaxDB instance that have been backed up. Select the objects you want to restore. To specify other options for your restore, click other tabs and set the desired options in the appropriate pages.

Name

The name of an object of the SAP MaxDB instance. The following may be helpful:

- To select a backup session from which to restore, right-click **Data** and click **Properties**. In the Properties for Data dialog box, select the desired backup session from the **Backup version** drop-down list.
- To restore only the SAP MaxDB instance archive logs, a Trans backup session has to be selected from the Backup version drop-down list.

Do not select the backup session for the Config item. The same session as selected for the Data item will be used, regardless of what you select for the Config item.

Lotus Notes/Domino Server - Include/Exclude Options

The options in this page apply to the specific object that you have selected.

Includes

Specify the Lotus Notes/Domino Server data directories that you want to include in the restore. Type the relative pathname to the Lotus Notes/Domino data directory in the text box and click **Add**. For example, if the selected object is a NSF database and you want to restore only the help directory, type help. To remove a data subdirectory from the Includes list, select it and click **Delete**. If no data subdirectories are listed, the entire object is selected for restore.

Excludes

Specify the Lotus Notes/Domino Server data directories that you want to exclude from the restore. Type the relative pathname to the Lotus Notes/Domino data directory in the text box and click **Add**. For example, if the selected object is a NSF database and you want to skip the help directory, type help. To remove a data subdirectory from the Excludes list, select it and click **Delete**. The Excludes option has higher priority than the Includes option. If you specify the same data directory in the Includes and Excludes fields, the directory will not be restored.

Informix Server Restore Options

In this page, you can select the backup specification, the user name and group (on UNIX systems), as well as the destination and backup version for the restore.

Backup specification

Specify a backup specification to be used for salvaging logical log files still on the disk before restoring. Preferably, specify the backup specification used for the backup of logical logs.

Username

If the target client is UNIX system, specify the user name of the Informix Server backup owner. The `onbar` command is started under the account of the specified user.

User group

If the target client is UNIX system, specify the user group of the Informix Server backup owner.

Restore to client

This is only valid for a whole-system restore. By default, you restore to the original backup client. To restore to another client, specify the client.

Restore by log number

(available if you selected Restore complete database in the Source page) Use this to restore data up to a specific log number. If further logs exist, ON-Bar does not restore them. This option invokes the `onbar -r -n last_log_number` command. For details, see the *Backup and Restore Guide of Informix Server*.

Restore by date

(available if you selected Restore complete database in the Source page) Use this to restore data to a specific point in time. This option invokes the `onbar -r -t time` command. For details, see the *Backup and Restore Guide of Informix Server*.

Restore the latest version

Select this option to restore the latest backup version.

Whole database restore

(available if you selected Restore complete database in the Source page) Select this option to perform a whole-system restore. If this option is selected, Data Protector searches for the last whole-system backup and restores from that. This option invokes the `onbar -r -w` command. For details, see the *Backup and Restore Guide of Informix Server*. Only use this option when restoring from a whole-system backup. Data Protector does not automatically detect if a whole-system backup exists.

Lotus Notes/Domino Server Restore Options

In this page, you can set restore options that are specific to Lotus Notes/Domino Server.

User and group

User name

(available for UNIX systems) Username of the Lotus Notes/Domino Server backup owner, for example, notes.

User group

(available for UNIX systems) User group of the Lotus Notes/Domino Server backup owner, for example, notes.

Backup version

By default, a restore is performed from the last full backup of the database. Click **Browse** to select a backup version other than the last one. Click **Clear** to clear the currently specified backup version.

Parallelism

Specify how many parallel streams should be used to restore your data. For example, suppose you used two devices for backup, one with concurrency 2 and the other with concurrency 1. Then, your data was backed up with 3 parallel streams. In this case, set the restore parallelism to at least 3. For best performance, set the restore parallelism as high as possible (the maximum value is 32). Then, Data Protector automatically creates the optimum number of streams. Default: 1

Recovery type

Recover (last possible consistent state)

Select this option to recover the database to the last possible consistent state. This also includes the restore of archived transaction logs if needed during recovery.

Point in time recovery

You can specify a point in time to which the database state should be recovered. Click **Browse** to specify the desired date and time. Only transactions written before the specified date and time are applied to the database.

Do not recover

This is the default option. Select this option to restore databases without recovering them from the backed up logs. Transactions made after the backup are not reflected in the restored databases.

Generate New ReplicaID

(available when Recover (last possible consistent state) is selected as the recovery type) If this option is selected, each restored storage database (NSF database) is assigned a new replica ID. Default: not selected

Oracle Restore Options

In this page, you specify the Data Protector Oracle integration restore, recovery, or duplicate options depending on the restore action you selected in the Source page.

General Options

Client

Select the client on which the Data Protector Oracle integration agent (ob2rman.pl) will be started.

Settings

Click to specify the login information (user name, password, and net service name) for the target database (in case of restore and recovery) or auxiliary database (in case of duplication) where you want the selected database objects to be restored or duplicated. If this is not specified in the case of restore or recovery, the login information of the selected database that resides on the selected client will be used. If this is not specified in the case of duplication, the duplication session will fail. Oracle Data Guard: If you restore the primary database, specify the login information for the primary database. If you restore the standby database, specify the login information for the standby database.

User name

(available for UNIX systems)

User group

(available for UNIX systems) Specify the user account under which you want the restore to start. This user must have Oracle rights to restore the database. Also, it must be added to the Data Protector admin or operator user group.

Restore mode

(depending on which restore action was selected in the Source page) Specify which type of restore you would like to perform:

- **Normal**: Use this option when a conventional backup or ZDB using the backup set method was performed.
- **Proxy copy**: Use this option when the original Oracle backup was made using the Oracle RMAN proxy-copy method. This option is disabled when you perform recovery only.

Parallelism

(disabled for Oracle proxy copy ZDB) Specify the number of concurrent data streams that can read from the backup device. The default value is one. In case of Normal restore mode, to optimize restore performance, use the same number of data streams as were used during the backup. For example, if you set the backup concurrency to 3, set the parallelism to 3 as well. Note that if a very high number of parallel data streams is specified, this may result in a resource problem because too much memory is being used. For Oracle proxy-copy ZDB, Data Protector automatically sets the number of parallel data streams to the value that was used at backup. If you are restoring an Oracle proxy-copy ZDB session performed with a previous version of Data Protector, parallelism is set to the number of devices that were used for backup, regardless of the concurrency numbers for these devices.

Restore Options

Restore until

(depending on which restore action was selected in the Source page) The options in this drop-down list allow you to limit the selection to those backups that are suitable for an incomplete recovery to the specified time.

- **Now**: Use this option to restore the most recent full backup. By default, this option is selected.
- **Selected time**: Use this option to specify an exact time to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified time.
- **Selected logseq/thread number**: A logseq number is a redo log sequence number. Use this option to specify a particular redo log sequence and a thread number which will act as an upper limit of redo logs to restore. Data Protector restores the backup that can be used in recovery to the specified log sequence number.
- **Selected SCN number**: Use this option to specify the SCN number to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified SCN number.

Duplicate Options

(available if Perform Duplication was selected in the Source page)

For Standby

Select this option to create a standby database.

DORECOVER

(available if For Standby is selected) Select this option if you want RMAN to recover the database after creating it

To database name

Select this option to create a new database copy. In the text box, specify its name. The name should match the name in the initialization parameter file that was used to start the auxiliary database instance. By default, the database name of the currently selected target database is set.

NOFILENAMECHECK

Select this option to disable RMAN to check whether the target datafiles share the same names with the duplicated datafiles. Select this option when the target datafiles and duplicated datafiles have the same names, but resides on different systems. Default: not selected.

Recovery Options

Recover until

The options in this drop-down list allow you to limit the selection to those backups that are suitable for an incomplete recovery to the specified time.

- **Now**: Use this option to restore the most recent full backup. By default, this option is selected.
- **Selected time**: Use this option to specify an exact time to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified time.
- **Selected logseq/thread number**: A logseq number is a redo log sequence number. Use this option to specify a particular redo log sequence and a thread number which will act as an upper limit of redo logs to restore. Data Protector restores the backup that can be used in recovery to the specified log sequence number.
- **Selected SCN number**: Use this option to specify the SCN number to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified SCN number.

Open database after recovery

(depending on which restore action was selected in the Source page) Select this option to automatically open the database after a recovery.

Reset logs

Select this option to reset the archive logs after the database is opened.

- Always reset the logs
  - After an incomplete recovery.
  - If a backup of a control file is used in recovery or restore and recovery.
- Do not reset the logs
  - After a complete recovery when the backup of a control file was not used in recovery or restore and recovery.
  - On the primary database, if the archived logs are used for a standby database. However, if you must reset the archive logs, you will need to recreate the standby database.

If you reset the logs when the **Restore until** option is set to **Now**, a warning is displayed, stating that you should reset the logs only if you use a backup of the control file for restore.

Oracle recommends to perform a complete backup immediately after a database was opened with the **Reset logs** option.

Restore Options - SAP MaxDB Integration

In this page, you can set restore options.

Restore to client

By default, you restore to the original backup client. If you want to restore to another client, select the corresponding name from the drop-down list. The selected SAP MaxDB Server must be a part of the Data Protector cell and must have the Data Protector SAP MaxDB Integration software component installed.

Restore to instance

By default, you restore to the original instance. If you want to restore to another instance, you can either select the corresponding name from the drop-down list of configured instances, or enter the name of an existing instance, which is not yet configured for use with this integration. But in the latter case, click **Settings** to configure the specified instance.

Settings

Click here to configure the specified instance, not yet configured for use with this integration.

User name

On UNIX systems, you can change the user name for the operational system user under whose account the SAP MaxDB application is running on the SAP MaxDB Server. By default, the user that started the Data Protector GUI is set for this option.

User group

On UNIX systems, you can change the group name for the operational system user under whose account the SAP MaxDB application is running on the SAP MaxDB Server. By default, the group for the user that started the Data Protector GUI is set for this option.

Force restore if database is online

When this option is not selected and target database (instance) is online, the restore fails with a warning and the target database is intact. When this option is selected and target database is online, the restore starts successfully. This option is not applicable when the target database is offline. The database is restored whether the option is selected or not.

Recovery

When this option is selected, the database is recovered after the restore (it is switched to the Online operating mode) by applying the redo logs until the latest version or until the specified date and time.

> **Important** When using this option, make sure that the selected backup version will restore enough data for the integration to apply the redo logs until the latest version or until the specified date and time. To select the backup version, click the **Source** tab, right-click **Data**, and click **Properties**.

When this option is not selected, all other recovery options are disabled and the following happens after the restore:

- If archive logs are not restored (if restore from a Full backup session is performed), the database remains in the Admin mode after the restore.
- If archive logs are restored, the database is switched to the Online mode, if the restored archive logs allow it. However, if the database cannot be switched to the Online mode (because the restored archive logs do not allow it), it remains in the Admin mode.

Latest version

Select this option to recover the database until the last archive log.

Until date

Select this option to recover the database until a specific point in time. The selected time is the system time on the system running the Data Protector GUI. If the system to be recovered is not in the same time zone as the system running the Data Protector GUI, the point of recovery is adjusted to the local time setting on the system to be restored.

Use existing archive logs

(disabled in case of an SAP MaxDB migration) Select this option to copy the existing archive logs on the SAP MaxDB Server to SAP MaxDB Server redo logs. If this option is not selected, the backed up archive logs on backup media are applied to the redo logs (if a Trans backup session is selected for restore), or the redo logs are left intact together with the existing archive logs on the SAP MaxDB Server (if a Full or Diff backup session is selected for restore). When a Trans backup session is selected for restore or when it is a part of the needed restore chain, and this option is selected, the archive logs from Data Protector media are applied to the redo logs. Thereafter, the archive logs on the SAP MaxDB Server are applied to redo logs. This option is disabled in case of SAP MaxDB migration, thus allowing only for the restore of redo logs from the backed up archive logs on backup media (if a Trans backup session is selected for restore).

Properties - Advanced

Specify the advanced option for your Microsoft SQL Server database restore.

Restore database with new name

Important If the logical and destination file names are not listed, add them to the list. Enter the names that were used in the backup session. Otherwise, the restore fails.

Add/Modify

After typing the destination file name in the appropriate text box, click here.

Remove

To cancel your selection, select the file and click here.

Important In an availability group configuration, restore to a different client and instance is mandatory. Before restoring such a database, make sure that you do not select an availability group listener for the target client and that the selected SQL Server instance exists on the target client. Also make sure that the database which you selected for the restore does not belong to any availability group. This requirement is not applicable for ZDB.

Microsoft SQL Server Options

In this page, specify the restore options for your Microsoft SQL Server database restore.

Restore to another client

Select this option to restore the database objects to another SQL Server. From the drop-down list, select a desired SQL Server.

Restore to another instance

(available if there is at least one running instance on the selected SQL Server) Specify new locations for the databases you want to restore: In the Source property page, right-click a database, click Properties, and then click Advanced.

In an availability group configuration, restore to a different client and instance is mandatory. Before restoring such a database, make sure that you do not select an availability group listener for the target client and that the selected SQL Server instance exists on the target client. Also make sure that the database which you selected for the restore does not belong to any availability group. This requirement is not applicable for ZDB.

Restore actions

Specify what you want to do with the selected backup session.

- **Restore data**: If this option is selected, the data from the session is restored.
- **Restore and display file list only**: If this option is selected, information about the files backed up in the session is displayed in the Monitor window.
- **Restore and display headers only**: If this option is selected, information about the session is displayed in the Monitor window.

Default: Restore data.

Tail log backup

Enable tail log backup

(not available for ZDB) If this option is selected, Data Protector performs a tail log backup, just before the restore session starts. This captures the logs from the tail that have not been backed up yet. Before selecting this option, ensure that:

- the option Put database in single user mode - log off all users is selected for all involved databases.
- the option Restore data is selected.

Default: not selected.

Backup specification

(available if the Enable tail log backup is selected) In the drop-down list, select a backup specification to be used for backing up a tail of the log.

MS VSS Options

In this page, you can set restore options for your Microsoft Volume Shadow Copy writers restore.

Restore to another client

(not supported for SharePoint Services writer) By default, you restore to the same client from which the application data was backed up. If this option is selected, you can select some other system in the cell. The Disk Agent is started on the selected client system and the data is restored there.

Restore to the following directory

Specify the path to the directory to which you want to restore the data.

Restore Options - Other

In this page you can set the report level and network load for your restore session.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: **High**.

Report level

This option defines the level of errors that will be reported for an object during a backup or restore session. Report levels are: **Warning**, **Minor**, **Major**, and **Critical**. Errors of the selected level and higher are reported. For example, by setting the level to Minor, only minor, major, and critical errors are reported in the Messages field. By default, the level is set to Warning. Messages of Normal level are always reported. The number of messages per backup system stored in the IDB is limited to 3000.

Enable resumable restore

If this option is selected, Data Protector creates checkpoint files during the restore session. The checkpoint files are needed if the restore session fails and you want to resume the session using the Data Protector resume session functionality.

Default: selected (you can change the default using the global option ResumableRestoreDefault).

Browse Drives

In this page you select the location for your restore.

If you restore to a UNIX client system, you can restore your data to another directory. If you restore to a Windows system, you can restore to another Windows system on the network and to another directory of the system. Enter the new path, or browse for it if possible.

Add Section

If a backup is not stored in the IDB, you can select the data for restore by adding the desired section(s) here.

In the text box, enter the pathname of a disk image section that you want to restore, and click **OK**.

- UNIX systems:
  - Enter: `/dev/vg01/rvol1` to add a raw logical volume
  - Enter `/dev/rdsk/c2t0d0` to add a disk image section
- Windows systems: Enter a disk image section in one of the following ways:
  - `\\.\drive_letter:` . For example: `\\.\E:`
    When a drive letter is specified for the volume name, the volume is not being locked during the backup. A volume that is not mounted or mounted as an NTFS folder cannot be used for disk image backup.
  - `\\.\PHYSICALDRIVE#` . For example: `\\.\PHYSICALDRIVE3` .

Disk Image Restore Destination

In this page you select the destination for the disk image restore.

Default destination

Target client

By default, you restore to the same client system from which the data was backed up. You can select another system in your cell from the drop-down list. The Disk Agent is started on the selected client system and the data is restored there.

You need to have the Restore to other clients user right to be able to restore to another client system.

Restore to original location

By default, you restore your data to the same directory in which it was located when the backup was performed. It can be on the original client system or on some other client system you have selected.

Restore to new location

(not available for disk image restore) This option enables you to restore your data to another directory. Specify the path to the directory to which you want to restore the data. You can browse for it if you are using the GUI on a Windows system. If you restore to a Windows system, you could select a directory on another system, but this is not recommended.

File Conflict Handling

(not available for disk image restore)

Keep most recent

If this option is selected, the most recent versions of files are kept. If a file on the disk is newer than the backed up version, the file is not restored. If a file on the disk is older than the backed up version, the file is overwritten with the newer version from the backup. By default, this option is enabled.

No overwrite

If this option is selected, files that exist on the disk are preserved. This means that they are not overwritten by other versions of these files from the backup. Only non-existing files are restored from the backup. By default, this option is disabled.

Overwrite

If this option is selected, existing files on the disk are replaced with files from the backup. By default, this option is disabled.

Disk Image Restore Devices

In this page, you select devices for restore.

Automatic device selection

This option is applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup.

By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option **AutomaticDeviceSelectionOrder**.

For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup. Default: selected.

Original device selection

This option is applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available. This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration. Default: not selected.

Original Device

The names of the devices that were used for the backup of your disk image are listed. By default, Data Protector restores selected data with the same devices that were used during backup.

Device status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here. If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility. The following may be helpful:

- To replace the original device with an alternative device, select the device and click **Change**. The new device will be used only for this session.
- For more information on a device, right-click the device and click **Info**.

Disk Image Restore Media

In this page, the media needed for the restore are displayed. If an object version that you want to restore exists on more than one medium, all media are listed, except those obtained using the media copy functionality. For more information on a medium, right-click the medium and click **Info**.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location.

By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Number of media

The number of media present in a location.

Change priority

To change the media location priority for this session, select a media location and click this button.

Disk Image Restore Options

In this page you can set restore options.

Restore options

(not all options are available for disk image restore)

Omit deleted files

For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

If this option is selected, Data Protector recreates the state of the backed up directory tree at the time of the last incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are not restored.

If this option is not selected, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

When using the **Restore As** or **Restore Into** functionality with this option enabled, carefully choose the restore location to prevent accidental removal of existing files.

Default: not selected.

Move busy files

This option is relevant if a file on the disk is being used by an application when a restore wants to replace this file. It only applies to the files that are locked by an operating system when they are used by the application or other process. The option is used with the Keep most recent or Overwrite options. By default, this option is disabled.

On UNIX systems, Data Protector moves the busy file filename to #filename (adds a hash in front of the filename). The application will keep using the busy file until it closes the file. Subsequently, the restored file is used.

On Windows systems, the file is restored as filename.001. All applications keep using the old file. When the system is rebooted, the old file is replaced with the restored file.

On Linux systems, this option is not supported.

List restored sections

Select this option if you want to view the names of the sections as they are restored.

Display statistical information

When this option is enabled, Data Protector reports statistical information (such as size and performance) for each object that is backed up or restored. You can view the information in the monitor window. By default, this option is disabled.

Restore sparse files

(available for UNIX systems)

This option restores sparse files in their original compressed form. This is important because sparse files can consume additional disk space unless they are restored in their original form. By default, this option is disabled.

This option applies to UNIX sparse files only. Windows sparse files are always restored as sparse.

Lock files during restore

This option denies access to files during the restore. By default, this option is disabled.

Restore time attributes

This option preserves the time attribute values of each restored file. When this option is disabled, Data Protector sets the time attributes of the restored objects to the current date and time. By default, this option is enabled.

Restore protection attributes

This option preserves the original protection attributes of each restored file. If this option is disabled, Data Protector applies the protection attributes of the current restore session. By default, this option is enabled.

On Windows systems, this option applies to file attributes only. Security information is always restored, even when this option is disabled.

Pre- and Post-exec commands

Use pre- and post-exec commands to dismount the disk before a disk image restore and mount it back afterwards.

Pre-exec

This option allows you to enter a command (or script) to be executed before the restore of each object is initiated. This command (or script) must return success for Data Protector to proceed with the restore.

The pre-exec command (or command) is executed on the client system where the Disk Agent is running. On a Windows system, the scripts must be located in the Data_Protector_home\bin directory or its sub-directory. On Unix systems, the scripts must be located in /opt/omni/lbin directory, or its sub-directories.

Note that only .bat, .exe, and .cmd are supported extensions for pre-exec scripts on Windows systems. To run a pre-exec script with an unsupported extension (for example, .vbs), create a batch file (.bat) that starts the script. Then configure Data Protector to run the batch file as a pre-exec command which then starts the script with the unsupported extension.

Post-exec

This option allows you to enter a command (or script) to be executed after the restore of each object is completed. The post-exec command (or script) is executed on the client system where the Disk Agent is running.

On a Windows system, the scripts must be located in the Data_Protector_home\bin directory or its sub-directory. On Unix systems, the scripts must be located in /opt/omni/lbin directory, or its sub-directories.

Note that only .bat, .exe, and .cmd are supported extensions for post-exec scripts on Windows systems. To run a script with an unsupported extension (for example, .vbs), create a batch file (.bat) that starts the script. Then configure Data Protector to run the batch file as a post-exec command, which then starts the script with the unsupported extension.

Advanced

Click here to set user-definable variables.

Disk Image Restore Source

In this page you select the disk image or its sections for restore.

To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

Select Version

Click here to select another version of the disk image backup data for restore. By default, the most recent backup version is selected for restore.

Add Section

Click here to manually add a section that you want to restore. Use this if the backup is not stored in the IDB.

Reset To Default

Removes the sections that you have added and deselects what you have selected.

Use pre- and post-exec commands in the Options page to dismount the disk before a disk image restore and remount it afterwards.

Drive Mapping

Select restore locations for the drives. Right-click each drive and click Map Drive to open the dialog box where you select a restore location for the drive.

Start Disk Administrator

Click here to access the Disk Administrator utility in order to partition the destination drives.

Map Drive

To perform a restore of the faulty system on the host, map the volume of the original system to a volume of the replacement disk.

Selected drive

The drive selected for mapping is displayed.

Map to

Select a drive letter of the replacement disk to which you want to restore the original volume.

Create ISO image

Select the DR OS image format, the destination where you want to place the created image, and other options.

Select image format

Create bootable ISO image

You can create a DR ISO image (by default, recovery.iso) that can be recorded on a CD or DVD by using any CD or DVD recording tool.

Create bootable USB drive

You can create a bootable USB drive. The DR OS image is written directly to a USB drive.

Create bootable network image

You can create an image bootable over the network (by default, recovery.wim). Use the Windows Deployment Server (WDS) to boot the DR OS network image.

Select the destination directory

(available for a bootable ISO image and network image)

Select the destination directory where the ISO image or network image should be placed.

Select the destination USB drive or disk number

(available for a bootable USB drive)

Specify the drive letter (mount point) of the USB drive or the disk number assigned to the USB drive, to which the DR POS image should be written.

You can protect the DR OS image from unauthorized use by setting a password. The lock icon indicates whether a password has been set.

Driver options

Lists the drivers that are required for a successful disaster and are inserted into the DR OS.

Use the buttons right of the list to add new drivers, delete selected drivers, or reload original drivers that are included in the recovery set of your Windows system.

Restore Recovery Information

Select one of the configuration objects that Data Protector will use to retrieve the recovery information.

To select a specific backup version, right-click an object and click *Properties*. By default, the latest backup version is selected for restore.

Password Protect Image

Set a password to prevent unauthorized recovery from a DR OS image. You have to provide the password after the DR OS image is booted, so make sure it is available at recovery time.

Type a password and confirm it.

The password must consist of ASCII characters only, namely a-z, A-Z, 0-9 and punctuation marks.

Properties - Version

This page displays information about available backup versions.

Select for restore

You can select or deselect the file for restore.

Backup version

Select a backup version of the file. By default, the most recent backup version is selected for restore. If you are restoring several databases from the same storage group, make sure that their backup versions are the same. Otherwise, you need to restore them in separate restore sessions.

Last backup version

The date, time, and type of the last backup version.

Properties - Version

This page displays information about available backup versions.

Select for restore

You can select or deselect the file or directory for restore.

Backup version

Select a backup version of the file or directory. By default, the most recent backup version is selected for restore.

Last backup version

The date, time, and type of the last backup version.

Selected version information

The information about the currently selected backup version is displayed if available.

Recovery Information Restore

In the Results Area, the restore session object, device, and messages are displayed. At the end of the session, a dialog box appears indicating the session status.

For the object in the restore session, all relevant information is displayed, such as the status of the object, its type, and so on.

For the device that is being used in the restore session, all relevant information is displayed, such as the status of the device, the name of the device, and so on.

Session messages are displayed at the bottom. Each session message has a severity level indicator (such as Normal, Warning, and so on).

The following may be helpful:

- To confirm a mount request or cancel the device, right-click the device and click the appropriate item.
- If a message has a link (blue message number), you can click it to see a detailed description of the error, as well as a list of possible actions.
- For more message options (save, find, and so on), right-click in the message area.

Save SRD Information

In this page you select the location where you want to store the updated SRD file.

Enter the path in the text box, or click Browse to search for the directory, CD-ROM, or floppy disk.

Store the SRD file in a safe place, secure and accessible in case of a disaster. Do not store the Cell Manager SRD file on the Cell Manager.

Select Recovery Set

Select the location for the DR image (recovery set) Data Protector will compile the DR image with the DR installation, SRD file and P1S file into an DR OS image.

Select the source location

Restore recovery set file from a backup

If you did not save the full DR image (recovery set) to disk during a full client backup, you have to restore it from the backup.

Path to the recovery set file

If you saved the full DR image (recovery set) to disk during a full client backup, enter its location or browse the file (recovery.img).

Select Backup Session

Select the full client backup session and for a Cell Manager the IDB backup session you want to use for a recovery.

Select backup session

Host backup session

Select a file system backup session to use for a disaster recovery. Only sessions that contain all critical volumes are listed.

IDB backup session

(available for Cell Managers)

Select an IDB backup session to use for a disaster recovery. If the IDB session is older that the host backup session, a warning is displayed.

Use raw image objects

(available if the session contains raw image objects)

Select this option to use raw image backups if both types of a backup are available for an object. If not selected, file system backups will be used by default.

List of volumes in a session

Lists all volumes that were backed up in the selected session and displays information about the type and label of the volume.

Disaster Recovery

In this page you select the client or Cell Manager system that you want to recover, the system on which you want to create the DR OS image and the disaster recovery method.

Select recovery and media creation host

Host to be recovered

The client or Cell Manager system that you want to recover. You can select a client or Cell Manager of the Data Protector cell from the drop-down list, or you can choose an arbitrary system (non-Data Protector cell client) by entering its fully-qualified domain name (FQDN) and clicking Validate to validate and add the system to the selection list.

Validate

Click to validate the host to be recovered and add it to the selection list.

Recovery media creation host

The system on which the recovery media (DR OS image) will be created. By default, this is the same client for which the DR OS image is prepared for. Make sure that the client on which you prepare the DR OS image has the:

- same OS type (Windows, Linux)
- Automatic Disaster Recovery and Disk Agent components installed
- appropriate version of the Windows Automated Installation Kit or Assessment and Deployment Kit.

Disaster recovery method

Enhanced Automated Disaster Recovery (available if the Data Protector Automatic Disaster Recovery component is installed)

You can use this method to recover your Windows or Linux systems. For a list of supported platforms for EADR, see the latest support matrices.

SRD file update

You can use this option to update the System Recovery Data (SRD) file, which contains critical information for your Cell Manager or client recovery.

Create Automated System Recovery Set

(available if the Data Protector Automatic Disaster Recovery component is installed)

You can use this option to prepare and update the ASR set. For a list of supported platforms, see the latest support matrices.

Build volume recovery set from

Backup session

Select recovery volumes object versions by a specific backup session. This method is recommended and elected by default.

Volume list

Select recovery volumes object versions for each host volume individually. This method is available for compatibility with previous releases of Data Protector. To use this method, all client volumes must be backed up.

Volume Selection

Data Protector scans the system that you have selected and determines what is needed for your disaster recovery disks.

You are prompted to select the objects and versions needed to restore the logical volumes (partitions) and the system's Configuration. On each Volume selection page, select the appropriate object and version.

To select another backup version, right-click an object and click **Properties**.

Application List - Microsoft Exchange Server Integration

Each client can be part of only one Microsoft Exchange Server environment.

Bar Name

Displays the name of the Microsoft Exchange Server environment.

Database Options - Microsoft Exchange Server Integration

In this page, specify the advanced restore options for the selected mailbox database.

Select for restore

Specify whether the database should be restored.

Restore method

In the drop-down list, select one of the following restore methods:

Repair all passive copies with failed status

This option is available for databases that are part of a DAG. It is useful if some of a database's passive copies become corrupt, acquiring the status Failed or FailedAndSuspended. This option automatically restores all the corrupt passive copies from the backup created in the last backup session (and the corresponding restore chain). After the data is restored, the copies are synchronized with the active copy, provided that the Resume database replication option is selected.

Restore to the latest state

This option is used to restore a corrupt database to the latest possible point in time. Data Protector restores the database from the backup created in the last backup session (and the corresponding restore chain).

Once the files are restored, all the logs (not only those restored from the backup, but also existing logs) are replayed to the database file.

DAG environment only: When a passive copy is restored, Microsoft Exchange Server ensures that the logs are replayed to the database file in accordance with the ReplayLagTime parameter setting.

Restore to a point in time

This option is used to restore a database to a specific point in time.

- Standard restore: Note that before the files are restored, the existing .log and .chk files are renamed (a .keep extension is added to their names). In a DAG environment, this only applies when you restore an active copy.
- DAG environment only:
  - When a passive copy is restored, the Microsoft Exchange Server ensures that the logs are replayed to the database file in accordance with the ReplayLagTime parameter setting.
  - For passive copies that are not restored, a full reseed is required once the restore session completes.

Restore to a new mailbox database

This option is used to restore data to a different database, either because the original database no longer exists or in order to move the data elsewhere.

Using it, you can also restore data to a Microsoft Exchange Server recovery database.

- Backups can be restored into *recovery database*.
- Data Protector creates *recovery database* automatically with name provided in the field “Database name” at the specified target physical location mentioned in the field “Restore into location”.
- Restore the selected backup session data into the created *recovery database.*
- *Recovery database* has restricted access and functionalities as compared to mailbox database, hence *recovery database* can be used as temporary database.

Instant recovery: This option is not available for replica types whose data can only be restored to the original storage volumes.

Restore to a temporary location

Using this option, you can restore database files to a location of your choice.

- When you restore from a differential or incremental backup session, you can either restore the complete restore chain or only files (.log) backed up in the selected session.
- When you restore data from a full backup session, you have an option to restore only the database file (.edb).

Instant recovery: This option is not available for replica types whose data can only be restored to the original storage volumes.

Backup version

(available for standard restore)

Specify from which backup data to restore. Select a backup session.

Last backup version

(available for standard restore)

This option shows the session in which the database was last backed up.

Restore additional logs until

(available for instant recovery, not available for the methods: Repair all passive copies with failed status and Restore to the latest state)

If a Differential backup session is selected, .log files backed up in the selected Differential backup session are restored.

If an Incremental backup session is selected, .log files backed up in all subsequent Incremental backup sessions, up to the selected Incremental backup session, are restored.

Restore chain

(available for the method Restore files to a temporary location)

If the Restore only this backup option is selected, only files backed up in the selected session are restored.

If the Full restore (full, incr, diff backups) option is selected, the complete chain is restored.

Target client

(available for the methods: Restore to a new mailbox database, Restore files to a temporary location)

Specify to which client to restore.

Restore into location

(available for the methods: Restore to a new mailbox database, Restore files to a temporary location)

Specify to which directory to restore.

Database name

(available for the methods: Restore to a new mailbox database, Restore files to a temporary location)

Specify which name to use for the new database. If another recovery database with the same name already exists, the files are not restored.

Perform database recovery

(not available when restoring a passive copy, not available for the method Repair all passive nodes with failed status)

Select this option to apply the logs to the database file after the restore completes.

Restore into Recovery database

(available for the method Restore to a new mailbox database)

Select this option to restore the data into a newly created Microsoft Exchange Server recovery database.

Restore database files only

(available for the method Restore files to a temporary location)

Select this option to restore the database file (.edb). Logs (.log) and checkpoint files (.chk) are not restored.

Mount database

(available when the Perform database recovery option is selected, not available for the methods: Repair all passive nodes with failed status, Restore to a temporary location)

Select this option to mount the database after the database recovery completes.

Resume database replication

(available in DAG environments, not available for the methods: Restore to a temporary location, Restore to a new mailbox database)

Select this option to resume the replication between the active and passive copies after the restore completes.

Target nodes

(available in DAG environments, not available for the methods: Repair all passive copies with failed status, Restore to a new mailbox database, Restore files to a temporary location)

Specify which clients (that is, database copies) to restore.

If the Restore to a point in time restore method is selected, the node (client) hosting the active copy is selected by default.

Restore Options - Microsoft Exchange Server Integration

In this page, specify the options for the Microsoft Exchange Server restore.

Startup client

Specify the client on which the integration agent (e2010_bar.exe) should be started. If the DAG virtual client (host) is selected, the integration agent is started on the currently active node. To find out which Microsoft Exchange Server node is currently active, connect to one of the nodes and run: cluster group.

Default: The same client that was specified for the backup session. If the DAG virtual client was specified, this client is now selected. However, note that the integration agent may not be started on the same physical node as during the backup session; it depends which node is currently active.

User and group/domain

User name

Group/domain name

Specify which Windows domain user account to use for the restore session. Ensure that the specified user has the appropriate Microsoft Exchange Server permissions to back up and restore databases.

If these options are not specified, the restore session is started under the user account under which the Data Protector Inet service is running.

Consistency check

Perform consistency check

If this option is selected, Microsoft Exchange Server checks the consistency of a database's backup data.

If this option is not selected, the session finishes earlier, but the backup data consistency is not guaranteed.

During a backup session, the check is performed on the backup media, or on the replica storage volumes during a ZDB backup session, after the backup data is created. If the data is found corrupt, it is discarded and the database backup fails.

During a restore session, the check is performed at the target location, or on the source storage volumes during a ZDB restore session, after the backup data is restored. You do not need to perform the consistency check if it was already performed at the time of backup.

Default: selected (in backup sessions), not selected (in restore sessions)

Check log files only

(available if the Perform consistency check is selected)

Checks only the log file backup data.

Default: selected.

Throttle check for 1 second every I/O operations

(available if the Perform consistency check is selected)

By default, the consistency check is I/O intensive, which can negatively affect disk performance. This option throttles down the consistency check to lessen impact on the disk performance. Specify after how many input or output operations the check should stop for one second.

Default: 400

Restore Source - Microsoft Exchange Server Integration

This page displays all Microsoft Exchange Server 2010 databases backed up from the selected DAG or standalone environment. Select which Microsoft Exchange Server databases to restore. When you select a database, the Properties for Database dialog box is displayed.

To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

To change a restore method for a database, right-click the database and click **Properties**.

For databases that are part of a DAG, the default restore method is **Repair all** passive copies with failed status. For standalone databases, the default is Restore to the latest state.

To view object properties, right-click an object and select **Properties**.

Select New Device

In this page you select a new device to be used for the restore.

Original Device

The name of the device that was used for writing the data, and is by default also used for the restore of the data.

New Device

If you want to use a different device for the restore, select the device and click OK. To revert to the original device, select (original device) and click **OK**.

Library

The name of the library in which the device resides.

Device Tag

Devices with the same device tag name can replace each other if needed. Such devices must be of the same media type and from the same library. Otherwise, automatic replacement is not successful.

Device Status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here.

If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility.

Properties for Devices

This window displays the properties of the original device(s), and the new device(s).

Device name

The logical name of the device.

Description

The description of the device.

Cell Manager

The Cell Manager on which the device is configured.

Media type

The media type of the device.

Policy

The policy of the device.

Properties for Medium

This page displays the properties of the medium.

NDMP Restore Options

In this page you can change options for NDMP objects.

NDMP user override

For each object that will be restored, you can specify a user name and password that will override the User name and Password values entered in the Import NDMP Host dialog box during the import of the NDMP Server to the Data Protector cell. Access rights must be set properly on the NetApp host in order to use user name and password overrides.

Advanced

Click here to specify NDMP environment variables for specific NDMP implementations.

Properties - Destination

This page displays information about the restore destination of the file or directory.

Restore

To default destination

The file or directory will be restored to the destination specified under Default destination in the Destination property page. If you leave the default there, the destination is the original directory on the original client system.

As

The path from the backup will be replaced with the new location specified below. The destination path can be a new directory or an existing one. You can rename the files and directories that you want to restore.

Into

The path from the backup will be appended to the new location selected below. The new location has to be an existing directory.

Drive

(available for Windows systems)

The original drive of the file or directory is displayed. To restore to another drive, select the drive from the drop-down list.

To restore to another client system, click **Browse**.

Location

Enter a new path for the file or directory.

Filesystem Restore Copies

In this page, the object versions that will be restored are displayed.

Selected Version

The object version that is selected for restore.

Auto select copy

If an object version exists on more than one media set, Data Protector selects the media set automatically by default. You can also select the media set manually.

Properties

If an object version that you want to restore exists on more than one media set, you can manually select the media set that will be used. Select the desired object version and click this button.

Version properties - Copy

If an object version exists on more than one media set, Data Protector selects the media set automatically by default. You can also select the media set manually.

Select source copy manually

Select this option to select the copy of the object version manually, and select a copy from the Source copy created drop-down list.

Needed media

Depending on the selected copy, the needed media are listed.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Filesystem Restore Destination

In this page you select the destination for the restore and specify how file conflicts should be handled.

Default destination

Some of these settings can also be set for each individual file or directory in the Source page. If you change the properties there, they will override the settings made in this page.

For block based restore, **Restore to original location** is selected by default and greyed out.

Target client

By default, you restore to the same client system from which the data was backed up. You can select another system in your cell from the drop-down list. The Disk Agent is started on the selected client system and the data is restored there.

You need to have the Restore to other clients user right to be able to restore to another client system.

Restore to original location

By default, you restore your data to the same directory in which it was located when the backup was performed. It can be on the original client system or on some other client system you have selected.

Restore to new location

This option enables you to restore your data to another directory. Specify the path to the directory to which you want to restore the data. You can browse for it if you are using the GUI on a Windows system. If you restore to a Windows system, you could select a directory on another system, but this is not recommended.

File Conflict Handling

File Conflict Handling is not available for NDMP restore as NDMP can be configured in only two ways; Perform NDMP restore or not. Hence, the Overwrite button is selected but greyed out in the GUI.

For block based restore, the **Keep most recent** option is selected by default. These options are greyed out.

Keep most recent

If this option is selected, the most recent versions of files are kept. If a file on the disk is newer than the backed up version, the file is not restored. If a file on the disk is older than the backed up version, the file is overwritten with the newer version from the backup. By default, this option is enabled.

No overwrite

If this option is selected, files that exist on the disk are preserved. This means that they are not overwritten by other versions of these files from the backup. Only non-existing files are restored from the backup. By default, this option is disabled.

Overwrite

If this option is selected, existing files on the disk are replaced with files from the backup. By default, this option is disabled.

Filesystem Restore Devices

In this page, you select devices for restore.

Automatic device selection

This option is applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup.

By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option AutomaticDeviceSelectionOrder.

For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup.

Default: selected.

Original device selection

This option is applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available.

This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration.

Default: not selected.

Original Device

The names of all configured devices are listed. By default, Data Protector restores selected data with the same devices that were used during backup.

Device Status

The configured devices can be Available, Already in Use, Disabled or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here.

If the Device Status is Disabled and the Original device selection option is set, the recommended replacement device tag is displayed to ensure compatibility.

The following may be helpful:

- To replace the original device with an alternative device, select the device and click **Change**. The new device will be used only for this session.
- For more information on a device, right-click the device and click **Info**.

Properties - General

This page displays general information about the file or directory.

Name

The name of the file or directory.

Pathname

The pathname of the file or directory.

Size

The size of the file.

Created

The date and time when the backup was configured.

Last backup

The date and time when the last backup was performed, and the type of backup.

Properties - Restore Only

In this page you can specify files for restore using wildcard characters. These options are not supported with Data Protector NDMP server integration.

Add

In the text box, enter a part of the name of the file(s) that you want to restore, using wildcard characters. For example, to restore all files that end in .exe, type *.exe and click **Add**.

Remove

To cancel a selection, select it and click **Remove**.

Filesystem Restore Media

In this page, the media needed for the restore are displayed.

If an object version that you want to restore exists on more than one medium, all media are listed, except those obtained using the media copy functionality. By default, Data Protector automatically selects the most appropriate media set.

If you use synthetic backup, there is often more than one restore chain of the same point in time of an object available. In such a case, Data Protector selects the most convenient restore chain by default, and selects the most appropriate media within the selected restore chain.

For more information on a medium, right-click the medium and click **Info**.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location.

By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB.

Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Number of media

The number of media present in a location.

Change priority

To change the media location priority for this session, select a media location and click this button.

Restore Options

In this page you can set restore options.

Restore options

Omit deleted files

For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

If this option is selected, Data Protector recreates the state of the backed up directory tree at the time of the last incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are not restored.

If this option is not selected, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

When using the **Restore As** or **Restore Into** functionality with this option enabled, carefully choose the restore location to prevent accidental removal of existing files.

Default: not selected.

Move busy files

This option is relevant if a file on the disk is being used by an application when a restore wants to replace this file. It only applies to the files that are locked by an operating system when they are used by the application or other process. The option is used with the **Keep most recent** or **Overwrite** options. By default, this option is disabled.

On UNIX systems, Data Protector moves the busy file filename to #filename (adds a hash in front of the filename). The application will keep using the busy file until it closes the file. Subsequently, the restored file is used.

On Windows systems, the file is restored as filename.001. All applications keep using the old file. When the system is rebooted, the old file is replaced with the restored file.

On Linux systems, this option is not supported.

List restored data

When this option is enabled, Data Protector displays the names of the files and directories in the monitor window as the objects are being restored. By default, this option is disabled.

Display statistical information

When this option is enabled, Data Protector reports statistical information (such as size and performance) for each object that is backed up or restored. You can view the information in the monitor window. By default, this option is disabled.

Omit unrequired object versions

This option applies if you select directories for restore and the backup was performed with the logging level Log All or Log Files.

If this option is selected, Data Protector checks in the IDB for each backup in the restore chain if there are any files to restore. Backups with no object versions to restore are skipped. Note that this check may take some time.

If this option is not selected, each backup in the restore chain is read, even if there was no change since the previous backup.

To restore empty directories, clear this option.

Default: selected.

Restore sparse files

(available for UNIX systems)

This option restores sparse files in their original compressed form. This is important because sparse files can consume additional disk space unless they are restored in their original form. By default, this option is disabled.

This option applies to UNIX sparse files only. Windows sparse files are always restored as sparse.

Lock files during restore

This option denies access to files during the restore. By default, this option is disabled.

Restore time attributes

This option preserves the time attribute values of each restored file. When this option is disabled, Data Protector sets the time attributes of the restored objects to the current date and time. By default, this option is enabled.

Restore protection attributes

This option preserves the original protection attributes of each restored file. If this option is disabled, Data Protector applies the protection attributes of the current restore session. By default, this option is enabled.

On Windows systems, this option applies to file attributes only. Security information is always restored, even when this option is disabled.

Restore share information for directories Specifies that share information for directories will be restored. By default, this option is selected.

When restoring a directory that was shared on the network when it was backed up, the directory will also be shared after restore if this option is selected, provided that the backup was made with the Backup share information for directories option selected.

Pre- and Post-exec commands

Pre-exec

This option allows you to enter a command (or script) to be executed before the restore of each object is initiated. This command (or script) must return success for Data Protector to proceed with the restore.

The pre-exec command (or script) is executed on the client system where the Disk Agent is running. On a Windows system, the scripts must be located in the Data_Protector_home\bin directory or its sub-directory. On Unix systems, the scripts must be located in /opt/omni/lbin directory, or its sub-directories.

Note that only .bat, .exe, and .cmd are supported extensions for pre-exec scripts on Windows systems. To run a pre-exec script with an unsupported extension (for example, .vbs), create a batch file (.bat) that starts the script. Then configure Data Protector to run the batch file as a pre-exec command which then starts the script with the unsupported extension.

Post-exec

This option allows you to enter a command (or script) to be executed after the restore of each object is completed. The post-exec command (or script) is executed on the client system where the Disk Agent is running.

On a Windows system, the scripts must be located in the Data_Protector_home\bin directory or its sub-directory. On UNIX systems, the scripts must be located in /opt/omni/lbin directory, or its sub-directories.

Advanced

Click here to set user-definable variables.

Filesystem Restore Summary

This page displays the summary of your restore.

Object Name

The names of the files and directories that you have selected for restore.

Version

The backup versions of the files.

Add

To select a file or directory to restore manually, enter its name and path in the text box and click**Add**.

Remove

To cancel your selection of a file or directory, select it and click**Remove**.

For more information on a file, right-click the file and click **Properties**.

Properties - Skip

In this page you can specify files that you do not want to restore, using wildcard characters. Skipping files for restore is not supported with Data Protector NDMP server integration.

Add

In the text box, enter a part of the name of the file(s) that you want to skip, using wildcard characters. For example, to skip all files that end in .exe, type *.exe and click **Add**.

Remove

To cancel a selection, select it and click **Remove**.

Filesystem Restore Source

This page displays the objects that have been backed up. Select directories or files that you want to restore.

By default, when you select a whole directory, only directories and/or files from the last backup session are selected for restore. Directories and files in the same tree structure that have not been backed up in the same backup session are shaded.

If you want to restore the data from any other backup session, right-click the selected directory and click **Restore Version**.

To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

To view object properties, right-click an object and select **Properties**.

Search interval

(available if an object or client is selected under Restore Objects)

You can set the time interval that will be used when browsing the IDB for object versions for restore. In the drop-down list, select one of the following:

- **Last ... months**: If you want to view object versions from the specified time period.
- **Interval**: If you want to set an absolute search interval. Specify the dates in the From and To fields and click Update.
- **Latest**: If you want to view the last backed up object versions. Select the number of object versions (1, 15, 30, 45, 60, 90) from the Versions drop-down list.
- **None**: If you want all object versions to be listed.

Show full chain

(available if an object is selected under Restore Sessions)

If this option is selected, Data Protector displays all the files and directories in the restore chain. By default, this option is selected and the entire restore chain is restored.

Show this session only

(available if an object is selected under Restore Sessions)

If this option is selected, Data Protector displays only the files and directories backed up in this session. This enables you to restore files and directories from an incremental backup session without restoring the entire restore chain.

Properties - Version

This page displays information about available backup versions of the file or directory.

Select for restore

You can select or deselect the file or directory for restore.

Backup version

Select a backup version of the file or directory. By default, the most recent backup version is restored.

Click "..." for more information on each version.

Last backup version

The date, time, and type of the last backup version.

Selected version information

The information about the currently selected backup version is displayed.

Backed up

The date and time when the file or directory was backed up, and the type of backup.

Modify time

The date and time when the file or directory was last modified before the backup.

Attributes

File permissions for UNIX systems, or file attributes for Windows.

User

(available for UNIX systems)

The user who owns the file or directory.

Group

(available for UNIX systems)

The group that owns the file or directory.

Size

The size of the file or directory when it was backed up.

Version type

One of the following is displayed here: Normal or NDMP.

Start Preview/Restore Session

In this page you can review the selection for the restore session.

Click **Next** if you want to set the network load and report level for the restore session.

Click **Finish** to start the preview or the restore. The Restore Monitor opens, showing the progress of the restore.

Limitations

Preview is not available for the Data Protector Internal Database restore and the restore sessions of Data Protector application integrations.

Client

The name of the client system that will have its data restored.

Name

The name of the object containing the data.

Type

The type of data to be restored.

Needed media

(not available for Data Protector Internal Database, Informix Server, and Oracle Server backup objects)

Click here to display the list of media needed for the restore.

Start Preview/Restore Session

In this page you can set the report level and network load for the restore session.

Report level

This option defines the level of errors that will be reported for an object during a backup or restore session. Report levels are: **Warning**, **Minor**, **Major**, and **Critical**. Errors of the selected level and higher are reported. For example, by setting the level to Minor, only minor, major, and critical errors are reported in the Messages field. By default, the level is set to **Warning**. Messages of **Normal** level are always reported.

The number of messages per backup system stored in the IDB is limited to 3000.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Enable resumable restore

(available for filesystem restore sessions)

If this option is selected, Data Protector creates checkpoint files during the restore session. The checkpoint files are needed if the restore session fails and you want to resume the session using the Data Protector resume session functionality.

Default: selected (you can change the default using the global option ResumableRestoreDefault).

Start Preview/Restore Session

In this page you can set options for the restore session.

Mirror mode

Selects a configuration.

Only the Business Copy configuration is supported.

MU Number(s)

This option defines the mirror unit (MU) number(s) of a replica or a replica set from which the Data Protector Agent, according to the replica set rotation, selects the replica to be used in the restore. The replica selection rule is described in the .

You can specify one or more non-negative integer numbers, one or more ascending ranges of such numbers, or any combination of both. Use a comma as the separator character. Examples:

5

7-9

4,0,2-3

When a sequence is specified, it does not define the order in which the replicas are used.

Default: 0 (nothing is specified).

Application system

Specifies the system to which your data will be restored. In cluster environments, specify the virtual server hostname (rather than the physical node hostname).

Backup system

Specifies the system to which your data will be restored from the backup media on LAN.

Stop/quiesce the application Optionally specifies the command/script to be run before the LDEV pairs are split (put into the SUSPENDED state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for stopping the application, dismounting the file systems that are not to be restored in the active session, but belong to the same volume group or disk, or preparing the volume group for deactivation.

If this command/script fails, the command/script specified with the option Restart the application is not executed. Therefore, you need to implement a cleanup procedure in this command/script. Note that if the omnirc option ZDB_ALWAYS_POST_SCRIPT is set to 1, the command/script specified with the option Restart the application is always executed. For details, see the .

Restart the application

Specifies the command/script to be run immediately after the LDEV pairs are resynchronized (put into the PAIR state). The command/script must reside on the application system in the default Data Protector administrative commands directory. It can be used, for example, for restarting the application or mounting the filesystems.

Resynchronize links before restore

Directs the Data Protector disk array agent to synchronize the LDEV pairs, that is, to copy the application data to the disks which store backup data. This is necessary to prepare the disks for restore and to enable consistent data restore. If the paired LDEVs have been split (put into the SUSPENDED state) before the restore, and only some files need to be restored, then this option updates the backup system. This will ensure that the correct data is resynchronized to the application system. If this

option is not selected, the synchronization is not performed.

Default: not selected.

Disable disks on the application system before split

Directs the Data Protector disk array agent to disable disks on the application system, that is, dismount the filesystems and deactivate the volume groups. This is performed before the LDEV pairs are split. The disks are enabled after the links are restored. Note that only filesystems selected for restore are dismounted. If other filesystems exist in the volume group or on the disk, appropriate commands/scripts must be used to dismount these filesystems (specified with the options Stop/quiesce the application and Restart the application). You must always select this option for restore when you want to copy data from the backup system to the application system, that is, to incrementally restore links. The application system disks have to be disabled to provide data integrity after the links are restored, that is, data is copied.

Default: selected.

Restore links after restore

Directs the Data Protector disk array agent to incrementally restore the links for the LDEVs that Data Protector has successfully restored to the backup system. The Agent also incrementally re-establishes links for the LDEVs for which the Data Protector restore failed.

Default: selected.

Cell Manager Selection - Internal Database Restore

In the Results Area, a list of Data Protector Cell Managers with their Internal Database backed up is displayed.

Client

The name of the Cell Manager system from where the Internal Database was backed up.

Configuration Files Property Page - Internal Database Restore

In this page, you can choose to restore the Cell Manager configuration files and define to which state you want to restore them. You can also narrow the restore scope and select additional restore options.

Restore configuration files

If selected, this option instructs Data Protector to restore the Cell Manager configuration data.

Use backup version applicable for selected database restore If this option is selected, Data Protector automatically selects and processes the restore chain that suits your restore chain selection for the basic IDB parts (CDB, MMDB, SMBF).

Default: selected.

Select version manually

Select this option and browse for an IDB backup session to restore the Cell Manager configuration files to the state that was backed up in the selected session.

Default: not selected.

In the object tree, you can narrow the scope of the Cell Manager configuration data restore to the selected files or folders only.

Restore to original location

If this option is selected, the original Cell Manager configuration data location is used for the restore session.

Default: selected.

Restore to other location

If this option is selected, it specifies the target directory on the Cell Manager where the Cell Manager configuration data should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space.

Default: not selected.

File conflict handling

This option defines the Data Protector behavior when the files corresponding to the Cell Manager configuration data included in the IDB backup image already exist on the Cell Manager system.

If you select Keep most recent, Data Protector keeps the most recent version of each Cell Manager configuration file: the existing version on the Cell Manager system (when newer from the version in the backup image) or the backed up version (when newer from the version that already exists on the Cell Manager system).

If you select No overwrite, Data Protector preserves each existing Cell Manager configuration file even when its counterpart is present in the IDB backup image. You can use this selection in the event that only a few configuration files are missing on the Cell Manager.

If you select Overwrite, Data Protector unconditionally overwrites each existing Cell Manager configuration file with its counterpart from the IDB backup image.

Default: Keep most recent.

Devices Property Page - Internal Database Restore

In this page, you select devices for restore.

Automatic device selection (Recommended)

This option is applicable when the original devices are not available for a restore or an object copy. Select this option to enable Data Protector to automatically replace unavailable devices with other devices that are selected for the restore or object copy and have the same device tag as the original device. If there are not enough available devices to replace the original devices, the restore or object copy is started with fewer devices than were used during backup.

By default, Data Protector attempts to use the original device first. If the original device is not selected for a restore or an object copy, then a global option is considered. To use alternative devices first or to prevent the use of the original device all together, modify the global option AutomaticDeviceSelectionOrder.

For the Data Protector SAP MaxDB, DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration, ensure that the number of available devices is equal to or greater than the number of devices that were used during backup.

Default: selected.

Original device selection

This option is applicable when the original devices are not available for a restore or an object copy at the moment. Select this option to instruct Data Protector to wait for the selected devices to become available.

This is the preferred option for the Data Protector SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server, and Microsoft SharePoint Server 2010/2013 integration.

Default: not selected.

Original Device

The names of all configured devices are listed. By default, Data Protector restores selected data with the same devices that were used during backup.

Device Status The configured devices can be Available, Already in Use, Disabled, or Undefined. The Undefined status means that the original device no longer exists. If you have changed the original device, the new device is listed here.

If the Device Status is Disabled, and the Original device selection option is selected, the recommended replacement device tag is displayed to ensure compatibility.

The following may be helpful:

To replace the original device with an alternative device, select the device and click **Change**. The new device will be used only for this session. To save all the selections made in this window as the defaults for the specified backup object, click **Save** device mapping. For more information on a device, right-click the device and click **Info**.

Internal Database Property Page - Internal Database Restore

In this page, you can choose which part of the Internal Database to restore, to which state you want to restore the data, and select additional restore options.

Restore Internal Database

If selected, this option instructs Data Protector to restore the basic IDB parts: the Catalog Database (CDB), the Media Management Database (MMDB), and the Session Messages Binary Files (SMBF).

If you leave the default values for specific options below, after a successful restore Data Protector starts the Internal Database Service, performs recovery of the basic IDB parts using both the backed up and the not yet backed up IDB archived log files, and finally starts using the recovered IDB as the new Internal Database of the cell.

However, if the restored database is not used as a new Internal Database (-nouseasnewidb option), then along with restore of Internal Database files (files in PG,IDB and JCE folder), all backed up Session Messages Binary files (SMBF) and all backed up Data Protector IDB specific files (DPSPEC) will be restored to the temporary location (the specified Restore location).

DPSPEC files are all Data Protector Internal Database specific files and these are not Postgres related files, DCBFs, SMBFs and Configuration files. These are usually: Auditing files, Data Protector logs, keystore, log files, meta, reportdb, smisdb, sqldb, sysdb, vssdb, and xpdb files.

If needed, this restored database can be used as an Internal Database. However, before switching over to the new Internal Database, all SMBF and DPSPEC files should be copied from the temporary location to the original location. This is required for the Cell manager functionality.

Default: selected.

Restore port

Specifies the number of the port that is temporarily used for the Internal Database Service during the restore process. After the process completes, this service is restarted on the original port defined during Data Protector Cell Manager installation.

Do not reuse the original Internal Database Service port as the temporary port. It is recommended to use the default option value.

Default: 7114.

Restore location

Specifies the target directory on the Cell Manager where the basic IDB parts (CDB, MMDB, SMBF) should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space. Note that the directory path length should not exceed 80 characters.

Do not reuse the original IDB directory as the restore location.

Default: no value.

Start the database server (recovery will be performed)

If selected, this option instructs Data Protector to start the Internal Database Service after a successful restore. In this case, recovery of the basic IDB parts (CDB, MMDB, SMBF) is performed using both the backed up and the not yet backed up IDB archived log files.

Default: selected.

Use the restored database as a new Internal Database

If selected, this option instructs Data Protector to use the recovered IDB as the new Internal Database of the cell.

Default: selected.

Restore catalog binary files

If selected, this option instructs Data Protector to restore the Detail Catalog Binary Files (DCBF) part of the IDB. A prerequisite for this operation is a successful restore of the basic Internal Database part in the same session (if the latter is also selected for restore).

Default: selected.

Restore to original location

If this option is selected, the DCBF part of the IDB is restored to its original location.

Default: not selected.

Restore to other location

If this option is selected, it specifies the target directory on the Cell Manager where the DCBF part of the IDB should be restored to. Before invoking the restore, make sure this directory is empty and provides enough free storage space.

Default: selected, no value.

Restore until

This options defines the restore chain of backup images that should be considered for the Internal Database restore.

If you select **Selected time**, a point-in-time restore is performed, returning the IDB to the state it was in at the specified date and time.

If you select **Now**, the restore process creates a copy of the IDB in the latest backed up state. Additionally, in this case, the not yet backed up IDB archived log files are copied from the original IDB location to the target restore location.

Default: Now.

Restore Objects - Internal Database Restore

In the Results Area, the only item can be selected.

Bar Name

The predefined string Internal Database which represents the Data Protector IDB backup object.

Media Property Page - Internal Database Restore

In this page, the media needed for the restore are displayed.

If an object version that you want to restore exists on more than one medium, all media are listed, except those obtained using the media copy functionality.

For more information on a medium, right-click the medium and click Info.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Location priority

The order in which media are selected for restore, object copying, object consolidation, or object verification when copies of the same object version exist in more than one location.

By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

Location

Media location information helps you find the medium. You should enter the location when you initialize media, and update it whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB.

Data Protector allows you to create a list of predefined locations to simplify vaulting and archiving.

Number of media

The number of media present in a location.

Change priority

To change the media location priority for this session, select a media location and click this button.

Options Property Page - Internal Database Restore

In this page, you can select additional Internal Database restore options.

Pre-exec and post-exec commands

Pre-exec

This option defines the Data Protector behavior when the files corresponding to the Cell Manager configuration data included in the IDB backup image already exist on the Cell Manager system.

If you select Keep most recent, Data Protector keeps the most recent version of each Cell Manager configuration file: the existing version on the Cell Manager system (when newer from the version in the backup image) or the backed up version (when newer from the version that already exists on the Cell Manager system).

If you select No overwrite, Data Protector preserves each existing Cell Manager configuration file even when its counterpart is present in the IDB backup image. You can use this selection in the event that only a few configuration files are missing on the Cell Manager.

If you select Overwrite, Data Protector unconditionally overwrites each existing Cell Manager configuration file with its counterpart from the IDB backup image.

Default: Keep most recent.

Post-exec

This option allows you to enter a command (or script) to be executed after the restore of each object is completed. The post-exec command (or script) is executed on the client system where the Disk Agent is running.

On a Windows system, the scripts must be located in the Data_Protector_home\bin directory or its sub-directory. On Unix systems, the scripts must be located in /opt/omni/lbin directory, or its sub-directories.

Note that only .bat, .exe, and .cmd are supported extensions for post-exec scripts on Windows systems. To run a script with an unsupported extension (for example, .vbs), create a batch file (.bat) that starts the script. Then configure Data Protector to run the batch file as a post-exec command, which then starts the script with the unsupported extension.

Applications

In the Results Area, a list of client systems with their application data backed up is displayed.

Client

The name of the client system with application data backed up.

DB2 Application Objects

In the Results area, a list of DB2 objects that have been backed up is displayed.

DB2 Instance Name

The name of the instance from which you restore the object.

Microsoft Exchange Application Restore

In the Results Area, a list of Microsoft Exchange Servers that have backups on the selected client system is displayed.

Bar Name

The name of the Microsoft Exchange Server used by Data Protector.

Bar Application

The name of the Microsoft Exchange Server.

Informix Server Application Restore

In the Results Area, a list of Informix database servers that have backups on the selected client system is displayed.

Informix Server Name

The name of the Informix database server.

Lotus Notes/Domino Server Application Restore

In the Results Area, a list of Lotus Notes/Domino Servers that have backups on the selected client system is displayed.

Lotus Server

The name of the Lotus Notes/Domino Server.

MS Exchange Single Mailbox Restore

In the Results Area, a list of Microsoft Exchange Mailboxes that have backups on the selected client system is displayed.

Bar Name

The name of the Microsoft Exchange Mailboxes used by Data Protector.

Recovery Catalog Settings - Login Information

Enter the Recovery Catalog Database login strings. Under normal circumstances the Recovery Catalog Database login strings appear by default in this dialog. In a disaster recovery situation it may be necessary to alter or re-enter these strings.

User name

Type the user name of the user who has permission to log in to the Recovery Catalog Database (usually a member of the DBA group).

Password

Type the password of the user who has permission to log in to the Recovery Catalog Database.

Service

Specify the net service name for the recovery catalog.

Target Client Settings - Login Information

Enter the login information for the database you are restoring.

User name

Enter the user name for the database you want to restore.

Password

Enter the password for the user.

Service

Specify the net service name for the target database (in case of restore and recovery) or auxiliary database (in case of duplication).

Oracle Application Restore

In the Results Area, a list of Oracle database instances that have been backed up on the specified client system is displayed.

SAP Application Objects

In the Results Area, a list of SAP objects that have been backed up is displayed.

Object

The name of the object that has been backed up. An object is <ORACLE_SID> of the database that is available for restore.

Label

For SAP R/3 objects, the label is always SAP.

Type

The type of data backed up (such as a UNIX or Windows filesystem).

Application Objects - SAP MaxDB Integration

In the Results Area, a list of the SAP MaxDB objects that have been backed up is displayed.

SAP MaxDB Instance

The name of the object that has been backed up. An object is a backed up SAP MaxDB instance.

Microsoft SQL Application Restore

In the Results Area, a list of Microsoft SQL Servers that have backups on the selected client system is displayed.

Bar Name

The name of the Microsoft SQL Server used by Data Protector.

Bar Application

The name of the Microsoft SQL Server.

MS VSS Writers Restore

In the Results Area, a list of Microsoft Volume Shadow Copy writers that have backups on the selected client system is displayed.

VSS Writers

The name of the MS Volume Shadow Copy Writer used by Data Protector.

If the name of the writer is expanded, its components are shown (if the restore mode is set to Restore components) or a list of all files backed up with this writer (if the restore mode is set to Restore files).

Disk Images

In the Results Area, disk images that have been backed up are displayed.

Type

The type of data backed up is disk image.

Label

The label helps you identify the disk image backup that you want to restore.

Disk Image

In the Results Area, a list of client systems with disk image backups is displayed.

Client

The name of the client system with a disk image backup.

Filesystem Objects

In the Results Area, a list of objects that have been backed up is displayed.

Object

An object is either a UNIX mountpoint or a Windows drive.

Label

The label helps you identify the backup that you want to restore.

Type

The type of data backed up (such as a UNIX or Windows filesystem).

Filesystem

In the Results Area, a list of client systems with data backed up is displayed.

Client

The name of the client system with data backed up.

To display the properties of the objects backed up on a client system, right-click the client system and click **Properties**.

Restore View

In the Scoping Pane, you can choose to restore according to objects or sessions. Click the Tasks navigation tab to perform certain predefined restore tasks.

Restore Objects

If this item is selected in the Scoping Pane, the types of data backed up (for example, Filesystem, Block based Filesystem, Internal Database, and so on) are listed in the Results Area.

Restore Sessions

If this item is selected in the Scoping Pane, filesystem sessions and their attributes are displayed in the Results Area.

To use the filters available for the displayed list, click on Show filter settings and modify the parameters.

The following may provide additional information:

- You cannot perform a restore of the Data Protector Internal Database or application integrations data from a specific backup session.
- Object copy sessions are not listed under Restore Sessions.

Restore Tasks

In the Results Area, restore tasks are listed. Double-click the desired restore task. The wizard will guide you through the necessary steps to perform the task. Click the Objects navigation tab if you want to perform a restore according to object types (such as filesystem, Microsoft Exchange Server, and so forth).

Lotus Notes/Domino Server Restore Destination

In this page, specify the destination for the restore of Lotus Notes/Domino Server objects.

Restore to client

By default, Lotus Notes/Domino Server databases are restored to the same client from which they were backed up. To restore to another client, select the new client from the drop-down list or type its name in the text box. The client must be part of the Data Protector cell and have the Lotus Notes/Domino Server integration installed.

Restore to instance

By default, Lotus Notes/Domino Server databases are restored to the same Lotus Notes/Domino Server instance from which they were backed up. To restore to another instance, select the new instance from the drop-down list or type its name in the text box. The instance must be configured for use with this integration.

Restore to the original location

By default, databases are restored to the same directory from which they were backed up (either on the original system or on some other system you selected).

Restore to a new location

This option enables you to restore your data to another directory.

For example, you can restore to the Lotus Notes/Domino Server data directory or to other location:

- To restore to the restore location: C:\Lotus\Domino\Data\Restore , type **Restore**. Database filenames will be the same as they were at the time of backup.
- To restore to other directory, type the relative path of the data directory of the current target instance.

Properties - Advanced

Specify the desired advanced options for the Microsoft Exchange Single Mailbox restore.

Restore chain

Restore only this backup Select this option to restore data only from the selected backup session.

Full restore of mailbox

Select this option to restore data, not only from the selected backup session, but also from:

- The latest full backup
- The latest incremental1 backup (if it exists)
- Any incremental backups from the last incremental1 up to the selected backup version

Note that any folder that was backed up in any of these sessions is displayed and can be selected for restore.

By default, this option is selected.

Destination

Restore to original folder

If this option is selected, Data Protector restores Exchange items to the folders from which they were backed up.

If Keep latest message is selected, existing messages in the destination mailbox or Public Folders are not restored, even if they differ from their backed up versions.

If Keep latest message is not selected, all messages are restored, replacing their current versions (if they exist). If different versions of the same message exist in the mailbox or Public Folders (for example, if you have a copy of the message), only one is replaced with the backed up version and all other versions remain intact.

The messages in the mailbox that were not backed up in the specified backup session (or the restore chain of backup sessions) always remain intact.

By default, this option is not selected.

Restore to new folder

If this option is selected, Data Protector creates a new folder in the root of the mailbox or in the root of All Public Folders and restores Exchange items into it.

For a mailbox restore, the folder is named Data Protector BackupDate BackupTime (for example, Data Protector 2012-05-27 15:30:04) and for a Public Folders restore, it is named Data Protector BackupDate BackupTime - public folder.

If you restore a mailbox or Public Folders from the same backup several times, a number is appended to the folder name. For example, in the second restore session of a mailbox, the folder Data Protectorbackup_datebackup_time (1) is created.

By default, this option is selected.

Restore into mailbox

By default, Exchange items are restored to the original mailbox or Public Folders. Select this option to specify a different destination mailbox. However, ensure that the destination mailbox exists on the Exchange Server.

Note that you can restore Exchange items from different mailboxes to the same mailbox. For privacy protection, you cannot restore Exchange items from mailboxes to Public Folders.

Properties - Version

This page displays information about the available backup versions.

Select for restore

If you select a backup session from the Backup version drop-down list, the Select for restore option is automatically selected. To set the last backup session again, clear the Select for restore option.

Backup version

Select the backup session to restore from. By default, the last backup session is used.

Last backup version

The date, time, and type of the last backup version are displayed.

MS Exchange Single Mailbox Restore Options

In this page, specify the restore options for the Microsoft Exchange Single Mailbox restore.

Restore to another host

By default, Exchange items are restored to the original Microsoft Exchange Server system. If you select this option, you can specify a different destination Microsoft Exchange Server system. However, ensure that the destination Microsoft Exchange Server system:

- Is part of the Data Protector cell.
- Has the MS Exchange Integration software component installed.
- Is configured for use with Data Protector.

MS Exchange Single Mailbox Restore Source

In this page, browse for and select the Exchange items you want to restore. Note that you can select individual folders from different mailboxes and Public Folders.

To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

To specify advanced restore options and the backup session to restore from, right-click the mailbox and select **Properties**.

Options Property Page - MySQL Restore

Select MySQL restore options. Most of the options are available only when databases, database tables, or both are selected for restore on the Source property page.

Restore to client

This option specifies the Data Protector client to restore data to. You can specify any client that hosts MySQL database management system and has the Data Protector MySQL Integration component installed. On this client, the Data Protector MySQL integration agent is started at the beginning of the restore session.

Default: Fully qualified domain name of the source client.

Restore as instance

This option specifies the name of the MySQL instance to restore data to. If the target instance does not exist, Data Protector automatically creates it and starts its services at the end of the restore session. If the target instance exists but is currently offline (with the in-place or copy-back method), Data Protector automatically configures it and starts its services at the end of the restore session.

Default: Name of the source instance.

Username

This option specifies the username of the operating system user account to use for the restore session. The chosen account must be granted appropriate privileges to access MySQL data (the SUPER privilege at least) and have a corresponding Data Protector user configured and assigned proper user rights for the restore scenario (Start restore, Restore from other users, Restore to other clients, and so on). If no value is specified, username of the Data Protector Inet account on the target client is used.

Default: Username of the user account that launched the local instance of the Data Protector GUI.

Group/domain

This option specifies the user group or domain of the operating system user account to use for the restore session. If no value is specified, user group or domain of the Data Protector Inet account on the target client is used.

Default: Group or domain of the user account that locally launched the Data Protector GUI.

Restore method

- Staged restore (available for restore of databases and/or database tables)
- Use custom stage directory (available if Staged restore is selected)
- Copy staged data to target directory (available if Staged restore is selected)
- Import tables to target instance (online restore) (available if Staged restore is selected)
- Staging only (available if Staged restore is selected)

In-place restore (available for restore of databases and/or database tables)

Restore redirection

- Use non-original target directory

Database recovery

- Perform recovery using binary log (available for restore of databases and/or database tables)

Roll forward until latest available state

(available if Perform recovery using binary log is selected)

If this options is selected,Data Protector applies transactions from the binary log and performs recovery by bringing the restored MySQL entity to the latest available state. The recovery includes only the selected instance, database, or database table.

Default: Selected.

Roll forward until

(available if Perform recovery using binary log is selected)

If this option is selected, Data Protector performs recovery by applying only those transactions from the binary log that bring the restored MySQL entity to the state as it was at the selected point in time. The date and time are interpreted as local date and time on the source client. The recovery includes only the selected instance, database, or table.

Default: Not selected.

Source Propery Page - MySQL Restore

You can select the MySQL components for restore, and define the restore chain (for restore of databases, database tables, or both) or select the names of binary log files you want to recover (for restore of the binary log).

Restore component

This option specifies what Data Protector should do in the restore session:

- Restore MySQL databases, database tables, or both using the MySQL integration agent.
  With the database recovery and the Perform recovery using binary log option selected, also the binary log is restored using the Disk Agent.
- Restore one or more MySQL binary log files using the Disk Agent.

Default: Databases and/or tables.

Backup version

(available for restore of databases and database tables)

This option tells Data Protector where to stop processing the restore chain. Data Protector considers the restore chain from its beginning up to and including the MySQL backup session with the selected session ID.

Default: Latest backup version of the latest restore chain.

Search time period

(available for restore of binary log files)

This option filters the list of the binary log files available in the MySQL backup images. You can choose from various predefined time periods, define your own period, or include the entire backup history.

Default: Last month.

Include entire backup image

(available for databases and database tables restore)

This option specifies that all MySQL backup image data backed up in the selected backup version (entire backup image) should be restored.

Restore Options - Destination

In this page you select the destination for the restore and specify how file conflicts should be handled.

Target client

By default, you restore to the same client system from which the data was backed up. You can select another system in your cell from the drop-down list. The Disk Agent is started on the selected client system and the data is restored there.

You need to have the **Restore to other clients** user right to be able to restore to another client system.

File Conflict Handling

Keep most recent

If this option is selected, the most recent versions of files are kept. If a file on the disk is newer than the backed up version, the file is not restored. If a file on the disk is older than the backed up version, the file is overwritten with the newer version from the backup. By default, this option is enabled.

No overwrite

If this option is selected, files that exist on the disk are preserved. This means that they are not overwritten by other versions of these files from the backup. Only non-existing files are restored from the backup. By default, this option is disabled.

Overwrite

If this option is selected, existing files on the disk are replaced with files from the backup. By default, this option is disabled.

Options Property Page - PostgreSQL Restore

Select PostgreSQL restore options.

Restore to client

This option specifies the Data Protector client to restore data to. You can specify any client that hosts PostgreSQL database management system and has the Data Protector PostgreSQL Integration component installed. On this client, the Data Protector PostgreSQL integration agent is started at the beginning of the restore session.

Default: Fully qualified domain name of the source client.

Restore to instance

This option specifies the name of the PostgreSQL instance you want to restore data to. If the instance does not exist yet, Data Protector automatically creates and starts it at the end of the restore session. If the target instance is not started (in-place or copy-back method), Data Protector automatically configures and starts it at the end of the restore.

Default: Name of the source instance.

Username

This option specifies the username of the operating system user account to use for the restore session. The chosen account must be granted appropriate privileges to access PostgreSQL data (at least, SUPER and have a corresponding Data Protector user configured and assigned proper user rights for the restore scenario (Start restore, Restore from other users, Restore to other clients, and so on). If no value is specified, username of the Data Protector Inet account on the target client is used.

Default: Username of the user account that locally launched the Data Protector GUI.

Group/domain

This option specifies the user group or domain of the operating system user account to use for the restore session. If no value is specified, user group or domain of the Data Protector Inet account on the target client is used.

Default: group/domain of the user account that locally launched the Data Protector GUI.

Restore redirection

- Use non-original target directory

Database recovery

Recover to the latest state This option specifies, that Data Protector applies the archived WAL files and brings the restored PostgreSQL instance to the latest available state.

Recover to

This option specifies, that Data Protector applies only those WAL files from the backed up archive log that bring the restored PostgreSQL instance to the state as it was at the selected point in time. The date and time are interpreted as local time on the source client.

Recover from backup version

This option specifies that the restored PostgreSQL instance are recovered from the specified backup version.

Properties - DB2 Options

In this page, you can specify the DB2 integration restore destination.

Restore Into

Restore into new database (available when restoring the whole database)

Select this option to restore the database to a new database. Before starting a restore, define new table space containers for non-system table spaces. For details, see the .

New database name

Type a name for the new database.

Restore options

Online restore

(available when restoring a table space)

Databases are restored offline, table spaces online, regardless of whether this option is selected or not.

Restore As

In this page you can change the restore destination of the file.

Location

The full pathname of the file to be restored is displayed.

Restore As

To restore the file to another location (directory), change the pathname of the file.

To restore the file under another name, change the name of the file.

Restore As

By default, data is restored to its original location. However, you can restore Oracle datafiles to a different location.

Location

The original location of the datafile is displayed, where it is restored by default.

Restore As

To restore the datafile to a different location, change the pathname of the datafile.

To restore the datafile under another name, change the name of the datafile.

Browse Directories

A list of backed up objects of the selected client system is displayed. Select a directory in which you want to search for files.

Note that the search is performed on all backed up objects that include the specified directory path, not just on the selected one.

Restore Properties - Version - SAP MaxDB Integration

This page displays information about available backup versions. Do not select the backup session for the Config item. The same session as selected for the Data item will be used, regardless of what you select for the Config item.

Select for restore

If you select this option and the set backup version is of a Trans or Diff type, the**Full restore of database** and **Restore only this backup** options are enabled. Note that the **Select for restore option** is selected automatically, if you select any backup session from the Backup version drop-down list. If you deselect this option, the last backup session is automatically set to be used for restore and the **Full restore of database** and **Restore only** this backup options are disabled.

Backup version

Select a backup version of the SAP MaxDB instance. By default, the most recent backup version is used for restore.

Last backup version

The date, time, and type of the last backup version.

Full restore of database

(disabled in case you have selected a full backup session from the Backup version drop-down list or if**Select for restore** is not selected)

This option is available if a Trans or a Diff backup session is selected from the Backup version drop-down list.

If you select this option, the integration automatically determines the chain of needed full, differential or transactional backup sessions when performing a restore. After the restore has finished, the database is, if the Recovery option is selected, switched to the Online mode.

Restore only this backup

(disabled in case you have selected a full backup session from the Backup version drop-down list or if**Select for restore** is not selected)

This option is available if a Trans or a Diff backup session is selected from the Backup version drop-down list.

If a database becomes consistent after such a restore and if the **Recovery option** is selected, the database is switched to the Online mode. Otherwise, it is left in the Admin mode.

Restoring only the selected trans or diff backup session is useful if the database remains offline or in the Admin mode after a restore from a full backup session, which is then followed by a restore from a diff or trans backup session.

Application List - Microsoft SharePoint Server Integration

In the Results Area, a list of applications that were backed up through the selected client is displayed. In case of Microsoft SharePoint Server, there is only one application - the Microsoft SharePoint Server farm. Each client can belong to only one Microsoft SharePoint Server farm.

Bar Name

Displays the predefined string MS SharePoint Server.

Bar Application

Displays the Microsoft SharePoint Server configuration database name. Each Microsoft SharePoint Server farm has only one configuration database, so this name is used as a farm identifier.

To display the properties of the object, right-click the object and click **Properties**.

Database Properties - Microsoft SharePoint Server Integration

You can restore a content database to a different Microsoft SQL Server client, to a different Microsoft SQL Server instance, under a different name, or to a different directory.

Database

Specify restore destination options for each database separately. The drop-down list contains databases that were backed up in the selected interval.

Restore destination

Client

Specify the Microsoft SQL Server client to which the database should be restored. The drop-down list contains the clients that have the MS SQL Integration component installed.

Instance

Specify the Microsoft SQL Server instance to which the database should be restored. All created instances on the target client are listed.

Database name

Specify the name under which the database should be restored.

Path

Specify the directory (pathname) to which the database files should be restored.

Force restore over existing database

If a database with the same name as the one you are restoring already exists at the target Microsoft SQL Server instance and has a different internal structure, Microsoft SQL Server does not let you to overwrite the database unless you select this option.

Unlink original content database

(available for content database restore)

If this option is selected, Data Protector removes the original content database from the farm. Available when at least one of the original values for restore redirection has been changed.

Connection

Windows authentication

If this option is selected, Data Protector connects to the database using the Windows domain user account under which the restore session is started.

SQL Server authentication

If this option is selected, Data Protector connects to the database using a Microsoft SQL Server user account.

Login

Password

Specify the Microsoft SQL Server user account.

Index Properties - Microsoft SharePoint Server Integration

You can specify the restore destination for the SSP's index files.

Restore destination

Client

Specify the Microsoft SharePoint Server client to which the index files of the selected SSP should be restored. The drop-down list contains all clients with the Data Protector MS SharePoint Server Integration installed.

Location

Specifies the directory (pathname) to which the SSP index files should be restored.

Restore Options - Microsoft SharePoint Server Integration

In this page, specify the Microsoft SharePoint Server specific restore options.

Restore client

Specify the client on which the Data Protector Microsoft SharePoint Server integration agent should be started. The client also specifies the farm to which the components should be restored. The drop-down list contains all clients with the Data ProtectorMS SharePoint Server Integration component installed.

Application database

Shows the Microsoft SharePoint Server configuration database name of the farm to which the selected client belongs.

Farm administrator user name

Specify the Microsoft SharePoint Server farm administrator (username) under which the Data Protector Microsoft SharePoint Server integration agent should run. Ensure that the administrator has been added to the Data Protector admin or operator user group and has been set up for the Data Protector Inet service user impersonation.

Farm administrator user group

Specify the Microsoft SharePoint Server farm administrator (user group) under which the Data Protector Microsoft SharePoint Server integration agent should run. Ensure that the administrator has been added to the Data Protector admin or operator user group and has been set up for the Data Protector Inet service user impersonation.

Restore Source - Microsoft SharePoint Server Integration

In this page, select which Microsoft SharePoint Server components to restore.

To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

You can view the objects to restore by **Component** or by **Server** in a specified time interval.

To specify restore destination for a Microsoft SharePoint Server object, right-click the object andf click Properties. The restore destination can be specified for each object separately.

The menu is available if **Component** is selected in the **View by** drop-down list. The options in the Properties dialog box are pre-filled with original data (names, locations, URLs).

Overwrite existing

Select this option to restore the components to the original location with the same settings as when they were backed up. If restored components still exist in the farm they will be overwriten. When this option is selected then object-specific restore destination options are not available.

SSP Properties - Microsoft SharePoint Server Integration

You can restore SSP sites under a different name, to a different Web application URL, or to a different My sites web application URL.

SSP

Shows the original Shared Services Provider (Microsoft Office SharePoint Server) name.

Restore destination

SSP name

Specify the name under which Shared Services Provider should be restored.

My sites Web application URL

Specify the URL of the Web application that should host personal sites and profiles.

Connection

Login

Specify the Windows domain user (Domain/Name) under which the timer job and web services should run.

Password

Specify the user's password.

Summary - Microsoft SharePoint Server Integration

In this page, a summary of the selected objects is displayed.

Web Application Properties - Microsoft SharePoint Server Integration

You can restore a Web application's settings under a different name or to a different URL.

Web application

Shows the original Web application name.

Restore destination

Web application name

Specify the name under which the Web application should be restored.

URL

Specify the URL to which the Web application should be restored.

Force restore over existing web application

If a web application residing at the target URL already exists, Data Protector does not overwrite the pre-existing web application unless you select this option.

Application pool account

Username/Password

Specify the Windows domain user account under which the newly created application pool should run.

Properties - Options

Specify the desired restore options for your Microsoft SQL Server database restore.

Force restore over existing database

Select this option if a database with the same name but a different internal structure already exists at the target Microsoft SQL Server instance.

If this option is not selected, the Microsoft SQL Server does not let you overwrite the existing database - the restore will fail.

If you are restoring a data file from the PRIMARY group to an existing database, you must specify the option at a data file level.

When using this option, ensure that the most recent logs are backed up before the restore.

Default: not selected.

Put database in single user mode - log off all users

Disconnects all users that are connected to the target Microsoft SQL Server database and puts the database in the single user mode.

If the database is not in the simple recovery mode, the **Force restore over the existing database** option should also be selected.

Recovery completion state

Specify the state of a database after the recovery.

- **Leave database operational**: No additional transaction logs can be restored. If this option is selected, the database returns to the operational mode. No additional transaction log or differential backups can be restored.
  Select this option when restoring the last in the chain of full, differential and transaction log backups, or when Full restore of database is selected.
- **Leave database nonoperational, but be able to restore additional transaction logs**: If this option is selected, the database is left in the non-operational mode. Additional transaction log or differential backups can be restored.
- **Leave database read-only and able to restore additional transaction logs**: Save to undo file (on SQL server). If this option is selected, the database is left in the standby mode, available for read-only operations. Additional differential or transaction log backups can be restored.

Properties - Version

This page displays information about available backup versions.

Select for restore

You can select or deselect the database for restore. This option is selected by default.

Restore to most recent state possible

(not available for ZDB)

You select the entire backup chain (the most recent full, differential, and transaction log backups) to be used for restore. This option is selected by default.

Backup version

Select a backup version of the database to be restored. By default, the most recent backup version is restored.

Last backup version

The date, time, and type of the last backup version.

Point in time restore

(available if a Trans backup version is selected)

Select this option to restore the database to a particular point in time.

Stop at

Specify the point in time for the rollforward of transactions to be stopped.

Restore only this backup

(available if a Diff or Trans backup version is selected)

Select this option if you have restored a full backup, leaving the database in the non-operational or standby mode, and now you want to restore a chain of particular differential and transaction log backups. After each restore, leave the database in the non-operational or standby mode, except when restoring the last backup.

Full restore of database

(available if a Diff or Trans backup version is selected)

If this option is selected, a chain of needed backup sessions is automatically restored, including the latest full backup, the latest differential backup (if one exists), and all transaction log backups from the last differential up to the selected version.

Properties - Options

In this page you can set SQL tablespace restore options.

Append restored tables

Select this option if the restored data should be appended to the existing table.

Restore table as

A single table can be restored to another one. If the table with the new name already exists, it can be appended or not by checking or clearing the **Append restored tables** option.

Media

This page displays the media needed for the restore. If an object version that you want to restore exists on more than one media set, Data Protector automatically selects the media set that will be used by default. In this case, all the media containing the object are listed. Any of them can be used for the operation.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Start Preview/Restore Session

In the drop-down list, select the object that you want to restore.

Start Preview/Restore Session

Choose whether you want to restore all selected objects in parallel, or a single object.

All selected objects (parallel restore)

Select this option to restore all selected objects concurrently to multiple disks, thus improving the speed of the restore.

I want to select an object (single restore)

Select this option if you want to restore only one of the objects that you have selected.

Start Preview/Restore Session

It is not possible to restore Data Protector objects and integration objects in parallel. Choose which objects you want to restore.

Data Protector objects (filesystem, disk image, database)

Select this option to restore the selected Data Protector objects.

Integrations (Informix Server, and so on)

Select this option to restore the selected integration object.

Restore by Query - Destination

In this page you select the destination for the restore and specify how file conflicts should be handled.

Default destination

The following options apply to all selected files. The restore destination of individual files can be changed in the Source page. If you change the properties there, they will override the settings made in this page.

Restore to original location

Select this option to restore each selected file to its original location. By default, each file is restored to the client system and the directory where it was located at the time of backup.

Restore to new location

Select this option to restore all the selected files to a new location, and specify the target client and location for the restore.

Target client

Specify the client where the data will be restored.

Location

Type the new location, or browse for it.

File Conflict Handling

Keep most recent

If this option is selected, the most recent versions of files are kept. If a file on the disk is newer than the backed up version, the file is not restored. If a file on the disk is older than the backed up version, the file is overwritten with the newer version from the backup. By default, this option is enabled.

No overwrite

If this option is selected, files that exist on the disk are preserved. This means that they are not overwritten by other versions of these files from the backup. Only non-existing files are restored from the backup. By default, this option is disabled.

Overwrite

If this option is selected, existing files on the disk are replaced with files from the backup. By default, this option is disabled.

Restore by Query - Devices

In this page, the devices needed for the restore of the selected files are displayed.

Show devices for

Using the drop-down list, you can display devices for all selected files/directories, or for a specific one.

Original Device

The names of the devices that were used for the backup of your data. By default, the data is restored from these devices.

New Device

If you have changed the original device, the name of the new device to be used for your restore appears here.

Change

After clicking the original device, click here to select a new device for your restore.

The following may provide additional information:

If devices for all selected files/directories are listed and you change a device, the device is changed for all files/directories that use it.

If you select a specific file in the drop-down list and change the device, it will be changed only for this file. In this case, when devices for all files/directories are listed, Multiple choices is displayed under New device.

Restore by Query - Source

This page displays a list of files that match the specified criteria. Select the files that you want to restore. Click **Finish** to start the session with the default options.

You can click other tabs (Destination, Options, ...) and specify options as desired. Click **Next** to specify the report level and network load of the session.

Name

The name of the file.

Located in

The original location of the file.

Client

The client system where the file was originally located.

Size

The size of the file at the time of backup.

Modify time

The time when the file was last modified before it was backed up.

Properties

After selecting a file, you can click here to select another backup version or change the restore destination of the file.

Restore by Query

You can search for files and directories if you know at least a part of the file name. Specify the criteria for the search.

Search for files on

All client systems

If you select this option, Data Protector will search for files on all client systems in the cell.

Specific client system

If you select this option, you specify a client system in the cell on which Data Protector will search for files.

Search for files matching criteria

Named

Enter the file name. If you do not know the exact name, use wildcard characters. For example, if you enter *.exe, Data Protector will search for all files that end in .exe.

When specifying non-ASCII characters, ensure that the current encoding in the Data Protector GUI and the encoding that was used when the file was created match. Otherwise, Data Protector will not find the files.

In the environment with a Linux Cell Manager, the wildcard character ? will not produce the desired results if you want to find a multi-byte character with it. You need to specify multiple wildcard characters ?. For example, if 3 bytes are used to represent the multi-byte character in the current encoding, add ??? to your string.

Look in

You can enter the name of the directory where you want Data Protector to search for the file(s), or you can browse for it.

Case sensitive search

Select this option if you want the search to be case-sensitive.

Restore by Query - Media

In this page, the media needed for the restore are displayed.

Show needed media for

Using the drop-down list, you can display the needed media for all selected files, or for a specific one.

Label

Labels help you identify media. They can have a maximum of 80 characters, including any keyboard character or space.

Location

If the medium is in a library device, the location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in a device.

Medium ID

A unique identifier assigned to a medium by Data Protector.

Restore by Query

You can limit the query based on when the files were backed up, or when they were last modified.

Search within timeframe

Set the time interval when the objects that you want to restore were backed up. Select one of the following:

Last ... months

Object versions from the specified time period will be considered.

Interval

Specify the dates in the From and To fields to set an absolute time interval.

None

All object versions will be searched.

Modification time

Set the time interval when the objects that you want to restore were last modified. Select one of the following:

Do not check the last modification

If you select this option, all files will be considered, regardless of their modification time.

Only restore files modified

If you select this option, only files within the specified time frame will be searched. You can specify the time frame in days or months.

Restore by Query - Options

In this page you can set restore options.

Restore options

Omit deleted files

For this option to function properly, the time on the Cell Manager and the time on the system where data is restored must be synchronized.

If this option is selected, Data Protector recreates the state of the backed up directory tree at the time of the last incremental backup session while preserving files that were created or modified afterwards. Files that were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup are not restored.

If this option is not selected, Data Protector also restores files that were included in the full backup image and were removed between the full backup (the initial session defining the restore chain) and the chosen incremental backup.

When using the **Restore As** or **Restore Into** functionality with this option enabled, carefully choose the restore location to prevent accidental removal of existing files.

Default: not selected.

Move busy files

This option is relevant if a file on the disk is being used by an application when a restore wants to replace this file. It only applies to the files that are locked by an operating system when they are used by the application or other process. The option is used with the **Keep most recent** or **Overwrite** options. By default, this option is disabled.

On UNIX systems, Data Protector moves the busy file filename to #filename (adds a hash in front of the filename). The application will keep using the busy file until it closes the file. Subsequently, the restored file is used.

On Windows systems, the file is restored as filename.001. All applications keep using the old file. When the system is rebooted, the old file is replaced with the restored file.

On Linux systems, this option is not supported.

List restored data

When this option is enabled, Data Protector displays the names of the files and directories in the monitor window as the objects are being restored. By default, this option is disabled.

Display statistical information

When this option is enabled, Data Protector reports statistical information (such as size and performance) for each object that is backed up or restored. You can view the information in the monitor window. By default, this option is disabled.

Omit unrequired object versions

This option applies if you select directories for restore and the backup was performed with the logging level**Log All** or **Log Files**.

If this option is selected, Data Protector checks in the IDB for each backup in the restore chain if there are any files to restore. Backups with no object versions to restore are skipped. Note that this check may take some time.

If this option is not selected, each backup in the restore chain is read, even if there was no change since the previous backup.

To restore empty directories, clear this option.

Default: selected.

Restore sparse files

(available for UNIX systems)

This option restores sparse files in their original compressed form. This is important because sparse files can consume additional disk space unless they are restored in their original form. By default, this option is disabled.

This option applies to UNIX sparse files only. Windows sparse files are always restored as sparse.

Lock files during restore

This option denies access to files during the restore. By default, this option is disabled.

Restore time attributes

This option preserves the time attribute values of each restored file. When this option is disabled, Data Protector sets the time attributes of the restored objects to the current date and time. By default, this option is enabled.

Restore protection attributes

This option preserves the original protection attributes of each restored file. If this option is disabled, Data Protector applies the protection attributes of the current restore session. By default, this option is enabled.

On Windows systems, this option applies to file attributes only. Security information is always restored, even when this option is disabled.

Restore share information for directories

Specifies that share information for directories will be restored. By default, this option is selected.

When restoring a directory that was shared on the network when it was backed up, the directory will also be shared after restore if this option is selected, provided that the backup was made with the Backup share information for directories option selected.

Advanced

Click here to set user-definable variables.

Restore by Query

In this page you can set the report level and network load for the restore session. Click **Finish** to start the restore.

Report level

This option defines the level of errors that will be reported for an object during a backup or restore session. Report levels are: Warning, Minor, Major, and Critical. Errors of the selected level and higher are reported. For example, by setting the level to Minor, only minor, major, and critical errors are reported in the Messages field. By default, the level is set to Warning. Messages of Normal level are always reported.

The number of messages per backup system stored in the IDB is limited to 3000.

Network load

Select the network load for the session.

Setting this option to Medium or Low reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Enable resumable restore

If this option is selected, Data Protector creates checkpoint files during the restore session. The checkpoint files are needed if the restore session fails and you want to resume the session using the Data Protector resume session functionality.

Default: selected (you can change the default using the global option ResumableRestoreDefault).

Select Version

Detailed information on backup versions of the file or directory is displayed.

Backed up

The date and time when the file or directory was backed up and the type of backup.

Modify time

The date and time when the file or directory was last modified before the backup.

Attributes

File permissions for UNIX systems, or file attributes for Windows systems.

User

(available for UNIX systems)

The user who owns the file or directory.

Group

(available for UNIX systems)

The group that owns the file or directory.

Size

The size of the file or directory when it was backed up.

Select Version By Date

In this page you select the backup version to be used for the restore by date and time.

Select latest version

If you select this option, the latest version of the file or directory will be restored.

Select version by date and time

If you select this option, specify the date and time of the backup that will be used for the restore.

Differences in backup time

Specify a time range within which Data Protector will search for the backup version closest to the specified time. If no backup was made within this time range, Data Protector selects a backup version based on the criteria below.

If selected date and time doesn't match with selected criteria

Select first available newer version

If no backup was made within the specified time range, Data Protector selects the first available newer version for restore.

Select first available older version

If no backup was made within the specified time range, Data Protector selects the first available older version for restore.

Select latest version

If no backup was made within the specified time range, Data Protector select the latest version for restore.

Restore Destination - Virtual Environment Integration

In this page, specify the destination for the virtual environment restore.

Backup host

Select the Data Protector client that you want to control the restore. The drop-down list contains all Microsoft Hyper-V clients that have the Data Protector Virtual Environment Integration component installed.

Restore client

Select the client that the selected virtual machine objects should be registered and restored to. By default, the client from which the virtual machines were backed up is selected.

Connect

Click this button to change the configuration of the restore client.

Restore to default location

Select this option to restore virtual machines to the original location.

Restore to target storage path

Select this option to specify the complete path for a different location where the virtual machines should be restored.

Restore to directory

Select this option to restore virtual machine files to a directory (outside of the datacenter) on the backup host. You can use the Browse button to find the target directory.

Application List - Virtual Environment Integration

In the Results Area, a list of applications that were backed up using the selected client is displayed.

Bar Name

Shows which Data Protector integration agent was used to create the backup - Data Protector Virtual Environment integration agent.

Bar Application

Displays the name of the application that was backed up. This depends on the selected client:

- VMware vCenter Server client: datacenter name.
- VMware ESX(i) Server client: predefined string /ha-datacenter.
- Microsoft Hyper-V client: predefined string /HyperV.

To display the properties of the object, right-click the object and click **Properties**.

Restore As New - Virtual Environment Integration

In this page, specify a new name for a virtual machine to be restored.

Original virtual machine name

Restore as new virtual machine

Select this option to restore a virtual machine under a new name.

Specify new name

(available when Restore as new virtual machine is selected)

Restore Options - Virtual Environment Integration

In this page, specify the options for the virtual environment restore. This page is disabled for Power On and Live Migrate operations.

Common options

Register virtual machines if needed

(VMware and H3C CAS specific option. Available for restore to a datacenter, cannot be modified for restore to an organization)

For H3C CAS, virtual machines are registered by default. This option will be greyed out.

Registers virtual machines once they are restored.

Consolidate snapshots to single file

(VMware specific option, available for restore to a datacenter)

Commits all snapshots to the virtual machine base once a virtual machine is restored.

Power-on virtual machines after restore

(not available for restore to a directory)

Powers the virtual machines on once they are restored.

Merge snapshots before restore

(Hyper-V specific option; not available for restore to a directory)

Consolidates all user-created and Data Protector created snapshots before performing the disk restore.

Existing virtual machine handling

(different parameters are available for Hyper-V, VMware and H3C CAS restore; not available for restore to a directory)

Specify how Data Protector should handle restore of existing virtual machines.

- **Delete before restore**: Data Protector should delete an existing virtual machine and then restore it from new. In a VMware environment, the virtual machine is deleted even if it resides in a different datacenter than your target datacenter. This is the space efficient option, but is less safe, since the old virtual machine is not available if the restore fails. Therefore, it should be selected with caution.
- **Skip restore**: Data Protector should skip the restore of an existing virtual machine. This allows you to restore missing virtual machines without affecting existing ones. When restoring multiple virtual machines, selecting this option enables you to restore only the virtual machines that do not exist at restore time.
- **Delete after restore**: (not available for Microsoft Hyper-V and H3C CAS clients) Data Protector should delete an existing virtual machine after it is restored. The virtual machine is deleted even if it resides in a different datacenter than your target datacenter. If the restore fails, the existing virtual machine is not deleted.
- **Keep for forensics**: (not available for Microsoft Hyper-V and H3C CAS clients) Data Protector should mark an existing virtual machine with a timestamp. The virtual machine which is kept for forensics is powered off after the restore and remains at the original location. It does not affect consecutive backups of the original virtual machine.

Defaults:

- **Hyper-V**: Delete before restore
- **VMware vCenter Server and VMware ESX(i) Server systems**: Delete after restore

Note that an VMware ESX(i) Server system is only aware of its own datacenter. So if you select an ESX(i) Server system as a restore client and a virtual machine exists in a different datacenter, it cannot be deleted. Consequently, you end up with two virtual machines having the same UUID. To resolve this, power the virtual machine on while connected to a vCenter Server. VMware will detect the duplicate UUID and ask whether the virtual machine has been copied or moved. If you select copied, VMware will automatically select a new UUID for the virtual machine.

File conflict handling

(VMware and H3C CAS specific option, available for restore to a directory)

Specify how Data Protector should handle restore of existing files.

- **Overwrite**: Data Protector should overwrite an existing file with the one from the backup.

- **Keep latest**: (Not supported for H3C CAS) Data Protector should leave an existing file intact if it is more recent than the one from the backup. Otherwise, the file should be overwritten. This is a VMware specific option.
- **Skip**: Data Protector should not overwrite an existing file (the file is not restored from the backup).

Default: Overwrite.

When **vStorage Image + OpenStack** method is selected, the following options are unavailable for user selection:

- Register virtual machines if needed
- Existing virtual machine handling
- File conflict handling

Categories and Tags

(Vmware VCenter specific option)

This section is available for selection only if you select a vCenter client as the Restore client in the destination page.

Category/Tag handling

Select any one of the following options from the drop-down to choose how to use categories and tags:

- **Skip attaching tags**: Skips attaching of a tag to the restored VM.
- **Attach tags from time of backup:** Retains tags that were attached at the time of backup.
- **Attach custom tags:** Enables you to attach custom tags to a VM.

Category

This option is enabled only when you select **Attach customer tag** in the **category/tag handling** drop-down.

Tag

This option is enabled only when you select a category. You can attach multiple tags to a single VM.

Restore Source - Virtual Environment Integration

In this page, browse for and select the virtual environment objects that you want to restore. You can select more than one object to restore in parallel.

Backup method

Defines which virtual environment objects are displayed - only those backed up with the selected method are displayed. Virtual environment objects that were created using different backup methods cannot be restored in the same session.

From

Defines the start of a time interval.

To

Defines the end of the time interval.

Use the **From** and **To** options to narrow the scope of displayed virtual machine objects to those that were created within the specified time interval. Each selected virtual machine object will be restored from the last backup created within this interval.

VMware specific: You can restore individual virtual disks only if the original virtual machine still exists. Otherwise, the restore fails.

The following information is **VMware specific**.

- To specify further restore options, click other tabs and set desired options in the appropriate pages.
- By right-clicking the selected virtual machine and clicking Restore As / Info, you can restore it as a new virtual machine. This option is disabled for Power On and Live Migrate operations.
  However, if clicking Restore Version, you can specify the backup version for the restore which will be appended to the virtual machine name.

Power On

Virtual machines can be powered on instantly within seconds from the Data Protector backup image that resides on the 3PAR replica (local or remote copy), Smart Cache, Data Domain, and StoreOnce Catalyst devices. Previously, virtual machines had to be powered on only after the complete data migration to the production data center. Use this feature if you want to verify the sanity of the backup. Note that the changes done to the virtual machine once it is powered on, will be available until you perform the clean up operation.

When you power on a virtual machine, the backup image is presented to the destination ESX server. A new virtual machine is created, whose data disks point to the Data Protector backup image. The other files reside on the destination data center.

Live Migrate

This option will power on the virtual machine from the backup image, and will simultaneously start the data migration to the destination datastore. During this process, the virtual machine will continue to be accessible. Since the data movement is a back end operation, it will have minimum impact on the usage and accessibility of the powered on virtual machine. Any modifications done to the virtual machine data will be consolidated, and the migrated virtual machine will have all the modified content on top of the restored image from the backup.

Once the data migration is complete, the virtual machine functions from the destination datastore, and has no dependency on the backup image. Also, the backup image presentation is removed.

You can perform Live Migrate of the virtual machine from a backed up image, Smart Cache, Data Domain, or a StoreOnce Catalyst device.

Hyper-V specific: You can restore individual virtual disks only if full backup is performed after installing Data Protector 9.07 or later.

The full backup must contain all the disks that were backed up. Based on the From and To options selected, you get to view all disks within that selected range.

Select Version - Virtual Environment Integration

This page displays information about available backup versions.

Select for restore

You can select a backup version that you want to restore.

Backup version

Select a backup version for restore. By default, the most recent backup version is already selected. The version will be appended to the virtual machine name.

Last backup version

The date, time, and type of the last backup version.

Restore Destination - Virtual Environment Integration

In this page, specify the destination for the virtual environment restore.

Backup host

Select the Data Protector client that you want to control the restore. The drop-down list contains all VMware vCenter, VMware ESX(i) and H3C CAS clients that have the Data Protector Virtual Environment Integration component installed.

Restore client

Select the client that the selected virtual machine objects should be registered and restored to. By default, the client from which the virtual machines were backed up is selected.

Connect

Click this button to change the configuration of the restore client.

Mount Proxy Client

(Not supported for H3C CAS)

Select the ESX(i) Server system that is used for mounting the replicas.

You can restore from either a 3PAR array or a tape. You can restore to a directory only from a tape.

You can select the blank option from the drop down options, and this allows you to restore from a tape to a directory.

Restore to datacenter

Select this option to restore virtual machines to a datacenter.

Datacenter/Hostpool

Select the datacenter or hostpool to which virtual machines should be restored. By default, the virtual machines are restored to the original datacenter or hostpool.

For VMware, you can restore from a 3PAR array to a datacenter by selecting the required ESX(i) server system in the Mount Proxy Client drop down.

Host/Cluster

Select the client or the cluster to which virtual machines should be restored. By default, the virtual machines are restored to the original client or cluster.

Specific host

Select the specific client in the cluster to which virtual machines should be restored. By default, the virtual machines are restored to the original client.

Resource pool

Select the resource pool on the client or the cluster to which virtual machines should be restored. By default, the virtual machines are restored to the original resource pool.

Datastore/Storage pool

Select a datastore or active storage pool to which virtual machines should be restored. The drop-down list contains all datastores or active storage pools that are accessible by the selected restore client. By default, the virtual machines are restored to the original datastore or storage pool.

Virtual Machine

(H3C CAS specific option, supported for individual disk restore using cached method only)

Select the virtual machine to which you want to restore the selected objects to. This option is available in the case of cached

restore. The VMs listed in this drop-down list are determined by the OS of object you want to restore. If the object is a Windows OS, then only Windows VMs will be listed here. This is not the case If you select multiple objects for restore. In this case, all VMs will be displayed in this drop-down, and not just those compatiable with the OS of the selected objects.

Network

(Not supported for H3C CAS)

Select a network to enable virtual machines communication. The target network can be selected for all virtual machines selected in the restore session. By default, the virtual machine is connected to the network available at the time of backup even though it might not be available anymore.

Category

(VMware specific option)

Select a category on the vCenter server to which the restored virtual machines are to be grouped by tag. This option is applicable if the selected restore client is a vCenter server.

Tags

(VMware specific option)

Select a tag to label the virtual machines that are being restored. This drop-down becomes available for selection only if the category is selected.

Restore to directory

Select this option to restore virtual machine files to a directory (outside of the datacenter) on the backup host. You can use the Browse button to find the target directory.

You can restore from a tape by selecting the blank option in the Mount Proxy Client drop down.

For H3C CAS Cached restore, this option is disabled.

Application Restore Source

This page displays the writers, components, or files that have been backed up. Here you select the objects to be restored.

For Exchange Server, in case you select a LCR or CCR copy for restore, note that restore will be performed to the production database (Exchange Information Store) and not to the database copy (Exchange Replication Service), because restore to a replicated storage group is not supported.

The following may be helpful:

- To view object properties, right-click an object and select **Properties**.
- To perform restore to a different location (in case of Exchange Server), right-click a storage group or a store or transaction logs and click Restore as.
- To specify further options for your restore, click other tabs and set the desired options in the appropriate pages.

Click **Restore** to start restore.

Restore Mode

Restore files to temporary location (not supported for SharePoint Services writer)

You can select individual files or group of files that were backed up using the selected writer. The files are restored using the Data Mover Agent and not the Volume Shadow Copy Service.

Restore components

The components are restored using Volume Shadow Copy Service. Individual files cannot be selected.

Add media to prealloc list

Select a medium to be added to the prealloc list and click **Add**.

Add new group

Enter a name for the new group of backup specifications or templates.

Object properties - Other

The options in this page apply to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

Software compression

Enables compressing the data read by the Disk Agent. The data is written to media in a compressed format, which reduces the number of media required for a backup and improves backup performance in some cases. By default this option is not selected.

Do use this option if the hardware provides built-in hardware compression, since double compression only decreases performance without providing better compression results.

You can use a custom compression library instead of that provided by Data Protector. Note that after changing the compression library, a full backup should be performed.

Display statistical info

When this option is enabled, Data Protector reports statistical information (such as size and performance) for each object that is backed up or restored. You can view the information in the monitor window. By default, this option is disabled.

- Is Public

Data security

- None
- Encode
- AES 256 bit

Options

The options in this page apply to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

If you schedule the backup and set the **Protection** option different from **Default** in the Schedule wizard dialog, it will override the selection made in this page.

- Protection

Object Properties - MS SQL Object

These options apply to the selected backup object.

General integration object information

Client

The name of the client with the object you want to back up.

Object

The database you want to back up.

- Use default concurrent streams (not available for ZDB)
- Concurrent streams
- SQL backup compression (available by Microsoft SQL Server 2008 Enterprise and later)

Object Properties - Sybase Object

The options in this page apply to the selected Sybase database.**General integration object information**

Client

The name of the client with the database to be backed up.

Object

The database to be backed up.

- Number of concurrent streams

Common Application Options - Other

The options in this page apply to all backup objects of the application backup.

With some applications (for example, Sybase), you can change options for a specific object. To do that, select that object's properties in the Backup Object Summary page of the backup specification.

- Software compression
- Display statistical info
- Is public

Data security

- None
- AES 256-bit
- Encode

Report level

This option defines the level of errors that will be reported for an object during a backup or restore session. Report levels are: **Warning**, **Minor**, **Major**, and **Critical**. Errors of the selected level and higher are reported. For example, by setting the level to Minor, only minor, major, and critical errors are reported in the Messages field. By default, the level is set to Warning. Messages of Normal level are always reported.

The number of messages per backup system stored in the IDB is limited to 3000.

Common Application Options

The options in this page apply to all backup objects of the application backup.

With some applications (for example, Sybase), you can change options for a specific object. To do that, select that object's properties in the Backup Object Summary page of the backup specification.

Application Specific Options - DB2

The options in this page apply to the DB2 integration backup.

General information

- Pre-exec
- Post-exec
- Parallelism (not available for the DB2 integration)

Application Specific Options - Microsoft Exchange Server Integration

The options in this page apply to the Microsoft Exchange Server integration backup.

General information

- Pre-exec
- Post-exec

Application Specific Options - Informix Server Integration

The options in this page apply to the Informix Server integration backup.

Backup type

Storage-space backup

If this option is selected, the onbar command backs up the selected storage-spaces and logical logs in parallel. When you restore from a storage-space backup, you also have to restore logical logs to make the data consistent. Storage-space backup is faster than whole-system backup on large databases. Default: selected

Whole-system backup

If this option is selected, all Informix instance's dbobjects from the onbar command are backed up. ON-Bar cannot back them up concurrently; they are backed up sequentially. Whole-system backup is useful for disaster recovery, or restore to another client. When you restore from a whole-system backup, you do not need to restore logical logs to make the data consistent.

- Pre-exec
- Post-exec

Application Specific Options - Oracle Integration

The options in this page apply to the Oracle integration backup.

Disable recovery catalog auto backup

Select this option to disable backup of the recovery catalog. By default, Data Protector backs up the recovery catalog in every backup session, or, in ZDB environment, after every ZDB to tape or ZDB to disk+tape.

Disable Data Protector managed control file backup

Select this option to disable backup of the Data Protector managed control file. By default, Data Protector backs up the Data Protector managed control file in every backup session, or, in ZDB environment, after every ZDB to tape or ZDB to disk+tape.

Back up standby database

(This option is applicable in Oracle Data Guard environment and if the database is configured with the standby connection. It is ignored for ZDB.) By default, RMAN backs up the database files and archived redo logson the primary system. Select this option to enable backup of the database files and archive logs on the standby system. However, only the archive logs created after the standby database was configured can be backed up at standby site. Archive logs created before the standby database was configured must be backed up on the primary database.

Note that the current control file or the control file for standby database will still be backed up from the primary system.

RMAN Script

The RMAN script section of the backup specification, created by Data Protector.

Edit

(available after the backup specification has been saved)

Click here to edit the RMAN script section of the backup specification.

Pre-exec

Specify a command or RMAN script that will be started by ob2rman.pl on the Oracle Server system before the backup. RMAN scripts must have the .rman extension. Do not use double quotes.

Provide the pathname of the command or RMAN script.

You can disable execution of pre-exec scripts by setting OB2OEXECOFF variable in omnirc file to 1. To disable the remote session pre- and post-exec command execution on any client, add the OB2REXECOFF=1 into the omnirc file on the specific client. The pre- and post-exec commands fail if you specify custom perl and openssl commands as pre- and post-exec commands, instead of scripts.

Post-exec

Specify a command or RMAN script that will be started by ob2rman.pl on the Oracle Server system after the backup. RMAN scripts must have the .rman extension. Do not use double quotes.

Provide the pathname of the command or RMAN script.

You can disable execution of post-exec scripts by setting OB2OEXECOFF variable in omnirc file to 1. To disable the remote session pre- and post-exec command execution on any client, add the OB2REXECOFF=1 into the omnirc file on the specific client.

To ensure that post-exec scripts are always run even if the pre-exec scripts fail, set the OB2FORCEPOSTEXEC variable in omnirc file to 1.

The pre- and post-exec commands fail if you specify custom perl and openssl commands as pre- and post-exec commands, instead of scripts.

Backup offline

(available for ZDB integrations)

If this option is selected, the Oracle database on the application system is shut down while the disk devices are split. The database backup is done on the backup system and is therefore consistent. For Oracle proxy-copy ZDB method, the backup is done without application binaries on the backup system and is therefore consistent.

If this option is not selected, an online backup is performed, which means that the Oracle database on the application system is available during backup. The tablespaces are in backup mode during the split command. The database is not consistent,

therefore you must back up the archive logs.

Application Specific Options - SAP Integration

The options in this page apply to the SAP R/3 integration backup.

Log file

Here the pathname of the local backint log file is specified. By default, this log file is not generated, as Data Protector stores all relevant information about backup sessions in the IDB. However, you can enable local logging by specifying a log file pathname.

BR Backup

Enter BRBACKUP command options. See SAP R/3 Online Documentation for information about BRBACKUP command options. For ZDB, use this option to modify the backup settings. For example, type -t online_mirror for an online backup using splitint .

Do not use the BRBackup and BRArchive -m option, which specifies backup objects. These objects have already been specified. If you specify the objects here, they will be overridden.

Backup Objects

When the backup specification is saved and reloaded, this field lists the string passed by the omnisap.exe to the BRBACKUP command.

BR Archive

(not available for ZDB to disk)

Enter BRARHIVE command options. See SAP R/3 Online Documentation for information about BRARCHIVE command options.

Balancing

By load

The default setting. Files are grouped in subsets by size so that the amount of data on all backup devices is approximately the same. Each subset is backed up by one sapback program, thus allowing concurrent backup of all subsets.

By time

Files are grouped in subsets so that the backup to all devices takes approximately the same time. This depends on file types, the speed of backup devices, and external influences, such as mount requests, and is therefore best suited for environments with large libraries of the same quality. Each subset is backed up by one sapback program, thus allowing for a concurrent backup of all subsets of the same type.

Manual

(not available for ZDB to disk)

Allows you to optimize the backup by giving you full control over grouping files into subsets and backing up these subsets on specific devices.

Pre-exec

Enter a command to be executed on the SAP client before the backup is started. The command/script is started by Data Protector omnisap.exe and has to reside in the following directories:

Windows systems: Data_Protector_home\bin

Linux and Solaris systems: /opt/omni/bin

Enter only the filename and not the whole path of the script.

You can disable execution of pre-exec scripts by setting OB2OEXECOFF variable in omnirc file to 1. To disable the remote session pre- and post-exec command execution on any client, add the OB2REXECOFF=1 into the omnirc file on the specific client.

The pre- and post-exec commands fail if you specify custom perl and openssl commands as pre- and post-exec commands, instead of scripts.

Post-exec

Enter a command to be executed on the SAP client before the backup is started. The command/script is started by Data Protector omnisap.exe and has to reside in the following directories:

Windows systems: Data_Protector_home\bin

Linux and Solaris systems: /opt/omni/bin

Enter only the filename and not the whole path of the script.

You can disable execution of post-exec scripts by setting OB2OEXECOFF variable in omnirc file to 1. To disable the remote session pre- and post-exec command execution on any client, add the OB2REXECOFF=1 into the omnirc file on the specific client.

To ensure that post-exec scripts are always run even if the pre-exec scripts fail, set the OB2FORCEPOSTEXEC variable in omnirc file to 1. The pre- and post-exec commands fail if you specify custom perl and openssl commands as pre- and post-exec commands, instead of scripts.

Backup mode

(disabled if tablespaces and not the whole database are configured to be backed up; not available for ZDB)

Specifies the type of RMAN backup to be used.

All

RMAN backs up the complete database.

Full

RMAN performs a full backup (level 0), thus enabling RMAN incremental backups.

Use default RMAN channels

(not available for ZDB)

If this option is selected, the concurrency value is taken from the SAP parameter file. If it is not selected, enter the desired concurrency value for your backup.

Objects outside database

With this option, you can specify arbitrary files or directories to be included in the backup. Separate file names with commas. You can use any option that is available with the BRBACKUP -m option. For additional information, see SAP R/3 Online documentation.

Application Specific Options - MS SQL Integration

The options in this page apply to the SQL integration backup. To change options for a specific backup object, select properties of the object in the Backup Object Summary page of the backup specification.

General information

- Pre-exec
- Post-exec

Options

- Concurrent streams (not available for ZDB)

Fast direct mode

- Fast direct mode (not available for ZDB)
- Check database integrity
- SQL backup compression (available by Microsoft SQL Server 2008 Enterprise and later)
- Exclude from backup (available for standalone instance backup only)

Application Specific Options - Sybase Integration

The options in this page apply to the Sybase integration backup.

If you have selected individual Sybase databases, you can set additional options for each database. Right-click the database in the Backup Object Summary page and click **Properties**.

General information

- Pre-exec
- Post-exec

Options Property Page

In this page you can set backup options for all backup objects in the backup specification. To set further options, click the appropriate **Advanced** button.

If you schedule the backup and set the **Protection** option different from **Default** in the Schedule wizard dialog, it will override the selection made in this page.

Backup Specification Options

These options apply to the entire backup specification.

Description

Type a description of your backup specification.

Common Application Options

These options apply to each object of an application backup. With some applications (for example, Sybase), you can change options for a specific object. To do this, select the object's properties in the Backup Summary page.

Application Specific Options

If the Application Specific Options window is not displayed when you click the **Advanced** button, that means that you have deselected all backup objects that were present in the backup specification.

Backup to Disk Device Options

- Source-side deduplication

Schedule page - Backup

This page provides options to create and view schedules for a backup specification.

Add

Schedules a backup on the date selected in the calendar.

Delete

Removes the backup selected in the list below the calendar.

Undo

Reverses the last action.

Reset

Resets the schedule.

Predefined

Selects one of the available predefined backup schedules:

- **Daily intensive**: Data Protector runs a full backup at midnight and two additional incremental backups at 12:00 (noon) and 18:00 (6 P.M.) every day.
- **Daily full**: Data Protector runs a full backup every day at 21:00 (9 P.M.).
- **Weekly full**: Data Protector runs a full backup every Friday and Incr1 backups every day from Monday to Friday at 21:00 (9 P.M.).
- **Fortnight full**: Data Protector runs a full backup every second Friday. Between these backups, Data Protector runs Incr1 backups every Monday to Thursday, all at 21:00 (9 P.M.).
- **Monthly full**: Data Protector runs a full backup on the first of every month, an Incr1 backup every week, and an incremental backup every other day.

Holidays

Select this option if you do not want backups to run on holidays. By default, Data Protector runs backups on holidays.

Disable schedule

Select this option to prevent the scheduled backups from being performed, or deselect it to enable the schedule.

Legend

The colors that represent the types of scheduled backups in the calendar.

- Red represents Full backup
- Blue represents Incremental backup
- Yellow represents Incremental+Full backup
- White with a red border represents holidays.

Navigation buttons

The **Previous** navigation button on the left displays the calendar view of the previous month.

The **Next** navigation buttons on the right displays the calendar view of the next month.
The schedule for each day is highlighted against each date.

Choose Predefined Schedule

This page allows you to choose one of the following predefined schedules:

- **Daily intensive**: Data Protector runs a full backup at midnight and two additional incremental backups at 12:00 (noon) and 18:00 (6 P.M.) every day.
- **Daily full**: Data Protector runs a full backup every day at 21:00 (9 P.M.).
- **Weekly full**: Data Protector runs a full backup every Friday and Incr1 backups every day from Monday to Friday at 21:00 (9 P.M.).
- **Fortnight full**: Data Protector runs a full backup every second Friday. Between these backups, Data Protector runs Incr1 backups every Monday to Thursday, all at 21:00 (9 P.M.).
- **Monthly full**: Data Protector runs a full backup on the first of every month, an Incr1 backup every week, and an incremental backup every other day.

Schedule Backup - Informix Server

This page allows you to specify the backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Note: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type: Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incr1-2**: Informix Server level 1 and 2 incremental backup. The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Schedule Backup - SAP MaxDB Integration

On this page, you select the time of the scheduled backup (for a date already selected), the intervals at which you want the backups to be performed, and further options for the scheduled backup.

> **Note**: The settings in this page apply to the individual or periodic scheduled backup. They do not apply to backups that are started interactively.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting (available for recurring backups): Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Important: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type:

> **Note:** With ZDB, only the **Full** backup type is supported.

Choose one of the following options:

- **Full**: This is a special mode of SAP MaxDB backup. If this option is selected, a full backup of SAP MaxDB instance data and configuration is performed.
- **Incr**: This is a special mode of SAP MaxDB backup. If this option is selected, a differential backup of SAP MaxDB instance data and configuration is performed.
- **Trans**: This is a special mode of SAP MaxDB backup. If this option is selected, a backup of SAP MaxDB instance's archive logs is performed.

Network load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. Default: High.

Backup protection:

> **Important:** The backup protection settings specified here override protection settings elsewhere in the backup specification.

Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Schedule Backup - SAP R/3

On this page you select the time of the scheduled backup (for a date already selected), the intervals at which you want the backups to be performed, and further options for the scheduled backup.

> **Note:** The settings in this page apply to the individual or periodic scheduled backup. They do not apply to backups that are started interactively.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting (available for recurring backups): Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Backup type:

> **Note:** With ZDB, only the **Full** backup type is supported.

Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incr**: Incr backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup. The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup. You can use this backup type if you are using Oracle RMAN to back up SAP R/3 objects. This backup type performs the Oracle RMAN backup incremental level 1. It backs up all changes to the selected SAP R/3 objects since the last full backup.

Network load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. Default: High.

Backup protection:

> **Important:** The backup protection settings specified here override protection settings elsewhere in the backup specification.

Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Split mirror/Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant

recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Filesystem

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Selects the time for the backup to start. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incr**: If this option is selected, only changes from the last protected backup are backed up, regardless of whether it was a full or incremental backup.
  The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.
- **Incr1-9:** Incr1-9, also called leveled incremental backup, backs up only changes made since the last protected backup of the next lower level. For example, an Incr1 backup saves all changes since the last full backup, and an Incr5 backup saves all changes since the last Incr4 backup. An Incr1-9 backup never references an existing Incr backup. If there is no protected full backup, Data Protector starts a full backup instead.

  The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

Network load: Set this option to **Medium** or **Low** to reduce the load on the network when running Data Protector. The default selection is **High**.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Split mirror/Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - MySQL

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Selects the time for the backup to start. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: Backs up all selected PostgreSQL databases and PostgreSQL Server transaction logs.
- **Incr**: Backs up all selected PostgreSQL databases and PostgreSQL Server transaction logs since the last protected backup.
- **Trans**: Backs up PostgreSQL Server transaction logs. When you select this backup type, you must ensure that a full backup exists in the IDB. .

Network load: Set this option to **Medium** or **Low** to reduce the load on the network when running Data Protector. The default selection is **High**.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten.

Schedule Backup - PostgreSQL

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Selects the time for the backup to start. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: Backs up all selected PostgreSQL databases and PostgreSQL Server transaction logs.
- **Trans**: Backs up PostgreSQL Server transaction logs. When you select this backup type, you must ensure that a full backup exists in the IDB. .

Network load: Set this option to **Medium** or **Low** to reduce the load on the network when running Data Protector. The default selection is **High**.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten.

Schedule Backup - Sybase

This page allows you to specify the backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Note: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type: Choose one of the following options:

- **Full**: Backs up all selected Sybase objects and Sybase transaction logs. If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Trans**: This incremental backup type backs up only transaction logs for the selected database(s) since the last backup of any backup type. If there is no full backup in the IDB, Data Protector starts a full backup instead. The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on the media and in the IDB. The disadvantage is that the restore is more complicated as you usually need all the media used since the last full backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Virtual Environment Integration

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Set the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incr**: If this option is selected, it backs up the changes based on the backup method selected. Under specific circumstances, the incremental backup session falls back and Data Protector performs a full backup instead.
  - **vStorage Image/vCD vStorage Image/ vStorage Image + Openstack:** Backs up changes made to a virtual machine since the last backup of any type. For a standard vStorage Image backup, the changes are identified using snapshots; if changed block tracking is used, the changes are identified from the storage blocks changed since the previous backup.
  - **Hyper-V Image:** Backs up changes made to a virtual machine since the last backup of any type.
  - **H3C CAS Backup Image**: Backs up changes made to a virtual machine while powered off (offline backup) or while actively used (online backup).
- **Diff**: This option is available for VMware and H3C CAS. It is not available for the Hyper-V Image backup method. Under specific circumstances, the differential backup session falls back and Data Protector performs a full backup instead.
  - **vStorage Image/vCD vStorage Image/ vStorage Image + Openstack:** Backs up changes made to the virtual machines since the last full backup. For a standard vStorage Image backup, the changes are identified using snapshots; if changed block tracking is used, the changes are identified from the storage blocks changed since the last full backup.
  - **H3C CAS Backup Image**: Backs up changes made to a virtual machine while powered off (offline backup) or while actively used (online backup) since the last full backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Schedule Backup - IDB

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Selects the time for the backup to start. To change the minutes, click the minutes and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to one minute, set the SchedulerGranularity option.

Use starting: This option is available only for recurring backups. Select this option if you want the backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.
- **Incr**: If this option is selected, it backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup.

Network load: Set this option to **Medium** or **Low** to reduce the load on the network when running Data Protector. The default selection is **High**.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten.

Schedule Backup - DB2

This page allows you to specify the backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Note: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type: Choose one of the following options:

- **Full**: Backs up all selected DB2 objects regardless of whether they have been changed after the last backup was made. Some data, such as database configuration, history file, which is important for restore, is included into the full backup automatically.
  If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incremental**: Backs up all the changes made to the database after the last full backup. Incremental backup (Incr, Incr 1, Incr 2, and so on) includes only the data that has been modified since the last full or incremental backup. Incremental backups are faster and need less media, but make the restore of all data more complicated as you usually need all the media used since the last full backup.
- **Delta**: Backs up all the changes made to the database from the last backup of any kind (full, incremental, or delta). A delta backup includes all changes since the last backup of any kind (full, incremental, or delta). The advantage of a delta backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

  If the last backup was a full backup, together with delta backup provide the most complete backup. If a delta backup is preceded by an incremental backup, you need the delta, the incremental backup, and the full backup on which the incremental is based. If a delta backup is preceded by one or more delta backups, you need all delta backups.

  Prerequisite

  To perform incremental or delta backup, the DB2 trackmod parameter must be set to ON.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Exchange

This page allows you to specify the backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Note: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type: Choose one of the following options:

- **Full**: Select this option to back up the database file (.edb), transaction logs (.log), and checkpoint files (.chk), and then to truncate the transaction logs.

  DAG environment only: If multiple copies of a database are selected for backup, Data Protector first performs a *full* backup of the passive copy that has the fewest logs applied to the database file, and then performs a *copy* backup of all the remaining copies, with the active copy being backed up last. The copies are backed up sequentially due to a Microsoft Exchange Server VSS writers limitation.

- **Copy**: Select this option to back up the database file (.edb), transaction logs (.log), and checkpoint files (.chk), without truncating the transaction logs.
- **Incr**: Select this option to back up the transaction logs (.log) that have been created since the last Full or Incremental backup, and then to truncate the transaction logs. Note that you cannot perform an Incremental backup of a database if a Full backup has not been performed. Also, you cannot perform an Incremental backup of a database if an Incremental backup is started just after a Differential backup has been performed, nor the other way around.

  DAG environment only: If multiple copies of a database are selected for backup, Data Protector backs up transaction logs from only one copy (one of the passive copies is selected).

- **Differential**: Select this option to back up the transaction logs (.log) that have been created since the last *full* backup, without truncating the transaction logs. Note that you cannot perform a *differential* backup of a database if a *full* backup has not been performed. Also, you cannot perform a *differential* backup of a database if an *incremental* backup is started just after a *differential* backup has been performed, nor the other way around.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Lotus Notes

This page allows you to specify the backup time, frequency, duration, and type.

Recurring

Sets the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Specify the backup type, network load, and backup protection for the scheduled backup.

Note: The backup protection settings specified here override protection settings elsewhere in the backup specification.

Backup type: Choose one of the following options:

- **Full**: Backs up the selected Lotus Notes/Domino Server databases and, if selected, transaction logs, including the one currently in use.
- **Incr**: Backs up the selected Lotus Notes/Domino Server databases that meet at least one of the following two conditions:
  - The size of the changes made to a database since it was last backed up exceeds the size set by the **Amount of log changes (KB)** option.
  - The Lotus Notes/Domino Server DBIID for a database has changed.
    Databases that do not meet at least one of the two conditions are not backed up.
    If archived logs are selected, it also backs up the archived logs that have not been backed up yet.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Schedule Backup - MS SQL server

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Set the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Backup type

Note: With ZDB, only the **Full** backup type is supported.
Choose one of the following options:

- **Full**: Backs up all selected Microsoft S SQL Server databases and Microsoft SQL Server transaction logs.
- **Trans**: Backs up MS SQL Server transaction logs. When you select this backup type, you must ensure that a full backup exists in the IDB. Make sure that you have the **Recovery model** option on the Microsoft SQL Server set to **Bulk-Logged** or to **Full** in order to perform MS SQL Server Trans backups.
- **Differential**: A database backup that records only the data changes made to the database after the last full database backup. Before you run a differential backup, make sure that a full backup exists. Otherwise, a restore from such a differential backup session fails. If you run a differential backup without running a full backup first, a full backup will be taken instead of a differential backup.
- **Copy**: A copy-only full backup is an independent full backup, which never truncates the transaction logs and does not affect an SQL Server restore chain. For this reason, it also cannot serve as a base of a differential backup. Run a copy-only full backup, if you do not want to influence a database backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- Default: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- None: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- Until: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- Weeks: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- Days: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- Permanent: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Microsoft SharePoint Server

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Set the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: Select this option to perform a *full* backup. The meaning depends on which object you select.
  - **Microsoft SQL Server database**: Performs a Microsoft SQL Server Full database backup; the complete database is backed up.
  - **Index files**: Performs a Full filesystem backup of all index files.
- **Incremental:** Select this option to perform an *incremental* backup. The meaning depends on which object you select.
  - **Microsoft SQL Server database**: Performs a Microsoft SQL Server transaction log backup. Backs up transaction logs (.log) that have been created since the last transaction log backup of the Microsoft SQL Server database, and then truncates the transaction logs.
  - **Index files**: Backs up only the index files that have been changed or created since the last backup of any type.

    > **Note**: If the Microsoft SQL Server database is in the simple recovery mode (has no transaction logs), a Differential backup will be performed for the database instead.

    For the metadata of the Microsoft SharePoint Server components, a Full backup is always performed due to a small amount of data.
- **Differential**: Select this option to perform a *differential* backup. The meaning depends on which object you select.
  - **Microsoft SQL Server database**: Performs a Microsoft SQL Server Differential backup of the database; backs up changes made to the database since the last Full backup.
  - **Index files**: Backs up the index files that have been changed since the last Full backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Schedule Backup - Oracle

This page allows you to specify the desired backup time, frequency, duration, and type.

Recurring

Set the frequency of the scheduled backup. If you do not want recurring backups, select **None**. If you want the backup to recur, select one of the intervals and specify more precisely when you want the backup to be performed.

Time options

Time: Select the time for the backup to start. To change the minutes, click the minutes, and then click the arrows to increase or decrease the value. By default, the granularity of the scheduler is 15 minutes. If you want to modify it to 1 minute, set the SchedulerGranularity global option.

Use starting: This option is available only for recurring backups. Select this option if you want the recurring backup to start on a specific date, and specify the starting date.

Session options

Backup type: Choose one of the following options:

- **Full**: If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup. The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup). The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.
- **Incr1-4:** Incr1-4, also called leveled incremental backup, backs up only changes made since the last protected backup of the next lower level. For example, an Incr1 backup saves all changes since the last full backup, and an Incr4 backup saves all changes since the last Incr3 backup. An Incr1-4 backup never references an existing Incr backup. If there is no protected full backup, Data Protector starts a full backup instead.

  The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB. The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

Network Load: Select the network load for the session. Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete. This option is set to **High** by default.

Backup protection: Specify the time period of protection of the data you back up to prevent the backup from being overwritten. The following options are available:

- **Default**: The default backup protection means that your backup has protection as specified on the backup specification level and backup object level. If you have not changed the defaults there, your backup is permanently protected.
- **None**: This backup protection option provides no protection. Media is removed/deleted before the next write operation/backup to the file library is started.
- **Until**: This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.
- **Weeks**: This backup protection option provides protection for a time period of your choice, specified in weeks. This means that the data on the medium cannot be overwritten for the specified number of weeks.
- **Days**: This backup protection option provides protection for a time period of your choice, specified in days. This means that the data on the medium cannot be overwritten for the specified number of days.
- **Permanent**: This backup protection option provides permanent protection. This means that the data is permanently protected from being overwritten.

Snapshot backup: This option is available with ZDB, but only in the case of a ZDB-to-disk+tape or instant recovery enabled ZDB-to-disk session.

- Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.
- Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Source Property Page

In this page, you select the objects that you want to back up.

Available objects can be selected individually or at various group levels. Note that if you select a group (and nothing within it) any objects added to the group after the specification is saved will also be backed up.

Show

In the drop-down list, select one of the following:

All

If this option is selected, all available backup objects in the cell are displayed.

Selected

If this option is selected, only selected objects are displayed.

IAP clients

If this option is selected, only the clients with the IAP Disk Agent Extension installed are displayed.

Source Property Page - Microsoft Exchange Server

In this page, you select the objects that you want to back up.

Show

In the drop-down list, select one of the following:

All

With this option, all available backup objects in the cell are displayed.

Selected

With this option, only the objects that are selected for backup or excluded from backup are displayed. If any objects are not displayed, it means that they are not excluded from the backup specification and will be backed up.

When a new database is added on the client selected for backup, it will be automatically included to the backup specification.

Source Property Page - VSS

In this page, you select the objects that you want to back up.

Show

In the drop-down list, select one of the following:

All

If this option is selected, all available backup objects in the cell are displayed.

Selected

If this option is selected, only selected objects are displayed.

To specify options for the consistency check of a Microsoft Exchange Server writer and cluster options for the Microsoft Exchange Server writer in CCR environment, right-click the writer and click **Additional options**.

Application Specific Options - SAP MaxDB Integration

The options in this page apply to SAP MaxDB integration backup.

- Change database state
- Keep archive logs

General information

(The Pre-exec and Post-exec options are not available for the SAP MaxDB integration.)

- Parallelism

Application Specific Options - Includes/Excludes

This applies to the specific backup object that you have selected.

Includes

Specify the Lotus Notes/Domino Server data directories that you want to include in the backup. Type the relative pathname to the Lotus Notes/Domino Server data directory in the text box and click Add. For example, if the selected object is a NSF database and you want to back up only the help directory, enter help.

To remove a data subdirectory from the Includes list, select it and click Delete. If you delete all listed data subdirectories, the entire object is selected for backup.

Excludes

Specify the Lotus Notes/Domino Server data directories that you want to exclude from the backup. Type the relative pathname to the Lotus Notes/Domino Server data directory in the text box and click Add. For example, if the selected object is a NSF database and you want to skip the help directory, enter help.

To remove a data subdirectory from the Excludes list, select it and click Delete.

The Excludes option has higher priority than the Includes option. If you specify the same data directory in the Includes and Excludes fields, the directory will not be backed up.

Application Specific Options - Lotus Notes/Domino Server Integration

The options in this page apply to the Lotus Notes/Domino Server integration backup.

Options

Amount of log changes (KB)

Applies to incremental backups. The backup skips the database if at least one of the following two conditions is met:

- The database to be backed up has a smaller log amount than specified by the option.
- The Lotus Notes/Domino Server DBIID for the database has not changed.

If the database exceeds the specified log amount or if the Lotus Notes/Domino Server DBIID for the database has not changed, the database is backed up.

Default

Sets the default log amount, which is equal to the size of one log extent.

- Pre-exec
- Post-exec

Backup buffer size (KB)

The size of the buffer used for reading and writing data during the backup.

Default

Sets the default backup buffer size, which is 32 kB.

General information

- Pre-exec
- Post-exec

Backup buffer size (KB)

The size of the buffer used for reading and writing data during the backup.

Default

Sets the default backup buffer size, which is 32 kB.

Apply Template

Apply one of the available templates to the backup specification.

The following may be helpful:

- For a description of a predefined template, position the cursor over the template.
- To customize the view, use the buttons above the Apply options field.

Apply options

(Availability of these depends on the selected template.)

You can apply certain options specified in the template to your backup specification.

Destination

Backup device settings apply to the backup specification.

Backup specification

Backup specification options apply to the backup specification.

Filesystem

Filesystem options apply to all filesystem objects of the backup specification.

Force to defaults

Filesystem options apply to all filesystem objects of the backup specification for which you have changed options in the Backup Object Summary page. ==Trees Tree options apply to the backup specification.

Schedule

Schedule settings apply to the backup specification.

Backup options

(These options are not available in this window. You must specify the backup type, subtype, and load balancing when creating a new backup specification.)

Specify Calendar Dimensions

In this page you set the dimensions of the calendar.

Calendar minimum size

Set the minimum width and height of the months. Use the preferred unit. You can choose between millimeters and pixels. The default width and height are 59 and 49 mm, respectively.

Calendar title percentage

Set the size of the month titles. The default is 22 percent.

Change Group

Specify the group to which the backup specification or template will be moved.

Name

Select an existing group from the drop-down list, or enter a name for a new one. In the latter case, the group will be created automatically.

Choose Cell Manager

Choose the Cell Manager where you want to start a new backup task and click OK.

Name

In the drop-down list, select one of the available Cell Managers.

Choose Template Type

Choose a type of template that you want to create (for example, Filesystem). The template types available in the drop-down list depend on the Data Protector components installed.

Choose Template Type

Choose the type of template that you want to create (for example, Filesystem), and the Cell Manager where you want the template to be created.

Type

Select the desired template type. The template types available in the drop-down list depend on the Data Protector components installed.

Cell Manager

Select the desired Cell Manager.

Object Properties - DB2

The options in this page apply only to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

General Integration Information

Client

The system from which you back up the object.

Instance Name

The name of the instance from which you back up the object.

Object

The name of your backup object.

Offline Backup

Select this option to back up the object offline.

Configure DB2

In this page you configure the DB2 integration.

General integration object information

Client

The system from which you back up the object.

Object

The name of your backup object.

Connection

Login

The username of the DB2 user. This is a DB2 user registered in the operating system and given either the SYSADM, SYSCTRL, or SYSMAINT DB2 authorities in order to perform backup and restore-related operations.

Password

The password of the user.

DB2 EEE

Select this option if you have a partitioned environment.

DB2 Home Directory

The home directory of the DB2 instance.

Start Backup - DB2

Select the backup type and network load for the backup.

Backup type

Full

Backs up all selected DB2 objects regardless of whether they have been changed after the last backup was made. Some data, such as database configuration, history file, which is important for restore, is included into the full backup automatically.

Incremental

Backs up all the changes made to the database after the last full backup.

Delta

Backs up all the changes made to the database from the last backup of any kind (full, incremental, delta).

Network Load

Prerequisite To perform incremental or delta backup, the DB2 trackmod parameter must be set to ON.

Start Preview - DB2

Select the backup type and network load for the preview.

Backup type

Full

Backs up all selected DB2 objects regardless of whether they have been changed after the last backup was made. Some data, such as database configuration, history file, which is important for restore, is included into the full backup automatically.

Incremental

Backs up all the changes made to the database after the last full backup.

Delta

Backs up all the changes made to the database from the last backup of any kind (full, incremental, delta).

Network Load

Prerequisite To perform incremental or delta backup, the DB2 trackmod parameter must be set to ON.

Add/Remove Disk Image Sections

Enter one or more raw logical volumes that you want to back up. Note that every raw logical volume results in a separate backup object.

New disk image section

Enter a raw logical volume and click **Add**. Use the following format, for example: `/dev/c15t2dx/r9376` To remove a raw logical volume, select it and click **Delete**.

Disconnect Network Shares

Select one or more available shared disk(s) from which you want to disconnect and click**OK**.

Browse Network Shares

In this page, browse for the destination where you want the RID (recovery information data) file to be stored after the backup session successfully finishes. If you want to select more destinations, use Apply.

Client system

(not available in this window)

Share name

Once you have browsed for the shared disk(s), the share name is displayed here. You can enter the share name if you know it (for example, \\AZTEC\DISKC).

Connect as

Enter your user name.

Shared directories

Browse for the shared disk(s) where you want to store the RID file.

One Button Disaster Recovery - Destination Property Page

Select the OBDR device to use for your backup. Only one device or drive can be selected.

Prerequisites

- Before adding an OBDR device, create a media pool for DDS and LTO media with a Non-appendableusage policy and Loose allocation policy. The media pool must be selected as the default media pool for the OBDR device. This device must be connected locally to the client.

Show selected

If this option is selected, only selected devices are displayed.

Show all

If this option is selected, all configured devices on the system are displayed.

Properties

(not available in this window)

Source Property Page

Select the system that you want to back up. This can only be a Data Protector client.

One Button Disaster Recovery - Source Property Page

Select the objects that you want to back up. Partitions important for One Button Disaster Recovery are selected automatically and you cannot deselect them. Additionally, select any other partitions that you find important so that you will be able to recover them.

Show

In the first drop-down list, select which systems will be displayed, depending on the OS platform or their selection for backup. In the second drop-down list, only Filesystem Backup is available.

Map Network Share

(not available in this window)

Disconnect Share

(not available in this window)

Add/Remove

(not available in this window)

Enter Network Password

Enter a user name and password. To access a shared disk, the user needs to have appropriate permissions.

Configure User Credentials for Exchange Remote Powershell Cmdlet Operations

In the Microsoft Exchange Server 2013 environment, this dialog box is displayed if no valid user credentials for executing the Exchange Management cmdlet operations remotely are specified.

Enter the Exchange domain user credentials that Data Protector should use to execute the Exchange Management cmdlet operations as part of Microsoft Exchange Server backup and restore operations.

Client and Application Database Select - Microsoft Exchange Server

Select the client system and the application that you want to back up.

Client

Select the client system in your cell that has the application to be backed up.

Application database

Select the instance of the Microsoft Exchange Server to be backed up.

Specify OS user

It is not mandatory to specify the **Username** and **Group/Domain name** options. If they are not specified, the backup runs under the Local System Account.

Username

Specify the user name.

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name Admin istrator , domain DP). Ensure that this user has been added to the Data Protector admin or operator user group, has the Exchange Server rights to back up the database, and has been set up for the Data Protector Inet service user impersonation.

This user becomes the backup owner.

Client and Application Database Selection - Microsoft Exchange Server

Select the client system and the application that you want to back up.

Client

Select the client system in your cell that has the application to be backed up.

Application database

Select the application database to be backed up. Select one of the following:

Microsoft Exchange Server (Microsoft Information Store)

Select this to back up the Information Store.

Microsoft Exchange Server (Microsoft Key Management Service)

(available if KMS is installed)

Select this to back up the Key Management Service.

Microsoft Exchange Server (Microsoft Site Replication Service)

(available if SRS is installed)

Select this to back up the Site Replication Service.

User and group/domain

(these options are disabled in this window)

Application Specific Options - Microsoft Exchange Server Integration

In this page, specify the options that apply to the Microsoft Exchange Server backup.

General Information

- Pre-exec
- Post-exec

Consistency check

- Perform consistency check
- Check log files only

(available if the **Perform consistency check** is selected)

- Throttle check for 1 second every I/O operations

(available if the **Perform consistency check** is selected)

Backup Policy - Microsoft Exchange Server Integration

In this page, specify your backup policy.

Backup policy

Back up active database

Select this option to back up the active copy.

Back up passive copy

Select this option to back up a passive copy. If a database has multiple passive copies, specify which particular copy you want to back up, using one of the following options:

- Passive copy policy

(available if the Back up passive copy is selected)

Use active copy for backup if no passive copies are available

(available if the Back up passive copy is selected)

Select this option to back up the active copy when no passive copy is available.

Back up all copies

(available if only one database is selected for backup)

This option should only be used in ZDB environments. Otherwise, it is enough that a single copy is backed up; you can restore different copies of a database from the backup of a single copy.

Select this option to back up all copies (active and passive). This is useful when you create ZDB-to-disk or ZDB-to-disk+tape backups (that is, backups that can be used for instant recovery). If multiple copies are backed up, multiple copies can be restored, as each copy has its own replica volumes to be restored from.

When you create a ZDB-to-tape backup, it is enough that a single copy is backed up; you can restore different copies of a database from the ZDB-to-tape backup of a single copy.

Exclude clients from backup

Specify from which clients database copies should not be backed up.

Client and Application Database Selection - Microsoft Exchange Server Integration

In this page, the client and the application database is displayed.

Application

Client

(not available)

The client that you specified in the **Application system** option is displayed.

Application database

(not available)

The Microsoft Exchange Server is displayed.

View type

(available if a DAG virtual system (host) is selected in the **Application system**)

Specify **View Type** to define how Microsoft Exchange Server databases should be organized in the next page (source page):

By Role

All databases in the DAG are displayed.

By Client

All clients in the DAG are displayed, together with all the databases (active or passive) residing on them. Active databases have the label (active) appended at the end. Passive databases have no label.

User and group/domain

Specify OS user

It is not mandatory to specify the **Username** and **Group/Domain name** options. If they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run. Ensure that this user has been added to the Data Protector admin or operator user group and has been set up for the Data Protector Inet service user impersonation.

This user becomes the backup owner.

Start Backup - Microsoft Exchange Server Integration

Select a backup type and network load for the backup session.

Backup type

- Full
- Copy
- Incr
- Differential

An incremental backup session cannot be followed by a differential backup session, nor the other way around. You must first run a full backup session.

- Network Load
- Snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled)

Start Preview - Microsoft Exchange Server Integration

Select a backup type and network load for the preview backup session.

Backup type

- Full
- Copy
- Incr
- Differential

An incremental backup session cannot be followed by a differential backup session, nor the other way around. You must first run a full backup session.

- Network Load
- Snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Object Properties - Other

The options in this page apply to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

- Enhanced incremental backup
- Use native Filesystem Change Log Provider if available
- Software compression
- Display statistical info
- Lock files during backup
- Do not preserve access time attributes
  (selected and disabled with the Use native Filesystem Change Log Provider if available option)
- Backup POSIX hard links as files
- Copy full DR image to disk

Data security

- None
- AES 256-bit
- AES 256-bit
- Encode

Logging

(not available for disk image backup)

- No Log
- Log All
- Log Directories
- Log Files

Backup files of size

- All sizes
- Bigger than (in KB)
- Smaller than (in KB)
- Range (in KB)

User defined variables

Click Edit to configure backup variables to enable flexible operation on some platforms and integrations.

Object Properties - Disk Image Options

In this page you can add or remove disk image sections. With NDMP, you can only review the object selection.

Sections

Enter a section and click **Add**. Use the following format:

UNIX systems:

/dev/rdsk/Filename ,for example: /dev/rdsk/c2t0d0

Windows systems: You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk. In case of ZDB, you must use the second way:

Windows systems: You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk. In case of ZDB, you must use the second way. In case of ZDB to tape using the 3PAR SMI-S Agent, you can also use the first way:

- \\.\DriveLetter: , for example: \\.\E :

When a drive letter is specified for the volume name, the volume is not being locked during the backup. A volume that is not mounted or mounted as an NTFS folder cannot be used for disk image backup.

- \\.\PHYSICALDRIVE# , where # is the current number of the disk you want to back up. For example: \\.\PHYSICALDRIVE3

To remove a section from the backup specification, select it and click **Delete**.

Object Properties - Edit Filters

In this page, you can select the types of files to be included in the backup or excluded from it. These options are not supported with Data Protector NDMP server integration.

Onlys

Use wildcard characters to back up only files that match specific criteria. For example, if you enter *.exe, only files with the extension .exe will be backed up.

Skips

Use wildcard characters to exclude files that match specific criteria from backup. For example, if you enter *.exe, files with the extension .exe will not be backed up.

Object Properties - General

The options in this page apply only to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

Client system

The client system from which you back up the object.

Object type

The type of your backup object.

Description

The description of your backup object.

Source

The pathname of your backup object.

Device

The device that will be used for backing up this object, unless the backup is load balanced.

Object Properties - NDMP

The options in this page apply only to the selected backup object.

NDMP User Override

For each backup object, you can specify a user name and password, which overrides the User name and Password values entered in the Import NDMP Host dialog box during the import of the NDMP Server to the Data Protector cell. Access rights must be set properly on the NetApp or Celerra host in order to apply user name and password overrides.

NetApp Options

Advanced

Click here to specify NDMP environment variables for a specific NDMP implementation.

NDMP backup type

- dump
- SMTape

Object Properties - NDMP - Celerra

The options in this page apply only to the selected backup object.

NDMP User Override

For each backup object, you can specify a user name and password, which overrides the User name and Password values entered in the Import NDMP Host dialog box during the import of the NDMP Server to the Data Protector cell.Access rights must be set properly on the NetApp or Celerra host in order to apply user name and password overrides.

Celerra Options

Advanced

Click here to specify NDMP environment variables for a specific NDMP implementation.

NDMP backup type

- dump
- NVB

Object Properties - Options

The options in this page apply only to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

If you schedule the backup and set the Protection option different from Default in the Schedule wizard, it will override the selection made in this page.

- Public
- Report level
- Pre-exec
- Post-exec
- Protection
- Catalog protection

Object Properties - Tree/Filters

The options in this page apply only to the selected backup object. If no files or directories are specified, the entire object is selected for backup. These options are not supported with Data Protector NDMP Server integration.

Trees

Enter the pathname of files or directories that you want to include for backup, and click Add. See the Example below.

Filter

Click here to select the types of files to be included in the backup or excluded from it.

Excludes

Enter the pathname of files or directories that you want to exclude from backup, and click Add. See the Example below.

For backup objects of the Client System type, you can modify the meaning of the Trees and Excludes backup options so that Data Protector interprets the specified directories as volumes and not as filesystem directory trees. Consequently, different data is backed up. To modify the meaning, use global options as described in the example below.

The global options have no effect on backup objects of the Filesystem or any other type.

On Linux systems, when you create a backup specification with the CONFIGRATION/SYSTEMRECOVERYDATA object selected, the folders /opt/omni/bin/drim/log and /opt/omni/bin/drim/tmp are by default excluded from the backup. However, this exclusion is not set if you manually update existing backup specifications.

Example:

- “Client System”/ “Host” (Checked checkbox next to client in backup specification):
  Tree: C:\
  Exclude: C:\folderToExclude

Above example only selects “C:” mountpoint on host for backup and excludes “folderToExclude” folder on “C: “.
In Unix: same without drive letter, only “/”.

- “Filesystem Windows/Unix” (Checked checkbox next to mountpoint or folder in backup specification):
  Tree: \folder
  Exclude: \folder\folderToExclude
  Above example selects “folder” and excludes “folderToExclude” on all selected filesystems.

Object Properties - WinFS Options

The options in this page apply only to the selected backup object. To change options for all objects, close this dialog and return to the Options property page.

- Report open locked files as

Open files

- Number of retries
- Time out
- Detect NTFS hardlinks
- Do not use archive attribute
- Backup share information for directories
- Asynchronous reading
- De-duplication volume backup

MS Volume Shadow Copy Options

- Use Shadow Copy
- Allow fallback (available if the **Use Shadow Copy** option is enabled)

Backup Options - 3PAR StoreServ Storage

The options in this page apply to the entire backup specification created for the 3PAR StoreServ Storage.

Client systems

This set of options can only be modified after the backup specification has been saved.

- Application system
- Backup system

Replication mode

3PAR Local copy

Select this option to configure a ZDB backup specification for 3PAR storage systems in normal scenarios.

3PAR Remote copy

Select this option to configure a ZDB backup specification for 3PAR storage systems, which are part of the remote copy group, in failover scenarios.

Replica handling during failover scenarios

Follow direction of replication

This option is only available if 3PAR Remote Copy option is selected.

Select to follow the replication direction and create replicas on the disk array remote to the current source. After a failover, the replication direction is reversed and the replicas are created on the disk array that was originally a source 3PAR storage system. **Maintain replica location** This option is only available if 3PAR Remote Copy option is selected.

Select to maintain replica location and create replicas on the disk array remote to primary array. After a failover, replicas will continue on the destination disk array that became the primary 3PAR storage system during the failover.

Snapshot management options

Snapshot type

The only available snapshot type is virtual copy.

Replica management options

- Keep the replica after the backup
- Number of replicas rotated
- Track the replica for instant recovery

Application system options

- Dismount the filesystems on the application system before replica generation
- Stop/quiesce the application command line
- Restart the application command line

Backup system options

- Use the same mountpoints as on the application system
- Root of the mount path on the backup system
- Add directories to the mount path
- Automatically dismount filesystems at destination mountpoints
- Leave the backup system enabled
- Enable the backup system in read/write mode

Backup Options - Other

The options in this page apply to the entire backup specification.

Reconnect broken connections

This option is useful if you have, for example, the Cell Manager on one LAN and Disk Agents or Media Agents on another, assuming that the connection between these two LANs is unreliable (WAN connections).

Ownership

Make sure to specify the information as it was specified when the user was configured.

Ownership is assigned only if you save your backup specification before you start the backup.

- User: Enter the name of the user who will be the owner of the backup specification. Use uppercase characters on Windows systems.
- Group: Enter the user's domain or UNIX group. Use uppercase characters on Windows systems.
- System: Enter the user's client system. Use uppercase characters on Windows systems.

Backup Options - Clustering

The cluster options in this page apply to the entire backup specification.

If a failover of Data Protector happens during backup, all running and pending backup sessions fail. Use the Automatic session restart options to define Data Protector behavior after the failover.

When a cluster-aware application other than Data Protector is running on another node and fails over to the node where Data Protector is running, it is possible to control the load on this system. Use the Abort session parameters and Abort ID parameters options together with the omniclus command to define the Data Protector behavior after the failover.

Automatic session restart

Specify the objects that will be restarted after a failover of Data Protector.

- Do not restart backups at failover
- Restart backup of failed objects
- Restart backup of all objects

Abort session parameters

Specify when to abort sessions based on how long they have been running. For example, Data Protector can abort the session if it has been running for less than 10 minutes.

- Do not check elapsed session time

Abort if less than

When a failover occurs and the `omniclus` command is started, Data Protector aborts the session if it has been running for less than the number of minutes specified in this option.

Abort if more than

When a failover occurs and the `omniclus` command is started, Data Protector aborts the session if it has been running for more than the number of minutes specified in this option.

Abort ID parameters

Specify an abort ID for the backup specification. For example, Data Protector can abort all running sessions, except for the one with a certain abort ID.

- Don't check abort ID
- Check against abort ID

Backup Options - SSEA

The options in this page apply to the entire backup specification.

Pre-exec

- On client: In the drop-down list, select the client system on which the pre-exec command will be executed.

Post-exec

- On client: In the drop-down list, select the client system on which the post-exec command will be executed.

Reconnect

- Reconnect broken connections: This option is useful if you have, for example, the Cell Manager on one LAN and Disk Agents or Media Agents on another, assuming that the connection between these two LANs is unreliable (WAN connections).

Ownership

Make sure to specify the information as it was specified when the user was configured.

Ownership is assigned only if you save your backup specification before you start the backup.

- User: Enter the name of the user who will be the owner of the backup specification. Use uppercase characters on Windows systems.
- Group: Enter the user's domain or UNIX group. Use uppercase characters on Windows systems.
- System: Enter the user's client system. Use uppercase characters on Windows systems.

Backup Options - Storage Provider

The options in this page apply to the entire backup specification created for the NetApp Storage and 3 PAR StoreServ Storage families.

Client systems

This set of options can only be modified after the backup specification has been saved.

- Application system
- Backup system

Add Storage Provider

Select and configure the storage providers, which you want to use for backup.

Add...

Click to select the storage provider, configure the provider-specific options, and add it to a list.

Edit...

Click to edit the selected storage provider.

Remove

Click to remove the selected storage provider from the list.

Storage provider:

Select the storage provider you want to use for backup.

Replica management options

(available only with 3 PAR Storage Provider)

- Keep the replica after the backup
- Number of replicas rotated
- Track the replica for instant recovery

Application system options

- Dismount the filesystems on the application system before replica generation
- Stop/quiesce the application command line
- Restart the application command line

Backup system options

- Use the same mountpoints as on the application system
- Root of the mount path on the backup system
- Add directories to the mount path
- Automatically dismount filesystems at destination mountpoints
- Leave the backup system enabled
- Enable the backup system in read/write mode

Copy As

Enter a new name for the backup specification or template and specify the group for it.

Name

You can use only alphanumeric and the following characters:

_ - ( ) .

Group

Select an existing group from the drop-down list, or enter a name for a new one. In the latter case, the group will be created automatically.

Create New Backup

Select one of the available templates that you want to use for the backup. Data Protector offers you a default template for each object type you are configuring the backup specification for:

- Blank Filesystem Backup for a filesystem, disk image, or application backup
- Blank Internal Database Backup for backup of the Data Protector Internal Database

In a default template, there are no objects or devices selected, and options have default values.

The following may be helpful:

- For a description of a predefined template, position the cursor over the template.
- To customize the view, use the buttons above the Apply options field.

Apply options

(not available with default templates and integration templates) When configuring a new backup, you can apply the following options specified in your template:

Destination

Backup device settings apply to the backup specification.

Backup specification

Backup specification options apply to the backup specification.

Filesystem

Filesystem options apply to all filesystem objects of the backup specification.

Force to defaults

(not applicable in this dialog)

Trees

Tree options apply to the backup specification.

Schedule

Schedule settings apply to the backup specification.

Backup options

Backup type

(available items depend on the object type you are configuring the backup specification for)

- For backups using data movement technology, select **Data mover backup**. You need to have the NDMP Media Agent installed on at least one client in your cell to gain access to this functionality.
- For local and network backups, select **Local or network backup**.
  This is the only backup type available for Internal Database backup objects.
- The **Direct backup** selection relates to the functionality that is officially no longer supported in the installed Data Protector version.
- For backups using snapshot or split mirror functionality (zerodowntime backup), select **Snapshot or split mirror backup**. Youneed to have either a disk array integration installed on at least one client in your cell to

gain access to this functionality.
Zero downtime backup is not available for the Data Protector Internal Database and most Data Protector software integrations.

- For VSS transportable backups, select **VSS transportable backup**. A hardware shadow copy provider is required for this functionality.
- For backups to IAP, select **Backup to IAP**. You need to have the IAP Disk Agent Extension and IAP Deduplication Agent installed on at least one client in your cell to gain access to this functionality. The backup sub type is automatically set to **CSF-R**.
- For RMC Integration backups, select **StoreOnce RMC**. As a prerequisite, you must add the RMC server details using the

command line interface.
- Load balanced

Sub type

(what is available here depends on your backup typeselection)

Select the desired backup subtype.

- Source-side deduplication

Change Order of Devices

If the backup is load balanced, you can set the order in which Data Protector uses the devices during the backup.

Select a device and use the **Move up** and **Move down** buttons.

Device Properties - General

In this page you can set options for the selected backup device.

CRC check

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during backup. The CRC checks allow you to verify the media after the backup. Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying media or verifying objects. By default this option is not selected.

This option can be specified for backup, object copy, and object consolidation operations.

Concurrency

(not available for Backup to Disk devices)

Concurrency allows more than one Disk Agent to write to one backup device concurrently. This helps Data Protector keep the device streaming because it can accept data faster than a Disk Agent can send it. The data from these Disk Agents is interleaved on the media.

The maximum concurrency value is 32.

Data Protector provides default concurrencies for all supported devices. The maximum device concurrency for devices that are used for backingup Microsoft Exchange Server data is 2 for devices connected to the ExchangeServer system directly and 1 for those connected to the Exchange Server systemremotely.

Specify the number of Disk Agents that can write concurrently to a device. This option can be specified for backup, object copy, and object consolidation operations.

Rescan

(not available for Backup to Disk devices)

If this option is selected, Data Protector updates repository information before starting your backup. This is useful when you manually change the media order in the slot or enter and eject media.

Drive-based encryption (not available for Backup to Disk devices)

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media.

- Media pool
- Prealloc list

(not available for Backup to Disk devices)

Add

Click here to display a list of media that can be added to the prealloc list.

Delete

Removes the selected medium from the prealloc list.

Use preferred Multipath host

(available for MultiPath devices) If this option is selected, you can select a preferred host from the drop down list. During a

backup session, Data Protector will try to use this host first, regardless of the predefined order.

Server-side deduplication

(not available for source-side deduplication gateways)

Enables server-side deduplication.

Default: Selected.

Max. Number of Parallel Streams per Gateway

Limits the number of streams on each gateway (you can specify up to a maximum of 100 streams).

If this option is not selected, the number of streams is not limited. Default: not selected.

Disk Image Specific Options

These options apply to all disk image objects that you select for your backup.

Sections

Enter a section and click **Add**. Use the following format:

UNIX systems:

/dev/rdsk/Filename , for example: /dev/rdsk/c2t0d0

Windows systems: You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk. In case of ZDB, you must use the second way:

Windows systems: You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk. In case of ZDB, you must use the second way. In case of ZDB to tape using the 3PAR SMI-S Agent, you can also use the first way:

- \\.\DriveLetter: , for example: \\.\E:

When a drive letter is specified for the volume name, the volume is not being locked during the backup. A volume that is not mounted or mounted as an NTFS folder cannot be used for disk image backup.

- \\.\PHYSICALDRIVE# , where # is the current number of the disk you want to back up. For example: \\.\PHYSICALDRIVE3

To remove a section from the backup specification, select it and click **Delete**.

Select Backup Object - Manual Add

Specify the type of object that you are adding to the backup specification.

UNIX filesystem

Select this to perform a UNIX filesystem or NFS backup.

Windows filesystem

Select this to perform a Windows filesystem backup.

OmniStorage VBFS

(this option is no longer available in the installed Data Protector version)

Client system object

Select this to perform a client system object backup.

Internal Database

(this option is no longer available in the installed Data Protector version)

Microsoft network share

(valid for Windows clients; not supported for VSS backup)

Select this to perform a Microsoft network share backup.

Disk image object

Select this to perform a disk image backup.

General Selection

Select the client and mount point or drive for the backup. If the backup is not load balanced, you need to specify the device that will be used.

Client system

Select the client where the object to be backed up is located.

Mount point

Select the mount point or drive that you want to back up.

Device

(not available with load-balanced backup)

If your backup is not load balanced, you need to select a device that will be used to back up this object. You can choose among the devices you have selected in the Destination property page of the backup specification.

Description

Enter a description to help you identify the object.

Browse Network Shares

Specify the desired network shared disks for backup.

You must change the Data Protector Inet account on the Disk Agent client in order to establish the required permissions to access the shared disk that you want to back up.

Microsoft network share backup is valid only for Windows clients.

Client system

Select the client system with the Disk Agent to be used for your backup. This must be a Windows system.

Share name

Type the share name (for example, \\AZTEC\DISKC), or browse for it if possible.

Connect as

Type your user name.

Shared directories

Specify the directories/files that you want to back up. Once you have connected to a share, you can browse its files and directories in the Source property page (unless you have connected via the Manual Add wizard). Browsing of Windows systems is not supported on UNIX systems.

Mirror Options

By default, devices used for writing mirrors are selected automatically. In this page, you can specify which device will be used for writing a specific mirror of the selected backup object.

To change the device for a mirror, make sure the mirror is selected, highlight the mirror, and select a device from the Device drop-down list.

You can also deselect a mirror for the selected backup object.

Filesystem/Disk Image Options - Other

This topic lists the advanced options applicable for the backup object. Most of the options apply for the Filesystem backup object. If the option does not apply for the backup object, it is either greyed out or is not listed. For example: **Enhanced incremental backup** option applies to only Filesystem backup objects, **No fallback to full** option applies to only incremental Block-based backup objects, where as **Display statistical info** applies to all types of backup objects.

- Enhanced incremental backup
- Use native Filesystem Change Log Provider if available
- Software compression
- Display statistical info
- Lock files during backup
- Backup POSIX hard links as files
- Do not preserve access time attributes
  (selected and disabled with the **Use native Filesystem Change Log Provider if available** option)
- Copy Recovery Set to disk
- No fallback to full

Data security

(Not applicable for block-based backup.)

- **None:** This data security option provides no protection. By default, the data security is set to None.
- **Encode:** Data Protector recommends using AES 256-bit encryption for data security during backup. Data Protector displays an error message when less-secure option Encode is selected.
- **AES 256-bit:** (Recommended option) Select this option to enable software encryption to protect your data. Data is encrypted before it is transferred over the network and before it is written to media. However, if you select AES-256 for data security, the Disk Agent will switch to Federal Information Processing Standard (FIPS) mode for data encryption.

Logging

(Not applicable for disk image backup and block-based backup.)

- **No Log**
- **Log All**
- **Log Directories**
- **Log Files**

Backup files of size

(Not applicable for disk image backup and block-based backup.)

- **All sizes**
- **Bigger than (in KB):** Specify the minimum file size to be backed up, in KB.
- **Smaller than (in KB):** Specify the maximum file size to be backed up, in KB.
- **Range (in KB):** Specify the file size range to be backed up, in KB.

User defined variables

(Not applicable for disk image backup and block-based backup.)

Click **Edit** to set backup variables to enable flexible operation on some platforms and integrations.

Filesystem/Disk Image Options

The options in this page apply to all objects of the filesystem, disk image, and block-based backup. To change options for a specific backup object, select that object's properties in the Backup Object Summary page of the backup specification.

- Public
- Report level
- Pre-exec
- Post-exec
- Catalog protection

Filesystem Options - WinFS Options

The options in this page apply to all Windows filesystem objects in this backup specification. To change options for a specific backup object, select that object's properties in the Backup Object Summary page of the backup specification.

- Report open locked files as

Open files

- Number of retries
- Time out
- Detect NTFS hardlinks
- Do not use archive attribute
- Backup share information for directories
- Asynchronous reading
- De-duplication volume backup

MS Volume Shadow Copy Options

- Use Shadow Copy
- Allow fallback
  (available if the **Use Shadow Copy** option is enabled)

Start Preview

Select the backup type and network load for the preview.

Backup type

- Full
- Incr
- Incr1-9
- Network Load

Preview is not available for zero downtime backup (ZDB).

Configure 3PAR StoreServ Storage

In this page, you configure the 3PAR StoreServ Storage integration for backup.

Client systems

- Application system
- Backup system

Replication mode

3PAR local copy

This is the only replication mode available.

Snapshot management options

Snapshot type

The only available snapshot type is virtual copy.

Replica management options

- Keep the replica after the backup
- Number of replicas rotated
- Track the replica for instant recovery

Application system options

- Dismount the filesystems on the application system before replica generation
- Stop/quiesce the application command line
- Restart the application command line

Backup system options

- Use the same mountpoints as on the application system
- Root of the mount path on the backup system
- Add directories to the mount path
- Automatically dismount filesystems at destination mountpoints
- Leave the backup system enabled
- Enable the backup system in read/write mode

Backup Object Summary

This page displays a summary of the backup specification.

All objects selected for backup are listed. For each backup object, the following is indicated: client, source, type, description, device order. In general, backup objects are processed in the same order as listed here. In complex environments, the order may change due to other factors, for example, load balancing functionality.

The following may be helpful:

- To change the position of a backup object, right-click the object and click **Move up** or **Move down**.
- You can copy options from an existing object in the backup specification to another object in the same backup specification. Use the right-click menu options **Copy options** and **Paste options**. Note that trees, filters, and exclude lists options will not be copied.

Manual Add

Click here to add objects to your backup specification manually. This option is disabled for block based backup.

Delete

Removes the selected object(s) from the backup specification.

Change device

(available for backup specifications that are not load balanced)

Click here to change the device for the selected object.

Change Mirror

Click here to change mirror options for the selected object.

Properties

Click here to view properties of the selected object or specify additional options for the object.

Destination Property Page - Mirror

In this page you select the devices to be used for the selected mirror from the list of configured devices.

Specify separate devices for the backup and for each mirror. Block size of the devices must not decrease within a mirror chain: the devices used for writing mirror 1 must have the same or a larger block size than the devices used for backup; the devices used for writing mirror 2 must have the same or a larger block size than the devices used for writing mirror 1, and so on.

Description

Type a description for the mirror.

Show selected

If this option is selected, only the selected devices are displayed.

Show all

If this option is selected, all configured devices in the cell are displayed.

Properties

(available when a selected device is highlighted)

Displays properties of the selected device.

Load balancing

By default, object mirroring is load balanced. If you do not want this mirror to be load balanced, specify which devices to use for individual objects in the Backup Object Summary.

Min

The minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be started) required for starting the session. If fewer devices are available than specified here, the session will queue. The default is 1.

Max

The maximum number of available devices that Data Protector will use in the session. The highest number you can specify here is 32. The default is 5.

Add Mirror

To add a mirror, click this button.

Remove Mirror

To remove the selected mirror, click this button.

Move Mirror <

To move the selected mirror towards the beginning of the mirror chain, click this button.

Move Mirror >

To move the selected mirror towards the end of the mirror chain, click this button.

Destination Property Page - Backup

In this page you select the devices to be used for the backup from the list of configured devices.

You can mirror the backup objects to one or more additional media sets. Specify separate devices for the backup and for each mirror. Block size of the devices must not decrease within a mirror chain: the devices used for writing mirror 1 must have the same or a larger block size than the devices used for backup; the devices used for writing mirror 2 must have the same or a larger block size than the devices used for writing mirror 1, and so on.

Limitations

- It is not possible to mirror objects backed up using the ZDB to disk or NDMP backup functionality.

Show all devices

Displays all configured devices in the cell.

Show selected devices

Displays only the selected devices.

Show selected devices (filtered)

Displays only the devices that were selected by using device filter options.

Set filter...

(available when the **Show selected devices (filtered)** option is selected)

Enables you to specify device filter options to narrow the scope of displayed devices. Click this button to enter new parameters or modify ones that are already specified by using the available filters. On how to use the filter settings, see the Using the Filter Settings task topic below.

Properties

(available when a selected device is highlighted)

Displays properties of the selected device.

- Load balancing

Load balancing

(If this option was selected in the Create New Backup dialog (the default), you cannot deselect it. If it is not selected, you can select it here, but this action is irreversible.)

Add Mirror

To add a mirror, click this button.

Remove Mirror

To remove the selected mirror, click this button.

Move Mirror <

To move the selected mirror towards the beginning of the mirror chain, click this button.

Move Mirror >

To move the selected mirror towards the end of the mirror chain, click this button.

Options Property Page

In this page you can set backup options for all objects in this backup specification. To set further options, click the appropriate **Advanced button**.

If you schedule the backup and set the **Protection** option different from **Default** in the Schedule wizard, it will override the selection made in this page.

Backup Specification options

Description

Type a description of your backup specification.

Filesystem Options

(available for filesystem backup)

- Protection

Disk Image or Block based options

(available in a saved backup specification for disk image and block based backup)

- Protection

Backup to Disk Device options

- Source-side deduplication
- Disable policy

Save, Start or Preview Backup

You can save, start, or preview the backup you have configured.

Save As

Click the button to save the backup specification.

Save and Schedule

Save and schedule the backup using Data Protector Scheduler.

Start Interactive Backup

Click the button to start the backup.

Start Interactive Preview

Click the button to preview the backup. Note that preview is not supported for some integrations and for ZDB.

Source Property Page

In this page you select objects to be backed up.

On UNIX systems, if you intend to perform instant recovery, select all filesystems inside the volume group to be backed up. Otherwise, instant recovery will not be possible using the Data Protector GUI or (if you perform instant recovery using the Data Protector CLI) data can be corrupted.

Show

In the first drop-down list, select which systems will be displayed, depending on the OS platform or their selection for backup.

In the second drop-down list, select between the following:

Filesystem backup

Select this to back up objects of clients in your cell.

Network share backup

(available for Windows clients; not available for VSS backup)

Select this to back up network shared filesystems. The systems need to have a Data Protector Disk Agent installed.

Block based backup

(available for Windows x64 clients only)

Select this to perform block based filesystem backup of clients on your cell.

Map Network Share

(available when Network share backup is selected)

Click here to select the client system with the Disk Agent to be used for your backup and specify the shared disk(s) to be backed up.

Once you have connected to a share, you can browse its files and directories in the Source property page. Browsing of Windows systems is not supported on UNIX systems.

Disconnect Share

Disconnects from shared disks.

Add/Remove

(available for NDMP)

Click here to add or remove disk mountpoints.

Source Property Page

This page displays the objects selected for backup in the backup specification.

Show

In the first drop-down list, select which systems will be displayed, depending on the OS platform or their selection for backup.

In the second drop-down list, select between the following:

Filesystem backup

Select this to back up objects of clients in your cell.

Network share backup

(available for Windows clients; not available for VSS backup)

Select this to back up network shared filesystems. The systems need to have a Data Protector Disk Agent installed.

Block-based backup

(available only for Windows x64 clients)

Select this to perform block-based backup of objects in your cell.

Map Network Share

(available when Network share backup is selected)

Click here to select the client system with the Disk Agent to be used for your backup and specify the shared disk(s) to be backed up.

Once you have connected to a share, you can browse its files and directories in the Source property page. Browsing of Windows systems is not supported on UNIX systems.

Disconnect Share

Disconnects from shared disks.

Add/Remove

(available for NDMP) Click here to add or remove disk mountpoints.

Configure

In this page, you configure the P9000 XP Disk Array Family integration for backup.

Client systems

- Application system
- Backup system

Mirror type

- Business Copy P9000 XP
- Continuous Access P9000 XP
- Combined (Continuous Access P9000 XP + Business Copy P9000 XP)
- MU number(s)

Replica management options

- Keep the replica after the backup
- Track the replica for instant recovery

At the start of the session

- Synchronize the disks if not already synchronized
- Abort the session if the mirror disks are not already synchronized

At the end of the session

- Prepare the next mirror disk for backup (resynchronize)

Application system options

- Dismount the filesystems on the application system
- Stop/quiesce the application command line
- Restart the application command line

Backup system options

- Use the same mountpoints as on the application system
- Root of the mount path on the backup system
- Add directories to the mount path
- Automatically dismount filesystems at destination mountpoints
- Leave the backup system enabled
- Enable the backup system in read/write mode

The single-host (BC1) configuration, in which a single system acts as the application system and the backup system, is not supported on Linux platform.

The BC1 configuration is also not recommended because of performance issues. Only disk image and filesystem backups are possible with a BC1 configuration.

Configure Storage Provider

In this page, you configure the NetApp Storage and 3 PAR StoreServ Storage for backup.

Client systems

- Application system
- Backup system

Add Storage Provider

Select and configure the storage providers, which you want to use for backup.

Add...

Click to select the storage provider, configure the provider-specific options, and add it to a list.

Edit...

Click to edit the selected storage provider.

Remove

Click to remove the selected storage provider from the list.

Storage provider:

Select the storage provider you want to use for backup.

Replica management options

(available only with 3PAR Storage Provider)

- Keep the replica after the backup
- Number of replicas rotated
- Track the replica for instant recovery

Application system options

- Dismount the filesystems on the application system before replica generation
- Stop/quiesce the application command line
- Restart the application command line

Backup system options

- Use the same mountpoints as on the application system
- Root of the mount path on the backup system
- Add directories to the mount path
- Automatically dismount filesystems at destination mountpoints
- Leave the backup system enabled
- Enable the backup system in read/write mode

Save As

Enter a name for the new backup specification or template and specify the group for it.

Name

You can use only alphanumeric and the following characters:

_ - ( ) .

Group

Select an existing group from the drop-down list, or enter a name for a new one. In the latter case, the group will be created automatically.

Start Backup

Select the backup type and the desired network load for the backup.

Backup type

Lists the backup types applicable for the backup object.

- Full
- Incr
- Incr 1 - 9 (does not apply for block-based backup)

Network Load

Select the desired network load (High, Medium, or Low) for the backup.

Split mirror/snapshot backup

This applies only for ZDB (Zero Downtime backup) to tape or disk (instant recovery enabled).

Client and Application Database Selection - IBM DB2 UDB

Select the client system that has the application you want to back up.

Application

Client

Select the client system in your cell that has the application.

Application database

Select the application database that you want to back up.

User and group/domain

Specify OS user

On UNIX systems, it is mandatory to specify the **Username** and **Group/Domain name** options.

On supported Windows system, it is not mandatory to specify these options and if they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name db2inst1, group db2grp, or Administrator, domain DP). Ensure that this user has been added to the Data Protector admin or operator user group and has the DB2 backup rights. This user becomes the backup owner.

On supported Windows system, this user must be set up for the Data Protector Inet service user impersonation.

Cell Manager Selection - Internal Database Backup

In this page, the required values are predefined for the Internal Database backup.

Application

Client

(the Cell Manager system is preselected for this option; it cannot be changed)

Application database

(DPIDP is preselected for this option; it cannot be changed)

User and group/domain

Specify OS user

(not available in this backup wizard)

Username

(not available in this backup wizard)

Group/Domain name

(not available in this backup wizard)

Application Specific Options - Internal Database Backup

In this page, you can select additional options for Internal Database backup sessions.

General information

- Pre-exec
- Post-exec

Options

Check the Internal Database

This option instructs Data Protector to perform a quick consistency check of the Internal Database before backing it up. This type of consistency check detects major inconsistencies within the IDB. If such an inconsistency is detected, the IDB backup image is not created and the session fails. This is to prevent data loss in situations when the Cell Manager is struck by a disaster and no backup image with a consistent IDB is available.

It is strongly recommended to keep this option selected.

Default: selected.

- Delete backed up archive log files

This option instructs Data Protector to remove the IDB archived log files at the end of a successful Internal Database backup session. Select this option to regain storage space on the Cell Manager volumes where the IDB resides. After the removal, recovery of the IDB can no longer be based on files that reside on the Cell Manager, but only on archive log files from an IDB backup image.

Default: selected.

Source Property Page - Internal Database Backup

In this page, the Internal Database of your cell is preselected for the backup as the only object.

Show

(not available in this backup wizard)

Start Backup - Internal Database Backup

Select the backup type and network load for the Internal Database backup session.

Backup type

You can select **Full** for a full backup or **Incr** for an incremental backup. Note that an incremental backup cannot be run without a previously successful full backup.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Backup view

In the Scoping Pane, you can choose among configured backup specifications and templates.

To back up using predefined backup tasks, click the **Tasks** navigation tab.

Backup Specifications View

In the Results Area, backup specification groups are displayed.

Backup Specifications View

In the Results Area, the Cell Managers imported to the MoM are displayed.

Cell Manager

The name of the Cell Manager.

Status

The status of the Cell Manager (for example, Up and Running, No Permissions, and so on).

Backup Specifications View

In the Results Area, you can see the types of data for which backup specifications can be configured. The data types displayed depend on which Data Protector components have been installed.

Backup Specifications View

In the Results Area, the Cell Managersimported to the MoM are displayed.

Cell Manager

The name of the Cell Manager.

Status

The status of the Cell Manager (for example, Up and Running, No Permissions, and so on).

Backup Tasks View

In the Scoping Pane, you can choose among the predefined backup wizards to configure a backup. These tasks do not apply to online database integrations.

To back up according to object types (Filesystem, and so on), click the Objects navigation tab.

Interactive Backup Wizard [Load Balanced]

Guides you through the procedure to configure a load balanced backup.

Interactive Backup Wizard

Guides you through the procedure to configure a backup that is not load balanced.

One Button Disaster Recovery Wizard

(for Windows and Linux systems only)

Guides you through the procedure to prepare your client for disaster recovery using the One Button Disaster Recovery method.

Prerequisites

- Before using the One Button Disaster Recovery Wizard, you must prepare for disaster recovery. It is recommended that you schedule the backup sessions to regularly update the data necessary for recovering your client systems.

Backup View

In the Scoping Pane, you can choose among configured backup specifications and templates.

To back up using predefined backup tasks, click the **Tasks** navigation tab.

Backup View

In the Scoping Pane, you can choose among configured backup specifications and templates.

To back up using predefined backup tasks, click the **Tasks** navigation tab.

Backup View

In the Scoping Pane, you can choose among configured backup specifications and templates.

To back up using predefined backup tasks, click the **Tasks** navigation tab.

Backup Specifications List

The saved backup specifications of the selected type are displayed in the Results Area.

Name

The name of the backup specification.

Scheduled

The date and time for which the backup is scheduled. If the backup is not scheduled, n/a is displayed.

Backup Type

The type of backup (full or incremental; some other backup types are available for specific integrations). If the backup is not scheduled, n/a is displayed.

Group

(available for Windows systems)

The name of the group to which the backup specification belongs.

To select the location for creating a shortcut of the selected backup specification on the disk, right-click the specification and click **Select the Location for the Shortcut**.

Backup Specifications List

The saved backup specifications in the selected group are displayed in the Results Area.

Name

The name of the backup specification.

Scheduled

The date and time for which the backup is scheduled. If the backup is not scheduled, n/a is displayed.

Backup Type

The type of backup (full or incremental; some other backup types are available for specific integrations). If the backup is not scheduled, n/a is displayed.

Application

The type of data to be backed up (for example, Filesystem).

Backup Templates List

In the Results Area, the configured backup templates in the selected group are displayed.

Name

The name of the backup template.

Application

The type of data to be backed up (for example, Filesystem).

Backup Specifications List

The saved backup specifications on the selected Cell Manager are displayed in the Results Area.

Name

The name of the backup specification.

Scheduled

The date and time for which the backup is scheduled. If the backup is not scheduled, n/a is displayed.

Backup Type

The type of backup (full or incremental; some other backup types are available for specific integrations). If the backup is not scheduled, n/a is displayed.

Group

The name of the group to which the backup specification belongs.

Application

The type of data to be backed up (for example, Filesystem).

Backup Templates List

In the Results Area, the configured backup templates on the selected Cell Manager are displayed.

Name

The name of the backup template.

Group

The name of the group to which the backup template belongs.

Application

The type of data to be backed up (for example, Filesystem).

Backup Specifications List

In the Results Area, the saved backup specifications are displayed.

Name

The name of the backup specification.

Scheduled

The date and time for which the backup is scheduled. If the backup is not scheduled, n/a is displayed.

Backup Type

The type of backup (full or incremental; some other backup types are available for specific integrations). If the backup is not scheduled, n/a is displayed.

Group

The name of the group to which the backup specification belongs.

Application

The type of data to be backed up (for example, Filesystem).

Backup Templates List

In the Results Area, the configured backup templates are displayed.

Name

The name of the backup template.

Group

The name of the group to which the backup template belongs.

Application

The type of data to be backed up (for example, Filesystem).

Client and Application Database Selection - Informix Server

Select the client system that has the application you want to back up.

Application

Client

Select the client system in your cell that has the application.

Application database

Select the application database that you want to back up.

User and group/domain

Specify OS user

Specify the **Username** and **Group/Domain name** options.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name `informix`, group `informix`, or `Administrator`, domain `DP`). Ensure that this user has been added to the Data Protector `admin` or `operator` user group and has the Informix Server backup rights. This user becomes the backup owner.

On supported Windows systems, this user must be set up for the Data Protector Inet service user impersonation.

Configure Informix Server

In this page, you configure the Data Protector Informix Server integration. For additional information, contact your Informix Server administrator.

Client

The name of the Informix Server system that has the database server to be backed up.

Informix Server name

The name of the database server to be backed up.

Informix Server home directory

Specify the pathname of the Informix Server home directory.

Full pathname of sqlhosts file

Windows systems: Specify the name of the system with the `sqlhosts` registry. Use the UNC notation, for example: `\\computer_name`.

UNIX systems: Specify the pathname of the `sqlhosts` file.

Name of ONCONFIG file

Specify the name of the database server ONCONFIG file.

Device Properties - Informix Server

In this page, you select Informix Server resource types. Each resource type determines specific database elements that will be backed up on the device.

It is recommended to add an additional device with no specified resource type to the device list for additional safety. In case of backup failure on any other device, data is backed up to this additional device.

B

If this resource type is selected, the blobspace will be backed up on this device.

CD

If this resource type is selected, the critical dbspace will be backed up on this device. The critical dbspaces are: the root dbspace, the dbspace that contains the physical log, and any dbspace that contains a logical-log file.

L

If this resource type is selected, the logical log will be backed up on this device.

MR

If this resource type is selected, the master root dbspace will be backed up on this device.

ND

If this resource type is selected, the noncritical dbspace will be backed up on this device.

R

If this resource type is selected, the root dbspace will be backed up on this device.

CF

If this resource type is selected, the critical files will be backed up on this device.

Start Preview - Informix Server

Select the backup type and network load for the preview.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

- Incr1-2

(Available incremental levels are different for specific integrations.)

Informix Server level 1 and 2 incremental backup.

Network Load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Start Backup - Informix Server

Select the backup type and network load for the backup.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

- Incr1-2

(Available incremental levels are different for specific integrations.)

Informix Server level 1 and 2 incremental backup.

Network Load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Backup Templates List

In the Results Area, the configured backup templates of the selected type are displayed.

Name

The name of the backup template.

Group

The name of the group to which the backup template belongs.

Templates View

In the Results Area, you can see the types of data for which backup templates can be configured. The data types displayed depend on which Data Protector components have been installed.

Templates View

In the Results Area, the Cell Managersimported to the MoM are displayed.

Cell Manager

The name of the Cell Manager.

Status

The status of the Cell Manager (for example, Up and Running, No Permissions, and so on).

Templates View

In the Results Area, the backup specification groups containing backup templates are displayed.

Configure Lotus - General

Before backing up, you need to configure Lotus Notes/Domino Server.

Client

The name of the client with the Lotus Notes/Domino Server that you want to back up.

Database

The name of the Lotus Notes/Domino Server that you want to back up.

Path to the notes.ini file

Specify the pathname of the Lotus Notes/Domino Server `notes.ini` file.

Unix specific options

(valid for UNIX systems only)

Lotus directory

Specify the pathname of the Lotus Notes/Domino Server home directory.

Domino data directory

Specify the pathname of the Lotus Notes/Domino Server data directory.

Domino executable

Specify the pathname of the Lotus Notes/Domino Server executables directory.

Client and Application Database Selection - Lotus Notes/Domino Server

Select the client system with the application to be backed up.

Application

Client

Select the client system in your cell with the application.

Application database

Select the Lotus Notes/Domino Server that you want to back up. If you are configuring the Lotus Notes/Domino Server for the first time, the Notes/Domino Server name must be typed in the field.

User and group/domain

Specify OS user

On UNIX systems, it is mandatory to specify the **Username** and **Group/Domain name** options.

On Windows systems, it is not mandatory to specify these options and if they are not specified, the backup runs under the Local System Account.

UsernameGroup/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name root, group notes, or user Administrator, domain DP). Ensure that this user has been added to the Data Protector admin or operator user group and has the Lotus Notes/Domino Server database backup rights. This user becomes the backup owner.

On Windows systems, this user must be set up for the Data Protector Inet service user impersonation.

Start Preview - Lotus Notes/Domino Server Backup

Select the backup type and network load for the preview.

Backup type

Full

Backs up the selected Lotus Notes/Domino Server databases and, if selected, transaction logs, including the one currently in use.

Incr

Backs up the selected Lotus Notes/Domino Server databases that meet at least one of the following two conditions:

- The size of the changes made to a database since it was last backed up exceeds the size set by the**Amount of log changes (KB)** option.
- The Lotus Notes/Domino Server DBIID for a database has changed.

Databases that do not meet at least one of the two conditions are not backed up.

If archived logs are selected, it also backs up the archived logs that have not been backed up yet.

Network Load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Start Backup - Lotus Notes/Domino Server Backup

Select the backup type and network load for the backup.

Backup type

Full

Backs up the selected Lotus Notes/Domino Server databases and, if selected, transaction logs, including the one currently in use.

Incr

Backs up the selected Lotus Notes/Domino Server databases that meet at least one of the following two conditions:

- The size of the changes made to a database since it was last backed up exceeds the size set by the**Amount of log changes (KB)** option.
- The Lotus Notes/Domino Server DBIID for a database has changed.

Databases that do not meet at least one of the two conditions are not backed up.

If archived logs are selected, it also backs up the archived logs that have not been backed up yet.

Network Load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Advanced Object Options

In this page you can specify advanced options for the backup object.

- Enhanced incremental backup
- Use native Filesystem Change Log Provider if available
- Software compression
- Display statistical info
- Lock files during backup
- Backup POSIX hard links as files
- Do not preserve access time attributes
  (selected and disabled with the **Use native Filesystem Change Log Provider if available** option)
- Copy full DR image disk

Data security

- None
  This data security option provides no protection. By default, the data security is set to None.
- Encode
  Data Protector recommends using AES 256-bit encryption for data security during backup. Data Protector displays an error message when less-secure option Encode is selected.
- AES 256-bit
  Recommended option. Select this option to enable software encryption to protect your data. Data is encrypted before it is transferred over the network and before it is written to media. However, if you select AES-256 for data security, the Disk Agent will switch to Federal Information Processing Standard (FIPS) mode for data encryption.

General Selection

Select a client with the Disk Agent and the mount point for backup. If the backup is not load balanced, you need to specify the device that will be used.

Client system

Select a client with the Disk Agent to use for your backup.

Mountpoint

Click Map and specify the shared disk.

Device

(not available with load-balanced backup)

If your backup is not load balanced, you need to select a device that will be used to back up this object. You can choose among the devices you have selected in the Destination property page of your backup specification.

Description

Enter a description to help you identify the object.

General Object Options

In this page you can specify the report level, protection, and pre- and post-exec commands for the backup object.

- Public
- Report level
- Protection
- Catalog protection
- Pre-exec
- Post-exec

General Selection

Select the client for backup. If the backup is not load balanced, you need to specify the device that will be used.

Client system

Select the client that you want to back up.

Device

(not available with load-balanced backup)

If your backup is not load balanced, you need to select a device that will be used to back up this object. You can choose among the devices you have selected in the Destination property page of the backup specification.

Description

Enter a description to help you identify the object.

General Selection

Select the client for backup. If the backup is not load balanced, you need to specify the device that will be used.

Client system

Select the client where the object to be backed up is located.

Device

(not available with load-balanced backup)

If your backup is not load balanced, you need to select a device that will be used to back up this object. You can choose among the devices you have selected in the Destination property page of the backup specification.

Description

Enter a description to help you identify the object.

Disk Image Object Options

Specify disk image sections for backup.

Disk image sections

In the text box, enter the name of a section and click **Add**. Use the following format:

UNIX systems:

To specify a disk image section, use the following format: /dev/rdsk/Filename , for example: /dev/rdsk/c2t0d0

To specify a raw logical volume section, use the following format: /dev/vgNumber/rlvolNumber , for example: /dev/vg01/rlvol1

If you intend to perform instant recovery, specify all raw logical volumes inside the volume group to be backed up. Otherwise, instant recovery will not be possible using the Data Protector GUI or (if you perform instant recovery using the Data Protector CLI) data can be corrupted.

Windows systems:

You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk.

In case of ZDB, use the second way:

You can specify a disk image section in two ways: the first way selects a particular volume, and the second way selects an entire disk.

In case of ZDB, use the second way. In case of ZDB to tape using the 3PAR SMI-S Agent, you can also use the first way:

\\.\DriveLetter: , for example: \\.\E :

When a drive letter is specified for the volume name, the volume is not being locked during the backup. A volume that is not mounted or mounted as an NTFS folder cannot be used for disk image backup.

\\.\PHYSICALDRIVE# , where # is the current number of the disk you want to back up. For example: \\.\PHYSICALDRIVE3

To remove a section from the backup specification, select it and click **Delete**.

Windows Object Specific Options

In this page you can specify Windows specific options for the backup object.

- Report open locked files as

Open files

- Number of retriesTime out
- Detect NTFS hardlinks
- Do not use archive attribute
- Asynchronous reading
- De-duplication volume backup
- Backup share information for directories

MS Volume Shadow Copy Options

- Use Shadow Copy
- Allow fallback(available if the **Use Shadow Copy** option is enabled)

Application Specific Options - MS Exchange Single Mailbox Integration

In this page, specify the options that apply to the Microsoft Exchange Single Mailbox backup.

General Information

- Pre-exec
- Post-exec

Selecting Objects for Backup

In this page, browse for and select the Exchange items you want to back up. Mailboxes are organized alphabetically. For example, mailboxes beginning with the letter S are collected under the **S** folder. Note that you can select individual folders from different mailboxes and Public Folders.

Configure Single Mailbox

In this page, configure the Microsoft Exchange Single Mailbox integration.

MS Exchange Admin

The username of the Microsoft Exchange administrator.

Password

The password of the Microsoft Exchange administrator.

Domain

The domain of the Microsoft Exchange administrator.

Client and Application Database Selection - Microsoft Exchange Single Mailbox

Select the client system and the application you want to back up.

Client

The Microsoft Exchange Server system with the mailboxes and Public Folders you want to back up. All the clients that have the Microsoft Exchange Server integration installed are listed.

Application database

Single Mailbox is selected.

User and group/domain

Specify OS user

It is not mandatory to specify the **Username** and **Group/Domain name** options. If they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name Administrator, domain DP). Ensure that this user has been added to the Data Protector admin or operator user group, has the Exchange Server rights to back up the database, and has been set up for the Data Protector Inet service user impersonation.

This user becomes the backup owner.

Start Backup - MS Exchange Single Mailbox

Select the backup type and network load for the backup.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

Incr

Incr backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup.

The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB.

The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

Incr1

Incr1 or differential backup backs up changes since the last full backup. This backup type limits the restore chain to two elements, but the backup can become large as the changes made since the full backup accumulate.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Start Preview - MS Exchange Single Mailbox Integration

Select the backup type and network load for the preview.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

Incr

Incr backs up only changes from the last protected backup, regardless of whether it was a full or incremental backup.

The advantage of an incremental backup is that it takes less time to complete (it backs up smaller quantities of data) and occupies less space on media and in the IDB.

The disadvantage is that a restore is more complicated as you usually need all the media used since the last full backup.

Incr1

Incr1 or differential backup backs up changes since the last full backup. This backup type limits the restore chain to two elements, but the backup can become large as the changes made since the full backup accumulate.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Missed Job Executions

A table of session executions, scheduled using Scheduler, that failed to trigger due to issues such as Cell Manager downtime, schedule not being configured properly, or backup specification being removed.

The sessions that had been triggered successfully, but failed afterwards due to Scheduler unrelated issues, do not appear in the table. Examples include issues such as resource failure or Data Protector being in maintenance mode.

To change the table appearance, click the arrow in the Schedules headings and select a filter.

To refresh the list of missed executions, right-click the page and select **Reload**.

Refresh

Click to refresh the list of missed sessions.

Run now

Click to the Run Now icon to start selected sessions.

Delete

Click the Delete icon to clear selected sessions from the list without running them.

Delete all

Click the Delete All icon to delete all missed sessions from the list without running them.

Start Backup - Microsoft Exchange Server

Select the backup type and network load for the backup.

With ZDB, only the **Full** backup type is supported.

Backup type

- Full

Backs up all selected Microsoft Exchange Server databases and Microsoft Exchange Server transaction log files.

- Incr

When you select this backup type, you must ensure that a full backup exists in the IDB.

Ensure that the Microsoft Exchange Server circular logging option is disabled before performing Microsoft Exchange Server incremental backups.

- Network Load

Start Backup - MS SQL Server

Select the backup type and network load for the backup.

With ZDB, only the **Full** backup type is supported.

Backup type

Full

Full database backup includes all data in a database regardless of whether the database has changed after the last backup was created. This means that the entire database backup does not depend on any other backup media.

In an availability group configuration, when you trigger a full backup of a database belonging to an availability group secondary replica, the backup type is automatically changed to a copy-only full backup.

- Trans

When you select this backup type, you must ensure that a full backup exists in the IDB.

Make sure that you have the **Recovery model** option on the Microsoft SQL Server set to **Bulk-Logged** or to **Full** to perform MS SQL Server Trans backups.

Differential

In an availability group configuration, when you trigger a differential backup of a database belonging to an availability group secondary replica, the backup type is automatically changed to a copy-only full backup.

Copy

A copy-only full backup is an independent full backup, which never truncates the transaction logs and does not affect an SQL Server restore chain. For this reason, it also cannot serve as a base of a differential backup.

Select this option, if you do not want to influence a database backup.

Network Load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Split mirror/snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.

Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Application Specific Options - MySQL Backup

You can select additional options for the MySQL backup sessions.

General options

- Pre-exec
- Post-exec

InnoDB storage engine options

- Enable backup data compression
- Level

Binary log options

- Parallelism
- Purge log after successful backup

Configure MySQL Instance

Configure the chosen MySQL instance for backup.

Client

(the chosen Data Protector client (MySQL host) is preselected here; it cannot be changed)

MySQL instance

(the chosen MySQL instance is preselected here; it cannot be changed)

Connection

Username

Specifies the name of an appropriate MySQL user account with sufficient privileges (the `SUPER` privilege at least) for accessing your MySQL database management system.

Selection of the **Use parameters from custom MySQL configuration file** option overrides this value.

When migrating an entire instance, specify the username and password of the source MySQL instance.

Password

Specifies the password of the MySQL system user account.

Selection of the **Use parameters from custom MySQL configuration file** option overrides this value.

Port

Specifies the port the MySQL instance is using.

Selection of the **Use parameters from custom MySQL configuration file** option overrides this value.

- Use parameters from custom MySQL configuration file

MySQL Enterprise Backup

Path to mysqlbackup command

Specifies the absolute path to the `mysqlbackup` command binary file on the MySQL host. For path delimiters, you can use either slashes or backslashes.

Client and Instance Selection - MySQL Backup

Select the MySQL host and specify the MySQL instance whose data you want to back up. Optionally, provide the username and password of the Data Protector user account that will run MySQL backup sessions.

Application

Client

This drop-down list contains all the clients of the Data Protector cell that have the Data Protector MySQL Integration component installed. Select the client from where you want to back up MySQL data.

Application database

Specify the name of the MySQL instance that you want to back up.

User and group/domain

Specify OS user

Select this option to use the integrated authentication and to run backup sessions with the operating system user account of your choice. If the option is not selected, the backup sessions run under the local System account.

Username

(available if **Specify OS user** is selected)

Specify the operating system account using which the backup sessions will run. Ensure this operating system user account is added to the Data Protector admin or operator user group. The corresponding Data Protector user becomes the backup owner of the backed up MySQL objects.

Group/Domain name

(available if Specify OS user is selected)

Specify the group of the MySQL user account using which the backup sessions will run and which you specified for the **Username** option.

Database and Database Table Selection - MySQL Backup

Select the MySQL entities you want to back up. An entity can be the entire instance, an individual database, or an individual database table. If you select an entity (and nothing at a lower level within it), any sub-entities added to it after the backup specification is saved will also be backed up.

Show

(available when editing a saved backup specification)

From the drop-down list, select one of the following:

Selected

This option displays only the MySQL entities include in the backup specification.

All

This option displays all contents of the MySQL instance.

Start Backup - MySQL Backup

Select the backup type and network load for the MySQL backup session.

Backup type

You can select **Full** for a full backup, **Incr** for an incremental backup, or **Trans** for a transaction log backup. Incremental backup cannot be invoked without at least one prior successful full backup.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network while the session is running. It prevents the backup data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Add/Remove Disk Mount Points

Enter one or more disk mount points that you want to back up, or remove disk mount points that you no longer want to back up. Note that every disk mount point results in a separate backup object.

New mount point

Type the name of the mount point and click **Add**.

Start Preview - Oracle

Select the backup type and network load for the preview.

With ZDB, only the **Full** backup type is supported.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

- Incr1-4

RMAN backup incremental level 1 to 4.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Split mirror/snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.

Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Start Backup - Oracle

Select the backup type and network load for the backup.

With ZDB, only the **Full** backup type is supported.

Backup type

Full

If this option is selected, all selected objects are backed up, even if there are no changes from the previous backup.

The advantage of a full backup is security (all data is backed up in one backup session) and a faster, simpler restore (you only need the media from the latest full backup).

The disadvantage is that a full backup takes longer to complete and occupies more space on the media and in the IDB, since the same version of a file can be backed up several times.

- Incr1-4

RMAN backup incremental level 1 to 4.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running Data Protector. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: High.

Split mirror/snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Select **To disk+tape** if you want mirror/snapshot data to be streamed to tape after a mirror/snapshot creation and also retained on the disk array after the backup.

Select **To disk** if you want mirror/snapshot data to be retained on the disk array after the backup, but not streamed to tape after a mirror/snapshot creation.

Configure Oracle - Primary

In this page, you configure the connection for the Oracle primary database.

Oracle login information to primary database

Provide the login information for the primary database.

User name

Type the user name for login to the primary database. The user must be granted the Oracle SYSDBA rights.

Password

Type the password for the specified user.

Services

Type the net service name for the primary database instance. The backup will be performed on the system where this database instance resides.

RAC: List all net services names for the primary database separated by a comma. Each net service name must resolve into a specific database instance.

Configure Oracle - General

In this page, you provide information on where the Oracle Server is installed.

Client

The name of the client where the database to be backed up resides.

Database name

The name of the Oracle database you are configuring.

Oracle Server home directory

Specify the pathname of the Oracle Server home directory.

Configure Oracle - Catalog

In this page, you configure the connection for the recovery catalog, if you use it. Ensure that the owner of the Oracle recovery catalog is granted the CREATE ANY DIRECTORY and the DROP ANY DIRECTORY system privileges, which are required to use the Data Pump Export (expdp) and the Data Pump Import (impdp) utilities.

Use target database control file instead of recovery catalog

Select this option if you want the information about the backup to be stored in a control file of the Oracle primary database.

Use recovery catalog

Select this option if you want to use the Oracle recovery catalog as an RMAN repositry for backup history and specify the login information to the recovery catalog.

Use recovery catalog in the following cases:

- For ZDB
- In Oracle Data Guard environment, if you intend to back up a standby database

Oracle login information to recovery database

This is the connection string for the Oracle recovery catalog database. The format of the connection string is user_name/password @service .

User name

Type the name of the owner of the Oracle recovery catalog.

Password

Type the password for the specified user.

Services

Type the net service name for the recovery catalog.

Configure Oracle - Standby

In this page, you configure the connection for the Oracle standby database in the Oracle Data Guard environment.

Configure standby database

Select this option if you intend to back up a standby database.

Oracle login information to standby database

Provide the login information for the standby database.

User name

Type the user name for login to the standby database.

Password

Type the password for the specified user.

Services

Type the net service name for the standby database instance.

RAC: List all net services names for the standby database separated by a comma. Each net service name must resolve into a specific database instance.

Configure Oracle - ZDB

In this page, you configure the Oracle integration for zero downtime backup.

Backup method

Select this option and then select the backup method from the drop-down list: **PROXY** or **BACKUP SET**.

Backup control file copy location

Optionally, select this option and then specify the location on the source volumes where a backup copy of the current control file will be made during ZDB to disk.

If you do not specify the location, ob2rman.pl will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

Parameter file (PFILE)

(available if backup method is **BACKUP SET**)

Select this option and then specify the pathname of PFILE residing on the application system if your database instance uses PFILE (and not SPFILE).

Client and Application Database Selection - Oracle Server

Select the client system that has the application you want to back up.

Application

Client

Select the Data Protector Oracle integration client. In a cluster environment, select the virtual server.

RAC: Select either the node or the virtual server of the Oracle resource group.

Oracle Data Guard: Select either a primary or secondary (standby) system.

Application database

Select or type the name of the application database to be backed up.

In a single-instance configuration, the database name is usually the same as its instance name. In this case, the instance name can be also used. In a multi-instance configuration (RAC), the database name is the same for all instances.

User and group/domain

Specify OS user

On UNIX systems, it is mandatory to specify the **Username** and **Group/Domain name** options.

On Windows system, it is not mandatory to specify these options and if they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name `ora`, group `dba`, or user `Administrator`, domain `DP`). Ensure that this user has been added to the Data Protector `admin` or `operator` user group and has the Oracle database backup rights. This user becomes the backup owner.

On Windows system, this user must be set up for the Data Protector Inet service user impersonation.

Application Specific Options - PostgreSQL Backup

You can select additional options for the PostgreSQL backup sessions.

General options

- Pre-exec
- Post-exec

Options

- Purge backed up archive log files

Configure PostgreSQL Instance - General

Configure the chosen PostgreSQL instance for backup.

Client

(the chosen Data Protector client - PostgreSQL host is preselected here; it cannot be changed)

PostgreSQL instance

(the chosen PostgreSQL instance is preselected here; it cannot be changed)

Connection

Username

Specifies the name of an appropriate PostgreSQL user account with sufficient privileges with (at least, `SUPER`) for accessing your PostgreSQL database server system.

Password

Specifies the password of the PostgreSQL system user account.

Port

Specifies the port the PostgreSQL instance is using.

PostgreSQL

PostgreSQL binaries directory

Specifies the absolute path to the PostgreSQL binaries directory on the PostgreSQL host.

Use predefined WAL Archive directory

Select this option, if the WAL archive directory (`archivedir`) is already created on the PostgreSQL host and is specified in the `archive_command` configuration parameter.

Specifies the absolute path to the WAL archive directory.

Configure PostgreSQL Instance - Standby Server

Configure a standby PostgreSQL server if you want to perform backups on standby instead of master server.

Backup from standby server

Select this option to perform backups on standby instead of master server.

Standby server hostname

Specify the hostname of the PosgreSQL standby server.

Standby server data directory

Specify a full pathname to the PostgreSQL data directory.

Master WAL archive directory accessible from standby

Specify the full pathname to the WAL archive directory of the master server that can be accessed from the standby server.

Client and Instance Selection - PostgreSQL Backup

Select the PostgreSQL host and specify the PostgreSQL instance whose data you want to back up. Optionally, provide user account of the Data Protector user that will be used for running PostgreSQL backup sessions.

Application

Client

This drop-down list contains all the clients in the Data Protector cell that have the Data Protector PostgreSQL Integration component installed. From the drop-down list, select the client from where you want to back up PostgreSQL data.

Application database

Specify the name of the PostgreSQL instance that you want to back up.

User and group/domain

Specify OS user

Select this option to use the integrated authentication and to run the backup session with the operating system user account of your choice. If the option is not selected, backups run under the Local System Account.

Username

(available if **Specify OS user** is selected)

Specify the operating system account using which you want the backup session to run. Ensure this operating system user account is added to the Data Protector admin or operator user group. The corresponding Data Protector user becomes the backup owner of the backed up PostgreSQL objects.

Group/Domain name

(available if **Specify OS user** is selected)

Specify the group of the PostgreSQL user account using which you want to run the backup session and which you specified as the value for the **Username** option.

Instance Selection - PostgreSQL Backup

Selected is the PostgreSQL instance that you want to back up.

Show

(available when editing a saved backup specification)

From the drop-down list, select one of the following:

Selected

This option displays the PostgreSQL instance included in the backup specification.

All

This option displays the PostgreSQL instance included in the backup specification.

Start Backup - PostgreSQL Backup

Select the backup type and network load for the PostgreSQL backup session.

Backup type

You can select **Full** for a full backup or **Trans** for a transaction log (WAL) backup. Transaction log backup cannot be invoked if no full backup had been successfully completed before.

Network load

Select the network load for the session.

Setting this option to **Medium** or **Low** reduces the load on the network when running. This prevents the data transmission from blocking the network for other users but increases the time required for the session to complete.

Default: **High**.

Client and Application Database Selection - SAP MaxDB Integration

Select the client system that has the application you want to back up.

Application

Client

Select the client system in your cell that has the application.

Application database

Select the application database that you want to back up.

User and group/domain

(available on UNIX and Windows clients)

Specify OS user

On UNIX systems, it is mandatory to specify the **Username** and **Group/Domain name** options.

On Windows server, it is not mandatory to specify these options and if they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name `sapdb`, group `sapsys`, or `Administrator`, domain `DP`). Ensure that this user has been added to the Data Protector `admin` or `operator` user group and has the SAP MaxDB backup rights. This user becomes the backup owner.On Windows server, this user must be set up for the Data Protector Inet service user impersonation.

Client and Application Database Selection - SAP HANA Integration

In this page, specify the SAP HANA system and the SAP HANA instance whose data you want to back up, and provide user account of the Data Protector user that will be used for running SAP HANA backup sessions.

Application

Client

This drop-down list contains all the clients in the Data Protector cell that have the Data Protector SAP HANA Integration component installed. From the drop-down list, select:

- The SAP HANA system

(if your SAP HANA Appliance is a single-server environment)

- The SAP HANA master host with the configured name server role MASTER1

(if your SAP HANA Appliance is a distributed environment; for instructions on how to determine the SAP HANA system with this role, see the SAP HANA documentation)

- The name of the virtual system configured in the DNS

(if your SAP HANA Appliance is a distributed environment, and TBD)

Application database

(not available)

Specify the name of the SAP HANA instance that you want to back up.

User and group/domain

Specify OS user

(not available)

Username

Specify the SAP HANA user account using which you want the backup session to run. The user account must have the following privileges in the SAP HANA Appliance:

- BACKUP ADMIN or BACKUP OPERATOR
- CATALOG READ

Ensure that this operating system user account has been added to the Data Protector admin or operator user group.

The corresponding Data Protector user becomes the backup owner of the backed up SAP HANA objects.

Group/Domain name

Specify the group of the SAP HANA user account using which you want the backup session to run and which you specified as the value for the Username option.

Configure SAP

In this page you configure the SAP R/3 integration.

Client

The name of the client where the application that you want to back up resides.

Oracle SID

The name of the Oracle Server instance (ORACLE_SID) on which the SAP R/3 Database Server is running.

Oracle Server home directory

Enter the name of the directory in which the Oracle Server is installed.

SAP Data home directory

Enter the name of the SAP R/3 data home directory (by default, it is set to ORACLE_HOME).

Oracle login information to target database

User name

The name by which a user is known to the Oracle Server. Every user name is associated with a password and both must be entered to connect to an Oracle database. This user must be granted Oracle SYSDBA rights.

Password

The password for the user.

Service

The name of a TNS connect descriptor. Each connect descriptor is assigned a service name in the network definition.

Backup and restore executables directory

The directory in which SAP R/3 backup utilities are stored. Usually, the utilities reside in the directory /usr/sap/ORACLE_SID/SYS/exe/run (on UNIX systems) and \\hostname\sapmnt\ORACLE_SID\sys\exe\run (on Windows systems). Enter the correct full path.

Configure - SAP MaxDB Integration

In this page, you configure the SAP MaxDB integration.

General

Client

The name of the SAP MaxDB Server, on which the SAP MaxDB instancethat you want to back up is running.

Database instance

The name of the SAP MaxDB instance.

SAP MaxDB independent program path

This parameter is the independent program path directory specified during the installation of the SAP MaxDB application on the SAP MaxDB Server. You can leave the Auto-detect option selected to automatically detect the directory on the SAP MaxDB Server.

Connection

Username

The name by which a user is known to the SAP MaxDB Server.This user must be granted the following SAP MaxDB permissions: Recovery , Backup , InstallMgm and ParamCheckWrite . The OS user under whose account the SAP MaxDB application is running must also be addedto the Data Protector admin group.

Password

Every user name is associated with a password and both must be entered to connect to the SAP MaxDB Server.

Start Backup - SAP MaxDB Integration

Select a backup type and network load for the backup.

Backup type

- Full
- Diff
- Trans
- Network load

Start Preview - SAP MaxDB Integration

Select a backup type and network load for the backup preview.

Backup type

- Full
- Diff
- Trans
- Network load

Start Preview - SAP R/3

Select the backup type and network load for the preview.

With ZDB, only the Full backup type is supported.

Backup type

- Full

Backs up all selected SAP R/3 objects.

- Incr

You can use this backup type if you are using Oracle RMAN to back up SAP R/3 objects. This backup type performs the Oracle RMAN backup incremental level 1. It backs up all changes to the selected SAP R/3 objects since the last full backup.

- Network Load
- Split mirror/snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Client and Application Database Selection - SAP R/3

Select the client system that has the application you want to back up.

Application

Client

Select the client system in your cell that has the application.

Application database

Select the application database that you want to back up.

User and group/domain

(available on UNIX and Windows clients)

Specify OS user

On UNIX and Windows clients, it is mandatory to specify the **Username** and **Group/Domain** name options.

Username

Group/Domain name

(available if **Specify OS user** is selected) Specify the operating system user account under which you want the backup session to run (for example, the user name ora, group dba, or Administrator, domain DP). Ensure that this user has been added to the admin or operator user group and has the SAP R/3 backup rights. This user becomes the backup owner.

On Windows client, this user must be set up for the Inet service user impersonation.

Start Backup - SAP R/3

Select the backup type and network load for the backup.

With ZDB, only the Full backup type is supported.

Backup type

- Full

Backs up all selected SAP R/3 objects.

- Incr

You can use this backup type if you are using Oracle RMAN to back up SAP R/3 objects. This backup type performs the Oracle RMAN backup incremental level 1. It backs up all changes to the selected SAP R/3 objects since the last full backup.

- Network Load
- Split mirror/snapshot backup

(available with ZDB, but only in the case of a ZDB to disk+tape or ZDB to disk session (instant recovery enabled))

Select Device

In this page you select the device to be used for backing up the selected object. You can choose among the devices selected for this backup specification.

Advanced - Set Environment Variables

In this page, you edit environment variables.

User defined variables

Variable name

In the drop-down list, select or type the name of the environment variable.

Value

Set the value for the specified variable and click **Add**.

The following may be helpful:

- To remove a variable from the list, select it and click **Remove**.
- To change the value of the variable in the list, select it, specify the new value, and click **Set**.

Application Specific Options - Microsoft SharePoint Server Integration

In this page, specify the options that apply to the Microsoft SharePoint Server integration backup.

General information

- Pre-exec
- Post-exec

Options

- Concurrent streams
- Offline backup

More on

- About Backup
- About Backup Options
- About Pre- and Post-Exec Commands

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Client and Application Database Selection - Microsoft SharePoint Server Integration

In this page, specify the Microsoft SharePoint Server farm administrator that should be used for the backup and the Microsoft SharePoint Server farm that should be backed up.

User and group/domain

Specify OS user

(not available)

Username

Group/Domain name

Specify the Microsoft SharePoint Server farm administrator under which you want the backup session to run. Ensure that this user has been added to the admin or operator user group and has been set up for the Inet service user impersonation.

This user becomes the backup owner.

Application

Client

Select any Microsoft SharePoint Server system that belongs to the farm you want to back up. The drop-down list contains all the clients with the MS SharePoint Integration component installed. The backup session (that is, the integration agent sharepoint_bar.exe) will be started on the client that you specify here.

Application database

(not available) Displays the name of the Microsoft SharePoint Server farm configuration database that serves as the farm’s identifier, since each Microsoft SharePoint Server farm has only one configuration database.

Start Backup - Microsoft SharePoint Server Integration

Select a backup type and network load for the backup session.

Backup type

- Full
- Incr
- Differential
- Network Load

MySQLStartPreview

Start Preview - Microsoft SharePoint Server Integration

Select a backup type and network load for the preview backup session.

Backup type

- Full
- Incr
- Differential
- Network Load

SQL backup preferences

In this page, you can set backup preferences to be used for an availability group configuration. This options are not available for ZDB.

Select backup preferences

Use SQL server settings

Performs a backup according to the Microsoft SQL Server settings. This is the default option.

Prefer Secondary

Performs a backup of availability group databases on an availability group secondary replica. If there is no availability group secondary replica available, the backup is performed on an availability group primary replica.

Secondary only

Performs a backup of availability group databases on an availability group secondary replica. If there is no availability group secondary replica available, the backup fails.

Primary

Performs a backup of availability group databases on an availability group primary replica.

Any replica

Performs a backup on any availability group replica in the availability group.

- Force full and diff backup on Primary Replica

Configure MS SQL

This dialog box is displayed if the SQL Server integration has not been configured yet or if the specified user account has no appropriate permissions to connect to the SQL Server instance. Specify the user account that should use to connect to the SQL Server instance.

Client

The name of the client on which the SQL Server instance is running.

SID

The name of the SQL Server instance.

Connection

- SQL Server authentication
- Windows authentication
- Integrated authentication

Configure MS SQL - Availability group level

This dialog box is displayed if the SQL Server integration has not been configured yet or if the specified user account has no appropriate permissions to connect to the SQL Server availability group listener.

Specify the user account that should use to connect to the SQL Server availability group listener.

Listener

The name of the availability group listener used to connect to the SQL Server.

Availability Group

The name of the SQL Server availability group corresponding to the selected listener.

Port

The port number used by the listener to connect to the SQL Server. The default is 1433.

Connection

- SQL Server authentication
- Windows authentication
- Integrated authentication

Client and Application Database Selection - Microsoft SQL Server

Select the client system and the application that you want to back up.

Client

Select the client system in your cell that has the application to be backed up.

Application database

Select the instance of the SQL Server to be backed up.

User and group/domain

(available on Windows system)

Specify OS user

If this option is not specified, the backup runs under the Local System Account.

Specify this option if you intend to use **Integrated authentication** and you want that the backup session runs under the specified operating system user account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name Administrator, domain DP). Ensure that this user has been added to the admin or operator user group, has the SQL Server rights to back up the database, and has been set up for the Inet service user impersonation.

This user becomes the backup owner.

More on

- About Backup
- About the Inet Service Configuration

Tasks

- Setting Up a User Account for the Inet Service User Impersonation

NetApp/3 PAR Storage Provider Options

Select NetApp/3 PAR Storage Provider options.

- Replica Provision

Click to select the NetApp/3 PAR Storage Provider, configure the provider-specific options, and add it to a list.

Replica Description

The description of the replica.

Destination Array

(applicable only with NetApp clusters)

Fully qualified domain name of the NetApp storage system that you specified when establishing connection to the NetApp storage system with the omnidbzdb commad.

Destination Vserver

(applicable only with NetApp clusters)

Name of the destination Vserver.

NetApp/3 PAR Storage Provider Options

Select the NetApp/3 PAR Storage Provider options.

- Replica Provision

Click to select the NetApp/3 PAR Storage Provider, configure the provider-specific options, and add it to a list.

Replica description

The description of the replica.

- Transportation mode

(applicable only with NetApp storage) Click to select the NetApp Storage Provider, configure the provider-specific options, and add it to a list.

Destination array

(applicable only with NetApp clusters)

Fully qualified domain name of the NetApp storage system that you specified when establishing connection to the NetApp storage system with the omnidbzdb command.

Destination Vserver

(applicable only with NetApp clusters)

Name of the destination Vserver.

EMC VMAX Storage Provider Options

Select EMC VMAX Storage Provider options.

Array model

Select the model of your EMC VMAX storage.

SYMCLI binaries path

Enter the path to the SYMCLI binaries.

Connection type

Enter the connection type.

Target pool

Enter the name of the pool in which the replica will be created.

Replica type

Select the Snapshot or Clone. Snapshot creates a TimeFinder VP Snap. Clone creates TimeFinder/Clone, which is a copy of VMAX production device. For more information on these two types, see EMC VMAX documentation.

Replica description

The description of the replica.

- Transportation mode

(available with Virtual Environment Integration for VMware)

Click to select the storage provider, configure the provider-specific options, and add it to a list.

EMC VNX Storage Provider Options

Select EMC VNX Storage Provider options.

NAVISEC CLI path

Enter the path to the Navisphere Secure Command Line Utility.

Replica type

Select the VNX Snapshot.

Replica description

The description of the replica.

- Transportation mode

(available with Virtual Environment Integration for VMware)

Click to select the storage provider, configure the provider-specific options, and add it to a list.

Client and Application Database Selection - Sybase Server

Select the client system that has the application you want to back up.

Application

Client

Select the client system in your cell that has the application.

Application database

Select the application database that you want to back up.

User and group/domain

(available on UNIX system)

Specify OS user

On UNIX systems, it is mandatory to specify the **Username** and **Group/Domain name** options.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name sybase, group sybase). Ensure that this user has been added to the admin or operator user group and has the Sybase Server backup rights. This user becomes the backup owner.

More on

- About Backup

Configure Sybase

Configure the Sybase Adaptive Server instance (Sybase instance). This dialog box is automatically displayed if the Sybase instance is not configured for use with Data Protector or the configuration is not correct (for example, because the configuration account in the Sybase Server database has been changed).

Client

The name of the Sybase Server system.

Sybase Server name

The name of the Sybase instance.

Connection

Sybase Server home directory The pathname of the Sybase Server home directory.

Full Pathname for Sybase isql command

The pathname of the Sybase isql utility.

Sybase User

The Sybase instance user that has the Sybase right to back up and restore databases.

Password of the Sybase User

The password of the Sybase instance user.

SYBASE_ASE (only for Sybase 12.x)

The name of the SYBASE_ASE directory.

SYBASE_OCS (only for Sybase 12.x)

The name of the SYBASE_OCS directory.

More on

- About Backup

Start Preview - Sybase

Select the backup type and network load for the preview.

Backup type

- Full

Backs up all selected Sybase objects and Sybase transaction logs.

- Trans
- Network Load

More on

- About Backup
- Backup Types

Tasks

- Previewing and Starting a Backup

Start Backup - Sybase

Select the backup type and network load for the backup.

Backup type

- Full

Backs up all selected Sybase objects and Sybase transaction logs.

- Trans
- Network Load

More on

- About Backup
- Backup Types

Tasks

- Previewing and Starting a Backup

Application Specific Options - Oracle Integration

The options in this page apply to the Oracle integration backup.

Disable recovery catalog auto backup

Select this option to disable backup of the recovery catalog. By default, backs up the database recovery catalog in every backup session, or, in ZDB environment, after every ZDB to tape or ZDB to disk+tape.

Disable managed control file backup

Select this option to disable backup of the managed control file. By default, backs up the managed control file in every backup session, or, in ZDB environment, after every ZDB to tape or ZDB to disk+tape.

Back up standby database

(This option is applicable in Oracle Data Guard environment and if the database is configured with the standby connection. It is ignored for ZDB.)

By default, RMAN backs up the database files and archived redo logs on the primary system. Select this option to enable backup of the database files and archive logs on the standby system. However, only the archive logs created after the standby database was configured can be backed up at standby site. Archive logs created before the standby database was configured must be backed up on the primary database.

Note that the current control file or the control file for standby database will still be backed up from the primary system.

RMAN Script

The RMAN script section of the backup specification, created by .

Edit

(available when creating a new template)

Click here to edit the RMAN script section of the backup specification.

General information

- Pre-exec: Specify a command or RMAN script that will be started by ob2rman.pl on the Oracle Server system before the backup. RMAN scripts must have the .rman extension. Do not use double quotes. Provide the pathname of the command or RMAN script.
- Post-exec: Specify a command or RMAN script that will be started by ob2rman.pl on the Oracle Server system after the backup. RMAN scripts must have the .rman extension. Do not use double quotes. Provide the pathname of the command or RMAN script.

Backup offline

(available for ZDB integrations)

If this option is selected, the Oracle database on the application system is shut down while the disk devices are split. The database backup is done on the backup system and is therefore consistent. For Oracle proxy-copy ZDB method, the backup is done without application binaries on the backup system and is therefore consistent.

If this option is not selected, an online backup is performed, which means that the Oracle database on the application system is available during backup. The tablespaces are in backup mode during the split command. The database is not consistent, however, so you must back up the archive logs.

More on

- About Backup
- About Backup Options

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Destination Property Page

In this page you select the devices to be used in the backup template.

Show selected

If this option is selected, only the selected devices are displayed.

Show all

If this option is selected, all configured devices in the cell are displayed.

Properties

(available when a selected device is highlighted)

Displays properties of the selected device.

More on

- About Backup
- About Backup Templates
- Device Options

Tasks

- Modifying a Backup Template

Options Property Page

In this page you can set backup options for the backup template. To set further options, click the appropriate Advanced button.

If you set a schedule with the Protection option different from Default in the Schedule wizardBackup dialog, it will override the selection made in this page.

Backup Specification options

Description

Type a description for the backup specifications to which you will apply this template.

Filesystem options

- Protection

Filter [Trees]

Click Advanced to specify directories and files to be included in your backup or excluded from it.

More on

- About Backup
- About Backup Templates
- About Backup Options

Tasks

- Modifying a Backup Template

Trees Properties

The options in this page apply to backup objects of the selected type (Windows clients, UNIX clients, and so on). These options are not supported with NDMP server integration.

Trees

Enter the pathname of filesystems, files, or directories that you want to include for backup, and click Add. See the Example below.

Filter

Click here to select the types of files to be included in the backup or excluded from it.

Excludes

Enter the pathname of filesystems, files, or directories that you want to exclude from the backup, and click Add. See the Example below.

For backup objects of the Client System type, you can modify the meaning of the Trees and Excludes backup options so that interprets the specified directories as volumes and not as filesystem directory trees. Consequently, different data is backed up. To modify the meaning, use global options as described in the example below.

The global options have no effect on backup objects of the Filesystem or any other type.

On Linux systems, when you create a backup specification with the CONFIGRATION/SYSTEMRECOVERYDATA object selected, the folders /opt/omni/bin/drim/log and /opt/omni/bin/drim/tmp are by default excluded from the backup. However, this exclusion is not set if you manually update existing backup specifications.

More on

- About Backup
- About Backup Templates

Tasks

- Modifying a Backup Template

Templates - Save As

Click the button to save the template.

More on

- About Backup
- About Backup Templates

Application Specific Options - Virtual Environment Integration

In this page, specify the options that apply to backup sessions using the Virtual Environment integration.

General Information

- Pre-exec
- Post-exec

More on

- About Backup
- About Backup Options
- About Pre- and Post-Exec Commands

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Application Specific Options - Virtual Environment Integration

In this page, specify the options that apply to backup sessions using the Virtual Environment integration.

General Information

- Pre-exec
- Post-exec

Hyper-V options

(Not applicable with Hyper-V RCT backup method)

- Enable incremental backup of VM(s)

(available for systems that support incremental backup of Hyper-V virtual machines)

- Back up selected VM(s)

(available for systems that support virtual machine replication)

- Back up replica VM(s)

(available for systems that support virtual machine replication and when Enable incremental backup of VM(s) is not selected)

- Use primary VM(s) if replication link is down

(available when **Back up replica VM(s)** is selected)

More on

- About Backup
- About Backup Options
- About Pre- and Post-Exec Commands

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Source Property Page - Virtual Environment Integration

On this page, you select the objects that you want to back up.

Available objects can be selected individually or at various group levels.

With VMware and H3C CAS cached backup method, you can also select individual disks for backup. Expand each VM and select the disks to be backed up. You can exclude disks under a VM which you do not require backup for.

If you select a group (and nothing within it) any objects added to the group after the specification is saved will also be backed up.

Show

In the drop-down list, select one of the following:

Hosts and Clusters

If this option is selected, it displays all available objects grouped by clients and clusters.

VMs and Templates

If this option is selected, it displays all available objects grouped by virtual machines and virtual machine templates. For H3C CAS, only the objects grouped by virtual machines are displayed. By default, **Hosts and Clusters** is selected. If you switch the view after you have already selected one or more objects for backup, a warning dialog is displayed. Its confirmation clears the already selected objects.

Tags and Categories

(VMware specific option)

If this option is selected, it displays all available objects grouped by tags and their categories. To use the **Tags and Categories** view, the vSphere user account must have vSphere tagging privileges to read and assign tags.

Datastores and Storage

(VMware specific option)

If this option is selected, it displays all available objects grouped by datastores and datastore clusters or storage pods.

Source Page Saved - Virtual Environment Integration

In this page, you can modify the objects that you have selected for backup.

Available objects can be selected individually or at various group levels.

If you select a group (and nothing within it) any objects added to the group after the specification is saved will also be backed up.

Show

In the drop-down list, select one of the following:

Selected

If this option is selected, only currently selected objects are displayed.

Hosts and Clusters

If this option is selected, all available objects grouped by clients and clusters are displayed.

VMs and templates

If this option is selected, all available objects grouped by virtual machines and virtual machine templates are displayed. For H3C CAS, only the objects grouped by virtual machines are displayed.

The view that you have used during the creation of your backup specification has the string (Original) appended. If you switch the view, a warning dialog is displayed and its confirmation clears the already selected objects.

To specify common virtual machine settings and technology specific settings for the selected virtual machine, right-click the virtual machine and click Configure virtual machines.

VE settings

Click this button to display or modify virtual environment settings.

More on

- About Backup

Tasks

- Modifying a Backup Specification

Configure Virtual Environment - Virtual Environment Integration

In this page, specify the login credentials that should use to connect to the selected Hyper-V system, VMware vCenter Server, or VMware ESX(i) Server system.

To be able to change the login credentials, you must have the Clients configurationClients configuration user right (for example, you must be in the admin user group).

Client

Displays the name of the selected client.

- Integrated security

(available for VMware vCenter Server clients, provided that both the application client and the backup host are Windows systems)

Standard security

Select this option if you want to specify all login credentials manually.

Username

Specify an operating system user name. For VMware, ensure that the specified user has the following VMware vSphere roles:

Datastore -> Allocate space Datastore -> Browse datastore Datastore -> Low level file operations Datastore -> Remove file Datastore -> Rename datastore Folder -> Delete folder Folder -> Rename folder Global -> Disable methods Global -> Enable methods Global -> Licenses Host -> Configuration -> Maintenance Host -> Inventory -> Add standalone host Network -> Assign network Resource -> Assign virtual machine to resource pool Resource -> Remove resource pool Resource -> Rename resource pool Sessions -> Validate session vApp -> Delete vApp -> Rename vApp -> Add virtual machine Virtual machine -> State -> Revert to snapshot Virtual machine -> Configuration * Virtual machine -> Interaction -> Answer question Virtual machine -> Interaction -> Power Off Virtual machine -> Interaction -> Power On Virtual machine -> Inventory -> Create new Virtual machine -> Inventory -> Register Virtual machine -> Inventory -> Remove Virtual machine -> Inventory -> Unregister Virtual machine -> Provisioning * Virtual machine -> State -> Create snapshot Virtual machine -> State -> Remove snapshot

Password

Specify the user's password.

Web service root

(not available for Microsoft Hyper-V clients) Specify the web service entry point URI. Default: /sdk

Port

(not available for Microsoft Hyper-V clients)

Specify the port that VMware (vCenter Server, vSphere) is using. By default, VMware uses the port 443.

The options are pre-filled with values that were saved to the cell_info file on the Cell Manager.

More on

- About Backup
- User groups

Tasks

- Changing User Rights
- Setting Up a User Account for the Inet Service User Impersonation

Configure Virtual Machines - Advanced - Virtual Environment Integration

Specify advanced configuration settings for the vStorage Image and vCD vStorage Image backup methods. These settings apply for virtual machines that you selected in the Settings page (either for all virtual machines or only for a specific one).

Configure virtual machines

Optimize disks

Select this option to defragment and shrink virtual machine disk files (.vmdk) before they are backed up. Shrinking a virtual machine disk reclaims unused space and so reduces the amount of space the disk occupies on the host drive. Consequently, this reduces the size of backup data. However, note that such a backup needs more time to complete.

Enable changed block tracking

Select this option to create space-efficient backups, without the need to keep snapshots on the datastore (which are otherwise needed to track virtual machine changes). Default: not selected.

Not all datastores support Changed Block Tracking (CBT). If this option is selected and the datastore does not support this functionality, incremental and differential backup sessions will fail.

Use changed block tracking

Select this option to enable CBT for the datastore containing the virtual machine being backed up. Default: not selected.

If CBT is enabled, you cannot disable it using the GUI.

Allow fallback to non-CBT backups

Select this option to continue backup in a non-CBT mode for successful backup of Data Protector. Default: not selected.

When you enable CBT for the first time in VMs that have snapshots, the backed up data becomes inconsistent. In such a case, to ensure that the backup runs successfully, enable the **Allow fallback to non-CBT backups** option. If you do not enable the Allow fallback to non-CBT backups option, the backup fails continuously as the snapshots cannot be consolidated or deleted.

If the **Allow fallback to non-CBT backups** option is enabled in earlier versions of 9.04, the backup continues in a non-CBT mode. But the user-created snapshots are not backed up in a non-CBT mode and the following message is displayed in the session:

```
[Normal] From: VEPALIB_VMWARE@<hostname> “<datacenter>" Time: : Date Time Virtual Machine 'VM': Usersnap found. But only Main VM will be backed up ...
```

Snapshot handling

Quiescence is supported only for Windows guest Operating System with VMware tools installed.

Use quiescence snapshots

Select this option to use Microsoft Volume Shadow Copy Service (VSS) functionality to quiesce all applications with VSS writers before performing the backup. Default: not selected.

Level of error

Select the level of error message to be generated if the quiescence snapshot fails. Default: Warning.

Transportation mode

Select the transportation mode (NBD, NBD (SSL), Hotadd, or SAN) for backups of this virtual machine according to your network requirements. Default: Fastest available.

Configure Virtual Machines - Settings - Virtual Environment Integration

Configure virtual machines

Specify on which level you want to set the options. If you select (Common VM settings), the options apply for all virtual machines. If you select a virtual machine, the options apply only for the selected virtual machine.

Common virtual machine settings are overridden by options set at a virtual machine level.

Default: (Common VM settings).

Use default settings

(available if (Common VM settings) is selected)

Select this option if you want that the default settings are used for all virtual machines. Default: selected.

Use common settings for selected VM

(available if a virtual machine is selected)

Select this option if you want the common virtual machine settings to be used for the selected virtual machine.

Default: selected.

Use changed block tracking

Select this option to enable CBT for the datastore containing the virtual machine being backed up.

With Hyper-V, this option is always enabled. It enables RCT (Resilient Change Tracking).

Default: not selected.

If CBT is enabled, you cannot disable it using the GUI.

Allow fallback to non-CBT backups

(This is a VMware specific option)

Select this option to continue backup in a non-CBT mode for successful backup of Data Protector. Default: not selected.

When you enable CBT for the first time in VMs that have snapshots, the backed up data becomes inconsistent. In such a case, to ensure that the backup runs successfully, enable the **Allow fallback to non-CBT backups** option. If you do not enable the Allow fallback to non-CBT backups option, the backup fails continuously as the snapshots cannot be consolidated or deleted.

If the **Allow fallback to non-CBT backups** option is enabled in earlier versions of 9.04, the backup continues in a non-CBT mode. But the user-created snapshots are not backed up in a non-CBT mode and the following message is displayed in the session:

```
[Normal] From: VEPALIB_VMWARE@<hostname> “<datacenter>" Time: : Date Time Virtual Machine 'VM': Usersnap found. But only Main VM will be backed up ...
```

Snapshot handling

(not available if **Use default settings or Use common settings for the selected VM** are selected. Applicable with VMware and Hyper-V RCT. Not supported for H3C CAS).

Quiescence is supported only for Windows guest Operating System with VMware tools installed.

Use quiescence snapshots

Select this option to use Microsoft Volume Shadow Copy Service (VSS) functionality to quiesce all applications with VSS writers before performing the VEPA backup.

Select this option to configure VMs for VMware and Hyper-V RCT application consistent backups.

Default: not selected.

Level of error

(available only if Use quiescence snapshots is selected)

Select the level of error message to be generated if the quiescence snapshot fails.

With Hyper-V RCT, if the level of error is set to **Warning**, the backup will fallback to non-quiescence (crash-consistent) snapshot backup. If it is set to **Fatal**, the backup will fail with error.

Default: Warning.

Transportation mode

(This is a VMware specific option)

Select the transportation mode (NBD, NBD (SSL), Hotadd, or SAN) for backups of this virtual machine according to your network requirements. Default: Fastest available.

H3C CAS options

These are H3C CAS specific options.

Backup mode

Indicates the transport protocol to be used by the H3C CAS APIs to stage the data onto the backup host.

Default:

Linux: SCP

Windows: FTP

Use compression

If this option is selected, compressed mode will be enabled during virtual machines backup.

Default: unchecked

Client and Datacenter or Organization Selection - Virtual Environment Integration

Application

Specify the application that you want to back up, the backup method that should be used, and other backup options.

Client

Select the application client (that is, the VMware vCenter Server, VMware ESX(i) Server, Microsoft Hyper-V client, or H3C CAS client). The drop-down list contains all clients that were imported into the cell as VMware vCenter, VMware ESX(i), Microsoft Hyper-V clients, H3C CAS clients, and have therefore the (VMware vCenter), (VMware ESX(i)), (Hyper-V), or (H3C CAS) label appended at the end of their names.

In a Microsoft Hyper-V cluster environment, select any of the cluster nodes or the virtual cluster system. The result will be the same.

Microsoft Hyper-V clusters: Make sure all physical cluster nodes and the virtual cluster system have been imported into the cell as Hyper-V clients.

Backup host

Select a system to be used to control the backup.

- If you have selected a VMware ESX(i) Server system, VMware vCenter Server system, or H3C CAS Server system in the Client option, the drop-down list contains all clients that have the Virtual Environment Integration component installed.
- If you have selected a Microsoft Hyper-V client in the Client option, the drop-down list contains all clients that have the Virtual Environment Integration and the MS Volume Shadow Copy Integration components installed.

Mount host

(available if using the Virtual Environment ZDB integration for VMware) The ESX(i) Server system used to mount the replicas to back up.

Backup method

Select a method for your backup. The following methods are available:

For VMware:

- vStorageImage

For Hyper-V:

- Hyper-V Image (VSS)
- Hyper-V RCT

For H3C CAS:

- H3C CAS Non-Cached
- H3C CAS Cached

Datacenter/Organization

(available for VMware)

Select a datacenter or a vCloud Director organization to back up from.

- If you have selected a standalone ESX(i) Server system in the Client option, there is only one datacenter available - /ha-datacenter.
- If you have selected a vCenter Server system in the Client option, you can select All Datacenters to back up virtual machines from different datacenters.
- If you have selected a vCloud Director in the Client option, you can select All Organizations to back up virtual machines from different organizations.
- Backup method

Select the method to be used for the backup.

RMC does not support the vStorage Image + OpenStack backup method.

Free space required (%)

(available for VMware)

Select the percentage of disk space that should be free on a datastore before a virtual machine is backed up. The free space is calculated based on the size of the datastore where the virtual machine disks reside.

The check is performed separately for each virtual machine.

Host Pool

(available for H3C CAS)

This field specifies the host pool to which the hosts or Virtual Machines belong. From the drop-down, select a host pool to backup from.

User and group/domain

(not available)

This option specifies the operating system user account under which the backup session should run.

Specify OS user

On ESX Server clients, it is mandatory to specify the **Username** and **Group/Domain** name options.

On Windows clients, it is not mandatory to specify these options and if they are not specified, the backup runs under the local System account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account (for example, the user name `root`, group `root`, or `Administrator`, domain `DP`). Ensure that this user has been added to the `admin` or `operator` user group. This user becomes the backup owner.

On Windows clients, this user must be set up for the Inet service user impersonation.

If you selected an ESX or ESXi Server client, ensure that this user also has the read, write, and execute permissions on the ESX or ESXi Server datastores.

Backup Host Staging Details

(available for H3C CAS non-cached backup)

This specifies the staging information on backup host where the Virtual Machines are downloaded before the backup to tape.

Username

Specify a username. The specified user should have appropriate privileges to perform backup and restore of Virtual Machine.

Password

Specify the user's password.

Staging Path

The staging path refers to FTP root directory or SCP root directory configured on the backup host.

The **Browse** button lists the directory structure of the selected backup host.

RMC Configuration

(available for VMware)

- **RMC Server**: Select the RMC server for backup.
- **Backup Policy** (available only for Express Protect backups): Select the policy name that you have created in RMC. The backup policy usually contains the backup system and the backup store. For more information, see the StoreOnce RMC User Guide.
- **Snapshot Count**: Specify the number of snapshotsthat you want to create in RMC.
- **Express Protect Count** (available only for Express Protect backups): Specify the number of Express Protect snapshots that you want to create in RMC.

More on

- About Backup

Virtual Environment Settings

The virtual environment settings, some of which can be modified.

Application

Client

(cannot be modified)

The application client (that is, the VMware vCenter Server, VMware ESX(i) Server, Microsoft Hyper-V, or H3C CAS client).

Backup host

The system used to control the backup.

- With a VMware ESX(i) Server, VMware vCenter Server system, or H3C CAS client in the Client option, the drop-down list contains all clients that have the Data Protector Virtual Environment Integration component installed. If using the Data Protector Virtual Environment ZDB integration for VMware, the list contains all clients that have the Data Protector NetApp Storage Provider and Data Protector Virtual Environment Integration components installed.
- With a Microsoft Hyper-V client in the **Client** option, the drop-down list contains all clients that have the Data Protector Virtual Environment Integration and the Data Protector MS Volume Shadow Copy Integration components installed.

Mount host

(available if using the Data Protector Virtual Environment ZDB integration for VMware) The ESX(i) Server system used to mount the replicas to back up.

Datacenter/Organization

(available if using the Data Protector Virtual Environment integration for VMware)

The datacenter or the organization to back up from.

With a standalone ESX(i) Server system in the Client option, there is only one datacenter available - /ha-datacenter.

With a vCenter Server system in the Client option, you can select All Datacenters to back up virtual machines from different datacenters.

If the selected client is a vCloud Director, you can select All Organizations to back up virtual machines from different organizations.

Backup method

(cannot be modified) The method to be used for the backup.

Free space required (%)

(available if using the Data Protector Virtual Environment integration for VMware) The percentage of disk space that should be free on a datastore before a virtual machine is backed up. The free space is calculated based on the size of the datastore where the virtual machine disks reside. The check is performed separately for each virtual machine.

Start Backup - Virtual Environment Integration

Select the backup type and network load for the backup.

Backup type

- Full
- Incr
- Differential

(not available for the Hyper-V VSS and Hyper-V RCT backup method)

- Network load

More on

- About Backup
- Backup Types

Tasks

- Previewing and Starting a Backup

Start Preview - Virtual Environment Integration

Select the backup type and network load for the preview.

Backup type

- Full
- Incr
- Differential

(not available for the Hyper-V Image backup method)

- Network load

More on

- About Backup
- Backup Types

Tasks

- Previewing and Starting a Backup

Application Specific Options - MS Volume Shadow Copy Integration

The options in this page apply to the VSS integration backup.

General information

- Pre-exec
- Post-exec

More on

- About Backup
- About Backup Options
- About Pre- and Post-Exec Commands

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Backup Options - Advanced backup options

Client systems

- Application system

(This option cannot be modified.)

Provider

Select **Use Hardware Provider** if you want to perform instant recovery or if you want to keep a replica on a disk array.

Replica management

- Track the replica for instant recovery

(not available for Virtual Environment integration with Microsoft Hyper-V)

- Keep the replica after the backup
- Replica type

(available if **Track the replica for instant recovery** is selected)

Settings

Opens the Replica and array settings dialog box where you can set additional replica and disk array options.

Mount options

- Mount the replica
- Enable the backup system in read/write mode

Settings

Opens the Mount settings dialog box where you can set additional mount options.

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Configure VSS Local and Network Backup

Client systems

- Application system

Provider

Select **Use Hardware Provider** if you want to perform instant recovery or if you want to keep a replica on a disk array.

Replica management

- Track the replica for instant recovery

(not available for Virtual Environment integration with Microsoft Hyper-V)

- Keep the replica after the backup
- Replica type

(available if **Track the replica for instant recovery** is selected)

Settings

Opens the Replica and array settings dialog box where you can set additional replica and disk array options.

Mount options

- Mount the replica
- Enable the backup system in read/write mode

Settings

Opens the Mount settings dialog box where you can set additional mount options.

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration

Mount settings

Mount directory on backup system

- Root of mountpoint
- Add directories to mount path
- Automatically dismount the filesystem at destination mountpoints

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Replica and array settings

Replica management

- Configuration check mode
- Number of replicas rotated

More on

- About Backup
- About the Data Protector Microsoft Volume Shadow Copy Service Integration

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Client and Application Database Selection - Microsoft Volume Shadow Copy Service

Select the application that you want to back up.

Client

(not available for VSS backup) The client system in your cell that has the application to be backed up is selected.

Application database

MS Volume Shadow Copy Writer is selected.

User and group/domain

(available on Windows clients)

Specify OS user

It is not mandatory to specify the **Username** and **Group/Domain name** options. If they are not specified, the backup runs under the Local System Account.

Username

Group/Domain name

(available if **Specify OS user** is selected)

Specify the operating system user account under which you want the backup session to run (for example, the user name Administrator, domain DP). Ensure that this user has been added to the admin or operator user group, has the VSS rights to back up the database, and has been set up for the Inet service user impersonation.

This user becomes the backup owner.

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration
- About the Inet Service Configuration

Tasks

- Setting Up a User Account for the Inet Service User Impersonation

Start Backup - VSS

Select the backup type and network load for the backup.

Backup type

This drop-down list contains the backup types currently available for the selected VSS writer.

- Full
- Incr

(not available for ZDB to disk+tape and ZDB-to-disk sessions, where instant recovery is enabled)

Diff

(not available for ZDB-to-disk+tape and ZDB to disk sessions, where instant recovery is enabled)

- Copy
- Network Load
- Split mirror/snapshot backup

(available for ZDB-to-disk+tape and ZDB-to-disk sessions, where instant recovery is enabled)

More on

- About Backup
- Backup Types

Tasks

- Previewing and Starting a Backup

Backup Options - Advanced backup options

Client systems

- Application system

(This option cannot be modified.)

- Backup system

Replica management

- Track the replica for instant recovery

(not available for Virtual Environment integration with Microsoft Hyper-V)

- Keep the replica after the backup
- Replica type

(available if Keep the replica after the backup is selected)

Settings

Opens the Replica and array settings dialog box where you can set additional replica and disk array options.

Mount options

- Mount the replica on backup system
- Enable the backup system in read/write mode

Settings

Opens the Mount settings dialog box where you can set additional mount options.

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration
- About ZDB and IR

Tasks

- Modifying a Backup Specification
- Setting Backup Options

Configure VSS Transportable Backup

Client systems

- Application system
- Backup system

Replica management

- Track the replica for instant recovery

(not available for Virtual Environment integration with Microsoft Hyper-V)

- Keep the replica after the backup
- Replica type

(available if Keep the replica after the backup is selected)

Settings

Opens the Replica and array settings dialog box where you can set additional replica and disk array options.

Mount options

- Mount the replica on backup system
- Enable the backup system in read/write mode

Settings

Opens the Mount settings dialog box where you can set additional mount options.

More on

- About Backup
- About the Microsoft Volume Shadow Copy Service Integration
- About ZDB and IR

MS Exchange Additional Options

In this page, you select the Microsoft Exchange Server specific options in CCR environment.

- Back up any available instance from node
- Revert to active node on failure
  (not available if Information Store instance is selected for backup)
- Perform consistency check
- Throttle check for 1 second every n I/O operations

MS Exchange Additional Options

In this page, you select the Microsoft Exchange Server specific options.

- Perform consistency check
- Throttle check for 1 second every n I/O operations

Add Device

Specify the name of the new device and provide the required information about the device.

Device name

Type the name of the device you want to add. A device name can have a maximum of 32 characters, including spaces. Double quotes (") are not allowed in the device name. This user-defined name is only used by Data Protector.

Description

It is recommended to add a description of the device for easier identification. For example, you can enter the location of the device or its user. A description can have a maximum of 80 characters, including spaces.

Device type

Select the type of the device you are configuring. The following device types are available:

- Standalone
- Backup to Disk
- Stacker
- SCSI Library

When configuring a magazine device, select **SCSI Library**.

- Jukebox
- File Library
- External control
- GRAU DAS Library
- StorageTek ACS Library
- IAP Device

Data format

(available for standalone devices) Select one of the available data formats: ,**NDMP-NetApp, NDMP-Celerra, NDMP-BlueArc, NDMP-Hitachi**, or **NDMP--X9000**. When IAP Device is selected in the **Device Type** drop-down list, the data format is automatically set to CSF-R and cannot be changed.

Interface type

(available for SCSI libraries and Backup to Disk devices) Select one of the available interface types:

- **SCSI, NDMP-NetApp, NDMP-NetApp CAB, NDMP-Celerra, NDMP-BlueArc, NDMP-Hitachi**, or **NDMP--X9000** (for SCSI libraries)
- **StoreOnce Backup system, Data Domain Boost, Smart Cache**(for Backup to Disk devices), or **StoreOnce Backup system (NDMP)**.
- **Cloud** for Cloud devices.
- **Data Protector** (for File Library).
- **File Library (NDMP)**.

Client

Select the client system to which the device is connected.

NDMP Server

(available for standalone devices and SCSI libraries) If you selected an NDMP data format or interface type, select the NDMP Server from the drop-down list. In the Cluster Aware Backup (CAB) environment, you can now search for the tape libraries and robotics.

Management Console URL

(available for SCSI libraries, Backup to Disk devices-StoreOnce and Data Domain Boost, Jukeboxes, External controls, ADIC/GRAU DAS libraries, StorageTek ACS libraries, and Cloud) This option can contain a valid URL of the library management console. Spaces and double quotes (") must be entered using safe URL codes.

MultiPath device

(not available for Jukebox and File Library devices) If this option is selected, you can assign multiple paths, that is client names and SCSI addresses (device files on UNIX systems) to a single physical device.

Virtual tape library - TB based licensing (Advanced backup to disk)

(available for SCSI libraries, external controls, ADIC/GRAU DAS libraries, and StorageTek ACS libraries) When selected, this option labels the device as a virtual tape library. As a consequence, the licensing model is changed to capacity based licensing (the advanced backup to disk license-to-use), therefore you must specify the estimated library capacity consumption in terabytes (TB). By default, Data Protector handles such devices as ordinary libraries (for example, SCSI II libraries).

Estimated library capacity consumption (TB)

Specify the library capacity in terabytes. The estimated value must be an integer.

Licensing details

Click the button to obtain detailed information about advanced backup to disk license.

Adjust device for MS SQL local backup

(available for standalone and stacker devices connected to systems with Microsoft SQL Server installed) Select this option if you intend to use fast direct mode to back up Microsoft SQL Server database objects.

Username and Password

(available for Smart Cache device only) Enter the username and password of the Media Agent host in which the Smart Cache device is located.

Block size (KB)

(available if **Adjust device for MS SQL local backup** is selected) Specify the size of blocks sent to the device.

Add Device - StorageTek ACS Library

Select the type of media that will be used with the device.

Media type

In the drop-down list, select a media type for the device.

Add Device - StorageTek ACS Library

Specify the ACS Server and busy drive handling.

ACSLM Hostname

Type the name of the ACS Server that controls the library robotics.

- Busy drive handling

Use volser as medium label on initialization

A volser is written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, generates medium labels based on media pool names.

This option is supported only on GRAU DAS and StorageTek ACS libraries.

Add Device - StorageTek ACS Library

Specify the paths to the device and busy drive handling.

ACSLM hostname

Select the client from the drop-down list and enter the name of the ACS Server that controls the library robotics. Click Add to add the path to the list of configured paths.

To modify the path, select and edit the path and click Set.

To delete a path from the list, select it and click Delete.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

- Busy drive handling

Use volser as medium label on initialization

A volser is written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, generates medium labels based on media pool names.

This option is supported only on GRAU DAS and StorageTek ACS libraries.

Add Device - StorageTek ACS Library

Specify the CAPs for the device that you are configuring.

To add a CAP, specify it and click Add.

To remove a CAP, select it in the list and click Delete.

Add Device - GRAU DAS Library

Select the type of media that will be used with the device.

Media Type

In the drop-down list, select a media type for the device.

Add Device - GRAU DAS Library

Specify the DAS Server and busy drive handling.

DAS Server

Type the name of the DAS Server that controls the library robotics.

- Busy drive handling

Use volser as medium label on initialization

A volser is written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, generates medium labels based on media pool names.

This option is supported only on GRAU DAS and StorageTek ACS libraries.

Add Device - GRAU DAS Library

Specify the paths and busy drive handling.

DAS Server

Select the client from the drop-down list and enter the name of the DAS Server. Click Add to add the path to the list of configured paths.

To modify the path, select and edit the path and click Set.

To delete a path from the list, select it and click Delete.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

- Busy drive handling

Use volser as medium label on initialization

A volser is written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, generates medium labels based on media pool names.

This option is supported only on GRAU DAS and StorageTek ACS libraries.

Add Device - GRAU DAS Library

Specify the import and export areas for the device that you are configuring.

To add an import and export area, specify it and click **Add**.

To remove an import and export area, select it in the list and click **Delete**.

Add Device - External control

Select the type of media that will be used with the device.

Media Type

In the drop-down list, select a media type for the device.

Add Device - External control

If does not support a particular device, you can write a script/program that will run the robotic control to load a medium from a particular slot into the specified drive.

Control device

Specify the pathname of the exchanger control script that will control the device.

Add Device - External control

If Data Protector does not support a particular device, you can write a script/program that will run the robotic control to load a medium from a particular slot into the specified drive.

Control device

Select the client from the Client drop-down list and specify the pathname of the exchanger control script that will control the device. Click **Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

Add Device - External Control

Specify the repository slots for the device that you are configuring.

To add a slot, specify it and click **Add**. To add multiple slots simultaneously, specify a range of slots separated by a dash, for example: 1-6. Make sure you use a format supported by your library.

To remove a slot, select it in the list and click **Delete**.

Add Device - Jukebox

Select the type of media that will be used with the device.

Media type

In the drop-down list, select a media type for the device.

Add Device - Jukebox

Specify a set of files or disks for the device that you are configuring. A set of files or disks represents each side of a magneto-optical platter in the jukebox.

To add a file or disk, specify it and click Add. To add multiple files or disks simultaneously, specify a range separated by a dash, for example: /tmp/FILE1-6 .

To remove a file or disk, select it in the list and click **Delete**.

For magneto-optical jukeboxes, the disk names have to end in A/a or B/b.

Add Device - SCSI Library

Select the type of media that will be used with the device.

Media type

In the drop-down list, select a media type for the device.

Add Device - SCSI Library

Specify the slots for the device that you are configuring.

To add a slot, specify it and click **Add**. To add multiple slots simultaneously, specify a range of slots separated by a dash, for example: 1-6. Do not use letters or leading zeros.

To remove a slot, select it in the list and click **Delete**.

Cleaning slot

(not available for libraries with the barcode reader support enabled)

Select this option to specify the slot where a cleaning tape will be stored. Select the desired slot from the drop-down list.

Add Device - SCSI Library

Specify the SCSI address (a device file on UNIX systems) of the physical device, and set other options as desired.

Library robotics SCSI address

How you specify this option depends on the type of system to which the library is connected:

- Library connected to a standard MA client
- Library connected to an NDMP server

Library connected to a standard MA client

Type the SCSI address or device filename for the library robotics, or use the drop-down arrow to auto-detect it. For example:/dev/scsi/ss_2848

Library connected to an NDMP server

If you are configuring a NetApp filer library robotics, specify the physical device name consisting of the following parts:

- mc - always present, means raw SCSI jukebox
- 0, 1, 2, ... - the number of the device

For example: mc0 .

To get this information, run the sysconfig -m command on the NDMP server.

If you are configuring a Celerra filer library robotics, you must first retrieve a list of all SCSI devices attached to the server by running the following command:

```
server_devconfig server_name-list -scsi -all
```

For example, you will receive the following information for the library robotics:

```
Name Address Type Description jbox1 c2t0l0 jbox ATL P1000 62200001.03
```

Use the acquired device address file to configure the Celerra filer library robotics.

Auto-detect is not supported with the NDMP server integration.

Data drive

Specify the SCSI address of the data drive.

If the Cluster Aware Backup (CAB) drive address appears in the Address list, you can select that to auto-detect address of tape drives.

To configure and add tape drive from the list, select it and click **Add Drive**.

To delete tape drive from the list, select it and click **Delete**.

To view properties of the tape drive from the list, select it and click **Properties**.

- Busy drive handling

Barcode reader support

If the device and media can handle barcodes, you can select this option to use the barcode functionality.

Use barcode as medium label on initialization

(available if **Barcode reader support** is enabled) A barcode will be written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, will generate medium

labels based on media pool names. This option is supported only on libraries with the barcode reader support.

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, this option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

SCSI Reserve/Release (robotic control)

When selected, this option prevents the SCSI robotic control from being used by any other process or application, reserving the robotic control only for operations.

Add Device - SCSI Library

Specify the client and the SCSI address (a device file on UNIX systems) of the physical device and click**Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

Library robotics SCSI address

How you specify this option depends on the type of system to which the library is connected:

- Library connected to a standard MA client
- Library connected to an NDMP server

Library connected to a standard MA client

Type the SCSI address or device filename for the library robotics, or use the drop-down arrow to auto-detect it.

For example: /dev/scsi/ss_2848

Library connected to an NDMP server

If you are configuring a NetApp filer library robotics, specify the physical device name consisting of the following parts:

- mc - always present, means raw SCSI jukebox
- 0, 1, 2, ... - the number of the device

For example: mc0 .

To get this information, run the sysconfig -m command on the NDMP server.

If you are configuring a Celerra filer library robotics, you must first retrieve a list of all SCSI devices attached to the server by running the following command:

server_devconfig server_name-list -scsi -all

For example, you will receive the following information for the library robotics:

```
Name Address Type Description jbox1 c2t0l0 jbox ATL P1000 62200001.03
```

Use the acquired device address file to configure the Celerra filer library robotics.

Auto-detect is not supported with the NDMP server integration.

- Busy drive handling

Barcode reader support

If the device and media can handle barcodes, you can select this option to use the barcode functionality.

Use barcode as medium label on initialization

(available if **Barcode reader support** is enabled)

A barcode will be written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, will generate medium labels based on media pool names. This option is supported only on libraries with the barcode reader support.

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

SCSI Reserve/Release (robotic control)

If this option is selected, prevents the SCSI robotic control from being used by any other process or application, reserving the robotic control only for operations.

Specify the Storage Unit and Gateways

Specify the storage unit and a list of gateways for the Backup to Disk device.

Deduplication system

Provide the IP address, hostname or FC identifier of the target deduplication system.

User Name

The user name used to authenticate the device.

Password

The password for accessing the storage unit.

Storage Unit

The name of the storage unit. Click **Select/Create Storage Unit** to select the storage unit from a list of already existing storage units or create a new storage unit.

Gateways

- Source-side deduplication

Click **Properties** to view and modify source-side deduplication properties.

To add or delete a gateway, select a gateway from a list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway, click **Check**. If a store does not exist, you are prompted to create one.

Note: The default interface for each gateway is provided in the Data Interface column of the displayed properties.

To view gateway properties, select the desired gateway and click **Properties**.

Specify the Store and Gateways

Specify the store and a list of gateways for the Backup to Disk device.

Deduplication system

Provide the IP address, hostname or FC identifier of the target deduplication system. To retrieve identifier information from the management interface click **Select Service Sets**.

Client ID

(available only for StoreOnce Backup system devices)

The ID used to authenticate the device.

Password

The password for accessing the store.

Store

The name of the store.

Click **Select/Create Store** to select the store from a list of already existing stores or create a new store.

Gateways

- Source-side deduplication

Click **Properties** to view and modify source-side deduplication properties. To add or delete a gateway, select a gateway from a list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway, click **Check**. If a store does not exist, you are prompted to create one.

Note: The default interface for each gateway is provided in the Data Interface column of the displayed properties.

To view gateway properties, select the desired gateway and click **Properties**.

Limit Gateway Network Bandwidth (Kbps)

(not available if the gateway is on the same client as the StoreOnce Software store)

Select this option to limit the network bandwidth used by Media Agents when transferring data between the gateway and the B2D device during a backup or object copy session. The limit is shared by all Media Agents on the selected gateway. For source-side gateways, the bandwidth is limited between the client that is backed up and the target B2D device.

When selected, the bandwidth limit must be specified in kilobytes per second.

Default: not selected.

Add Device - Stacker

Select the type of media that will be used with the device, the default media pool, and specify further options as desired.

Media type

In the drop-down list, select a media type for the device.

Default Media Pool

Specify a media pool for media of the selected type. By default, the device will add initialized and imported media to this pool, and use media from this pool for backup.

You can either select an existing pool from the drop-down list, or create a new pool by typing its name in the text box.

If you are using the Network Data Management Protocol Server integration, It is recommended to create a special media pool for NDMP media, since the same backup medium cannot store NDMP objects and backup objects at the same time.

Disable device

If you disable a backup device, all subsequent backups skip the device. The next available device that is defined in the list of devices for the backup specification is used instead.

This enables you to avoid failed backups if a device needs service, provided that other devices are available and configured for backup.

Advanced

Click here to specify further device options.

Add Device - Stacker

Specify the SCSI address (a device file on UNIX systems) of the physical device.

Data device

Type the SCSI address or device filename of the physical device, or use the drop-down arrow to auto-detect it.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, Data Protector sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Add Device - Stacker

Specify the paths to the physical device.

Data device

Select the client from the drop-down list and enter the SCSI address (a device file on UNIX systems) of the physical device. Click **Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Add Device - Standalone

Specify the paths to the physical device.

Data device

Select the client from the drop-down list and enter the SCSI address (a device file on UNIX systems) of the physical device. Click **Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Add Device - Standalone

Select the type of media that will be used with the device, the default media pool, and specify further options as desired.

Media type

In the drop-down list, select a media type for the device.

Default Media Pool

Specify a media pool for media of the selected type. By default, the device will add initialized and imported media to this pool, and use media from this pool for backup.

You can either select an existing pool from the drop-down list, or create a new pool by typing its name in the text box.

If you are using the Network Data Management Protocol Server integration, It is recommended to create a special media pool for NDMP media, since the same backup medium cannot store NDMP objects and backup objects at the same time.

Disable device

If you disable a backup device, all subsequent backups skip the device. The next available device that is defined in the list of devices for the backup specification is used instead.

This enables you to avoid failed backups if a device needs service, provided that other devices are available and configured for backup.

Advanced

Click here to specify further device options.

Add Device - Standalone

Select the client from the drop-down list and enter the SCSI address (a device file on UNIX systems) to the physical device. Click **Add** to add the path to the list of configured paths.

To modify a path, select and edit the path and click **Set**.

To remove a path, select it in the list and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

If you are configuring a file device, specify the path of the file instead.

You can specify multiple addresses to create a device chain.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the `C` character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Settings - Data Domain Boost

Specify the store settings. For information about the store settings, review the following:

Max. Number of Connections per Store

The median of maximum write and read streams limits the physical connection.
If the number of connections exceed the maximum write or read streams, the performance starts to degrade.

Default: not set.

Backup Size Soft Quota (GB)

Enter the backup size soft quota (in GB). If the size of the data before deduplication exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the backup size quota is smaller than the store size quota, an error displays and the store size quota isn't effective.

If set to 0 or if the field is empty, the quota isn't set.

Default: not set.

Store Unit Size Soft Quota (GB)

Supported if one storage unit is created, or if quotas are manually enabled for the entire Data Domain Operating System (DD OS) and specified when the storage unit is created.

Store Media Size Threshold (GB)

Defines the threshold size of the store medium. When this size is exceeded, the objects will no longer be appended to the current store medium. By default, the store medium size is unlimited.

Single Object per Store Media

This setting applies only to backup sessions. Select this setting to enable one object per store medium.

Settings

Specify the store settings. For information about the store settings, review the following:

Max. Number of Connections per Store

Limits the number of Media Agents that can connect to each store. If this option isn't selected, the number of connections isn't limited.

Default: not selected.

Backup Size Soft Quota (GB)

Enter the backup size soft quota (in GB). If the size of the data before deduplication exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the backup size quota is smaller than the store size quota, an error displays and the store size quota isn't effective.

Default: not set. If set to 0 or if the field is empty, the quota isn't set.

Store Size Soft Quota (GB)

Enter the store size soft quota (in GB). If the size of deduplicated data on the store exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the store size quota is bigger than the backup size quota, an error displays and the store size quota isn't effective.

If set to 0 or if the field is empty, the quota isn't set.

Default: not set.

Store Media Size Threshold (GB)

Defines the threshold size of the store medium. When this size exceeds, the objects don't append to the current store medium. By default, the store medium size is unlimited.

Single Object per Store Media

This setting applies only to backup sessions. Select this setting to enable one object per store medium.

Add Drive

Select the device policies for the new drive and specify the device tag.

Device Policies

Device may be used for restore

(available for library drives)

A device with this option selected may replace any device of the same device tag. If the original device is not available for a restore session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device may be used as source device for object copy

(available for library drives)

A device with this option selected may replace any device of the same device tag. If the original device is not available for an object copy session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device Tag

(available for library drives)

Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

Add Drive

Specify the name of the new drive and provide the required information about the drive.

Device Name

Type the name of the drive you want to add. A drive name can have a maximum of 32 characters, including spaces.

Description

It is recommended to add a description of the drive for easier identification. For example, you can enter the location of the drive or its user. A description can have a maximum of 80 characters, including spaces.

Device Type

The type of the backup device.

Data Format

(available for standalone devices)

Select one of the available data formats: , **NDMP-NetApp, NDMP-Celerra, NDMP-BlueArc, NDMP-Hitachi**, or **NDMP--X9000**.

Client

(available if **MultiPath device** is not selected, not available for file jukebox devices and file libraries)

Select the client system to which the drive is connected.

NDMP Server

If you selected an NDMP data format, select the NDMP Server from the drop-down list.

MultiPath device

(not available for Jukebox and File Library devices)

If this option is selected, you can assign multiple paths, that is client names and SCSI addresses (device files on UNIX systems) to a single physical device.

Virtual tape library - TB based licensing (Advanced backup to disk)

(available when configuring new devices or changing device properties for SCSI libraries, external controls, ADIC/GRAU DAS libraries, and StorageTek ACS libraries)

When selected, this option labels the device as a virtual tape library. As a consequence, the licensing model is changed to capacity based licensing (the advanced backup to disk license-to-use), therefore you must specify the estimated library capacity consumption in terabytes (TB).

By default, handles such devices as ordinary libraries (for example, SCSI II libraries).

Adjust device for MS SQL local backup

(available for devices connected to systems with Microsoft SQL Server installed)

Select this option if you intend to use **fast direct mode** to back up Microsoft SQL Server database objects.

Block size (KB)

(available if Adjust device for **MS SQL local backup** is selected)

Specify the size of blocks sent by to the device.

Add Drive

Specify the address or filename of the data drive and the name of the drive.

Data drive

Type the address or filename of the data drive, or use the drop-down arrow to auto-detect it.

Hardware compression

(available if the device supports it)

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Drive name

Specify the name of the drive in the library.

Add Drive

Select the default media pool for the drive, and specify further options as desired.

Media type

The media type of the device.

Default Media Pool

Specify a media pool for media of the selected type. By default, the device will add initialized and imported media to this pool, and use media from this pool for backup.

You can either select an existing pool from the drop-down list, or create a new pool by typing its name in the text box.

If you are using the Network Data Management Protocol Server integration, It is recommended to create a special media pool for NDMP media, since the same backup medium cannot store NDMP objects and backup objects at the same time.

Disable device

If you disable a backup device, all subsequent backups skip the device. The next available device that is defined in the list of devices for the backup specification is used instead.

This enables you to avoid failed backups if a device needs service, provided that other devices are available and configured for backup.

Advanced

Click here to specify further device options.

Add Drive

Specify the SCSI address or device filename of the data drive and further options.

Data drive

Type the SCSI address or device filename of the data drive, or use the drop-down arrow to auto-detect it.

NDMP dedicated drives

If you are configuring a NetApp filer dedicated drive, specify the physical device name consisting of the following parts:

- rst - always present, means raw SCSI tape
- prefix: n, u - means no rewind and unload/reload, respectively
- first suffix: 0, 1, 2, ... - represents the number of the device
- second suffix: l, m, h, a - represents the data density and compression

To get this information, run the sysconfig -t command on the NetApp filer.

For example: nrst0m - no rewind device, format is: 42500 bpi 6.0GB. (The example is for a DLT4000 drive.)

If you are configuring a Celerra filer dedicated drive, you must first retrieve a list of all SCSI devices attached to the server by running the following command:

server_devconfig server_name -list -scsi -all For example, you will receive the following information for connected drives:

```
Name Address Type Description tape2 c2t3l0 tape QUANTUM DLT7000 1624q
```

Use the acquired device address file to configure the Celerra filer drives.

Auto-detect is not supported with the NDMP server integration.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Drive Index

Specify the index of the drive in the library.

Add Drive

Specify the path of the data drive and further options.

Data drive

Specify the client and the SCSI address (a device file on UNIX systems) of the physical device and click**Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

NDMP dedicated drives

If you are configuring a NetApp filer dedicated drive, specify the physical device name consisting of the following parts:

- rst - always present, means raw SCSI tape
- prefix: n, u - means no rewind and unload/reload, respectively
- first suffix: 0, 1, 2, ... - represents the number of the device
- second suffix: l, m, h, a - represents the data density and compression

To get this information, run the sysconfig -t command on the NetApp filer.

For example: nrst0m - no rewind device, format is: 42500 bpi 6.0GB. (The example is for a DLT4000 drive.)

If you are configuring a Celerra filer dedicated drive, you must first retrieve a list of all SCSI devices attached to the server by running the following command:

```
server_devconfig server_name -list -scsi -all
```

For example, you will receive the following information for connected drives:

```
Name Address Type Description tape2 c2t3l0 tape QUANTUM DLT7000 1624q
```

Use the acquired device address file to configure the Celerra filer drives.

Auto-detect is not supported with the NDMP server integration.

Hardware compression

Most modern backup devices provide built-in hardware compression. A device receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

If this option is set, sends the device an instruction to use hardware compression.

If you select the SCSI address from the drop-down list, automatically determines whether this device can use hardware compression.

On Windows, if the detection is not successful and you manually enter the SCSI address, add the C character at the end of the SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows systems, add N to the end of the device/drive SCSI address, for example: scsi:0:3:0N.

On UNIX systems, hardware compression is enabled by the selection of a hardware compression device file.

For multipath devices, this option is set for each path separately.

For a device chain, this option is set for each address (device file on UNIX systems) separately.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Drive Index

Specify the index of the drive in the library.

Add Volsers

Select the volsers that you want to add to the configured library.

Prefix

Enter the volser's prefix. It usually consists of three letters.

From

Specify the start number of the range of volsers that you want to add to the library.

To

Specify the end number of the range of volsers that you want to add to the library.

Advanced Options - Settings

In this page, advanced options for the device are specified.

Some of these options can also be set when configuring a backup. Device options set in a backup specification override options set for the device in general.

Concurrency

Concurrency allows more than one Disk Agent to write to one backup device concurrently. This helps keep the device streaming because it can accept data faster than a Disk Agent can send it. The data from these Disk Agents is interleaved on the media. The maximum concurrency value is 32. provides default concurrencies for all supported devices. The maximum device concurrency for devices that are used for backing up Microsoft Exchange Server data is 2 for devices connected to the Exchange Server system directly and 1 for those connected to the Exchange Server system remotely.

Specify the number of Disk Agents that can write concurrently to a device. This option can be specified for backup, object copy, and object consolidation operations.

Eject media after session

Use this option to have media ejected from the device after a backup or restore session has been completed. This is a safety feature that helps prevent accidental overwrites of the media by other applications. By default, media are not ejected.

Do NOT enable this option if you have previously selected the **Appendable** media usage policy; otherwise, will issue a mount request depending on media allocation policy and device type.

CRC Check

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during backup. The CRC checks allow you to verify the media after the backup. re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying media or verifying objects. By default this option is not selected. This option can be specified for backup, object copy, and object consolidation operations.

Rescan

If this option is selected, updates repository information before starting your backup. This is useful when you manually change the media order in the slot or enter and eject media.

Detect dirty drive

Select this device option to instruct to use the dirty drive functionality of a device. handles dirty drives in two ways:

If a device has no cleaning media repository, issues a 'cleanme' request. Clean the dirty drive by inserting a cleaning tape and confirm the 'cleanme' request.

If a device supports cleaning tapes and has a cleaning slot configured, automatically inserts the cleaning tape when the 'dirty drive' status is signaled by the device.

SCSI Reserve/Release (drive)

If this option is selected, prevents the SCSI drive from being used by any other process or application, reserving the drive only for operations.

Use direct library access

(available for SCSI, GRAU DAS, and StorageTek ACS libraries)

By default, the library robotics device is configured as belonging to one host only. The **Use direct library access** option enables every system to send control commands directly to library robotics. In the case of multiple systems operating the same library, this communication has to be synchronized.

The libtab file must be created on the Media Agent client for this functionality to work.

If direct access is enabled for multipath libraries, local paths (paths on the destination client) are used to control library robotics first, regardless of the configured path order.

Drive-based encryption

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media.

Advanced Options - Settings

In this page, advanced options for the gateway are specified.

Some of these options can also be set when configuring a backup. Device options set in a backup specification override options set for the device in general.

Concurrency

(not available for Backup to Disk devices)

Concurrency allows more than one Disk Agent to write to one backup device concurrently. This helps keep the device streaming because it can accept data faster than a Disk Agent can send it. The data from these Disk Agents is interleaved on the media. The maximum concurrency value is 32. provides default concurrencies for all supported devices. The maximum device concurrency for devices that are used for backing up Microsoft Exchange Server data is 2 for devices connected to the Exchange Server system directly and 1 for those connected to the Exchange Server system remotely.

Specify the number of Disk Agents that can write concurrently to a device. This option can be specified for backup, object copy, and object consolidation operations.

Eject media after session

(not available for Backup to Disk devices)

Use this option to have media ejected from the device after a backup or restore session has been completed. This is a safety feature that helps prevent accidental overwrites of the media by other applications. By default, media are not ejected.

Do NOT enable this option if you have previously selected the **Appendable** media usage policy; otherwise, will issue a mount request depending on media allocation policy and device type.

CRC Check

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during backup. The CRC checks allow you to verify the media after the backup. re-calculates the CRC during a restore and compares it to the CRC on the medium.

It is also used while verifying and copying media or verifying objects. By default this option is not selected. This option can be specified for backup, object copy, and object consolidation operations.

Rescan

(not available for Backup to Disk devices)

If this option is selected, updates repository information before starting your backup. This is useful when you manually change the media order in the slot or enter and eject media.

Detect dirty drive

(not available for Backup to Disk devices)

Select this device option to instruct to use the dirty drive functionality of a device. handles dirty drives in two ways:

If a device has no cleaning media repository, issues a 'cleanme' request. Clean the dirty drive by inserting a cleaning tape and confirm the 'cleanme' request.

If a device supports cleaning tapes and has a cleaning slot configured, automatically inserts the cleaning tape when the 'dirty drive' status is signaled by the device.

Drive-based encryption

(not available for Backup to Disk devices)

Select this option to enable hardware encryption of your backups, which prevents unauthorized access to your data during media storage and transportation. Data is compressed, encrypted, and formatted, thus completely secured before it is written to media.

For an up-to-date list of media that support drive-based encryption, see the latest support matrices.

Max. Number of Parallel Streams per Gateway

Limits the number of streams on each gateway (you can specify up to a maximum of 100 streams). If this option is not selected, the number of streams is not limited.

Default: not selected.

Limit Gateway Network Bandwidth (Kbps)

(not available if the gateway is on the same client as the StoreOnce Software store)

Select this option to limit the network bandwidth used by Media Agents when transferring data between the gateway and the B2D device during a backup or object copy session. The limit is shared by all Media Agents on the selected gateway. For source-side gateways, the bandwidth is limited between the client that is backed up and the target B2D device.

When selected, the bandwidth limit must be specified in kilobytes per second.

Default: not selected.

Server-side deduplication

(not available for source-side deduplication gateways)

Enables server-side deduplication.

Default: Selected.

Multi-Interface Support

(not available in the Solaris environment or if FC is configured as the identifier for the deduplication target)

This option applies to StoreOnce backup systems and DD Boost only. If you have configured an IP address or FQDN as your deduplication target, then **Use FC** and **Fallback to IP** options are available and they are selected by default. It is recommended that you use the IP address or the FQDN to take advantage of the multi-interface feature.

However, if you have FC configured as the identifier for the deduplication target, then you can use the merge command in CLI to move the identifiers from FC to IP.

Advanced Options - Other

In this page, advanced options for the device are specified.

Mount request

Specify the mount request script and the delay for its execution.

Delay (minutes)

Specify the delay (in minutes) before the mount request script of a device is executed. The delay is the number of minutes from the time when the mount request is issued until the time when the script is executed. This option is required if you have specified a mount request script.

Script

Specify the mount request script for this device. The mount request script is executed when there is a mount request for this device. You can use this script to perform an automatic action in response to a mount request. The action is in addition to the standard mount request dialog shown on the system.

This is useful when you want to configure unattended backups. This selection is optional, but if you enter a mount request script, you must also enter a mount request delay.

Device Lock Name

(Not available for Backup to Disk device gateways)

Specify the lock name for the device.

Use Lock Name

The device lock name prevents from using the same physical device with a different name at the same time. The**Use lock name** option locks the device during a backup or restore session. In the field, enter a lock name for the device you are configuring. For example, if you configure two backup devices using one physical device, you must use the same lock name for both.

Advanced Options - Sizes

In this page, specify the advanced options for the device.

Block size (KB)

When a device receives data, it processes it using a device-type-specific (DDS, LTO) block size. You can set the block size in the Advanced Options of the backup device by selecting a value from the drop-down list or manually typing even a higher value. supports block sizes from 8 kB to 1024 kB.

Check for supported block sizes of the current host adapter before using a higher block size. For NDMP controlled devices, check for the supported block sizes (record sizes) of the NDMP Server.

Note that can only append to media written with the same block size.

Defaults:

QIC: 32 kB

Other device types and models: 256 kB

Segment size (MB)

(not available for NDMP controlled devices)

Select the size of the data segments on the media.

The segment size affects the speed of restore and of the import of media. A smaller segment size requires additional space on the media because each segment has a fast-search mark. The additional fast-search marks result in faster restores because the Media Agent can quickly locate the segment containing the restore data. On the other hand, with smaller segments, there are more catalog segments, which makes the importing of media slower. An optimal segment size depends on the media type used in the device and the kind of data backed up. The default segment size depends on the media type.

The minimum value you can specify is 10.

Disk agent buffers

(not available for NDMP controlled devices)

The Media Agent and Disk Agent use memory buffers during data transfer. This memory is divided into a number of buffer areas. The buffer size is the number of Disk Agent blocks that a Media Agent can hold in its buffer. Values from 1-32 can be specified.

The default number of Disk Agent blocks is 8.

Device Autoconfiguration Wizard - Client Systems

Select client systems with connected backup devices that you want to autoconfigure.

Device Autoconfiguration Wizard - Devices

Select backup devices that you want to autoconfigure. Expand a device to display the robotics paths and the drives of the device.

You can switch between two views:

Group by Devices

This view displays a list of devices. Expand a device to see the robotics paths, the drives, and the clients to which the devices are connected.

Group by Hosts

This view displays a list of clients. Expand a client to see the connected devices.

To configure a device using a different name, right-click it and click **Rename**.

Automatically configure MultiPath devices

Select this option to enable automatic configuration of Multipath devices.

Device Autoconfiguration Wizard - Options

Specify additional options for the devices that will be autoconfigured.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Copy Media

In this page you select the library drive for the source medium.

Library drive

Select the library drive that will be used for the source medium.

Control

In this page, the ACS Server and busy drive handling are specified.

ACSLM Hostname

The name of the ACS Server that controls the library robotics.

- Busy drive handling

Control

In this page, the ACS Server and busy drive handling are specified.

ACSLM Hostname

Select the client from the drop-down list and enter the name of the ACS Server that controls the library robotics. Click**Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

- Busy drive handling

Repository

In this page, the CAPs of the device are specified.

To add a CAP, specify it and click **Add**.

To remove a CAP, select it in the list and click **Delete**.

Control

In this page, the DAS Server and busy drive handling are specified.

DAS Server

The name of the DAS Server that controls the library robotics.

- Busy drive handling

Control

In this page, the DAS Server and busy drive handling are specified.

DAS Server

The name of the DAS Server that controls the library robotics.

- Busy drive handling

Repository

In this page, the import and export areas of the device are specified.

To add an import and export area, specify it and click **Add**.

To remove an import and export area, select it in the list and click **Delete**.

Control

In this page, the import and export areas of the device are specified.

To add an import and export area, specify it and click **Add**.

To remove an import and export area, select it in the list and click **Delete**.

Control

If does not support a particular device, you can write a script/program that will run the robotic control to load a medium from a particular slot into the specified drive.

Control device

Select the client from the Client drop-down list and specify the pathname of the exchanger control script that will control the device. Click **Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

Control

In this page, the repository slots of the device are specified.

To add a slot, specify it and click **Add**. To add multiple slots simultaneously, specify a range of slots separated by a dash, for example: 1-6.

Make sure you use a format supported by your library. For example, when adding slots to a SCSI library, do not use letters or leading zeros.

To remove a slot, select it in the list and click **Delete**.

Device Policies

In this page, the device policies can be changed. A single device or multiple devices can be selected for the modification.

Device Policies

Device may be used for restore

(available for library drives)

A device with this option selected may replace any device of the same device tag. If the original device is not available for a restore session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device may be used as source device for object copy

(available for library drives)

A device with this option selected may replace any device of the same device tag. If the original device is not available for an object copy session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device Tag

(available for library drives)

Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

Repository

In this page, a set of files or disks for the device is specified. A set of files or disks represents each side of a magneto-optical platter in the jukebox.

To add a file or disk, specify it and click **Add**. To add multiple files or disks simultaneously, specify a range separated by a dash, for example: /tmp/FILE1-6 .

To remove a file or disk, select it in the list and click **Delete**.

For magneto-optical jukeboxes, the disk names have to end in A/a or B/b.

Settings

In this page, device settings are specified.

Media type

The media type used with the device.

Distributed file media format

(file library specific option)

Use distributed file media format

Select this option to enable the file library for virtual full backup. Backing up to a file library with distributed file media format is a prerequisite for virtual full backup.

If you are not planning to use virtual full backup, do not select this option.

Media that use distributed file media format cannot be exported or imported.

Devices - Store and Gateways

Deduplication system

The name of the deduplication system.

An IPv4 or IPv6 address, fully qualified domain name (FQDN), or an FC global identifier is supported.

Client ID

(available for StoreOnce Backup system devices)

The ID used to authenticate the device.

Password

The password for accessing the store.

Store

The name of the store.

Click **Select/Create Store** to select the store from a list of already existing stores or create a new store.

Gateways

- Source-side deduplication

Click **Properties** to view and modify source-side deduplication properties.

A list of gateways configured for this device is displayed. To add or delete a gateway, select a gateway from a list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway, click **Check**. If a store does not exist, you are prompted to create one.

To view gateway properties, select the desired gateway and click **Properties**.

Devices - Cloud Settings and Gateways

Authentication service

The Authentication Service URL of the Cloud object store.

In the Public Cloud, this is the Service API Endpoint URL of the Service Type **identity** for your region .

If you specify **Access keys** as the Authentication mode, the Authentication Service URL must end in the /v3 suffix.

For example:

https://region-b.geo-1.identity.hpcloudsvc.com:35357/v3/

Authentication mode

Specify the authentication mode: **Username and password** or **Access keys**.

Tenant / Project

The Project name of the Cloud object store.

In the Public Cloud, this is the Project name of the object store.

User Name

(available for Username and password authentication mode)

The user name used to authenticate the connection to the HPE Public Cloud.

Password

(available for Username and password authentication mode)

The password used to authenticate the connection to the HPE Public Cloud.

Access key ID

(available for Access keys authentication mode)

The access key ID for accessing the HPE Public Cloud object store.

In the Public Cloud, this is the Access Key.

Secret key

(available for Access keys authentication mode)

The secret key for authenticating the connection to the HPE Public Cloud object store.

In the Public Cloud, this is the Secret Key.

Container

The name of the Cloud object store container.

Click **Select/Create Container** to select the container from the list of already existing containers or create a new container.

Gateways

To view gateway properties, select the desired gateway and click **Properties**.

A list of gateways configured for this device is displayed. To add or delete a gateway, select a gateway from a list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway and to the Cloud, click**Check**. If a container does not exist, you are prompted to create one.

Devices - Cloud (Azure) Settings and Gateways

Storage Account Name

This is created on the Microsoft Azure portal and then used during device creation.

Access keys

The access keys are used for accessing the Azure storage. Two access keys are generated for one storage account and they can be copied from the **Microsoft Azure portal** to the device creation page in **Access Key 1** and **Access Key 2** fields.

If the first access key is invalid then the second access key is used. Each access key is of 88 character in length.

Container

The name of the Azure storage container.

Click **Select/Create Container** to select the container from the list of already existing containers or create a new container.

Following are the rules for naming a container:

- The name must start with a letter or number, and can contain only letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in container names.
- All the letters in a container name must be in lowercase.
- Container names must be in the range of 3 to 63 characters long.

Gateways

To view gateway properties, select the desired gateway and click **Properties**.

A list of gateways configured for this device is displayed. To add or delete a gateway, select that gateway from the list of available gateways and click **Add** or **Delete**. To verify if a device can connect to a gateway and to the Cloud, click **Check**. If a container does not exist, you are prompted to create one.

Devices - Cloud (Amazon S3 API compatible) Settings and Gateways

S3 Region/Glacier Region

Select the region where the bucket or vault is available or, the region where you want the bucket or vault to be created.

Access keys

The access keys (Access Key ID and Secret Access Key) are used for accessing the Amazon S3, Amazon S3 Glacier, and the Amazon S3 Glacier Deep Archive storage. Two access keys are generated for one storage account that you can access after you log in to the AWS console. Copy these keys to the device creation page in Access Key ID and Secret Access Key fields.

Bucket/Vault

The name of the Amazon S3 or Amazon S3 Glacier Deep Archive storage bucket, or Amazon S3 Glacier Vault.

Click **Select/Create Bucket** in case of Amazon S3 or Amazon S3 Glacier Deep Archive, or**Select/Create Vault** incase of Amazon S3 Glacier, to select the bucket or vault from the list of already existing ones or create a new bucket or vault.

Following are the rules for naming a bucket:

- Bucket names must be in the range of 3 to 63 characters long. The name must start with a lowercase letter or number, and can contain only lowercase letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in bucket names.
- You cannot use underscores, consecutive periods, or use dashes adjacent to periods in a bucket name. Additionally, the bucket name cannot end with a dash.
- Bucket names must be globally unique.

For more information on the bucket naming rules, see AWS documentation at https://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html.

Following are the rules for naming a vault:

- Vault names must be in the range of 3 to 63 characters long. The name must start with a letter or number, and can contain only letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in vault names.
- You cannot use underscores, consecutive periods, or use dashes adjacent to periods in a vault name. Additionally, the bucket name cannot end with a dash.
- Vault names must be globally unique.

Gateways

To view gateway properties, select the desired gateway and click**Properties**.

A list of gateways configured for this device is displayed. To add or delete a gateway, select that gateway from the list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway and to the Cloud, click**Check**. If a bucket or vault does not exist, you are prompted to create one.

Devices - Storage Units and Gateways

Deduplication system

The name of the deduplication system.

User Name

The user name used to authenticate the device.

Password

The password for accessing the storage unit.

Storage Unit

The name of the storage unit.

Click **Select/Create Storage Unit** to select the storage unit from a list of already existing storage units or create a new storage unit.

Gateways

- Source-side deduplication

Click **Properties** to view and modify source-side deduplication properties.

A list of gateways configured for this device is displayed. To add or delete a gateway, select a gateway from a list of available gateways and click **Add** or **Delete**. To verify if can connect to a gateway, click **Check**. If a store does not exist, you are prompted to create one.

To view gateway properties, select the desired gateway and click **Properties**.

Devices - Settings

Specify the store settings. For information about the store settings, review the following:

Max. Number of Connections per Store

Limits the number of Media Agents that can connect to each store. If this option isn't selected, the number of connections isn't limited.

Default: not selected.

Backup Size Soft Quota (GB)

Enter the backup size soft quota (in GB). If the size of the data before deduplication exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the backup size quota is smaller than the store size quota, an error displays and the store size quota isn't effective.

If set to 0 or if the field is empty, the quota isn't set.

Default: not set.

Store Size Soft Quota (GB)

Enter the store size soft quota (in GB). If the size of deduplicated data on the store exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the store size quota is bigger than the backup size quota, an error displays and the store size quota isn't effective.

Default: not set. If set to 0 or if the field is empty, the quota isn't set.

Store Media Size Threshold (GB)

Defines the threshold size of the store medium. When this size exceeds, the objects don't append to the current store medium. Note that the media size isn't unlimited. By default, there is a 500 GB limit enforced on Backup to Disk (B2D) libraries.

The Store Media Size Threshold only works on integration backups, such as Oracle, where the same B2D media (in sequence) backs up several data files . When the size threshold reaches, no further append is possible and a new media gets allocated. It doesn't work on file system objects, if you try to limit the media size to a user defined limit (for example, 200 GB) to reduce data loss in case of a failed media.

Single Object per Store Media

This setting applies only to backup sessions. Select this setting to enable one object per store medium.

StoreOnce Backup System (NDMP) has this setting enabled by default and you can't change it

Devices - Data Domain Boost Settings

Note: If the Data Domain device is configured for multiple storage units (LSU) by the same or different backup application, it is highly recommended to enable soft or hard quotas on the storage units used by Data Protector. This allows proper reporting of the Advanced Backup to Disk license requirements.

Max. Number of Connections per Storage Unit

The median of maximum write and read streams limits the physical connection.

If the number of connections exceed the maximum write or read streams, the performance starts to degrade.

Backup Size Soft Quota (GB)

Enter the backup size soft quota (in GB). If the size of the data prior to deduplication exceeds the set quota, the session displays a warning, but the data is still written to the store. The quota is effective for backup, replication, and object consolidation sessions.

If the backup size quota is smaller than the store size quota, an error is displayed and the store size quota is not effective.

Default: not set. If set to 0 or if the field is empty, the quota is not set.

Storage Unit Size Soft Quota (GB)

Supported if one storage unit is created, or if quotas are manually enabled for the entire Data Domain Operating System (DD OS) and specified when the storage unit is created.

Storage Unit Item Size Threshold (GB)

Defines the threshold size of the storage unit item. When this size is exceeded, the objects will no longer be appended to the current storage unit item. By default, the storage unit item size is unlimited.

Single Object per Storage Unit Item

Select to enable one object per storage unit item.

Devices - Gateways

In this page, the type of media used with the gateway, the default media pool, and some further options are specified.

Media type

The media type used with the gateway is displayed.

Default Media Pool

(not available for Backup to Disk devices.)

Specify a media pool for media of the selected type. By default, the device will add initialized and imported media to this pool, and use media from this pool for backup.

You can either select an existing pool from the drop-down list, or create a new pool by typing its name in the text box.

If you are using the Network Data Management Protocol Server integration, It is recommended to create a special media pool for NDMP media, since the same backup medium cannot store NDMP objects and backup objects at the same time.

Disable gateway

If you disable a gateway, all subsequent backups skip the gateway. The next available gateway that is defined in the list of gateways for the backup specification is used instead.

This enables you to avoid failed backups if a gateway is not accessible, provided that other gateways are available and configured for backup.

Advanced

Click here for further gateway options.

Devices - General

This page displays general information about the device.

Device name

The user-defined name of the device. A device name can have a maximum of 32 characters, including spaces.

Description

A description of the device, if one was provided. A description can have a maximum of 80 characters, including spaces.

Device type

The type of the device. The following device types are available:

- Standalone (also for standalone file device)
- Backup to Disk
- Stacker
- SCSI Library
- Jukebox
- File Library
- External control
- GRAU DAS Library
- StorageTek ACS Library
- IAP Device

Data Format

(available for standalone devices) One of the available data formats: ,**NDMP-NetApp, NDMP-Celerra, NDMP-BlueArc, NDMP-Hitachi**, or **NDMP-HPE-X9000**. When **IAP Device** is selected in the **Device Type** drop-down list, the data format is automatically set to CSF-R and cannot be changed.

Interface type

(available for SCSI libraries and Backup to Disk devices)

One of the available interface types:

- **SCSI, NDMP-NetApp, NDMP-NetApp CAB, NDMP-Celerra, NDMP-BlueArc, NDMP-Hitachi**, or **NDMP-HPE-X9000** (for SCSI libraries)
- **StoreOnce software deduplication, StoreOnce Backup system, DataDomain Boost**, **Smart Cache**, **Cloud**, or **Deduplication Store** (for Backup to Disk devices)

Client

(not available if **MultiPath device** is selected)

The client system to which the device is connected.

NDMP Server

(available for standalone devices and SCSI libraries)

An NDMP Server is needed if an NDMP data format or interface type was selected.

Management Console URL

(available for SCSI libraries, jukeboxes, external controls, ADIC/GRAU DAS libraries, StorageTek ACS libraries and Cloud.)

This option can contain a valid URL of the library management console. Spaces and double quotes (") must be entered using safe URL codes.

The option is available for SCSI libraries, Backup to Disk devices (StoreOnce and Data Domain Boost), jukeboxes using optical media, external controls, GRAU DAS libraries, and StorageTek ACS libraries. It can also be used in NDMP environments.

MultiPath device

(not available for Jukebox and File Library devices)

If this option is selected, you can assign multiple paths, that is client names and SCSI addresses (device files on UNIX systems) to a single physical device.

Virtual tape library - TB based licensing (Advanced backup to disk)

(available when configuring new devices or changing device properties for SCSI libraries, external controls, ADIC/GRAU DAS libraries, and StorageTek ACS libraries)

When selected, this option labels the device as a virtual tape library. As a consequence, the licensing model is changed to capacity based licensing (the advanced backup to disk license-to-use), therefore you must specify the estimated library capacity consumption in terabytes (TB).

By default, handles such devices as ordinary libraries (for example, SCSI II libraries).

Estimated library capacity consumption (TB)

Specify the library capacity in terabytes. The estimated value must be an integer.

Licensing details

Click the button to obtain detailed information about advanced backup to disk license.

Device filter tag

Helps identify device targets for backup.

- Name

Source-side gateway properties - General

This page displays general information about the device.

Gateway name

The user-defined name of the gateway. A gateway name can have a maximum of 32 characters, including spaces.

Description

A description of the gateway, if one was provided. A description can have a maximum of 80 characters, including spaces.

Device type

(set to Backup to disk)

Interface type

(set to StoreOnce software deduplication or StoreOnce Backup system, or Data Domain Boost, depending on the type of the device)

Gateway system

(set to localhost)

NDMP Server

(not available for source-side gateways)

Management Console URL

(not available for Backup to Disk devices)

MultiPath device

(not available for Backup to Disk devices)

Virtual tape library - TB based licensing (Advanced backup to disk)

(not available for Backup to Disk devices)

Estimated library capacity consumption (TB)

(not available for Backup to Disk devices)

Licensing details

(not available for Backup to Disk devices)

Device filter tag

Helps identify device targets for backup.

- Name

Settings

In this page, the type of media used with the device the default media pool, and some further options are specified.

Media type

The media type used with the device or gateway is displayed.

Default Media Pool

Specify a media pool for media of the selected type. By default, the device will add initialized and imported media to this pool, and use media from this pool for backup.

You can either select an existing pool from the drop-down list, or create a new pool by typing its name in the text box.

If you are using the Network Data Management Protocol Server integration, It is recommended to create a special media pool for NDMP media, since the same backup medium cannot store NDMP objects and backup objects at the same time.

Disable device

If you disable a backup device, all subsequent backups skip the device. The next available device that is defined in the list of devices for the backup specification is used instead.

This enables you to avoid failed backups if a device needs service, provided that other devices are available and configured for backup.

Advanced

Click here for further device options.

Devices - Policies

In this page, device policies for the device are specified.

Device policies

Device may be used for restore

(available for library drives) A device with this option selected may replace any device of the same device tag. If the original device is not available for a restore session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device may be used as source device for object copy

(available for library drives)

A device with this option selected may replace any device of the same device tag. If the original device is not available for an object copy session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Device tag

(available for library drives)

Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

Control

In this page, the SCSI address (a device file on UNIX systems) of the physical device is specified.

Library's robotic SCSI address

You can type the SCSI address or device filename for the library's robotics. If the Media Agent client is running on a Windows or Linux operating system, you can use the drop-down arrow to auto-detect the SCSI address or device filename.

Data drive

Specify the SCSI address of the data drive.

If the Cluster Aware Backup (CAB) drive address appears in the Address list, you can select that to auto-detect address of tape drives.

To configure and add tape drive from the list, select it and click **Add Drive**.

To delete tape drive from the list, select it and click **Delete**.

To view properties of the tape drive from the list, select it and click **Properties**.

- Busy drive handling

Barcode reader support

If the device and media can handle barcodes, you can select this option to use the barcode functionality.

Use barcode as medium label on initialization

(available if **Barcode reader support** is enabled)

A barcode will be written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, will generate medium labels based on media pool names. This option is supported only on libraries with the barcode reader support.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive. SCSI Reserve/Release (robotic control)

If this option is selected, prevents the SCSI robotic control from being used by any other process or application, reserving the robotic control only for operations.

Control

In this page, the SCSI address (a device file on UNIX systems) of the physical device is specified.

Library's robotic SCSI address

You can type the SCSI address or device filename for the library's robotics. If the Media Agent client is running on a Windows or Linux operating system, you can use the drop-down arrow to auto-detect the SCSI address or device filename.

- Busy drive handling

Barcode reader support

If the device and media can handle barcodes, you can select this option to use the barcode functionality.

Use barcode as medium label on initialization

(available if **Barcode reader support** is enabled)

A barcode will be written as a medium label to the medium header on the tape each time you initialize a medium using the library with this option set. If this option is not selected, will generate medium labels based on media pool names. This option is supported only on libraries with the barcode reader support.

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Repository

In this page, the slots of the device are specified.

To add a slot, specify it and click **Add**. To add multiple slots simultaneously, specify a range of slots separated by a dash, for example: 1-6.

Make sure you use a format supported by your library. For example, when adding slots to a SCSI library, do not use letters or leading zeros.

To remove a slot, select it in the list and click **Delete**.

Cleaning slot

(not available for libraries with barcode reader support enabled)

Select this option to specify the slot where a cleaning tape will be stored. Select the desired slot from the drop-down list.

Drive

In this page, the SCSI address (a device file on UNIX systems) of the physical device is specified.

Data device

You can type the SCSI address or device filename of the physical device, or use the drop-down arrow to auto-detect it.

- Hardware compression

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB. Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option. Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled) This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drive

Data device

Specify the client and the SCSI address (a device file on UNIX systems) of the physical device and click**Add** to add the path to the list of configured paths.

To modify the path, select and edit the path and click **Set**.

To delete a path from the list, select it and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

- Hardware compression

Automatically discover changed SCSI address

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drives

In this page, the SCSI address (a device file on UNIX systems) of the physical device is specified.

To add a SCSI address or device file, specify it and click **Add**. To remove a SCSI address or device file, select it in the list and click **Delete**.

For file devices, the path of the file is specified.

You can specify multiple addresses to create a device chain.

- Hardware compression

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drives

In this page, the client and the SCSI address (a device file on UNIX systems) of the physical device are specified.

Data drive

To add path to the list of configured paths, select the client from the Client drop-down list and enter the SCSI address (a device file on UNIX systems) of the physical device are specified. Click **Add**.

To modify a path, select and edit the path and click **Set**.

To remove a path, select it in the list and click **Delete**.

To change the path priority, select the path and use the arrow buttons on the right side of the list to move the path up or down in the list.

For file devices, the path of the file is specified.

You can specify multiple addresses to create a device chain.

- Hardware compression

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drive

In this page, the SCSI address or device filename of the data drive and some further options are specified.

Data drive

You can type the SCSI address or device filename of the data drive, or use the drop-down arrow to auto-detect it.

Auto-detect is not supported with the NDMP server integration.

- Hardware compression

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if **Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drive Index

The index of the drive in the library.

Drive

In this page, the SCSI address or device filename of the data drive and some further options are specified.

Data drive

You can type the SCSI address or device filename of the data drive, or use the drop-down arrow to auto-detect it.

Auto-detect is not supported with the NDMP server integration.

- Hardware compression

Automatically discover changed SCSI address

(available if only one SCSI address is specified)

With this option selected checks the serial number of the SCSI device. In case that the serial number differs from the number stored in the IDB, a process of device path discovery is launched. The found new address is added to the IDB.

Additionally, the option enables to recognize that a physical device has been replaced with another one based on a stored location of a drive in a library. The serial number of the old (failed) device is then automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only.

If this option is not selected and the SCSI address of the device changes, the backup session will fail. In SAN environments it is recommended to use this option.

Do not use this option for devices without serial numbers.

Device serial number

(available if**Automatically discover changed SCSI address** is enabled)

This field displays the device serial number. To reload the serial number on the next operation, click on the **Reload** button. The serial number is replaced with the text stating that the serial number will be reloaded.

In case that a physical device is changed, the serial number of the old device is automatically replaced by a new one (of the new device). This is available for SCSI tape drives located in SCSI libraries only. For libraries using other protocols (ACSLS, DAS, NDMP devices), you must manually reload the device serial number after replacing the drive.

Drive Index

The index of the drive in the library.

Drive

Data drive

You can type the SCSI address or device filename of the data drive, or use the drop-down arrow to auto-detect it.

- Hardware compression

Drive Name

The name of the drive in the library.

Eject Media

Specify the new media location and other eject options for the media that you want to eject.

Specify new location

Select to change the location information for the media. Specify the new location.

Media location information helps you find the medium. You should update the location whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB. allows you to create a list of predefined locations to simplify vaulting and archiving.

CAP or Import/Export Area

Select the CAP or Import/Export Area that you want to use for ejecting the media.

Auto Export

Select this option if you want to automatically export the ejected media from the IDB.

Eject Medium

Specify the new location for the media that you want to eject.

Specify new location

Select to change the location information for the media. Specify the new location.

Media location information helps you find the medium. You should update the location whenever you move media (for example, to off-site storage). The location information is written on the media and in the IDB.

allows you to create a list of predefined locations to simplify vaulting and archiving.

Enter Media

Specify the CAP or Import-Export Area to be used for entering the media.

CAP or Import/Export area

Select the CAP or Import/Export Area that you want to use for entering the media.

Erase

Select the library drive that will be used for the operation.

Library drive

Select a drive that will be used to erase the selected media.

Erase Medium

Specify options for the operation.

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed.

If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

(not available for erasing media)

Format Media

Select a media pool for the medium.

Media Pool

Select the media pool to which the formatted medium will be added.

Gateways - Policies

In this page, device policies for the gateway are specified.

Gateway policies

Gateway may be used for restore

(available for B2D stores)

A device with this option selected may replace any device of the same device tag. If the original device is not available for a restore session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Gateway may be used as source device for object copy

(available for B2D stores)

A device with this option selected may replace any device of the same device tag. If the original device is not available for an object copy session, automatically selects an alternative device of the same type, located in the same library.

Default: not selected.

Gateway Tag

(available for B2D stores)

Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

Import Media

Select the library drive or gateway that will be used for the operation.

Library Drive

Select the drive that will be used to import the selected media.

Gateway

(available for backup to disk (B2D) devices)

Select the gateway that will be used to format the selected media.

Import Media

Select a media pool for the medium.

Media Pool

Select the media pool to which the imported medium will be added.

Container

This tab displays details of the current Cloud backup to disk container settings. This includes the following information:

Container

The Cloud container to which the Cloud device is configured.

Used Size

The total storage usage as reported by the HPE Public Cloud object store.

Container

This tab displays details of the current Cloud (Azure) backup to disk container settings. This includes the following information:

Container

The Cloud container to which the Cloud (Azure) device is configured.

Used Size

The total storage usage as reported by the Cloud (Azure) object store.

Container - Bucket/Vault

This tab displays details of the current Cloud (Amazon S3 , Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) backup to disk bucket/vault settings. This includes the following information:

Bucket/Vault

The Cloud bucket or vault to which the Cloud (Amazon S3 API compatible, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) device is configured.

Used Size

The total storage usage as reported by the Cloud (Amazon S3 API compatible, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) object store.

S3 Tiers

You can set S3 Glacier and Deep Archive tiers. For more information and pricing details, see the AWS S3 Glacier documentation.

Standard

With the **Standard** tier, the restore will start in 3-4 hours for S3 Glacier and in 4-12 hours for Deep Archive Glacier.

The **Standard** tier has three data retrieval policies based on data retrieval limits. These data retrieval policies are applicable to S3 Glacier only. They are:

- Free tier only
- Maximum retrieval rate
- No retrieval limit

If you select **Maximum retrieval rate**, the **GB/Hour** option appears where you can specify the maximum retrieval rate. By default it is set to 1.

Bulk

With the **Bulk** tier, the restore will start in 5-12 hours for S3 Glacier and in 12-48 hours for Deep Archive Glacier.

Expedited

With the **Expedited** tier, the restore will start in 1-5 minutes and is applicable only for S3 Glacier.

Gateways

This tab is for information purposes and shows you details of the current backup to disk gateway settings. It includes the following information:

Name

The name of the gateway.

B2D Device

The name of the Backup to Disk device for which the gateway is configured.

Gateway system

The name of the system which provides the gateway.

Policy

The type of the device.

Media / Interface type

The type of the interface.

Description

A description of the gateway, if one was provided.

Lock name

(Not available for Backup to Disk device gateways)

The lock name of the gateway, if one was provided.

Restore Policy

The configured gateways can be enabled or disabled for a restore.

Copy Policy

The configured gateways can be enabled or disabled for an object copy.

Device Tag

The device tag name of the gateway, if one was provided.

Max. Number of Parallel Streams

The maximum number of parallel streams allowed for the gateway.

Server-side Deduplication

(available for StoreOnce Backup system devices) Displays if server-side deduplication is enabled for the gateway.

Right-click a gateway to scan, enable or disable the gateway, delete or change gateway policies, or display the properties of the gateway.

Libraries

In the Results Area, you can choose between slots and drives of the selected library.

The following may provide additional information:

- To display the properties of a library, right-click the library and click **Properties**.
- To display the configured drives of the library, double-click **Drives** in the Results Area.
- To display the slots of the library, double-click **Slots** in the Results Area.
- To display the containers and gateways of a Cloud library, double-click **Containers** or **Gateways** in the Results Area.

Drives

In the Results Area, a list of configured drives of a specific library is displayed.

Name

The logical name of the configured drive.

Library

The name of the library in which the drive resides.

Client system

The name of the client system to which the drive is connected.

Policy

The type of the drive.

Media Type

The media type of the drive.

Description

A description of the drive, if one was provided.

Lock Name

The lock name, if one is used.

Restore Policy

(available for library drives) The configured drives can be enabled or disabled for a restore.

Copy Policy

(available for library drives) The configured drives can be enabled or disabled for an object copy.

Device Tag

(available for library drives) Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

Right-click a drive to scan, delete or change device policies, or display the properties of the drive. Note, that scanning the file library device is available, if it contains file depots, which means that a backup has been performed to this device.

Robotics Paths

In the Results Area, a list of paths which are used for controlling the robotics of a specific library is displayed.

The path is displayed as *clientname : SCSI address*.

Slots

In the Results Area, a list of slots of a specific library is displayed.

File Depot's Name

(Cloud devices specific) The name of the Cloud file depot in the HPE Public Cloud.

Size (GB)

(Cloud devices specific) The amount of space used by the file depot in the HPE Public Cloud.

Slot (Side)

The number of the slot in the library. If the slot contains a medium and barcode reader support is enabled, the barcode of the medium is also listed (in brackets).

Quality

The physical condition of the medium in the slot. It can be good, fair, or poor. Media in poor condition should be replaced.

Volser

(ADIC/GRAU and StorageTek devices specific) The volser of the medium.

Location

The location of the medium in the slot (enclosed in brackets), and if provided, the location of the medium when it is not in the library.

Format

The format of the medium recognized by Data Protector, such as Data Protector, Data Protector foreign, tar, cpio, cleaning tape, blank, unknown, empty (if there is no medium

in the slot), and so on.

Protection

The protection of the data on the medium.

Available Space (MB)

The amount of space that is still available on the medium.

Pool

The name of the media pool to which the medium belongs.

Description

A description of the medium. If available, the barcode is also provided (enclosed in brackets).

To display the properties of a slot and the medium in it, right-click the slot and click Properties.

Devices

The table below describes the device properties that are displayed in the results area. For more information on Devices and Device Types, see About Backup Devices.

Device properties

Property	Description
Name	The logical name of the configured device.
Library (*available for libraries*)	The name of the library in which the device resides.
Client System	The name of the client system to which the device is connected.
Policy	The type of the device.
Media Type	The media type of the device.
Description	A description of the device, if provided.
Lock Name	The lock name, if used.
Restore Policy (*available for libraries*)	The configured devices can be enabled or disabled for a restore.
Copy Policy (*available for libraries*)	The configured devices can be enabled or disabled for an object copy.
Device Tag (*available for libraries*)	Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces. The following may provide additional information: • To add a new device, right-click **Devices** and click **Add Device**. • To display the properties of a device, right-click the device and click **Properties**.

To use the filters available for the displayed list, click on **Show filter settings** and modify the parameters. On how to use the filter settings, see the Using the Filter Settings task topic below.

Name

The logical name of the configured device.

Library

(available for libraries)

The name of the library in which the device resides.

Client System

The name of the client system to which the device is connected.

Policy

The type of the device.

Media Type

The media type of the device.

Description

A description of the device, if one was provided.

Lock Name

The lock name, if one is used.

Restore Policy

(available for libraries) The configured devices can be enabled or disabled for a restore.

Copy Policy

(available for libraries)

The configured devices can be enabled or disabled for an object copy.

Device Tag

(available for libraries)

Specify a name for the device tag. Devices with the same device tag name can replace each other if needed. Ensure that such devices are of the same media type and from the same library. Otherwise, the automatic replacement cannot be successful. The name can consist of maximum 80 characters, including spaces.

The following may provide additional information:

- To add a new device, right-click **Devices** and click **Add Device**.
- To display the properties of a device, right-click the device and click **Properties**.

Devices by Host

In the Results Area, a list of clients is displayed. When you double-click on the client name, a list of configured devices for the selected client is displayed, provided that devices have already been configured.

Stores

This tab is for information purposes and shows you details of the current Backup to Disk store settings. It includes the following information:

Store

The name of the store (including the hostname).

Used size (GB)

The amount of space allocated to the store which has already been used for backups.

Deduplication Ratio

The ratio between size of the source data that was backed up and the size of the actual data which is written to the store.

Federation Members

This tab lists all the members of the selected federated store. It includes the following information:

Federation Member

The hostname of the store's federation member.

Status

The status (Online or Offline) of the federation member.

Environment

In the Scoping Pane, you can choose among Automated Operations, Devices, Devices by host, and Media.

To display Help on a specific item, select the desired item in the Scoping Pane.

Formatting Media

Select the library drive that will be used for the operation.

Library Drive

Select the drive that will be used to format the selected media.

Scan Media

Select the library drive that will be used for the operation.

Library Drive

Select a drive that will be used to scan the selected media.

Scan a Medium

Specify options for the operation.

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

(not available for scanning)

Select or Create Container

Select a container from a list of already existing containers. Alternatively, create a container.

Select existing container

If you have already configured containers, select a container from the list of existing containers, and click OK.

Create new container

Select to create a new container.

Container name

Enter the name for the container.

Select or Create Container

Select a container from a list of already existing containers. Alternatively, create a container.

Select existing container

If you have already configured containers, select a container from the list of existing containers, and click**OK**.

Create new container

Select to create a new container.

Container name

Enter the name for the container.

Select or Create Bucket

Select a bucket/Vault from a list of already existing buckets/vaults. Alternatively, create a new one.

Select existing bucket/vault

If you have already configured buckets or vaults, select a one from the list, and click OK.

Create new bucket/vault

Select to create a new bucket or vault.

Bucket/Vault name

Enter the name for the bucket or vault.

Select Service Set

Specify the management console account details.

StoreOnce

Enter the details for the following fields:

- Management System
- Username
- Password

Click **Query Service Sets**, to retrieve the list of IP or FC identifiers.

Service Sets

The available Service Sets are displayed in this section of the dialog box. Select the required IP or FC identifiers.

Note: FC identifiers are displayed only if IP identifiers are not available.

Select Storage Unit

Select a storage unit from a list of already existing teamed and non-teamed storage units. Alternatively, create a non-teamed storage unit.

You cannot create a teamed storage unit using the GUI.

Select existing storage unit

If you have already configured storage units, select a storage unit from a list of existing storage units, and click OK.

Create new storage unit

Select to create a non-teamed storage unit.

Storage unit name

Enter the name of the storage unit.

Cloud options

Local cache (GB)

When you opt for cloud support, some of your data will still be saved on a local drive. In this text box, you can enter how much of data you want to save on the local drive. By default, the value is 30 GB. You can choose to save upto 999999 GB on local drive.

Storage type

Select the type of cloud device you want to save your data to. The following cloud storage types are supported:

Amazon S3

S3 Region

Select the region where the bucket or vault is available or, the region where you want the bucket or vault to be created.

Access Key ID and Secret Access Key

The access keys (Access Key ID and Secret Access Key) are used for accessing the Amazon S3 storage. Two access keys are generated for one storage account that you can access after you log in to the AWS console. Copy these keys to the device creation page in Access Key ID and Secret Access Key fields.

Bucket

The name of the Amazon S3 storage bucket.

Following are the rules for naming a bucket:

- Bucket names must be in the range of 3 to 63 characters long. The name must start with a lowercase letter or number, and can contain only lowercase letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in bucket names.
- You cannot use underscores, consecutive periods, or use dashes adjacent to periods in a bucket name. Additionally, the bucket name cannot end with a dash.
- Bucket names must be globally unique.

Amazon S3 compatible cloud targets

S3 Target Gateway URL

Enter the S3 Target Gateway URL.

Access Key ID and Secret Access Key

The access keys (Access Key ID and Secret Access Key) are used for accessing the Amazon S3 compatible cloud target storage. Two access keys are generated for one storage account that you can access after you log in to the AWS console. Copy these keys to the device creation page in Access Key ID and Secret Access Key fields.

Bucket

The name of the Amazon S3 compatible cloud target storage bucket.

Following are the rules for naming a bucket:

- Bucket names must be in the range of 3 to 63 characters long. The name must start with a lowercase letter or number, and can contain only lowercase letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in bucket names.
- You cannot use underscores, consecutive periods, or use dashes adjacent to periods in a bucket name. Additionally, the bucket name cannot end with a dash.
- Bucket names must be globally unique.

Azure

Storage Account Name

This is created on the Microsoft Azure portal and then used during device creation.

Access key

The access key used for accessing the Azure storage. It is generated for one storage account and it can be copied from the **Microsoft Azure portal** to the device creation page in **Access Key** fields.

The access key is of 88 character in length.

Container

The name of the Azure storage container.

Following are the rules for naming a container:

- The name must start with a letter or number, and can contain only letters, numbers, and the dash (-) character.
- Each dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in container names.
- All the letters in a container name must be in lowercase.
- Container names must be in the range of 3 to 63 characters long.

Google cloud

Google region

This is a non-changable field. The default selection is **Multi-Regional storage**.

Access Key ID and Secret Access key

The Access Key ID and Secret Access key are used to access the google cloud storage. Enter these keys manually.

Bucket

The name of the Google cloud bucket. Enter the name manually.

Select or Create Store

To create a B2D device, select an existing store or create a new store.

With StoreOnce software deduplication, you cannot create a federated store using the Data Protector GUI.

Select existing store

(StoreOnce specific option)

If you have already configured stores, select a store from a list of existing stores, and click**OK**.

Select existing deduplication store

(Deduplication store specific option)

If you have already configured stores, select a store from a list of existing stores, and click**OK**.

Encryption Filter

(available for the StoreOnce Backup system interface only)

Filters the selection of already existing encrypted and non-encrypted stores. You can choose among the following:

Option	Description
Any	All configured stores are displayed.
Encrypted	Only encrypted stores are displayed.
Non-Encrypted	Only non-encrypted stores are displayed.

Federation Filter

(available for the StoreOnce Backup system interface only)

Filters the selection of already existing federated and non-federated stores. You can choose among the following:

Option	Description
Any	All configured stores are displayed.
Federated	Only federated stores are displayed.
Non-Federated	Only non-federated stores are displayed.

Create new store

Select to create a non-federated store.

Creation of store through Data Protector is no longer supported for StoreOnce device.

Create new deduplication store

(Deduplication store specific option)

Select this option to create a new deduplication store. When selected, the **Create new store** section is activated.

Store name

Enter the name of the store based on the following:

Interface type	Supported characters
Data Domain Boost	[a-z][A-Z][0-9][_-.+]
StoreOnce software deduplication	[a-z][A-Z][0-9][_]
Deduplication store	[a-z][A-Z][0-9][_]

Dedupe directory

(Deduplication store specific option)

Browse and select a path where you want to create a store on the deduplication server. You can create a new folder by entering the folder name in the path.

Metadata directory

(Deduplication store specific option)

You can choose to save the metadata on a directory other than the dedupe directory in order to speed up the deduplication process. Browse and select the directory of your choice. By default, the dedupe directory is selected. This is an optional field.

Encrypt store

(Deduplication store specific option)

Select this option to encrypt the data after the deduplication process.

Use a dedicated port

(Deduplication store specific option)

By default, there is a common port used for all stores that are created. Select this check-box if you want to use a separate port for the store you are creating.

Cloud support

(Deduplication store specific option)

Select this option for creating deduplication store on a cloud storage:

- For AWS S3 and Azure, use the Data Protector GUI to directly create the container used for creating the Deduplication Store.
- For Google and S3 compatible supported cloud targets, create the container by using the respective cloud interface and then specify the container name in the Data Protector GUI to create the deduplication store on it.

Usage

The pie chart displays estimated free space and used space on the medium.

Summary Tab - Cloud (Azure) Device

This tab is for information purposes and shows you details for the current Cloud (Azure) settings. This includes the following information:

Container

The Cloud container to which the Cloud (Azure) device is configured.

Used Size

The total storage usage as reported by the Cloud (Azure) object store.

Summary Tab - Cloud Device

This tab is for information purposes and shows you details of the current Cloud settings. It includes the following information:

Container

The Cloud container to which the Cloud device is configured.

Used Size

The total storage usage as it is reported by the HPE Public Cloud object store.

Summary Tab - Cloud (Amazon S3 API compatible) Device

This tab is for information purpose. It shows you details for the current Cloud (Amazon S3 API compatible, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) settings. This includes the following information:

Bucket/Vault

The Cloud bucket/vault to which the Cloud (Amazon S3 API compatible, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) device is configured.

Used Size

The total storage usage as reported by the Cloud (Amazon S3 API compatible, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive) object store.

Session Options

Specify options for the operation.

Eject medium after operation

This option is available for standalone and stacker devices. If it is enabled, ejects the medium from the device or from the device chain (cascade) once the operation on the medium has been completed. If this option is selected for a media copy operation, both the source and the target medium are ejected.

Force operation

(not available for verifying media)

Users

In the Results Area, the configured user groups are displayed.

To display the user rights of a specific user group, select the group, right-click it, click Properties, and click the User Rights tab.

Add User Group

Add a user group by entering information about it in the appropriate text boxes.

Name

Enter the name of the new user group. A name can have a maximum of 20 characters; spaces are not allowed.

Description

Optional explanatory text about the group. For example, you can enter the tasks that can be performed by members of the group (such as Creating Reports).

A description can have a maximum of 80 characters, including spaces.

More on

- About User Management
- User Groups

Tasks

- Adding a User Group

Add User Group

Select the user rights you want to assign to the user group. You must assign at least one user right to the group.

- Clients configuration
- User configuration
- Device configuration
- Media configuration
- Reporting and notifications
- Start backup
- Start backup specification
- Save backup specification
- Back up as root
- Switch session ownership
- Monitor
- Abort
- Mount request
- Start restore
- Restore to other clients
- Restore from other users
- Restore as root
- See private objects
- Security admin
- Dashboard access
- Telemetry subscription management

Add User Group

Select a user group, and then add Data Protector users to the group or delete them from the group.

To add a user, provide the required information about the user, or select the user from the network if possible. Click **>>**.

To delete a user, select the user in the user list and click **<<**.

Group

The name of the user group to which you want to add a user.

Manual

Enter the required information.

Type

Select the type of the user: Windows systems user, Linux systems user, or LDAP user/group.

Name

Enter the logon name of an existing Windows or Linux user. Select **<Any>** to accept all Windows or Linux logon names.

Group/Domain

(available when Windows is selected)

Enter the Windows domain the user belongs to. Select **<Any>** to allow access from any domain.

UNIX Group

(available when UNIX is selected)

Enter the UNIX group the user belongs to. Select **<Any>** to allow access from any UNIX group.

Description

Optionally, enter explanatory text about the user for easier identification.

Client

Enter the client name or the IP address of the client system from which the user can access Data Protector functionality. The drop-down list contains the clients currently configured in the cell. Selection of **<Any>** option is disabled. To enable this option, manually change the value of global option EnableAnyOptionUserCtx to **1** in the global options file available at:

- *Windows: <PROGRAMDATA>\Config\Server\Options*
- Linux: /etc/opt/omni/server/options

Select **<Any>** to allow access from any computer.

Password

(Optional) Specify the password.

The following conditions apply for the password

- Must be minimum 8 characters and a maximum of 20 characters
- Includes at least one upper case letter, one lower case letter, and one numeral
- Includes at least one of these special characters: an asterisk (*), a dot (.), an hyphen (-), or an underscore (_)
- Does not include spaces

The password has to be set for the user to access Data Protector.

Browse

Explore the Microsoft Windows Network and search for an existing user you want to add to the user group.

Important Selection of **<Any>** in the **Name**, **Domain or Group** and **Client system** fields in the User Management context is disabled. To enable this option, manually change the value of global option EnableAnyOptio

nUserCtx to **1** in the global options file available at:

- *Windows*: <PROGRAMDATA>\Config\Server\Options
- *Linux*: /etc/opt/omni/server/options .

By selecting to enable and use the **<Any>** option for user, group or client fields in User Management context, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and hold Micro Focus harmless for the same.

In case of enabling and using the **<Any>** option for user, group or client fields in User Management context, Micro Focus encourages you to add relevant protection measures against risks associated with user privileges, which is not provided by Micro Focus. By not implementing relevant protection measures, you may be exposing the system to increased security risks. You understand and agree to assume all associated risks and hold Micro Focus harmless for the same. It remains at all times your sole responsibility to assess your own regulatory and business requirements. Micro Focus does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to you in conducting your business.

Add User to Other Cells

Add the user to other cells by selecting one or more Cell Managers.

Clearing user password

You can clear or delete the password associated with the user.

Prerequisite

You need to have the User configuration right to be able to clear user password.

User with user configuration rights can clear password for all the users.

Steps using GUI

1. In the Context List, click **Users**.
2. In the Scoping Pane, expand **Users**.
3. Click the user group to which the user belongs.
4. Right-click the user you want to reset password and click **Clear Password....**
5. Clear or delete the password from the **Password** field.
6. Click **OK** and confirm at the prompt to clear the password.

User Group Properties - General

In the Results Area, the properties of the user group are displayed.

Name

The name of the user group. A user group name can have a maximum of 24 characters; spaces are not allowed.

Description

Optional descriptive text with a maximum of 80 characters, including spaces.

User Group Properties - User Rights

In the Results Area, the user rights of the user group are displayed.

- Clients configuration
- User configuration
- Device configuration
- Media configuration
- Reporting and notifications
- Start backup
- Start backup specification
- Save backup specification
- Back up as root
- Switch session ownership
- Monitor
- Abort
- Mount request
- Start restore
- Restore to other clients
- Restore from other users
- Restore as root
- See private objects
- Security admin
- Dashboard access
- Telemetry subscription management

User Groups

In the Scoping Pane, the configured user groups are displayed.

In the Results Area, the users of the selected group are displayed.

Name

The user's logon name.

Domain or UNIX Group

The Windows domain or UNIX group the user belongs to. If access is allowed from any Windows domain or UNIX group, <Any> is displayed in the field.

Client System

The name of the computer from which the user can access the Cell Manager. If access is allowed from any computer, <Any> is displayed in the field.

Description

Optional explanatory text about the user.

Enterprise Users

In the Results Area, the configured Cell Managers are displayed. You can configure users and user groups for any Cell Manager that is configured in the Enterprise environment.

Cell Manager

The name of the Cell Manager configured in the Enterprise environment.

Status

The status of the Cell Manager.

LDAP configuration

To configure LDAP, the following prerequisites apply:

- The Cell Manager must be able to communicate with the LDAP server on the configured port.
- LDAP users used in Data Protector must have User Logon Name in userPrincipalName format configured (e.g user@domain.tld).
- When configuring the LDAP login module in MoM environments, ensure that you perform the steps described below on every Cell Manager. Every Cell Manager in the MoM environment needs to have the same configuration for the LDAP login module.

Configure LDAP

To configure the LDAP login module, perform the following steps:

1. In the **Context Menu** click **Users**, and then select **LDAP Configuration...** under the **Actions** menu. The LDAP Configuration window is displayed with existing LDAP configuration information. If LDAP is not configured, you can configure a new LDAP user.
2. Specify or edit the values of the following fields:

Name	Description	Value
Vendor	LDAP server vendor	Specify the LDAP server vendor as ActiveDirectory.
Name	LDAP configuration name	Specify the name for LDAP configuration.
LDAP Server	LDAP server host name or IP address.	Specify the LDAP server host name or IP address.
LDAP port	Port on LDAP server	Specify the port number to be used by LDAP server. Default port number is 389.
Users DN	Full DN of LDAP tree where your users are. This DN is parent of LDAP users.	Specify the DN of the LDAP tree that contains the users.
Bind DN	User that is used to initial bind with LDAP server	Specify the DN of LDAP user, which will be used by keycloak to access LDAP server.
Bind Credential	Password of Bind DN user.	Specify the password for the Bind LDAP user.
Roles Context DN	The fixed DN of the context to search for user groups	Specify the DN of the LDAP location that contains the user group. Modifying and listing/displaying Roles Context DN is not supported.
Test Connection	Tests LDAP server connection	Check if you can connect to the LDAP server with the specified server host name/IP address and port number.
Test Authentication	Tests LDAP server authentication	Check if you can connect to the LDAP server with the specified Bind DN and Bind Credential.

3. Click **Add** to create a new LDAP configuration or **Modify** to confirm changes to existing configuration.
4. Restart the Data Protector AppServer service to apply changes in LDAP configuration, for example, adding a new user or changing credentials of an existing user. It is not required to stop all the services and running sessions.
   - When you create a new user or change credentials of existing users in LDAP module, LDAP does not sync with Keycloak automatically. Restart Data Protector services to sync LDAP and Keycloak.
   - When a new user is added, it does not create any entry in IDB for that user unless the user log in to Data Protector for the first time. Also, sync happens between IDB and keycloak and it generates a token for that user.
   - When you add a user group in LDAP, the group is updated in IDB after a restart of Data Protector services, however, you cannot see individual members of that group in Data Protector GUI.

Configure LDAP securely

To configure LDAP securely, follow these steps:

1. Import SSL certificate from LDAP server.
2. Modify the LDAP attributes in keycloak.

Import SSL certificate from LDAP server

1. Get the SSL certificate from LDAP server and store it at a temporary location in DP Cell Manager. openssl.exe s_client -connect <LDAP Server>:636
2. Create a certificate file C:\Temp\ldap_certificate.pem and copy the lines from BEGIN CERTIFICATE to END CERTIFICATE.
3. Import the LDAP server certificate that you generated in step 1 into Cell Manager JRE Trust store: ""%DP_HOME_DIR% \jre\bin\keytool.exe -import -file <LDAP_certificate_path> -alias "ldap" -keystore % %DP_DATA_DIR%\config\server\certificates\server\server.truststore -storepass <storepass>
4. Restart Data Protector Application server.

Modify LDAP attributes in Keycloak

1. Reset DpKeycloakUser password by running the following command: omniusers.exe -resetpass -name DpKeycloakUser -pass Password_123
2. Open the keycloak admin console in any browser and modify the LDAP settings as per your environment. **URL** : https://<Ho

stname>:7116/auth/admin/DataProtector/console Use the following credentials to connect the Keycloak console: **User** : DpKeycloakUser and **Password** : Password_123

3. Modify LDAP attributes:
   1. Click **User Federation** and choose **Add provider** from the drop-down list.
   2. Click **ldap** and specify the settings as follows:
      - **Vendor**: Active Directory
      - **Connection URL**: ldaps://<hostname_of_domain_controller>:636
      - **Users DN**: CN=Users,DC=domain,DC=net
      - **Bind DN**: CN=user1,CN=Users,DC=domain,DC=net
      - **Bind Credential**: Password for Bind DN userPrincipalName
   3. Save the settings.
4. Modify Email attributes of LDAP Mapper:
   1. Click **Mappers** next to the **Settings** tab and select **Email**.
   2. Specify the value of **LDAP Attribute** as **userPrincipalName** and click **Save**.
   3. Connect to the Data Protector GUI from a client that has no access credentials (login window displayed) with a LDAP user (use userPrincipalName as user name).

Related topic

- For more information on LDAP, see User authentication and LDAP.

Move User

Move the user from the current user group in to the target user group.

Remove User From Cells

Remove the user from one or more cells.

Resetting user password

You can reset a user's password, either to replace an old password or to assign a password, if one was not set during user creation.

Prerequisite

- To reset user passwords without knowing the previous password or to reset passwords for other accounts, you need to have the user configuration right.
- If you do not have the user configuration right, you can only reset your own password, using the omniusers -resetpass command. The command does not require the old password if one was not associated previously with the account.

Steps using GUI

1. In the Context List, click Users.
2. In the Scoping Pane, expand Users.
3. Click the user group to which the user belongs.
4. Right-click the user you want to reset password and click Reset Password....
5. Specify the new password in Password and Confirm Password fields.The password must comply to the following conditions:
   - Must be minimum 8 characters and a maximum of 20 characters
   - Includes at least one upper case letter, one lower case letter, and one numeral
   - Includes at least one of these special characters: an asterisk (*), a dot (.), an hyphen (-), or an underscore (_)
   - Does not include spaces
6. Click OK and confirm at the prompt to reset the password.

User Properties - General

In the Results Area, the user's properties are displayed.

Name

The user's logon name.

Domain or UNIX Group

The Windows domain or UNIX group the user belongs to. If access is allowed from any Windows domain or UNIX group,**<Any>** is displayed in the field.

Client system

The name of the computer from which the user can access the Cell Manager. If access is allowed from any computer,**<Any>** is displayed in the field.

Description

Optional explanatory text about the user.

Web User Name

- By default, all the users have web service access.
- The users can access dashboard or REST APIs using their web user name.
- The web user name is in the format: <name>|<domain>|<client>.

Important Selection of **<Any>** in the **Name**, **Domain or Group** and **Client system** fields in the User Management context is disabled. To enable this option, manually change the value of global option EnableAnyOptionUserCtx to **1** in the global options file available at:

- *Windows*: <PROGRAMDATA>\Config\Server\Options
- *Linux*: /etc/opt/omni/server/options .

By selecting to enable and use the **<Any>** option for user, group or client fields in User Management context, you are disabling or bypassing security features, thereby exposing the system to increased security risks. By using this option, you understand and agree to assume all associated risks and hold Micro Focus harmless for the same.

In case of enabling and using the **<Any>** option for user, group or client fields in User Management context, Micro Focus encourages you to add relevant protection measures against risks associated with user privileges, which is not provided by Micro Focus. By not implementing relevant protection measures, you may be exposing the system to increased security risks. You understand and agree to assume all associated risks and hold Micro Focus harmless for the same. It remains at all times your sole responsibility to assess your own regulatory and business requirements. Micro Focus does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to you in conducting your business.

Change the mount proxy

If you are accessing the Advanced GRE Web Plug-in for the first time, you must select a Cell Manager (if there is only one, it is selected automatically). If more than one exists, then you will not be able to cancel or close the operation. However, the next time you access the plug-in, you can change the Cell Manager.

To change the Cell Manager:

1. In the Granular Recovery Extension for VMware vSphere Web Client, click the **Tools** icon.
2. Click **Change Cell Manager**. The Select Cell Manager box appears.
3. Select the required Cell Manager from the drop-down list and click **Select**.
4. If you select a different Cell Manager and click **Cancel** or **Close**, the previously selected is still applicable. However, if there is only one Cell Manager, then selection is not required. The available Cell Manager is displayed briefly and you are re-directed to the GRE Requests page.

The GRE Request page appears with the list of requests available for the selected Cell Manager.

Identify the HTML5 GRE Web Plug-in version

To determine the VMware Granular Recovery Extension agent and HTML5 Plug-in version, click **About** on the Granular Recovery page.

Configure GRE settings

In this page, you can modify the options for retention time. In addition, you can configure, add, or modify the mount proxy system used as a target location for restoring virtual machine disks.

Retention time

To modify the options for retention time:

1. In the Granular Recovery Extension for VMware vSphere Web Client, click the **Tools** icon.
2. Click **GRE Settings**. The GRE Settings page is displayed.
3. Under **Retention Time Options**, enter the retention period for the following text boxes:
   - Remove Non-Cached Disks After
   - Remove Cached Disks After
     The default retention period of the Non-Cached backup is 7 days (maximum can be set to 7 days). The default retention period for the Cached backup is 1 day (maximum can be set to 7 days).
4. Click **Back to GRE Request** to return to the list of requests available in the GRE Request page.

Configure the mount proxy

To configure, add or modify the mount proxy system used as a target location for restoring virtual machine disks:

1. From the **Windows** or **Linux Host** drop-down list, select the required Windows or Linux mount proxy system.
   You can configure multiple mount proxies and restore paths.
2. In the Windows and/or Linux **Restore Paths** text box, enter the path to a location on the mount proxy system. Use the following format:
   - DriveLetter:\Folder\Subfolder (Windows mount proxy system)
   - /Directory/Subdirectory (Linux mount proxy system)
3. Click + to add the specified path to the applicable list of restore or presentation paths. You can add more restore paths, if required.
4. Click - to delete the required restore path(s). You cannot delete a restore path if it is the only one for the mount proxy system.
5. Click **Save**.
6. Click **Back to GRE Requests** to return to the list of requests available in the GRE Requests page.

View the list of requests

The GRE requests page is the landing page for the Advanced GRE Web Plug-in. In this page you can view the list of requests and perform actions that are described in this section.

1. The Status, ID, Date Submitted, Type, and Time of Backup information is available for each of the requests. You can also filter the list of requests using the **Backup Type** (**All**, **Cached Backup**, **Non-Cached Backup**) in the right pane.
2. You can click **Refresh** to update the status of your request.
3. A request can have the following status:
   - Cached
   - Caching
   - Aborted
   - Recovered
   - Recovering
4. Select the required request and depending on the state of the request, appropriate buttons or actions become available.

Status	Actions available
Caching	Abort
Recovering	Session Report
Cached	Session Report , Browse
Recovered	Session Report

1. You can perform the following actions:
   - Click **Browse** to browse the disks that are selected while creating a request. You can browse partitions in disk/s and select the files or folders for recovery. However, browsing multiple disk at the same time is not allowed. At a given point of time you can browse only one disk . The Recover Files page appears.
   - Click **Session Report** to display the log messages for the actions that were taken most recently by the selected GRE request.
   - Click **New Request** to create a new request for a Cached or Non-Cached operation. The New Request page appears.
   - Click **Abort** to stop the restore or recovery that is in progress.

Create a new request

The New Request page lists all the available backups for the selected VM. You can filter the results using the options available under **Backups From** and **Backup Type** fields in the right pane.

Backups From - All, Last 30 Days, Last 90 Days, Last 6 Months, Last Year.

Backup Type - All, Cached Backup, Non-Cached Backup.

Configure the mount proxy from the GRE Settings page before proceeding to create a new request for Non-Cached backups. However, it is not necessary to configure mount proxies for Cached backups.

1. Select the required backup. Proceed as follows:
    1. From the **Virtual Disks** section, select single or multiple virtual disks for restore /presentation. The virtual disks are selected by default for 3PAR cached sessions.
    2. In the **Disk Retention Time** text box, enter the retention period. This period starts from the restore or presentation operation. After the retention period, the virtual disks are not available. The default retention period of the Non-Cached backup is 7 days (maximum can be set to 7 days). The default retention period for the Cached backup is 1 day (maximum can be set to 7 days).
    3. From the **ESX Host** drop-down list, select the required ESX host. For 3PAR cached sessions, the production ESX is selected by default.
    4. From the **Select Mount Proxy** drop-down list, select the required mount proxy.
    5. From the **Restore Path** drop-down list, select the required restore path. The restore path is required only for Non-Cached Backup.
2. For Cached / Non-Cached Backups, click **Send Request**. The GRE Request page appears and you can monitor the status of the request. For more information on how to proceed with the request, see the GRE Request section.
3. Click **Refresh** to update the list of backups.

When the GRE mount proxy host is rebooted, the requests that are browsed at least once become invalid. Hence these requests must be re-created to perform GRE operations.

If you want to delete a request created for a StoreOnce catalyst, run the following command to force clean up the StoreOnce Catalyst request IDs:

vmwaregre-agent.exe -force_cleanup <request_id> -vcenter <hostname>

where,

- request_id: StoreOnce Catalyst request ID that needs to be cleaned up
- hostname: vCenter host name on which the request is made

Recover files

Recovery of files from virtual machine disks fails if the user does not have sufficient permissions.

Cause

File recovery fails if the user does not have appropriate permissions on the target virtual machine.:

- For Samba, the username and password of the Samba user must be provided. This user should have permissions to mount network share to which files have to be recovered.
- For a Linux target VM, the VM username and password must be provided. However, these credentials are not used because an NFS share is exported.

Solution

To verify the list of exported directories, run the following command on Linux mount proxy host:

```
showmount -e
```

To recover files from virtual machine disks:

1. The Recover Files page appears. It is assumed that you have selected a restored or recovered request and clicked **Browse** from the GRE Request view. The file structure of the VMs is displayed in the Available Files section of the main content area.
2. Under the Available Files section, select the virtual machine disk containing the files to recover. For Cached 3PAR sessions, selecting the virtual machine disk mounts a backup replica, mounts datastores, and registers the VM resulting in the display of the following message: `Request submitted successfully and is in progress. Please try browsing after some time.` Selecting the virtual machine disk when the process is still in progress results in the display of the following message: `Request is still in progress. Please try browsing after some time.` Browsing enables the user to expand one disk and one partition at a time, since only one disk and one partition is supported for recovery. Proceed as follows:
    1. Click the disk name to expand the required partition. If a Linux partition is selected, then select the logical volumes from the available logical volumes list. If the user has selected files or folders, browse will not allow another disk/partition to be selected until the files/folders have been deselected.
    2. Select the files to recover from the selected disk.
3. Under Virtual Machine OS Credentials, select the virtual machine from the **Target VM** drop-down list, and enter its credentials in the **VM Username** and **VM Password** text boxes. The **Target VM** lists all the running VMs under the selected vCenter. Ensure to complete the following steps on the target Linux VM:
    1. Resolve any Hostname or IP conflicts for Target VM.
    2. NFS services must be configured and running.
4. Under the Recovery Options section, in the **Location** text box, enter the target recovery location path.
    - For locations on Windows systems, use the format *DriveLetter*:*Folder**Subfolder*.
    - For locations on Linux systems, use the format */Directory/Subdirectory*. For shared directories, enter the path without the hostname. For example, in the case of an NFS share hostname, use: `/shared_dir/subdir`. Files get recovered to `shared_dir/subdir/<target location specified>`. Also, ensure that the Samba and NFS shares are set up correctly. The NFS share must also be exported as pseudo root shares. Any missing directories in the path are created automatically. For example, if you specify `/shared_dir/subdir1/subdir2`, the `subdir1/subdir2` subdirectories are automatically created inside `/shared_dir`, if they do not already exist.
5. If the file already exists on the target system, select one of the following recovery options:
    - **Overwrite**: deletes the original files, and saves the latest files.
    - **Rename**: keeps the original files, and saves the recovered files with a unique number (generated by).
    - **Skip**: keeps the original files.
6. Select **Keep Directory Structure** to maintain the original directory structure of the source virtual machine disk on the target system.
7. Click **Recover Files**. A confirmation message appears and the GRE Request page is displayed, where you can monitor the recovery.

Browse Drives

In this page you select the location for your depot or pack file on the Cell Manager.

If you are specifying a location for a depot, select the directory in which a `dlc` directory will be created.

If you are specifying a location for a pack file, you must specify the full path, even if you are using the default file name.

Debug File Operations - Clients

Debug file operations can be performed on all clients in a cell. This page allows you to reduce the information involved by filtering according to criteria such as backup session ID. The clients involved in the relevant backups are displayed and can be selected or deselected.

Depending on the start point for the wizard, session ID, or client, pre-filtering may be performed when this page is opened.

Filters

In the drop-down list, select the criterion for filtering the clients to be included in the operation, as follows:

SessionID

The backup session for which debug files were produced. If a session ID was pre-selected for you, you cannot change it.

DebugID

The debug session for which debug files were produced.

Postfix

The debug filename.

No filter

All debug files on the selected clients are available for processing (dependent upon directory and option selections made in the rest of the wizard).

In the text entry box, enter the relevant ID.

Client selection and deselection

After filtering, the clients containing relevant debug files are selected.

Deselect any clients that you want to exclude from the debug file operation.

Debug File Operations - Directories

Debug files are written, by default, to the default temporary files directory.

By default, these directories are searched for debug files during debug files operations.

This page allows you to specify extra non-default directories to search for debug files and additional directories containing relevant information.

Directories selected here are applicable to all clients selected in the Clients page.

Non-default debug files directories

In the text box, enter the path of each extra directory to be searched for debug files and click**Add**. The directories are added to the selection list. Note that sub-directories are not searched.

Additional directories

(not available for debug files deletion) In the directory tree, select any additional directories whose contents you want included in debug file operations.

Debug File Operations - Options and Operations

This page displays:

- The options available for debug files collection from the selected clients (or space calculation).
- The operations that can be performed on the information received on the Cell Manager.

When the page is first opened, the selections match the default settings with the `omnidlc` command.

Options in this page are not available for debug files deletion.

Options

(available for debug files collection and space calculation)

By default, the following options are selected for a debug files collection or space calculation. Deselect any of the options you do not want to use.

The debug files are always collected in the temporary files directory. They cannot be deselected.

Compress

Files to be collected on a client are compressed before collection or space calculation. Specify the debug range, and add *gz*. The logs will be created with the *.gz* extension.

Include get_info file

The `get_info.txt` file is collected from the default temporary files directory.

Include configuration files

All cell and server configuration information is collected.

Include logs

The contents of the default log files directory are collected.

Telemetry files

This option is not selected by default. Select it to include the telemetry data.

Verbose reporting

Details of every individual file collection are presented in the Results Area.

Filters

You can specify multiple filter options for collecting the debug logs. The following filter options are available:

- Session ID: The backup session for which the debug files were produced.
- Debug ID: The debug session for which debug files were produced.
- Postfix: The debug filename.
- Module/s: The modules for which you need the debug logs. You can enter multiple modules, each separated by a comma. Example: BSM,BDSM,VBDA.

Operation

(available for debug files collection)

Select the operation to be used for storing the debug files on the Cell Manager:

Create Depot directory

Select this to store files (not packed) in a depot, within a dlc subdirectory of the default temporary files directory.

To specify an alternative location for the dlc directory, enter this in **Target Path**.

The directory specified must exist, or the collection will fail.

Create Pack File

This option is selected by default. Select it to create a pack file (default dlc.pck) in the current directory.

To specify an alternative directory and filename, enter the full path in **Target Path**.

The file specified must exist, or the collection will fail.

Debug File Operations - Results

In the Results Area, the results of the debug file operation being performed are displayed.

Status

The current status of the operation in progress

Client

The client for which operations are being performed.

Progress

The current progress with the operation

Description

The type of debug file operation being performed

Message area

The following items are displayed in the message area at the bottom of the page:

- The `omnidlc` command used to perform the operations selected in the GUI
- All progress messages regarding the current operation
- Session status of the current operation

MS SharePoint GRE options

In the MS SharePoint GRE options dialog box, specify the user name and password of the Microsoft Office SharePoint Server Farm Administrator user account to use for installation of the MS SharePoint Granular Recovery Extension component.

Add Components

Specify the platform of the client(s) to which you want to add components and the Installation Server that will be used for adding components.

The following prerequisite applies:

- At least one Installation Server must be installed for the platform of the client system(s) to which you want to add components. Otherwise, only local installation is possible.

Platform of target machines

Select the platform of the client system(s) on which you want to install components.

Installation Server

Select the Installation Server that will be used for the installation.

Add Components

Select the clients on which you want to install the Data Protector components.

Select All

Click here to select all listed clients.

Clear All

Click here to deselect all listed clients.

Add Components

Select the Data Protector components you want to install on the selected client(s).

Components

Select the components you want to distribute to the clients. Note that you can select only one type of Media Agent.

Configure...

(enabled only when the MS SharePoint Granular Recovery Extension component is highlighted)

This button enables you to choose specific options for highlighted components where such options are available.

Add Components

For each client, select the Data Protector components that support configuration and you want to install.

Add installation server

Importing an Installation Server adds the system to the list of available software depots that can be used by the Cell Manager. An Installation Server can be imported to more than one cell.

Prerequisite The Installation Server must be installed before it can be imported.

Name

Type the name of the Installation Server that you want to import.

If you are importing an Installation Server for Windows systems, you can browse the network for the Installation Server system.

Add license

In this page, specify the password for the license you have installed.

License

Type the password exactly as it appears on the *Password Certificate*. A password consists of eight 4-character groups, separated by a space and followed by a string. Make sure that you do not have a line-feed or a return character within this sequence.

The following is an example of a password:

```
4PXV EG9S B6WS 2VX3 5967 XEZK AAA9 MQJB "Product: B6963AA"
```

After you have specified the password, check the following:

- Make sure the password appears correctly on the screen.
- Make sure there are no leading or trailing spaces or extra characters.
- Double-check "1" (number one) characters and "l" (letter l) characters.
- Double-check "O" (uppercase letter O) characters and "0" (number zero) characters.
- Make sure that you have used the correct case. The password is case-sensitive.

Advanced Notification Options

Specify advanced notification options for the selected client system.

In the drop-down list, select a notification method. In the text box, specify the recipient of the notification and click **Add**. You can add several recipients.

To remove a recipient from the list, select the recipient and click **Delete**.

To use the client notification, you need to configure a report group. The report group must contain the Session Per Client report with multiple options set and with %host_owner as a destination for the desired method.

Check Installation

Select the client systems for which you want to check the Data Protector installation. This includes the DNS configuration check.

Select All

Click here to select all available clients.

Clear All

Click here to clear the selected clients.

Check Client Systems Installation

Specify the platform of the client and the Installation Server that will be used to check the installation.

Prerequisite At least one Installation Server must be installed for the platform of the client system that you want to check.

Platform of target machines

Select the platform of the client system that you want to check.

Installation Server

Select the Installation Server that will be used to check the installation on the client.

Client System Properties - Administration

Set the owner for the client system. This user is notified about the client system backup status.

General Owner

The owner of the client system (e-mail address).

Broadcast to selected machine

(available for Windows systems)

Select this option to enable broadcast to the local machine.

Advanced

Click **Advanced** to set advanced notification options for the client system.

To use the client notification, you need to configure a report group. The report group must contain the `Session Per Client` report with multiple options set and with `%host_owner` as a destination for the desired method.

Client System Properties - Advanced

In this page, advanced properties of the selected client are displayed.

Device Server

- Client is Device Server (available if you have a Media Agent installed)

Magic Packet

(available for Data Protector Windows clients) Magic Packet enables you to remotely power client systems in the same subnet on.

- MAC Address
- Enable Magic Packet
- Client device filter tag
- Name

Client System Properties - General

In this page, general properties of the selected client are displayed.

Name

The name of the client.

Platform

The platform of the client.

Patches

Click this button for a list of Data Protector patches installed on the client.

Installed components

The Data Protector software components and their versions currently installed on the client.

Client System Properties - Security

In this page, the names of the systems that are allowed to access the client are displayed.

To add a system, type the name of the system or search for it and click Add to add it to the list.

To remove a system from the list, select it in the list and click Remove.

Name

Type the name of the system that will be allowed to access the client.

Network

Browse the network to find the systems that will be allowed to access the client.

Search

Specify the IP address interval within which the systems that will be allowed to access the client will be searched for. Click Search to display the systems that match the search criteria.

Client Systems

The names of the systems that are allowed to access the client are displayed.

Cluster Node Properties - General

In this page, general properties of the selected cluster node are displayed.

Name

The name of the cluster node.

Platform

The platform of the cluster node.

Patches

Click this button for a list of Data Protector patches installed on the cluster node.

Installed components

The Data Protector software components and their versions currently installed on the cluster node.

Cluster Properties - General

In this page, general properties of the selected cluster-aware client are displayed.

Name

The name of the cluster client.

Platform

The platform of the cluster client.

Patches

Click this button for a list of Data Protector patches installed on the cluster client.

Installed components

The Data Protector software components and their versions currently installed on the cluster client.

Connect to a Cell Manager

Connect to a Cell Manager of choice. Recently connected Cell Managers are listed.

Connect

Click here to connect to the Cell Manager specified in the text box.

Delete

Click here to delete the selected Cell Manager from the list.

Close

Close the dialog box without connecting.

Home Context

- Dashboard
- Telemetry
- Scheduler
- Reports

Delete Client Systems

Specify the platform of the client and the Installation Server that will be used to uninstall Data Protector from the client.

Prerequisite

- At least one Installation Server must be installed for the platform of the client system from which you want to uninstall Data Protector. Otherwise, only local uninstallation is possible.

Platform of target machines

Select the platform of the client system from which you want to uninstall Data Protector.

Installation Server

Select the Installation Server that will be used to uninstall Data Protector from the client.

When a client is uninstalled from the Install Server system that has a Cell Manager installed, Data Protector displays a message <client_hostname> No valid software found on client <client_hostname> .... However, the client is uninstalled successfully.

Component options

Configure component-specific options

Select this check box to choose component-specific options for each component where they are available.

Distribute Files

You can distribute configuration data from the Data Protector Manager-of-Managers to Cell Managersconfigured in the MoM environment.

Class Specifications

Select this option to distribute Data Protector class specification files.

Holidays

Select this option to distribute the Holidays file.

Globals

Select this option to distribute the Data Protector global options file.

Vaulting

Select this option to distribute the Data Protector vaulting locations file.

SNMP

Select this option to distribute the Data Protector SNMP trap configuration files.

Cell Manager

Select the Cell Managers to which you want to distribute the selected configuration files.

Import a virtual client system

Importing is the process of manually adding a system to a cell after the Data Protector software has been installed. When added to a Data Protector cell, the system becomes a Data Protector client.

The Data Protector Hyper-V client host system needs to be imported as a client first and then re-imported as a Hyper-V system, following the procedure stated below.

Follow the steps below to import virtual client systems into a cell with Data Protector Express license:

1. Click **Clients** in the context list.
2. Right-click **Clients** and click **Import Client** in the Scoping Pane.
3. Enter the client name in the **Name** option, select the appropriate client type (VMware ESX(i) for a standalone VMware ESX(i) Server system, VMware vCenter for a VMware vCenter Server system, or Hyper-V for a Microsoft Hyper-V system) from the **Type** drop-down list in the Import client page. Click **Next** and specify login credentials.
4. Click **Next**. The systems(ESX(i), vCenter, or Hyper-V) in the selected client are listed, along with the Host Name, Host Sockets(s), and Host UUID information.
5. Click the systems that you want to license and click **Finish**.The selected systems will get licensed with sockets.
   Add and re-claim licenses
   To add or re-claim the license(s), re-import the virtual client or go to the Client properties page.In such cases, the unlicensed clients are listed along with the already licensed clients in the results area.
   - To reclaim, de-select the system(s) and select Finish to unlicense the system(s).
   - To add, select new system(s) and select Finish to license the system(s). You can use the Select all option to select or deselect all the systems at once.

Note: If a host is deleted outside the Data Protector environment, and it is re-imported, the deleted host is marked as **Disconnected** in the system client properties, in the host name column.

Important fields

Licensed Host tab: This tab is a new field in the client properties page that can be accessed by clicking on the client from scoping pane. It lists the systems in the selected client along with the host name, host socket(s) and host UUID information. By clicking the "Refresh" button, the information from the live environment gets updated in the results area, along with the unlicensed systems. You can choose to add or reclaim license(s) by selecting and deselecting the systems and clicking **Apply**.

Total sockets: The number of sockets you are entitled to use.

Available sockets: The number sockets available after considering the sockets already consumed. This count changes based on the dynamic selection of systems for licensing.

Import Client

Specify the name of the client or virtual server that you want to import.

Accept Fingerprint

When the user select **Accept Fingerprint** option, the fingerprint window does not appear and host is accepted without user confirmation. In case the option is not selected, the fingerprint window is displayed and user has to manually accept the fingerprint option.

Accept Fingerprint option is applicable for Data Protector Client and Foreign Cell Manager.

Name

Type the name or the IP address of the client. When importing a non-Microsoft Cluster Server virtual server, provide the hostname of the virtual server as specified in the package of the cluster-aware application.

You can also browse the network for the client.

Type

- To import a standard Data Protector client, select **Data Protector Client**.
- To import a cluster virtual server or a client configured with multiple LAN cards, select **Virtual Host**. For clients configured with multiple LAN cards, selecting this option keeps Data Protector from assigning licenses to all the network names of the same system.
- To import an NDMP Server, select **NDMP Server**.
- To import an IAP Server, select **IAP Server**.
- To import a VMware ESX(i) Server system, VMware vCenter Server system, Microsoft Hyper-V, or H3C CAS system for the Data Protector Virtual Environment integration, select **VMware ESX(i), VMware vCenter, Hyper-V**, or **H3C CAS** respectively.

Import Cluster Node

Specify the name of the Microsoft Cluster Server node that you want to import.

Name

Type the name of the cluster node.

You can also browse the network for the client.

Import Cluster

Specify the name of the Microsoft Cluster Server client that you want to import.

Name

Type the name of the virtual server representing the cluster-aware client.

You can also browse the network for the client.

Import Cluster Virtual Server

Specify the name of the Microsoft Cluster Server virtual server that you want to import.

Name

Type the name of the virtual server.

You can also browse the network for the client.

Import Cell Manager

Specify the name of the Cell Manager that you want to import.

Name

Type the name of the Cell Manager.

You can also browse the network for the Cell Manager.

Import NDMP Host

Specify information about the NDMP Server.

Port

Specify the TCP/IP port number of the NDMP Server. The default is 10000.

User name

Type the user name that Data Protector will use to establishthe connection to the NDMP Server.

Password

Type the password of the user.

NDMP Server Type

Select one of the available NDMP types: **NetApp, NetApp_CAB, Celerra, BlueArc, Hitachi,** or **X9000**.

Inet Service User Impersonation - Add, Modify, or Delete User

In this page, update the Windows Registry that stores Windows domain user accounts for the Data Protector Inet service impersonation. You can add a new user account, or modify or delete an existing one.

User

Specify the user name.

Group/Domain

Specify the Windows domain name.

Old Password

(available when modifying a user)

Specify the user's old password.

Password

(not available when deleting a user)

Specify the user's password.

Inet Service User Impersonation - Select Client Systems

Select the client systems for which you want to configure the Data Protector Inet service user impersonation.

Cell

In the Scoping Pane, you can choose among Clients, Installation Servers, and MS Clusters. The MS Clusters list includes virtual server names of Microsoft Cluster Servers that are configured in the cell.

The following may be helpful:

- To add a license to the Data Protector cell, right-click Data Protector Cell and click Add License.
- To add a certificate to the Data Protector cell that will be used for connecting to the IAP appliance, right-click Data Protector Cell and click Add Certificate.
- To display Help on a specific item, select the desired item in the Scoping Pane.

Clients

In the Results Area, a list of configured clients in the Data Protector cell is displayed, including the Cell Manager.

The Clients list also includes the virtual server and the cluster nodes for each Microsoft Cluster Server that is part of the cell. If the Microsoft Cluster Server has additional cluster groups with the Network Name resource configured, these groups are displayed as virtual servers as well.

To use the filters available for the displayed list, click on Show filter settings and modify the parameters. On how to use the filter settings, see the Using the Filter Settings task topic below.

Name

The name of the system.

Operating System

The operating system running on the system.

Disk Agent

Version of the Data Protector Disk Agent installed on the system.

Media Agent

Version of the Data Protector Media Agent installed on the system.

User Interface

Version of the Data Protector User Interface (GUI and CLI) installed on the system.

The following may be helpful:

- To display properties of a system, right-click the system and click Properties.
- To upgrade a system, right-click the system and click Upgrade.

Client System List

In the Results Area, a list of configured clients in the selected Data Protector cell is displayed. The list includes the configured Cell Manager.

Name

The name of the client system.

Operating System

The operating system running on the client system.

Disk Agent

Version of the Data Protector Disk Agent installed on the client system.

Media Agent

Version of the Data Protector Media Agent installed on the client system.

User Interface

Version of the Data Protector User Interface (GUI and CLI) installed on the client system.

The following may be helpful:

- To display properties of a system, right-click the system and click **Properties**.
- To install Data Protector components on a system, right-click the system and click *Add Components*.
- To upgrade a system, right-click the system and click **Upgrade**.
- To verify the installation of Data Protector components on a system, right-click the system and click **Check Installation**.
- To secure or unsecure a system, right-click the system and click **Secure** or **Unsecure**.
- To export a client from the selected Data Protector cell or uninstall Data Protector from the client, right-click the client and click **Delete**.
- To add clients to a Data Protector cell, right-click the Cell Manager in the Scoping Pane and click **Add Clients**.
- To import a client to a Data Protector cell, right-click the Cell Manager in the Scoping Pane and click **Import Client**.
- To add a license to a Data Protector cell, right-click the Cell Manager in the Scoping Pane and click **Add License**.
- To add a certificate to the Data Protector cell that will be used for connecting to the IAP appliance, right-click **Data Protector Cell** and click **Add Certificate**.

Cluster Nodes and Virtual Servers

In the Results Area, the virtual server and the configured cluster nodes of the selected Microsoft Cluster Server are listed. If the Microsoft Cluster Server has additional cluster groups with the Network Name resource configured, these groups are displayed as virtual servers as well.

Name

The name of the cluster node or virtual server.

Operating System

The operating system running on the cluster.

Disk Agent

Version of the Data Protector Disk Agent installed on the cluster.

Media Agent

Version of the Data Protector Media Agent installed on the cluster.

User Interface

Version of the Data Protector User Interface (GUI and CLI) installed on the cluster.

The following may provide additional information:

- To display properties of a cluster node or a virtual server, right-click the cluster node or virtual server and click Properties.
- To import an additional cluster node or a virtual server to the Data Protector cell, right-click its cluster in the Scoping Pane and click Import Cluster Node or Import Cluster Virtual Server.

MS Clusters

In the Results Area, a list of configured Microsoft Cluster Servers in the Data Protector cell is displayed. Each Microsoft Cluster Server is referred to by its virtual server name.

Name

The virtual server name that represents the cluster.

Operating System

The operating system running on the cluster.

Disk Agent

Version of the Data Protector Disk Agent installed on the cluster.

Media Agent

Version of the Data Protector Media Agent installed on the cluster.

User Interface

Version of the Data Protector User Interface (GUI and CLI) installed on the cluster.

The following may be helpful:

- To display properties of a Microsoft cluster, right-click the cluster and click **Properties**.
- To import a cluster node of a Microsoft cluster to the Data Protector cell, right-click the cluster and click **Import Cluster Node**.
- To import a virtual server of a Microsoft cluster to the Data Protector cell, right-click the cluster and click **Import Cluster Virtual Server**.

Enterprise Clients

In the Results Area, a list of configured Cell Managers in the Data Protector Manager-of-Managers environment is displayed.

Cell Manager

The name of the Cell Manager.

Status

The current status of the Cell Manager.

MMDB Server

The name of the Centralized Media Management Database (CMMDB) server, if the Cell Manager does not use a local Media Management Database (MMDB). The following may be helpful:

- To distribute the Data Protector configuration from the MoM server to Cell Managers, right-click **Enterprise Clients** in the Scoping Pane and click **Distribute Configuration**.
- To add clients to a Data Protector cell, right-click the Cell Manager and click **Add Clients**.
- To import a client to a Data Protector cell, right-click the Cell Manager and click **Import Client**.
- To add a new license to a Data Protector cell, right-click the Cell Manager and click **Add License**.

Installation Servers

In the Results Area, a list of configured Installation Servers in the cell is displayed. To use the filters available for the displayed list, click on **Show filter settings** and modify the parameters. On how to use the filter settings, see the Using the Filter Settings task topic below.

Name

The name of the Installation Server.

Operating System

The operating system running on the Installation Server.

Disk Agent

Version of the Disk Agent installed on the Installation Server.

Media Agent

Version of the Media Agent installed on the Installation Server.

User Interface

Version of the User Interface (GUI and CLI) installed on the Installation Server. The following may be helpful:

- To display properties of an Installation Server, right-click the Installation Server and click **Properties**.
- To export an Installation Server from the cell, right-click the Installation Server and click **Delete**. Note that this action does not physically remove the Installation Server from the cell.

Add Client System

Specify the platform of the client(s) you want to install and the Installation Server that will be used for the installation.

Prerequisite

At least one Installation Server must be installed for the platform of the client system(s) that you want to install. Otherwise, only local installation is possible.

Platform of target machines

Select the platform of the client system(s) that you want to install.

Installation Server

Select the Installation Server that will be used for the installation.

Add Client System

Specify the clients you want to install.

To add a client, type the name of the client or search for it and click **Add** to add it to the list.

To remove a client from the list, select it in the list and click **Remove**.

Name

Type the name of the client you want to install.

Network

Browse the network to find the client you want to install.

Search

Specify the IP address interval within which the clients will be searched for. Click **Search** to display the clients that match the search criteria.

Client Systems

The names of the selected clients are displayed.

Add Client System

Select the components you want to install on the selected client(s).

Components

Select the components you want to distribute to the clients. Note that you can select only one type of Media Agent.

Configure

(enabled only when the MS SharePoint Granular Recovery Extension component is highlighted)

This button enables you to choose specific options for highlighted components where such options are available.

Options

Use default system account

By default, uses a default system account while connecting to the specified client to install the components. If this option is not selected, specify another account.

Directory

(available on Windows systems)

By default, the components are installed in the %ProgramFiles% and %ProgramData% system directories. Use this option to specify a different directory for installing the components.

Add Client System

For each client, specify the target directory for the client installation (for Windows clients only), user account to be used for connecting to the client, and select the components to be distributed to the client.

On Windows Server 2008 and Windows Server 2012, will be installed into the directories and by default. You can specify different directories. If you do not specify full paths, the specified directories will be created in the system directories %Program Files% and %ProgramData% .

On other Windows systems, by default, will be installed into the directory . You can specify a different directory. If you do not specify a full path, the specified directory will be created in the system directory %ProgramFiles% .

Installation Server Properties - General

In this page, general properties of the selected Installation Server are displayed.

Name

The name of the Installation Server.

Platform

The platform of the Installation Server.

Patches

Click this button for a list of patches installed on the Installation Server.

Components available for installation

software components that can be installed on clients using this Installation Server.

Licensing Information

In this page, license configuration for the selected Cell Manager is displayed. To add licenses from the Manager-of-Managers, right-click a Cell Manager and click **Add license**.

Type of Licensing

Used

(displayed if Type (at the bottom) is Local) The number of licenses assigned to the Cell Manager. You can modify this number if the licensing mode is set to `Remote`. The column name changes to `Allocated`.

Allocated

(displayed if Type (at the bottom) is Remote) The number of licenses assigned to the Cell Manager. Increasing the number in this column will correspondingly decrease the number of available licenses, and the other way round. To modify the number of allocated licenses for a specific licensing category, click to the right of the number.

Available

The number of licenses available to the entire enterprise for a specific licensing category. This is the number of licenses not taken by any cell within the enterprise environment.

Total

The total number of licenses, both used and available, in the entire enterprise for a specific licensing category.

Type

The following licensing modes are available:

Local

The default mode after installation. Licenses are read from `\Config\Server\cell\lic.dat` on Windows systems or `/etc/opt/omni/server/cell/lic.dat` on UNIX systems.

Remote

Licenses are allocated to the Cell Manager from the MoM server.

Server

The mode of the MoM server.

Select Cell Manager

Select the Cell Manager of the cell to which you want to move the client.

Name

The name of the client system.

Platform

The platform of the client system.

Available Cell Managers

Select the Cell Manager to which you want to move the client system.

Cell Manager Properties - Administration

Set the owner for the Cell Manager. This user is notified about the Cell Manager backup status.

General

Owner

The owner of the Cell Manager (e-mail address).

Broadcast to selected machine

(available for Windows systems) Select this option to enable broadcast to the local machine.

Advanced

Click **Advanced** to set advanced notification options for the Cell Manager. To use the Cell Manager notification, you need to configure a report group. The report group must contain the Session Per Client report with multiple options set and with %host_owner as a destination for the desired method.

Cell Manager Properties - Advanced

In this page, advanced properties of the selected Cell Manager are displayed.

Device Server

- Client is Device Server

(available if you have a Media Agent installed)

Magic Packet

(available for Windows clients)

Magic Packet enables you to remotely power client systems in the same subnet on.

- MAC Address
- Enable Magic Packet

Host filter tag

Host filter tag helps identify devices for the host.

- Name

Cell Manager Properties - General

In this page, general properties of the selected Cell Manager are displayed.

Name

The name of the Cell Manager.

Platform

The platform of the Cell Manager.

Patches

Click this button for a list of patches installed on the Cell Manager.

Installed components

The software components and their versions currently installed on the Cell Manager.

Cell Manager Properties - Security

In this page, the names of the systems that are allowed to access the Cell Manager are displayed.

To add a system, type the name of the system or search for it and click **Add** to add it to the list.

To remove a system from the list, select it in the list and click **Remove**.

Name

Type the name of the system that will be allowed to access the Cell Manager.

Network

Browse the network to find the systems that will be allowed to access the Cell Manager.

Search

Specify the IP address interval within which the systems that will be allowed to access the Cell Manager will be searched for. Click **Search** to display the systems that match the search criteria.

Cell Managers

The names of the systems that are allowed to access the Cell Manager are displayed.

Add Certificate

In this page, you specify the certificate filename and enter the content of a certificate file.

Certificate File Name

Type the filename of the certificate you want to add. You can also click **Browse** to select the filename from a list of available certificates. In this case, the file content will be automatically uploaded from the certificate file.

Content of the Certificate File

If you typed the certificate filename, paste here the content of a certificate file. If you selected the certificate filename from the list, the content is displayed here automatically.

Clicking **OK** uploads the file to the Certificates subdirectory in the default server configuration directory.

Cell Manager Properties - Certificates

In this page, the names of all certificates added to the cell are displayed.

Name

Lists the filenames of the certificates.

Created on

Lists the date when the file containing the certificate was created on the Cell Manager.

Display Certificate

Clicking this check box displays the certificate content.

Client System Properties - Storage Appliance

The functionality this Help topic used to describe is officially not supported in the installed version. In this page, you can view and change IAP Server specific properties.

Port

IAP port number. The default value is 8081.

User name

IAP user name. This name does not represent any actual user, but rather a synthetic principal created on behalf of the system or application that uses the IAP API.

Password

The password for the specified user.

Mode

Use known certificate

- Download certificate on first login
- Certificate File Name

(available only if **Use known certificate** is selected)

The certificate that will be used for connecting to the IAP appliance.

Enable Security on Selected or All Clients in the Cell

Specify the systems that will be allowed to access the selected client(s) or all clients in the cell. Include the Cell Manager, the Installation Server(s), and the Media Agent clients that will access the library robotics remotely.

To add a system, type the name of the system or search for it and click **Add** to add it to the list.

To remove a system from the list, select it in the list and click **Remove**.

Name

Type the name of the system that will be allowed to access the client(s).

Network

Browse the network to find the systems that will be allowed to access the client(s).

Search

Specify the IP address interval within which the systems that will be allowed to access the client(s) will be searched for. Click **Search** to display the systems that match the search criteria.

Cell Managers

The names of the selected systems are displayed.

Telemetry Registration

The customer can subscribe or unsubscribe the telemetry updates from the Telemetry page. When the user is on the Telemetry page, the following fields needs to be entered:

- **Customer Name**: Name of the customer.
- **SAID**: SAID number.
- **Frequency of data collection**: The user can select the frequency in which the data can be collected, that is: Daily, Weekly, Monthly and Quarterly.

After entering the above fields and selecting the frequency of data collection, accept the terms and conditions and click **Subscribe**.

Upgrade Client Systems

Upgrading a client installs a new version of the software components installed on that client. Select the client systems that you want to upgrade.

Select All

Click here to select all available clients.

Clear All

Click here to clear the selected clients.

Check Version

Click here to check the version installed on the selected clients and verify whether the clients need to be upgraded.

Upgrade Client Systems

Upgrading a client installs a new version of the software components installed on that client.

Prerequisite

At least one Installation Server must be installed for the platform of the client system that you want to upgrade. Otherwise, only local installation is possible.

Platform of target machines

Select the platform of the client system that you want to upgrade.

Installation Server

Select the Installation Server that will be used for the upgrade of the client.

Component options

Configure component-specific options

Select this check box to configure component-specific options for each component where they are available.

Use same options for all clients

(available if **Configure component-specific options** is selected)

Select this check box to use the same options for all selected client systems.

System Properties - Login

In this page, specify the login credentials that To be able to change the login credentials, you must have the Clients configuration user right (for example, you must be in the admin user group).

Port

(not available for Microsoft Hyper-V clients)

Specify the port that VMware (vCenter Server, vSphere) is using. By default, VMware uses the port 443.

Specify the https port that H3C CAS is using. By default H3C CAS uses port 8443.

Integrated security

(available for VMware vCenter Server clients, provided that both the application client and the backup host are Windows systems)

Standard security

Select this option if you want to specify all login credentials manually.

Username

Specify an operating system user name. For a VMware vCenter Server or VMware ESX(i) Server client, the specified user must have the following VMware vSphere roles:

- Datastore -> Allocate space
- Datastore -> Browse datastore
- Datastore -> Low level file operations
- Datastore -> Remove file
- Datastore -> Rename datastore
- Folder -> Delete folder
- Folder -> Rename folder
- Global -> Disable methods
- Global -> Enable methods
- Global -> Licenses
- Host -> Configuration -> Maintenance
- Host -> Inventory -> Add standalone host
- Network -> Assign network
- Resource -> Assign virtual machine to resource pool
- Resource -> Remove resource pool
- Resource -> Rename resource pool
- Sessions -> Validate session
- vApp -> Delete
- vApp -> Rename
- Virtual machine -> Configuration *
- Virtual machine -> Interaction -> Answer question
- Virtual machine -> Interaction -> Power Off
- Virtual machine -> Interaction -> Power On
- Virtual machine -> Inventory -> Create new
- Virtual machine -> Inventory -> Register
- Virtual machine -> Inventory -> Remove
- Virtual machine -> Inventory -> Unregister
- Virtual machine -> Provisioning *
- Virtual machine -> State -> Create snapshot
- Virtual machine -> State -> Remove snapshot

For a Microsoft Hyper-V client, the specified user must have appropriate permissions to access Microsoft Hyper-V VMI services. The User Account Control on the Microsoft Hyper-V system must be configured to elevate user rights automatically.

For H3C CAS server, the specified user should have appropriate privileges to perform backup and restore of Virtual Machines.

Password

Specify the user's password.

Web service root

(not available for Microsoft Hyper-V clients and H3C CAS clients)

Specify the web service entry point URI. Default: /sdk

Virtual Server Properties - General

In this page, general properties of the selected cluster virtual server are displayed.

Name

The name of the virtual server.

Platform

The platform of the virtual server.

Patches

Click this button for a list of patches installed on the virtual server.

Installed components

The software components and their versions currently installed on the virtual server.

Session ID

Specify the session ID of the backup, copy, or consolidation session for which you want to generate a report and the level of messages that will be displayed in the report output. (Session per Client Report includes only backup specifications.)

Access Points - Windows Application log

Some system and application management applications monitor the Windows Application log. Note that this is supported on Windows Cell Manager systems only.

To enable the automatic forwarding of all Data Protector messages and any messages about Data Protector services (ifthey are stopped) to Windows Application log, use EventLogMessages global variable.

故障诊断

本节介绍如何对在使用 Data Protector 时遇到的问题进行故障诊断。它包含一般问题及其建议解决操作。包括以下主题:

如何排查问题

要快速高效地解决问题，请遵循以下要求：

1. 熟悉常规故障排除信息。
2. 查看在 Data Protector 帮助文件或适用部分的故障诊断部分中是否描述了您的问题:
   - 要对安装和升级进行故障诊断，请参阅“Data Protector 安装”一节。
   - 要对应用程序集成会话进行故障诊断，请参阅“Data Protector 集成”一节。
   - 要对零宕机时间备份和即时恢复进行故障诊断，请参阅“Data Protector 零宕机时间备份和即时恢复”一节。
   - 要对灾难恢复进行故障诊断，请参阅“Data Protector 恢复”一节。
3. 如果找不到问题的解决方案，请将问题报告给 Micro Focus 支持人员。

常规检查

在继续之前，请确保：

- 没有遇到当前无法克服的已知限制。有关 Data Protector 限制和建议的特定信息，以及已知的 Data Protector 和非 Data Protector 问题，请参阅已知问题。
- 您的问题与第三方硬件或软件无关。否则，请与各自的供应商联系以获得支持。
- 安装了最新的 Data Protector 修补程序。可以从以下位置获取修补程序：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=。

  有关如何检查您的系统上安装了哪些 Data Protector 补丁的信息，请参阅《Data Protector 帮助》索引: “修补程序”。
- 安装了适当的操作系统修补程序。

  在支持矩阵中列出了所需操作系统补丁。
- 对于应用程序备份，备份没有因为应用程序关闭而失败。
- 调试日志或重做日志文件系统没有溢出。
- 应用程序数据文件系统没有溢出。
- 系统运行没有导致内存不足。
- (*适用于 Linux*)。存在 **hpdp** 用户。**hpdp** 用户对于 Data Protector 的正常运行至关重要。确保在安装期间或安装之后不会意外删除 **hpdp** 用户。如果在安装期间不存在 **hpdp** 用户，则安装将失败。如果 **hpdp** 用户在安装后被删除，则您可能会遇到任务的问题，例如添加用户、IDB 更新问题等等。

安装问题的故障诊断

本节包含与安装问题相关的信息。

使用日志文件

如果在安装 Data Protector 时遇到问题，可以检查任一以下日志文件来确定问题:

- 安装日志文件 (Windows)
- 系统日志文件 (Linux)
- Data Protector 日志文件

出现安装问题时应检查哪些日志文件取决于安装类型（本地或远程）以及操作系统。

本地安装

本地安装出现问题时，请检查以下日志文件：

Linux Cell Manager:

/var/opt/omni/log/debug.log

Windows 客户机（运行安装程序的系统）：

- Temp\SetupLog.log
- Temp\OB2DBG_did__setup_HostName_DebugNo_setup.txt （有关更多详细信息）

  其中：

  - did （调试 ID）是接受调试参数的第一个进程的进程 ID。此 ID 用作调试会话的 ID。所有后续进程将使用此 ID。
  - *HostName* 是创建跟踪文件的主机的名称。
  - *DebugNo* 是 Data Protector 生成的编号。
- Temp\CLUS_DBG_DebugNo.TXT （在群集环境中）

Temp 目录的位置由 TEMP 环境变量指定。要检查此变量的值，请运行 set 命令。

远程安装

远程安装出现问题时，请检查以下日志文件：

Linux 安装服务器:

/var/opt/omni/log/IS_install.log

Windows 客户机（组件将要安装到的远程系统）：

- SystemRoot\TEMP\OB2DBG_did_INSTALL_SERVICE_DebugNo_debug.txt
- SystemRoot\TEMP\CLUS_DBG_DebugNo.TXT

Temp 目录的位置由 TEMP 环境变量指定，并且 SystemRoot 是在 SystemRoot 环境变量中指定的路径。

如果没有创建安装日志文件，请带调试选项运行远程安装。

Data Protector 日志文件

下面列出的 Data Protector 日志文件位于:

Windows 系统： Data_Protector_program_data\log

Solaris 和 Linux 系统: /var/opt/omni/log 以及 /var/opt/omni/server/log

下面的日志文件对于安装故障诊断非常重要：

debug.log	包含意外情况。虽然其中的某些内容可能对您有意义，但是这些信息主要供支持人员或支持部门使用。

inet.log	包含发给 Data Protector Inet 服务的请求。它对于检查客户机上 Data Protector 的近期活动很有用。
IS_install.log	包含远程安装的跟踪，并且位于安装服务器上。
omnisv.log	包含有关 Data Protector 服务停止和启动时间的信息。

创建安装执行跟踪

如果客户支持服务要求，请使用 debug 选项运行安装。

要调试远程安装，请运行带调试选项的 Data Protector GUI：

```
Manager -debug 1-200 DebugPostfix
```

会话完成/终止后，从以下位置收集调试输出：

- 在安装服务器系统上:

  Data_Protector_program_data\tmp\OB2DBG_did__BM_ Hostname_DebugNo_DebugPostfix

- 在远程系统上：

  SystemRoot:\Temp\OB2DBG_did__INSTALL_SERVICE_Hostname_DebugNo_DebugPostfix

验证 Data Protector 单元中的 DNS 连接

DNS（域名系统）是 TCP/IP 主机的名称服务。DNS 配置了主机名和 IP 地址的列表，使用户能够按主机名而不是按 IP 地址指定远程系统。DNS 确保 Data Protector 单元的成员之间正确通信。

如果 DNS 配置不正确，Data Protector 单元中可能会发生名称解析问题，并且其成员将无法相互通信。

Data Protector 提供了 omnicheck 命令来验证 Data Protector 单元各成员间的 DNS 连接。虽然可以用此命令检查单元中所有可能的连接，但是只需验证以下连接即可，这些连接在 Data Protector 单元中非常重要：

- Cell Manager 与单元其他成员的双向连接
- 介质代理与单元其他成员的双向连接

使用 omnicheck 命令

omnicheck 命令的语法为：

```
omnicheck -dns [-host Client | -full] [-verbose]
```

可以使用不同的选项在 Data Protector 单元中验证以下 DNS 连接：

- 要检查 Cell Manager 和单元中的每个介质代理是否可以正确解析与单元中每个 Data Protector 客户机之间的 DNS 连接 (反之亦然)，请执行以下命令:

  omnicheck -dns [-verbose]

- 若要检查某个特定的 Data Protector 客户机是否可以正确解析与单元中每个 Data Protector 客户机的双向 DNS 连接，则执行：

  omnicheck -dns -host client [-verbose]

  其中 *client* 是受检查的 Data Protector 客户机的名称。

- 若要检查单元中所有可能存在的 DNS 连接，则执行：

  omnicheck -dns -full [-verbose]

如果指定 [-verbose] 选项，命令将返回所有消息。如果不设置此选项（默认），那么将只返回检查失败的结果的消息。

有关详细信息，请参阅 omnicheck 手册页。

返回消息将列出 omnicheck 命令的返回消息。如果返回消息指出 DNS 解析出现问题，请参阅《Data Protector 故障诊断部分》的“网络和通信故障诊断”一章。

返回消息

返回消息	含义

client_1 cannot connect to client_2	连接 *client_2* 超时。
client_1 connects to client_2, but connected system presents itself as client_3	*client_1* 上的 *%SystemRoot%*\System32\drivers\etc\hosts /etc/hosts（Linux 系统）文件配置不正确，或者 *client_2* 的主机名与其 DNS 名称不匹配。
client_1 failed to connect to client_2	*client_2* 不可访问（例如，断开连接），或者 *client_1* 上的 *%SystemRoot%*\System32\drivers\etc\hosts（Windows 系统）或 /etc/hosts（Linux 系统）文件配置不正确。
checking connection between client_1 and client_2	
all checks completed successfully.	
number_of_failed_checks checks failed.	
client is not a member of the cell.	
client contacted, but is apparently an older version. Hostname is not checked.	

限制

- 该命令只验证单元成员之间的连接；一般不验证 DNS 连接。

调整操作系统参数

单元请求服务器 (CRS) 会调整其 ulimit 以支持大量打开的文件和套接字，但当前值通常足以满足需求。

在某些情况下，会报告以下错误:

"too many open files" error

如果遇到“打开的文件过多”错误，则您需要调整操作系统参数。

操作系统参数涵盖两个方面：

- 它们更改针对打开的文件和套接字的限制。
- 它们影响存在大量套接字连接时的性能。

以下列表不是确切的。有关详细信息，请参见 OS 文档。

Linux

内核参数保存在以下位置：

/etc/sysctl.conf

可以编辑 sysctl.conf 文件或调用 sysctl –w name=value。您还可以使用 sysctl –p 加载正在运行的内核或修改其相应的 procfs 文件。例如，变量 fs.file-max 与 /proc/sys/fs/file-max 对应。

默认值取决于可用内存。

变量	注意
fs.file-max	系统范围的最大文件描述符数量。
net.core.somaxconn	侦听套接字的挂起连接队列可增长到的最大长度。
net.ipv4.tcp_max_syn_backlog	尚未从连接客户机收到确认的已记录连接请求的最大数量。

此外，每进程限制的默认值存储在以下位置： /etc/limits.conf（或）/etc/security/limits.conf

问题

下面是安装过程中可能会遇到的一些问题：

- IPC 连接关闭错误
- 安装服务器进行标记以重新启动
- 使用 DNS 或 LMHOSTS 时名称解析失败
- 系统上未安装和配置 TCP/IP 协议
- 主机名长度检查失败
- NetBIOS 长度检查失败
- 主机名验证失败
- 未在所有 Cell Manager 中更新端口号
- 无法访问 Windows Installer 服务
- Windows 系统上的 Cell Manager 安装失败

IPC 连接关闭错误

在 Linux 计算机上远程安装期间同时选择 Vepa 和 VMware GRE 组件时，会显示以下错误消息:
IPC Connection Closed

原因

此问题的原因未知。

解决方案

重新运行安装。

安装服务器进行标记以重新启动

在安装过程中，会显示以下错误消息:
Installation Server is marked for restart, please restart Installation Server and retry installation.

原因

如果添加或修改以下注册表项，则会发生此问题:
HKEY_LOCAL_MACHINE\\SOFTWARE\\Hewlett-Packard\\OpenView\\OmniBackII\\RebootVolatile

解决方案

将 omnirc 变量 OB2WAITTIMEOUT 的值设置为 180。

Failed to install Visual Studio redistributable

Data Protector installation fails with the following message:

Failed to install Visual Studio redistributable. Please refer the product documentation for troubleshooting.

Cause

This issue occurs if either or both of these Microsoft Visual Studio redistributable versions are already installed on the system:

- Microsoft Visual Studio 2015
- Microsoft Visual Studio 2017 with version earlier than 14.16.27012

If any other application installed on the system is using Dynamic Link Libraries (DLLs) shipped by the above versions of Microsoft Visual Studio during Data Protector upgrade, the Microsoft Visual Studio 2017 redistributable fails to replace those DLLs.

Solution

Apply the most recent version of Visual Studio 2019 (x64) redistributable from Microsoft. If the Microsoft Visual Studio 2015 or 2017 (x86) redistributable was installed earlier, it is recommended to apply the most recent version of Visual Studio 2019 (x86) redistributable as well. Reboot the system if requested by the installer and retry Data Protector installation.

使用 DNS 或 LMHOSTS 时名称解析失败

名称解析失败且显示以下错误，并中止安装:

error expanding hostname

原因

- 如果在使用 DNS 时遇到解析问题，您将获得有关当前 DNS 配置的警告消息。
- 如果在使用 LMHOSTS 文件时遇到解析问题，您将获得要求检查 LMHOSTS 文件配置的警告消息。
- 如果尚未配置 DNS 或 LMHOSTS，您将获得警告消息，提示在 TCP/IP 属性对话框中启用 DNS 或 LMHOSTS 解析。

解决方案

检查 DNS 或 LMHOSTS 文件配置或将其激活。

全新安装后，仪表板不显示备份数据的大小

如果在成功安装 DP 2019.08 或更高版本之后执行备份，则 DP 仪表板和 omnicc -cbl_detail 命令行界面不会显示此备份的大小。

原因

DP 仪表板和 omnicc -cbl_detail 命令行界面从数据库表 'DP_CATALOG_CBL' 中读取“受保护的数据总计”。在每天运行一次的日常维护作业期间，'DP_CATALOG_CBL' 表中将计算并更新“受保护的数据总计”。因此，在日常维护作业之前进行的任何备份都不会显示在仪表板以及 omnicc -cbl_detail 命令行界面的输出中。

解决方案

1. 运行以下命令以计算并更新 'DP_CATALOG_CBL' 表中的“受保护的数据总计”：
   Windows： Program Files\OmniBack\bin\omnidbutil -update_total_protected_data
   Linux： /opt/omni/sbin/omnidbutil -update_total_protected_data
2. 在仪表板上或使用 omnicc -cbl_detail 命令行界面检查备份大小。

系统上未安装和配置 TCP/IP 协议

Data Protector 使用 TCP/IP 协议进行网络通信。在单元中的每个客户机上安装和配置它。否则，安装将中止。

原因

如果未在单元中的每个客户机上安装和配置 TCP/IP 协议，则会发生此问题。

解决方案

检查 TCP/IP 设置。

主机名长度检查失败

在 Windows 上进行 Data Protector 安装期间，安装向导将检查主机名长度是否在 Microsoft 允许的限制范围内。如果此检查失败，则安装状态将显示此错误。

原因

主机名长度超过 60 个字符。

解决方案

主机名或 Cell Manager 名称必须小于或等于 60 个字符。

NetBIOS 长度检查失败

此问题是 Windows 平台特定问题。

原因

NetBIOS 长度超过 15 个字符。

解决方案

NetBIOS 名称必须多于 2 个字符且不超过 15 个字符。

主机名验证失败

安装期间主机名验证失败。

原因

当前主机名以下划线 "_" 开头。

解决方案

主机名或 Cell Manager 名称必须以字母开头，且不得包含下划线 "_"。

无法访问 **Windows Installer** 服务

系统报告以下某条错误消息：

- The Windows Installer Service could not be accessed.
- This application must be installed to run.
- This patch package could not be opened.
- The system cannot open the device or file specified.

原因

安装 Data Protector 后，Windows 可能报告某些应用程序未安装，或者需要重新安装。

原因是 Microsoft 安装程序升级过程中出现错误。Microsoft Installer 1.x 版数据信息未迁移到 Data Protector 在计算机上安装的 Microsoft Installer 2.x 版。

解决方案

有关如何解决该问题的信息，请参见 Microsoft 知识库文章 Q324906。

Windows 系统上的 Cell Manager 安装失败

系统报告以下消息：

Setup is unable to match the password with the given account name.

原因

如果将要安装 Cell Manager 的 Windows 系统不是域的一部分，则会发生此问题。

解决方案

有两种解决方案：

- 确保将要安装 Cell Manager 的 Windows 系统加入域。
- 对 CRS 服务使用本地管理员帐户。

找不到 **msvcr90.dll** 文件

系统显示以下错误消息：

msvcr90.dll file is not found.

原因

找不到 MSVCR90.dll 库（大写），因为网络共享上只有 msvcr90.dll （小写）。由于 MSVCR90.dll 和 msvcr90.dll 未被视作同一个文件，因此 setup.exe 未能找到相应的 dll 。

解决方案

将 msvcr90.dll （小写）文件重命名为 MSCVCR90.dll （大写），或者将网络共享重新配置为不区分大小写。

取消安装未卸载已经安装的组件

如果取消 Data Protector 安装，但是某些组件已经安装，那么 Data Protector 不会卸载已经安装的组件。安装将完成，并带有错误。

原因

如果取消 Data Protector 安装，但是某些组件已经安装，那么 Data Protector 不会卸载已经安装的组件。

解决方案

取消安装后，手动卸载已经安装的组件。

UNIX 客户机远程安装失败

远程安装 UNIX 客户机失败，并出现以下错误消息:

Installation/Upgrade session finished with errors.

原因

远程安装 UNIX 客户机时，客户机系统上 /tmp 文件夹下的可用磁盘空间应至少为要用于安装的最大包的大小。在 Solaris 客户机系统上，/var/tmp 文件夹下也应该有相同的磁盘空间量。

解决方案

检查上面提到的目录中是否有足够的磁盘空间，然后重新启动安装过程。

安装 HP-UX 客户机时出现问题

在将新的 HP-UX 客户机添加到 Data Protector 单元时，出现以下错误消息:

```
/tmp/omni_tmp/packet:您没有执行此 SD 函数所需的权限... 访问根目录以及在已注册库 /tmp/omni_tmp/packet 上启动代理被拒绝。主机上无插入权限。
```

原因

如果在将 HP-UX 客户机添加到 Data Protector 单元时 swagent 进程未运行，则会发生此问题。

解决方案

按如下方式先停止再重新启动 swagent 后台程序: 终止该进程，然后通过运行 /opt/omni/sbin/swagentd 命令重新启动该进程；或者运行 /opt/omni/sbin/swagentd -r 命令。

确保 hosts 文件 (/etc/hosts) 中有 local host, loopback 条目。

无法启动 **omniinet** 服务

启动 Cell Manager 时，出现以下错误消息:

ERROR: Cannot start "omniinet" service, system error: [1053] Unknown error 1053.

解决方案

检查 inetd、 systemd 或 xinetd 服务是否正在运行。如果 /etc/xinetd.d/omni 存在，则 DP 是使用 inetd 或 xinetd 配置的。如果它不存在，则 DP 是使用 systemd 配置的。

xinetd: ps -ef | grep xinetd 或 pidof xinetd

systemd: ps -ef | grep systemd或 pidof systemd

要启动该服务，请执行：

xinetd: systemctl start xinetd

systemd: systemctl start omni.socket

在具有有效凭据的 Linux 客户机上推送安装失败

具有有效凭据的 Linux 客户机上的推送安装失败，并显示以下错误消息：

```
[严重] <iwf1114165.hostname.net> SSH 配置失败。输入的凭据不正确或者发生了某个错误。 <iwf1114165.hostname.net>：跳过 0% [严重] <iwf1114165.hostname.net> 连接到客户机 iwf1114165.hostname.net 时出错 正在跳过客户机! [正常] 安装会话已于 Mon 14 Nov 2016 03:13:52 PM IST 完成。 已完成安装。
```

原因

如果您的环境中未启用身份验证，则可能会发生此问题。

解决方案

确保在 Linux 客户机上为 ssh 服务启用密码身份验证。否则，请执行以下步骤：

1. 通过将以下行添加到 ssh 配置文件中来启用身份验证:
   PasswordAuthentication yes
2. 重新启动 ssh 服务。

Inet 服务在 NIS 环境中无法启动

在 NIS 环境中安装 Data Protector 后， Data Protector Inet 服务无法启动。

原因

如果 /etc/nsswitch.conf 文件未按照 Data Protector 要求进行更新，则可能会发生此问题。

解决方案

检查 /etc/nsswitch.conf 文件。

如果找到下面一行：

```
services: nis [NOTFOUND=RETURN] files
```

将该行替换为：

```
services: nis [NOTFOUND=CONTINUE] files
```

客户机远程安装失败

在 Windows Server 2008 和 Windows Server 2012 上远程安装客户机失败，并出现以下错误消息:

Could not copy client's self-signed certificate from a pipe.

原因

如果未复制客户机的自签名证书，则会发生此问题。

解决方案

使用以下命令在 Cell Manager 中导入客户机:

- 对于新安装:

1. 删除以下路径中的文件 _cert.pem>：OMNI_HOME\config\client\sscertificates\ (Cell Manager 中):
2. 使用以下命令再次导入主机:
   omnicc -import_host <client_hostname>

- 对于升级:

1. 使用以下命令导出客户机:
   omnicc -export_host <client_hostname>
2. 使用以下命令再次导入主机:
   omnicc -import_host <client_hostname>

计划迁移失败或跳过

升级期间计划迁移失败或跳过。

原因

此问题的原因未知。

解决方案

如果在升级过程中计划迁移失败或跳过，您可以手动运行以下命令，以便将现有计划成功迁移到新的计划程序：

```
omnidbutil -migrate_schedules
```

用户迁移失败或跳过

升级期间用户迁移失败或跳过

原因

此问题的原因未知。

解决方案

如果在升级过程中用户迁移失败或跳过:

1. 使用命令 omnisv -status 检查 appserver 服务是否正在运行。
2. 运行以下命令以迁移现有用户:
   - Windows： <*DP_HOME*>\bin\perl.exe <*DP_HOME*>\bin\userMigrate.pl
   - Linux： /opt/omni/bin/perl /opt/omni/sbin/userMigrate.pl

Windows 上的 InstallShield 错误

在应用补丁或升级 Data Protector 时，InstallShield 向导会显示错误：

An error (- 5012 : 0x80070005) has occured while running the setup.

原因

发生此错误的原因是第三方防病毒软件阻止了某些安装组件。

解决方案

完成以下步骤：

1. 在升级过程中暂时禁用第三方防病毒软件。
2. 成功安装/升级后启用第三方防病毒软件。

群集升级导入失败

在集群环境中安装会显示一条消息 [WARNING] Import of cluster or node has not been completed successfully.

原因

如果在安装过程中未生成证书，则会发生此问题。

解决方案

1. 在导入失败的节点上执行以下步骤:
    1. 将 localhost_key.enc 和 localhost_cert.pem 从 \config\server\sscertificates\ 复制到被动节点中的 Data_Protector_program_data\Config\client\sscertificates 文件夹。
    2. 在被动节点上重新启动 INET 服务。
2. 在主动/主节点上执行以下步骤:
    1. 运行以下命令： omnicc -update_host <node>
    2. omnicc -import_cluster <failedClusterName> -server <cellmanagerName>.

推送安装期间出现“找不到 sh: sudo:”错误

在 HP-UX 上推送安装期间显示 sh: sudo: not found 错误。

原因

当 sudo 二进制文件不是 PATH 变量的一部分时，会发生此错误。

解决方案

先执行以下步骤，再继续安装:

1. 打开 /etc/opt/ssh/sshd_config 文件并将 **PermitUserEnvironment** 变量值更改为 **Yes**。
2. 重新启动 **sshd** 服务。执行以下命令：
   - /sbin/init.d/secsh stop
   - /sbin/init.d/secsh start
3. 在路径 <user_homedirectory>/.ssh 下为每个 SUDO 用户创建一个名为 **environment** 的文件，并添加 **PATH** 变量。**PATH** 变量必须包含 sudo 二进制文件的安装路径。
   添加具有为所有 SUDO 用户定义的 PATH 变量的环境文件。

   environment 文件中的 PATH 变量定义示例:

   ```
   PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/contrib/bin:/usr/contrib/Q4/ bin:/opt/perl/bin:/opt/gvsd/bin:/opt/ipf/bin:/opt/nettladm/bin:/opt/fcms/
   bin:/opt/wbem/bin:/opt/wbem/sbin:/opt/sas/bin:/opt/graphics/common/
   bin:/opt/hpvm/bin:/opt/atok/bin:/usr/bin/X11:/usr/contrib/bin/X11:/opt/ sec_mgmt/bastille/bin:/opt/caliper/bin:/opt/drd/bin:/opt/dsau/bin:/opt/
   dsau/sbin:/opt/resmon/bin:/opt/firefox:/opt/perf/bin:/usr/contrib/kwdb/ bin:/opt/perl_32/bin:/opt/perl_64/bin:/opt/prm/bin:/opt/propplus/bin:/
   opt/sfm/bin:/etc/cmcluster/scripts/tkit/vtn:/opt/swm/bin:/opt/sec_mgmt/
   spc/bin:/opt/ssh/bin:/opt/swa/bin:/opt/hpsmh/bin:/opt/thunderbird:/opt/
   sentinel/bin:/opt/langtools/bin:/opt/gwlm/bin:/opt/VRTS/bin:/opt/VRTS/
   vxfs5.0/man:/opt/omni/bin:/usr/local/sbin/:/usr/local/bin:/sbin:/home/root:/
   usr/local/bin:/usr/sbin:/usr/bin:/usr/sbin:/sbin:/usr/bin:/usr/sbin:/etc:/usr/local/
   bin:/usr/sam/lbin:/usr/sbin/acct:.:/sbin:/home/root:/usr/local/bin:/usr/local/bin:DP
   ```

   (上述路径必须在一行输入，且不得包含任何空格)。
4. 重新启动 **sshd** 服务。执行以下命令：
   - /sbin/init.d/secsh stop
   - /sbin/init.d/secsh start
5. 通过在安装服务器上执行以下命令来验证 sudo 二进制文件是否是 PATH 变量的一部分:
   /opt/omni/lbin/omnissh.sh / test@<client_hostname> 'sudo -S [-d /tmp/omni_tmp]'

卸载 Linux 客户机时发出警告

在 Data Protector GUI 中远程卸载 Linux 客户机时，出现以下警告:

[Warning] <client_hostname> No valid software found on client <client_hostname>...

原因

当用于卸载的安装服务器系统还安装了 Cell Manager 时，会发生此问题。

解决方案

无需执行操作。客户机将成功卸载。

用户名无效或密码错误

推送安装到 UNIX 客户机时要求提供用户凭据。

原因

<User_HomeDirectory>/.ssh/authorized_keys 文件中的权限不正确。

解决方案

将 <User_HomeDirectory>/.ssh/authorized_keys 文件的权限设置为 640。

许可证不可用

系统显示以下错误消息：

License not available "Feature is not licensed with Express edition of this product. Upgrade to Premium edition to use all features".

原因

尝试将 Premium 功能与 Data Protector Express 许可证一起使用时，将会出现此错误消息。

解决方案

请升级到 Data Protector Premium 版本以使用所有功能。

重新安装 REST 服务器失败

卸载后，在同一台计算机上重新安装 REST 服务器失败。

原因

此问题的原因未知。

解决方案

请执行以下操作：

1. 卸载后删除以下目录:
   - Windows： C:\ProgramFiles\Omniback 和 C:\ProgramData\Omniback
   - Linux： /opt/omni/ 、 /var/opt/omni/ 和 /etc/opt/omni/
2. 尝试重新安装 REST 服务器。

未在所有 Cell Manager 中更新端口号

对于多个 Cell Manager 设置，未在所有 Cell Manager 中更新端口号。

原因

您需要在多个 Cell Manager 设置中的所有 Cell Manager 中手动更新端口号。

解决方案

在一个 Cell Manager 中更改端口号后，请确保在所有 Cell Manager 中更新端口号。

Windows 客户机远程安装失败

将 Data Protector 客户机远程安装到 Windows 系统失败，系统报告以下错误消息：

```
[正常] 正在连接到客户机 computer.company.com... [正常] 已完成。 [正常] 正在 客户机 computer.company.com 上安装引导服务... [严重] 无法连接到客户机 computer.company.com 上的 SCM（服务控制管理器）：[5] 访问被拒绝。
```

原因

发生此问题是由于用户权限不足以运行远程安装。

解决方案

请执行以下操作：

1. 在安装服务器系统上，执行下面的命令将本地操作系统管理员用户组中的某个用户帐户标记为在远程安装期间可用:
   omniinetpasswd –inst_srv_user User@Domain
   请注意，必须先将用户帐户添加到本地 Inet 配置。
2. 再次启动 Data Protector 客户机的远程安装。

客户机远程安装失败

在 Windows Server 2012 上远程安装客户机失败，并显示以下错误消息:

Could not copy client's self-signed certificate from a pipe

原因

此问题的原因未知。

解决方案

使用以下命令在 Cell Manager 中导入客户机:

- 对于新安装：omnicc -import_host <client_hostname>
- 对于升级:

1. 使用以下命令导出客户机：omnicc -export_host <client_hostname>
2. 使用以下命令再次导入主机：omnicc -import_host <client_hostname>

数字签名验证可能会失败

数字签名验证失败，并显示以下错误消息：

```
[严重] <computer.company.com> [70:32] 安装工具包的数字签名验证失败。
```

原因

如果 Windows 2008 R2 系统断开连接，数字签名验证可能会失败。

解决方案

执行以下操作之一：

- 启用 Internet 连接，并等待直至正确的证书自动导入到受信任的根证书颁发机构和中间证书颁发机构。
- 要了解如何在断开连接的系统上更新受信任的根证书，请参见以下文章：
  - https://support.microsoft.com/en-us/kb/3004394
  - https://support.microsoft.com/en-us/kb/2813430

安装 Cell Manager 时应用程序服务器服务无法启动

应用程序服务器服务无法启动，并显示以下消息:

> 启动 Data Protector Application Server 之前已超时。

安装摘要日志文件中记录了以下错误:

> 因 org.jboss.as.cli 所致。 CommandLineException：控制器在本地主机上不可用：9999

原因

由于 PATH 系统环境变量未包含 %SystemRoot%\system32 目录，因此安装进程无法访问各种实用程序。

解决方案

将 %SystemRoot%\system32 目录添加到 PATH 变量。

以下文件位于 Windows 系统上的 %SystemRoot%\system32 文件夹 (取决于所选组件) 中:

- BrandChgUni.dll: 该资源库包含注册表设置的路径，因此请将其放在众所周知的位置，以便集成库可以访问它。
- libarm32.dll: 该 NULL 共享库用于 ARM 仪器。第三方监视软件可以替换它。
- ob2informix.dll: 该库用于与 Informix Server 数据库集成。
- snmpOB2.dll: 该库用于实现系统 SNMP 陷阱。

Cell Manager 安装/升级失败

安装状态报告 (可在 **%TEMP%** 目录下找到，文件名为: **DP_xxxx-xxxx_setup_status.txt**，其中 xxxx-xxxx 是一组任意字符) 中的以下消息表明，由于 Java 堆大小不足，安装失败:

```
已选取 _JAVA_OPTIONS: -Xmx512M
```

以上消息表明，堆大小已手动设置为 512 MB。

原因

如果手动将 Java 堆大小设置为小于 2 GB，则 Cell Manager 安装/升级将失败。

解决方案

要解决此问题，请从计算机中删除 _JAVA_OPTIONS 环境变量，然后重新启动 Cell Manager 安装。

在 Windows 系统上客户端的本地安装失败

本地安装客户机失败，并出现以下错误消息:

```
未验证对象的数字签名
```

原因

在 Windows Server 2008 R2 系统中，会发生此问题。

解决方案

要解决此问题，请安装以下 Windows 修补程序，然后重试安装客户机：

- KB4474419
- KB4493730

在灾难恢复期间重复计算容量

如果在不同的硬件上执行灾难恢复或者更改了主机名/IP 地址，并且在 Cell Manager 中导入了主机，则将重复计算备份的容量。

原因

如果您在不同的硬件上执行灾难恢复或更改了主机名/IP 地址，然后在 Cell Manager 中导入主机，则会出现此问题。

解决方案

执行以下操作可避免重复计算:

- 使用相同的主机名/IP 地址执行灾难恢复。

对备份装载点采用嵌套形式的文件系统日期进行重复计算

Data Protector 可以备份在驱动器号或文件夹上装载的卷/存储 (嵌套装载)。如果在装载此类卷时更改了驱动器号或文件夹名称，则此类卷可能会额外消耗许可证的容量。

原因

如果在装载此类卷时更改了驱动器号或文件夹名称，则在嵌套装载上执行的备份可能会额外消耗许可证的容量。

解决方案

为避免重复计算容量，请勿更改卷驱动器号或文件夹名称。

在虚拟机迁移期间消耗额外的容量

在虚拟机迁移期间消耗额外的容量。

原因

如果跨 vCenter/ESXi 迁移虚拟机，并且迁移后的虚拟机获取的新实例 UUID 与原始实例不同，则可能导致重复计算容量。

解决方案

为避免重复计算容量，请在跨 vCenters/EXSi 迁移虚拟机时不要为迁移后的虚拟机配置新 UUID。

恢复群集时会发生容量的重复计算

在恢复群集或者在 Data Protector 外部重新创建群集时重复计算容量。

原因

使用 Data Protector 恢复群集时，或者在 Data Protector 外部使用不同或相同的主机名或 IP 地址重新创建群集时，会导致重复计算容量。

解决方案

为避免重复计算容量，请勿在 Data Protector 外部重新创建新群集。

将系统重新导入 Cell Manager 时重复计算容量

将系统重新导入到更换了物理硬件的 Cell Manager 时重复计算容量。

原因

如果更换系统主板时系统的 BIOS ID 和主机名/IP 地址等物理唯一实体发生变化，则会导致重复计算容量。

解决方案

为避免重复计算容量，请在更换系统主板时保留相同的主机名/IP地址。

重新导入虚拟机导致重复计算容量

重新导入虚拟机导致重复计算容量。

原因

如果在选中“更改 UUID”选项时重新创建相同的虚拟机，将会导致重复计算容量。

解决方案

为了避免在重新创建虚拟机时将容量计算两次，请保留该虚拟机的“UUID”。

添加取证虚拟机进行备份将会额外增加容量

添加取证虚拟机进行备份将会额外增加容量。

原因

Data Protector 将考虑添加使用“保留以用于取证”选项还原的虚拟机作为单个虚拟机。

解决方案

为避免在备份期间计算额外的容量，请不要添加取证虚拟机。

克隆的虚拟机会导致重复计算容量

克隆的虚拟机会导致重复计算容量。

原因

Data Protector 将克隆的虚拟机视为单个虚拟机。

解决方案

为避免在备份期间计算额外的容量，请不要添加克隆的虚拟机。

升级到 Data Protector 2018.08 后，备份会增加额外的容量

升级到 Data Protector 2018.08 后，备份会增加额外的容量。

原因

低于 2018.08 版本的 Data Protector 的备份对象位于 IDB 中。

解决方案

为避免计算额外的容量，请在升级后为所有的现有备份规范执行全新备份。

执行群集主机备份会导致重复计算容量

同一群集文件系统对象上发生备份数据的重复计数。

原因

如果在执行群集文件系统备份时选择群集主机以及群集主机的主动节点，则会出现此问题。

解决方案

为避免重复计算备份大小，请在执行群集文件系统备份时仅选择群集主机。

omnicc -query 命令的输出显示不正确

omnicc -query 、 omnicc -check_license 、 omnicc -check_license -detail 和 omnicc -password_info 命令的输出显示不正确。

原因

即使在应用新许可证后，紧急许可证仍处于活动状态，这种情况下便会出现该问题。

解决方案

要正确显示命令输出，请从 \programdata\config\server\cell\ (Windows) 或 /etc/opt/omni/server/cell/ (Linux) 路径下的 **lic.dat** 文件中删除紧急许可证密钥及其注释。

许可证信息显示不正确

GUI 的“帮助”>“许可证”>“密码信息”选项卡中未正确显示许可证信息。

原因

即使在应用新许可证后，紧急许可证仍处于活动状态，这种情况下便会出现该问题。

解决方案

要显示正确的许可证信息，请从 \programdata\config\server\cell\ (Windows) 或 /etc/opt/omni/server/cell/ (Linux) 路径下的 **lic.dat** 文件中删除紧急许可证密钥及其注释。

HPEDpHsm 驱动程序代码签名错误

加载 HPEDpHsm 驱动程序的命令失败，并显示以下消息：

Load failed with error: 0x80070241

Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

原因

如果驱动程序未经过 WHQL 签名，则会出现此问题。在没有 Internet 访问权的系统上可以观察到该现象。

解决方案

1. 打开管理命令提示符，运行以下命令：
   bcdedit /set TESTSIGNING ON
2. 重新启动计算机。
3. 安装驱动程序。
4. 再次打开管理命令提示符，然后运行以下命令：
   bcdedit /set TESTSIGNING OFF
5. 重新启动计算机。

Linux 上的 DP 客户机卸载失败

Linux 上的 DP 客户机卸载失败，并显示以下错误:

'''[root@myserver /tmp]# cat OmniBack_rpmrm.log''' 正在删除 OB2-TS-CORE OB2-DA OB2-MA OB2-CC OB2-CORE 正在删除 OB2-TS-CORE 错误: 无法执行 scriptlet interpreter /bin/sh: 权限被拒 错误: %preun(OB2-TS-CORE-A.10.70-1.x86_64) scriptlet 失败，退出状态 127 错误: OB2-TS-CORE-A.10.70-1.x86_64: 擦除失败

原因

SELinux 配置为 "enforcing" 模式，该模式限制了来自远程主机的 rpm 删除请求。

解决方案

1. 检查虚拟机上的 SELinux 状态。

   [root@myserver idbdata]# sestatus

   SELinux status: enabled

   SELinuxfs mount: /sys/fs/selinux

   SELinux root directory: /etc/selinux

   Loaded policy name: targeted

   Current mode: enforcing

   Mode from config file: enforcing

   Policy MLS status: enabled

   Policy deny_unknown status: allowed

   Max kernel policy version: 31

   上面的输出显示 SELinux 模式设置为 "enforcing"。
2. 将 SELinux 模式更改为 "permissive"。
   1. 打开文件 /etc/selinux/config 。
   2. 更改 'SELINUX=permissive' 并保存更改。
3. 重新启动 VM。运行以下命令：
   sudo shutdown -r now
4. 如果防火墙正在运行，请停止防火墙。运行以下命令：
   systemctl stop firewalld

升级问题故障诊断

如果在升级 Data Protector 时遇到问题，可以检查以下日志文件来确定问题:

upgrade.log	此日志是在升级期间创建的，并包含升级核心部分 (UCP) 和升级详细信息部分 (UDP) 消息。
OB2_Upgrade.log	此日志是在升级期间创建的，并包含升级过程的跟踪。

本节包含与升级问题相关的信息。它包括以下故障排除主题：

群集客户机未导入

在“群集感知”客户机上升级 Data Protector 或安装 Data Protector 补丁时，将群集客户机导入 Cell Manager 失败并显示以下消息:

```
Import of cluster client has not been successfully completed.
```

原因

import cluster 命令在该客户机上运行。但是，Cell Manager 上的用户列表不包括该客户机，因此会显示“权限不足”错误。

解决方案

将客户机手动导入单元，并为导入的客户机设置用户帐户。请参阅以下主题:

- 将群集感知客户机导入到单元。
- 配置用户

升级期间和之后的其他应用程序服务器问题

升级过程中或升级后可能会出现以下问题:

- 用户迁移在升级期间失败
- 计划迁移在升级期间失败
- 升级后无法执行用户管理任务，例如列出用户
- 升级后无法执行高级计划管理操作
- 升级后应用程序服务器服务（hpdp-as）无法正确启动
- 升级后未部署 Data Protector 服务（war 文件部署）
- 应用程序服务器未按预期运行的其他问题

原因

原因是升级期间应用程序服务器配置不一致或失败。

解决方案

要修复不一致的应用程序服务器配置，请使用应用程序服务器重新配置实用程序。请参见 omniasfix 。

未列出 **omniusers -list** 用户

升级失败并显示以下消息:

omniusers -list users not listed

原因

出现此问题可能有各种原因。一些常见原因如下:

- LDAP 服务器不可访问。
- 运行单元请求服务器 (CRS) 的用户帐户在 UserList 文件中不可用。
- 应用程序服务器、CRS 或 IDB 服务已关闭。

解决方案

要解决此问题，请按照下列步骤操作:

1. 检查 LDAP 服务器是否可访问。如果不可访问:
    1. 从 Cell Manager 中删除 LDAP 服务器配置。
    2. 在 LDAP 服务器与 Cell Manager 之间建立连接。
    3. 在 Cell Manager 中重新配置 LDAP 服务器。
2. 验证 UserList 文件中是否存在 CRS 用户帐户。如果它不可用，请手动添加它。
3. 运行以下命令以检查应用程序服务器、CRS 和 IDB 服务是否正在运行:
   omnisv -status
   如果这些服务已关闭，请通过运行 omnisv -start 命令启动它们。
4. 运行 omniusers -list 命令以验证该问题是否已解决。

没有可用于所选客户机系统类型的安装服务器

客户机的推送升级失败，并显示以下消息:

Cannot proceed. There are no Installation Servers available for the type of client system(s) that you selected.

原因

出现此问题可能有多种原因。原因之一是 cell_info 文件损坏。如果 cell_info 文件中的客户机主机名格式不正确，则升级失败并显示上述消息。

解决方案

- 如果从 DP 10.x 版升级客户机，请在 Cell Manager 上运行以下命令并重试客户机升级:
  omnicc -update_host <client_hostname>
- 如果从 DP 9.x 版升级，请在 Cell Manager 上运行以下命令并重试客户机升级:
  a. omnicc -secure_comm -configure_for_legacy_client <client_hostname>
  b. omnicc -update_host <client_hostname>

数据库实用程序在升级期间已停止工作

从 DP 版本 2019.05、2019.08、2019.12、2020.05、2020.08、2020.11 或 2021.02 升级时，升级崩溃并显示以下错误:
Database Checking has stopped working

原因

出现此问题可能有多种原因。原因之一是 omnirc 文件损坏。

解决方案

按照以下步骤解决此问题:

1. 将 omnirc 文件重命名为 omnirc_bkp 并再次运行升级。
2. 升级完成后，将 omnirc_bkp 文件重命名回 omnirc 。

升级后调试保持已启用状态

升级到较新版本后，Data Protector 会记录计划作业或其他操作的调试。您可能在 Windows 环境中遇到此问题。

解决方案

请遵循以下步骤：

1. 以执行升级的用户身份登录 Cell Manager。
2. 转至“这台电脑”（“我的电脑”）>“属性”>“高级系统设置”>“环境变量”。从“用户变量”中选择 OB2DBG ，然后单击“删除” 。如果未在环境变量列表中定义 OB2DBG ，请继续下一步。

> 注意**:** 在 Cell Manager 群集设置中，在主节点和所有辅助节点上执行此步骤。

3. 为运行 Data Protector 服务 (请参阅 services.msc) 的用户重复步骤 1 和 2。
4. 重新启动 Data Protector Cell Manager 服务，包括 Data Protector INET。
   - 在单独的 Cell Manager 上，运行以下命令:
     omnisv -restart
   - 在 Cell Manager 群集设置中，执行以下操作:
     - 从故障转移群集管理停止 Data Protector 群集角色。
     - 要重新启动 Data Protector INET 服务，请在所有群集节点上运行以下命令:
       sc stop omniinet
       sc start omniinet
     - 从故障转移群集管理启动 Data Protector 群集角色。
5. 删除在 Cell Manager 和客户机系统上创建的 OB2DBG*.txt 文件。您可以手动删除它们，也可以使用 Data Protector GUI 中的“删除调试文件” 选项 (“客户机” 上下文) 或运行 omnidlc 命令来删除。

打开内部数据库时出错

从 DP 2020.05 (10.70) 之前的 DP 版本升级辅助节点时，将显示以下错误消息:

Error in opening the internal database.

Could not update telemetry details.

原因

仅当在 SG 群集辅助节点上从 DP 10.70 (DP 2020.05) 之前的版本进行 DP 升级期间才看到此问题。这是因为主要节点上的 PostgreSQL 版本高于辅助节点上的 PostgreSQL 版本。

解决方案

您可以忽略该错误消息，因为两个节点 (主节点和辅助节点) 都升级后，所有 DP 功能均按预期工作。

无法创建服务帐户

执行 DP 升级后，显示以下警告:

Unable to create service account

原因

如果没有将正在执行升级的用户添加为 DP 中的用户，则会发生此问题。升级过程在内部运行 omniusers 命令以创建 Keycloak 服务帐户。如果执行升级的用户不是有效的 DP 用户，则 omniusers 命令将失败，并在调试日志中记录以下消息:
You have inadequate user privileges to perform attempted operation.

解决方案

在“用户” 上下文中将执行升级的用户添加为 DP 用户，然后重试升级。
DP 用户是用户名的组合。域/组和客户机。

无法安装 Visual Studio 可再发行组件

Data Protector 安装失败，并显示以下消息：

Failed to install Visual Studio redistributable. Please refer the product documentation for troubleshooting.

原因

在以下情况下会出现此问题:

- 原因 **1:** 如果以下 Microsoft Visual Studio 可再发行版本中的一个或两个都已安装在系统上:
  - Microsoft Visual Studio 2015
  - 版本早于 14.16.27012 的 Microsoft Visual Studio 2017

  如果在 Data Protector 升级期间，系统上安装的任何其他应用程序正在使用上述版本的 Microsoft Visual Studio 附带的动态链接库 (DLL)，则 Microsoft Visual Studio 2017 可再发行组件将无法替换这些 DLL。
- 原因 **2:** 您从安装服务器计算机上的 OmniBack 共享在 Windows Server 2008 R2 系统上本地安装或升级 Data Protector。

解决方案

- 原因 **1** 的解决方案**:** 应用可从 Microsoft 重新发行的 Visual Studio 2019 (x64) 最新版本。如果以前安装了 Microsoft Visual Studio 2015 或 2017 (x86) 可再发行版本，则建议也应用最新版本的 Visual Studio 2019 (x86) 可再发行版本。重新启动系统 (如果安装程序要求)，然后重试 Data Protector 安装。
- 原因 **2** 的解决方案**:** 将安装程序文件复制到要安装或升级 Data Protector 的系统，并使用复制到系统的安装程序文件安装或升级 DP。

从 DP 10.04 版本升级后无法添加 LDAP 用户

从 DP 10.04 升级后，添加新的 LDAP 用户失败。

解决方案

删除现有的 LDAP 配置，然后再次添加相同的 LDAP 配置。

SLES 15 上的升级失败

当从 DP 2019.12 或早期版本升级到更高版本时，升级脚本无法停止 hpdp-idb-cp 服务，并发出 SIGTERM 信号。升级失败并显示以下消息:

```
已通过:  已验证应用程序服务器一致性。所有检查已成功。 验证系统要求已成功完成。 从系统删除产品 Data Protector... 无法停止 "hpdp-idb-cp" 服务，系统错误: [1053] 未知错误 1053
```

原因

当早期版本的 DP 中的 Cell Manager 安装在 SUSE Enterprise Linux Server (SLES) 15 上时，会发生此问题。

解决方案

升级 DP 之前，修改 /etc/init.d/hpdp-idb-cp 文件以使用 SIGKILL 终止进程:

```
41 _stop() 42 { 43 PID=`ps -waef | grep '/opt/omni/idb/bin/pgbouncer -d /etc/opt/omni/server/idb//hpdp-idb-cp.cfg' | grep -v grep | awk '{print $2}'` 44 45 if [ "x$PID" = "x" ]; 46 then 47 echo "hpdp-idb-cp not running" 48 else 49 kill -9 $PID 50 echo "hpdp-idb-cp stopped" 51 fi 52 }
```

主机名长度检查失败

升级期间主机名长度检查失败。

原因

主机名长度超过 60 个字符。

解决方案

主机名或 Cell Manager 名称必须小于或等于 60 个字符。

NetBIOS 长度检查失败

原因

NetBIOS 长度超过 15 个字符。

解决方案

NetBIOS 名称长度必须介于 2 到 15 个字符之间。

主机名验证失败

升级期间主机名验证失败。

原因

主机名以下划线 "_" 开头。

解决方案

主机名或 Cell Manager 名称必须以字母开头，且不得包含下划线 "_"。

升级前主机名已更改和/或主机名未正确配置

如果在未正确配置升级或主机名之前更改了主机名，升级将失败。

原因

当前主机名未配置为 Data Protector 单元名称。

解决方案

要正确配置 Cell Manager 名称，请参阅主题系统准备和维护任务下的“更改 Cell Manager 名称”一节。

Data Protector 升级后，未安装某些应用程序

升级 Data Protector 后，Windows 可能报告某些应用程序未安装，或者需要重新安装。系统报告以下某条错误消息：

- The Windows Installer Service could not be accessed.
- This application must be installed to run.
- This patch package could not be opened.
- The system cannot open the device or file specified.

原因

Microsoft 安装程序升级过程中出现错误。Microsoft Installer 1.x 版数据信息未迁移到 Data Protector 在计算机上安装的 Microsoft Installer 2.x 版。

解决方案

请参阅 Microsoft 知识库中的文章 Q324906。

升级后，仪表板不会显示受保护的数据总数

如果从较旧的 DP 版本升级后执行备份，则 DP 仪表板和 omnicc -cbl_detail 命令行界面不会正确显示受保护的数据总计。

原因

DP 仪表板和 omnicc -cbl_detail 命令行界面从数据库表 'DP_CATALOG_CBL' 中读取受保护的数据总计。在每天运行一次的日常维护作业期间，'DP_CATALOG_CBL' 表中将计算并更新受保护的数据总计。因此，在日常维护作业之前进行的任何备份都不会显示在仪表板以及 omnicc -cbl_detail 命令行界面的输出中。

解决方案

1. 运行以下命令以计算并更新 'DP_CATALOG_CBL' 表中的受保护的数据总计:
   Windows： Program Files\OmniBack\bin\omnidbutil -update_total_protected_data
   Linux： /opt/omni/sbin/omnidbutil -update_total_protected_data
2. 在仪表板上或使用 omnicc -cbl_detail 命令行界面检查受保护数据总计。

UNIX 客户机远程升级失败

远程升级 UNIX 客户机失败，并出现以下错误消息:

```
Installation/Upgrade  session finished with errors.
```

原因

远程安装 UNIX 客户机时，客户机系统上 /tmp 文件夹下的可用磁盘空间应至少为要用于安装的最大包的大小。在 Solaris 客户机系统上，/var/tmp 文件夹下也应该有相同的磁盘空间量。如果没有足够的磁盘空间，则远程升级失败。

解决方案

检查上面提到的目录中是否有足够的磁盘空间，然后重新启动升级过程。

如果将以前版本的产品安装在长路径中，则升级将失败

如果将以前版本的产品安装在长路径中，则升级将失败。

原因

Data Protector 不支持将 Cell Manager 安装到长于 80 个字符的路径中。结果是升级失败。

解决方案

1. 将 omnimigrate.pl 脚本从安装程序包的目录 x8664\tools\Upgrade 复制到一个临时目录（例如 c:\temp ）。
2. 使用 omnimigrate 命令导出 IDB： perl c:\temp\omnimigrate.pl -export -shared_dir c:\output 使用在 Data Protector 安装中提供的 Perl 版本，并驻留在默认命令目录中。
3. 删除以前版本的 Data Protector，但保留其配置和数据库数据。不要删除 Data_Protector_program_data\db40 目录。
4. 安装 Data Protector。确保您要安装的路径短于 80 个字符。
5. 停止所有 Data Protector 服务： omnisv –stop
6. 将文件从旧的 Data_Protector_program_data\db40 目录 (在删除以前版本的 Data Protector 之后保留的目录) 复制到新的 Data_Protector_program_data\db40 文件夹。确保不移动 DCBF 目录。
7. 将配置从旧的 Data_Protector_program_data\Config\Server 文件夹复制到新的文件夹：
    1. 将旧的配置目录复制到新的目录，但保留旧的文件。不要复制 Data_Protector_program_data\Config\Server\install 目录中的文件。
    2. 如果要保留单元配置 (客户机、安装服务器)，请复制和覆盖 Data_Protector_program_data\Config\Server\cell\cell_info 和 Data_Protector_program_data\Config\Server\cell\installation_servers 文件。
8. 合并新的通知和全局选项文件：
    1. 要合并通知，请执行 omninotifupg.exe 工具： omninotifupg.exe -quiet
    2. 要合并全局选项文件，请执行： mrgcfg.exe –global -except BackupDeviceIdle -rename DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp=SessSuccessfulWhenNoObjectsBackedUp 或者，可以从旧的安装手动合并全局选项文件。
9. 启动 Data Protector 服务： omnisv -start
10. 将 IDB 导入到新的安装。执行： omnimigrate.pl -import -shared_dir c:\output -force

如果将以前版本的产品安装在不受支持的字符的路径中，则升级将失败

如果将以前版本的产品安装在具有不支持字符的路径中，则升级将失败。

原因

Data Protector 不支持将 Cell Manager 安装在以下路径：

- 包含非 ASCII 字符
- 包含“@”或“#”字符
- 包含以“!”字符结尾的目录

结果是升级失败。

解决方案

1. 将 omnimigrate.pl 脚本从安装程序包的目录 x8664\tools\Upgrade 复制到一个临时目录（例如 c:\temp）。
2. 创建两个使用 ASCII 名称的目录，例如：

   c:\output\cdb

   c:\output\mmdb
3. 导出 MMDB 和 CDB：

   omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb

   此过程将需要一段时间。当开始导出文件名时，可以使用 **Ctrl+C** 停止 omnidbutil 进程，因为升级不需要此数据。
4. 使用 omnimigrate 命令导出 IDB：

   perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output

   使用在 Data Protector 安装中提供的 Perl 版本，并驻留在默认命令目录中。
5. 创建一个 ANSI 字符集文件，c:\output\old_cm。此文件应包含以下两行：

   ```
   OLDCM_SHORTNAME=OldCmName OLDCM_ENDIANNESS=LITTLE_ENDIAN
   ```

   使用 Cell Manager 的短名称替代 *OldCmName*。
6. 删除以前版本的 Data Protector，但保留其配置和数据库数据。不要删除 Data_Protector_program_data\db40 目录。
7. 安装 Data Protector。确保您要安装的路径不包含任何非 ASCII 字符。
8. 停止所有 Data Protector 服务：

   omnisv –stop
9. 将文件从旧的 Data_Protector_program_data\db40 目录 (在删除以前版本的 Data Protector 之后保留的目录) 复制到新的 Data_Protector_program_data\db40 文件夹。确保*不*移动 DCBF 目录。
10. 将配置从旧的 Data_Protector_program_data\Config\Server 文件夹复制到新的文件夹：
    a. 将旧的配置目录复制到新的目录，但保留旧的文件。不要复制 Data_Protector_program_data\Config\Server\install 目录中的文件。
    b. 如果要保留单元配置 (客户机、安装服务器)，请复制和覆盖 Data_Protector_program_data\Config\Server\cell\cell_info 和 Data_Protector_program_data\Config\Server\cell\installation_servers 文件。
11. 合并新的通知和全局选项文件：
    a. 要合并通知，请执行 omninotifupg.exe 工具：

       omninotifupg.exe -quiet
    b. 要合并全局选项文件，请执行：

       mrgcfg.exe –global -except BackupDeviceIdle -rename DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp =SessSuccessfulWhenNoObjectsBackedUp

       或者，可以从旧安装中手动合并全局选项文件。
12. 启动 Data Protector 服务：

    omnisv -start
13. 将 IDB 导入到新的安装。执行：

    omnimigrate.pl -import -shared_dir c:\output -force

如果旧的 (基于 Raima DB) IDB 损坏，升级过程将中止

如果旧的 (基于 Raima DB) IDB 损坏，升级过程将中止。

原因

在升级期间，将检测并更正 IDB 中的以下损坏字段：

- 介质 blocks_used 设置为 0
- 介质 blocks_total 设置为 blocks_used
- 池 media_age_limit 设置为默认值（相同介质类的默认池的 media_age_limit ）
- 池 media_overwrite_limit 设置为默认值（相同介质类的默认池的 media_overwrite_limit ）

但是，如果 IDB 中的其他任何字段损坏，升级就会中止。

解决方案

将 Data Protector 安装还原到旧版本：

1. 删除当前版本的 Data Protector。
2. 重新安装以前版本的 Data Protector。
3. 还原旧的 IDB。

尝试安装其他升级时，需要修复旧的 IDB。要获得进一步协助，请与支持人员联系。

升级之后，omnidbcheck -bf 失败并显示错误

在先前版本的 Data Protector 中，由于 DC 二进制文件中介质的实际大小和头大小不一致，因此 omnidbcheck -bf 无法正确报告错误。

omnidbcheck -bf 可以正确报告升级之前 IDB 中可能存在的所有一致性错误。

原因

发生此问题是由于升级之前 IDB 中存在不一致。

解决方案

如果 DC 二进制文件损坏，可以删除 DC 二进制文件并通过导入具有正确日志记录级别的介质来重新创建它们。删除文件所产生的唯一影响是某些介质位置将指向不存在的二进制文件，因此在浏览相关的文件系统时将显示错误消息。

1. 从 omnidbcheck -dc 输出中，找出损坏的 DC 二进制文件的介质 ID。
2. 运行 omnimm -media_info medium-id 命令以获取介质的其他属性，如介质标签和介质池。
3. 找出受影响介质的 DC 二进制文件。DC 二进制文件的名称为： MediumID_TimeStamp.dat（在 MediumID 中，冒号 ":" 替换为下划线 "_"）。
4. 删除损坏的 DC 二进制文件。
5. 运行 omnidbutil -fixmpos 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
6. 从介质导入编目，以重新创建二进制文件。有关详细信息，请参阅《Data Protector 帮助》和“Data Protector 故障诊断”一节“处理 DCBF 部分中的细微 IDB 损坏”。要获得进一步协助，请与支持人员联系。

如果 Velois IDB 损坏，升级过程将中止

如果 Velois IDB 损坏，升级过程将中止。

原因

在升级期间，将检测并更正 IDB 中的以下损坏字段：

- 介质 blocks_used 设置为 99
- 介质 blocks_total 设置为 blocks_used
- 池 media_age_limit 设置为默认值（相同介质类的默认池的 media_age_limit ）
- 池 media_overwrite_limit 设置为默认值（相同介质类的默认池的 media_overwrite_limit ）

如果 IDB 中的以下任何字段损坏，升级将会中止。

介质： LAST_SEGMENT

位置：

SEQUENCE_NR

START_SEGMENT

START_OFFSET

LOG_LEVEL

DCBF_OFFSET

DCBF_NUMOFDIRS

DCBF_NUMOFITEMS

DCBF_SIZE

解决方案

将 Data Protector 安装还原到旧版本：

1. 删除当前版本的 Data Protector。
2. 重新安装以前版本的 Data Protector。
3. 还原旧的 IDB。

尝试安装其他升级时，需要修复旧的 IDB。要获得进一步协助，请与支持人员联系。

IDB 和配置文件在升级后不可用

从以前的发布版本升级 Cell Manager 后，IDB 和所有配置文件不可用。

原因

如果升级过程出于任何原因而中断，则会出现此问题。

解决方案

从升级前生成的备份还原 Data Protector，消除造成中断的原因，然后再次启动升级。

升级后，旧的 Data Protector 补丁没有删除

如果在 Data Protector 升级完成后运行 swlist 命令，那么旧的 Data Protector 补丁会作为已安装的程序列出。这些补丁在升级期间已从系统中删除，但是它们仍保留在 sw 数据库中。

原因

此问题特定于 HP-UX 平台。

解决方案

若要从 sw 数据库中移除旧补丁，请运行下面的命令：

swmodify -u *patch*.* *patch*

例如，要从 sw 数据库中删除补丁“ PHSS_30143 ”，则运行下面的命令：

swmodify -u PHSS_30143.* PHSS_30143

升级使用 StorageTek 库的“介质代理”客户机会导致连接问题

在使用 StorageTek 库的系统上升级 Data Protector 介质代理组件后，与库的连接会丢失，涉及该库的 Data Protector 会话可能会停止响应或异常结束。

解决方案

重启 StorageTek 库支持服务或守护程序可以解决此问题：

- *Windows 系统：*使用管理工具服务重新启动 LibAttach 服务。
- *Solaris 系统：*运行命令 /opt/omni/acs/ssi.sh stop 和 /opt/omni/acs/ssi.sh start ACSLS_hostname ，其中 *ACSLS_hostname* 是安装自动磁带盒系统库软件的系统的名称。
- *AIX 系统：*运行命令 /usr/omni/acs/ssi.sh stop 和 /usr/omni/acs/ssi.sh start ACSLS_hostname ，其中 *ACSLS_hostname* 是安装自动磁带盒系统库软件的系统的名称。

升级后会显示 DCBF 错误消息

在升级 Data Protector 后执行还原操作时，会出现 DCBF 错误消息。在 Data Protector GUI 的“还原”上下文中，当您选择某个对象并尝试浏览文件时，系统将显示以下消息：

[12:10907] Invalid format of detail catalog binary file.

由于 DCBF 文件并未损坏，因此 omnidbcheck –dc 不会报告任何错误。

原因

发生这种情况的原因是系统读取了两个不同版本的文件，从而导致版本不匹配。

解决方案

选项 1：转至“恢复会话”上下文并尝试恢复单个文件。

选项 2：导出/导入介质，此时，系统将创建 DCBF 编目。有关详细信息，请参阅《*Data Protector 帮助*》的“导入介质”和“导出介质”一节。

选项 3：编目迁移。 perl omnimigrate.pl –start_catalog_migration

完整编目迁移完成后 (没有旧编目之后)，将全局变量 SupportOldDCBF 更改为 0。

计划迁移失败或跳过

升级期间计划迁移失败或跳过。

原因

此问题的原因未知。

解决方案

如果在升级过程中计划迁移失败或跳过，您可以手动运行以下命令，以便将现有计划成功迁移到新的计划程序：

```
omnidbutil -migrate_schedules
```

用户迁移失败或跳过

升级期间用户迁移失败或跳过

原因

此问题的原因未知。

解决方案

如果在升级过程中用户迁移失败或跳过:

1. 使用命令 omnisv -status 检查 appserver 服务是否正在运行。
2. 运行以下命令以迁移现有用户:
   - Windows： <*DP_HOME*>\bin\perl.exe <*DP_HOME*>\bin\userMigrate.pl
   - Linux： /opt/omni/bin/perl /opt/omni/sbin/userMigrate.pl

从 Data Protector 9.06 升级失败

从 Data Protector 9.06 升级失败，并显示以下错误消息:

"hostname.com:/": 1 配置或取消配置脚本失败。

"hostname.com:/" 的执行阶段失败。

分析和执行出错。

原因

这是一个间歇性问题。

解决方案

用户可以忽略上述错误，因为 Data Protector 在迁移后继续正常运行。无需执行操作。

在 Windows 上升级 Data Protector 时 InstallShield 出错

在应用补丁或升级 Data Protector 时，InstallShield 向导会显示错误“错误 (- 5012：0x80070005)”。

原因

发生此错误的原因是第三方防病毒软件阻止了某些安装组件。

解决方案

请遵循以下步骤：

1. 在升级过程中暂时禁用第三方防病毒软件。
2. 成功安装/升级后启用第三方防病毒软件。

群集导入失败

在群集环境下升级会显示消息“[警告] 群集或节点的导入尚未成功完成。”。

原因

群集导入可能由于与证书相关的问题而失败。

解决方案

1. 在导入失败的节点上执行以下步骤:
    1. 将 localhost_key.enc 和 localhost_cert.pem 从 <DP share>\config\server\sscertificates\ 复制到被动节点中的 Data_Protector_program_data\Config\client\sscertificates 文件夹。
    2. 在被动节点上重新启动 INET 服务。
2. 在主动/主节点上执行以下步骤:
    1. 运行以下命令： omnicc -update_host <*node*>
    2. omnicc -import_cluster <*failedClusterName*> -server <*cellmanagerName*>.

升级后，备份会增加额外的容量

升级到 Data Protector 2018.09 或更高版本后，备份会增加额外的容量。

原因

早于发布 2018.09 的 Data Protector 备份对象位于 IDB 中。

解决方案

要避免额外的容量计算，在升级后为所有现有备份规范执行备份。

升级过程由“外部应用程序保留的 Data Protector 资源 JRE\lib\font 文件夹”消息中止

这是 Microsoft 的已知问题。

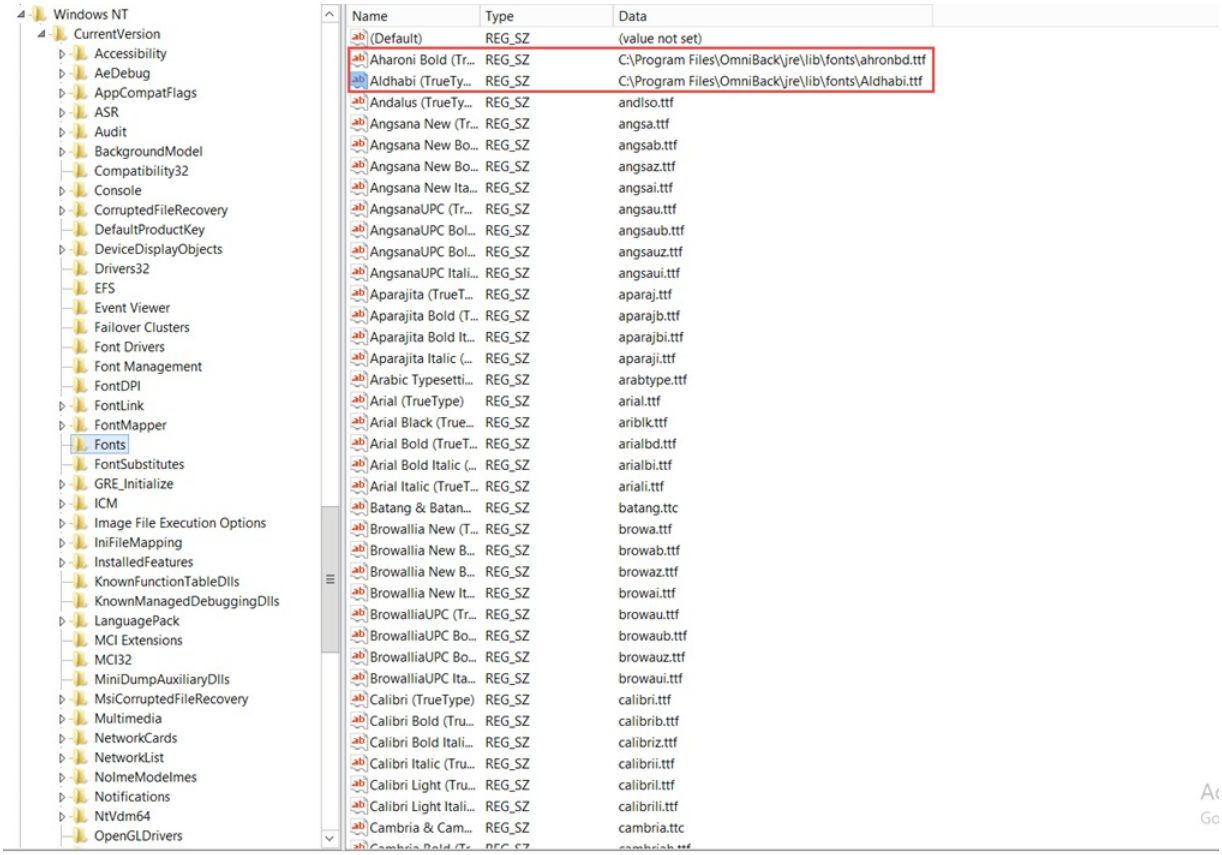
原因

这是由于安全升级 MS14-045 引起的。有关此问题的详细信息，请参阅 https://support.microsoft.com/en-us/help/2982791/ms14-045-description-of-the-security-update-for-kernel-mode-drivers-au。

解决方案

要解决此问题，请按照下列步骤操作：

1. 在 Windows 系统上，单击“开始”>“运行”。
2. 在“打开”框中输入“regedit”，然后单击“确定”。此时显示注册表编辑器窗口。
3. 进行任何更改之前，请备份注册表。
4. 在注册表中找到并选择以下子项：**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Fonts**
5. 在“Fonts 注册表”子项下找到其数据字段符合以下条件的所有注册表值：
   - 包含 Data Protector 文件夹的完整文件路径以及字体名称。例如： C:\ProgramFiles\Omniback\lib\jre\fonts\
   - 完整文件路径以 **.otf** 或 **.ttf** 扩展名结尾。



6. 删除与 Data Protector <*DP_HOME*>\JRE\lib\fonts 文件夹关联的所有字体项。
7. 重新启动系统。

群集升级后，辅助节点对象的备份失败

从 Data Protector 10.x 升级到 Data Protector 10.x 后，辅助节点的对象备份失败，并显示以下错误消息：

[警告] 来自：BSM@<Cell Manager> "<备份规范>" 时间: <时间戳> 尝试建立连接时，发生安全通信协议协商错误。 检查证书及其配置的有效性。

解决方案

要解决此问题，请在群集的两个节点上执行以下命令：

1. /opt/omni/bin/omnicc -secure_comm -remove_peer <Active node Hostname>
2. /opt/omni/bin/omnicc -secure_comm -remove_peer <Passive node Hostname>
3. /opt/omni/bin/omnicc -secure_comm -remove_peer <Cluster Virtual Hostname>

升级后，最新报告不可用

升级到最新版本的 Data Protector 后，该版本中引入的新报告不可用。

原因

仅在完成同步后，升级后才能使用新报告。

解决方案

要查看新报告，请在升级后执行手动同步，或等待下一个同步周期完成。

IDB 的当前状态不一致

由于 IDB 中的某些字段已损坏，Data Protector 无法连接到数据库。

原因

IDB 中的某些字段已损坏。

解决方案

有关解决此问题的信息，请参阅内部数据库故障排除主题。

无法启动 Data Protector、IDB 或应用程序服务器服务

Data Protector 无法启动服务。

原因

如果在开始升级之前所有 Data Protector 服务都未运行，则会发生此问题。

解决方案

在升级 Data Protector 之前手动运行 `omnisv start` 命令。

如果仍然无法启动服务，请参阅服务和后台程序故障排除，以获取有关启动 Data Protector 服务和后台程序的信息。

无法升级 Inet 配置数据库中的用户

用户的 Inet 配置在升级过程中失败，并显示以下错误消息：

> [警告] 无法升级 Inet 配置数据库中的用户。使用 omniinetpasswd 命令可以手动添加或修改用户。

原因

此问题的原因未知。

解决方案

对配置失败的每个用户手动运行以下命令：

```
omniinetpasswd -modify <username> <password>
```

只有拥有管理员权限，才能运行 omniinetpasswd 命令。

Windows 系统上客户端的推送升级失败

客户机的推送升级失败，并出现以下错误消息:

```
[严重] <主机名> [70:32] 安装工具包的数字签名验证失败。 [严重] <主机名> [110:1026] 断开与客户机 <主机名> 的连接： [5] 访问被拒绝。
```

原因

在 Windows Server 2008 R2 系统上，会发生此问题。

解决方案

要解决此问题，请执行以下步骤:

1. 手动将证书从 Cell Manager 系统 *<programdata>*\omniback\newconfig\client\certificates 文件夹复制到客户机系统中的临时文件夹。例如： C:\TempCert
2. 在客户机系统中运行以下命令:
   - C:\Windows\SysWOW64\certutil.exe –addstore root *<Path_of_Entrust.cer>* .例如： C:\Windows\SysWOW64\certutil.exe –addstore root C:\TempCert\Entrust.cer .
   - C:\Windows\SysWOW64\certutil.exe –addstore root *<Path_of_UserTrust.cer>* .例如： C:\Windows\SysWOW64\certutil.exe –addstore root C:\TempCert\UserTrust.cer .
   - C:\Windows\SysWOW64\certutil.exe –addstore CA *<Path_of_UserTrustRSA.cer>* .例如： C:\Windows\SysWOW64\certutil.exe –addstore CA C:\TempCert\UserTrustRSA.cer .
   - C:\Windows\SysWOW64\certutil.exe –addstore CA *<Path_of_SectigoRSA.cer>* .例如： C:\Windows\SysWOW64\certutil.exe –addstore CA C:\TempCert\SectigoRSA.cer .
   - C:\Windows\SysWOW64\certutil.exe –addstore CA *<Path_of_MicroFocus.cer>* .例如： C:\Windows\SysWOW64\certutil.exe –addstore CA C:\TempCert\MicroFocus.cer .
3. 安装以下 Windows 修补程序：
   - KB4474419
   - KB4493730
4. 在客户机系统上将环境变量 DP_SKIPSIGN_VERIFICATION 值设置为 1。
5. 重新启动 INET 服务，然后重试客户机的安装。

升级后不显示许可证

从 Data Protector 9.x 或更早版本升级到 Data Protector 10.00 或更高版本时，Data Protector UI 中不显示许可证。

原因

在 Data Protector 9.x 及更早版本中获得的许可证密钥和密码与 Data Protector 10.0 及更高版本不兼容。

解决方案

如果要升级到 Data Protector 10.00 或更高版本，请获取新许可证。

启动安装过程时出错

当使用 Data Protector 远程安装功能升级 Windows 客户机时，您收到以下错误：

Error starting setup process, err=[1326] Logon failure: unknown user name or bad password.

原因

远程计算机上的 Data Protector Inet 服务在运行时所用的用户帐户无权访问安装服务器计算机上的 OmniBack 共享。该帐户极有可能是本地用户。

解决方案

将 Data Protector Inet 服务的用户更改为可访问 Data Protector 共享的用户。

Data Protector 单元请求服务器 (CRS) 在升级后无法启动

手动启动 CRS 时，显示以下错误消息:

Windows could not start the Data Protector CRS on Local Computer.

有关详细信息，请查看系统事件日志。对于非 Microsoft 服务，请与服务供应商联系，并参阅特定于服务的错误代码 1007。

安装后显示以下错误消息:

Timeout reached before Data Protector CRS started.

原因

如果 Data Protector 服务在升级过程中仍在运行，则会发生此问题。

解决方案

请遵循以下步骤：

1. 使用 omnisvstop 命令停止 Data Protector 服务。
2. 打开任务管理器并结束剩余的 Data Protector 进程。
3. 使用 omnisvstart 命令启动 Data Protector 服务。

对报告服务器进行故障诊断

本节包含的信息特定于报告服务器的相关问题:

导入报告服务器失败

将报告服务器导入 Cell Manager 失败。

原因

发生此问题的原因如下:

- hosts 文件中的条目不正确。
- 无法从 Cell Manager 获取 IDB 密码。

解决方案

执行以下某项或所有操作:

- 验证在 Cell Manager 和报告服务器上 hosts 文件是否包含格式为 <计算机>.<公司>.com 的完全限定域名 (FQDN)。hosts 文件位于以下路径下:
  - Windows： \%SystemRoot%\system32\drivers\etc\
  - Linux： /etc/hosts
- 检查用户名、密码、端口号或主机名信息是否正确。如果不正确，请指定正确的用户名、密码、端口号或主机名。
- 检查 Cell Manager 上 C:\ProgramData\OmniBack\log\AppServer\ (Windows) 或 /var/opt/omni/log/AppServer/ (Linux) 中的 **DPServer.log** 文件是否存在以下错误消息:
  Unable to get IDB password from Cell Manager. Restart the CRS service and then import the Reporting Server.
  若要解决此问题，请在 Cell Manager 上重新启动 CRS 服务。

安装报告服务器失败，并出现复合回滚错误

安装报告服务器失败，并显示 Composite Rollback operation occurred while deploying the Reporting.war file错误。

原因

如果在安装过程中指定的端口号正在被使用，则会发生此问题。

解决方案

验证安装期间指定的端口号是否正在使用中。如果是，请卸载报告服务器，重新启动系统，然后使用其他端口重新安装。

无法查看或打开以 PNG 格式保存的报告

如果在 Windows 平台上将报告以 .png 图像格式保存和查看，系统会提示您安装 Windows Desktop Experience。

原因

如果未设置查看 .png 图像的默认程序，则会发生此问题。

解决方案

要查看 .png 图像，请执行以下操作之一:

- 关联用于查看 .png 图像的默认程序。
- 安装 Windows Desktop Experience。

当报告服务器和 Cell Manager 中的时间不同步时显示未经授权的访问错误

如果报告服务器和 Cell Manager 中的时间不同步，则会显示未经授权的访问错误消息。

原因

如果报告服务器和 Cell Manager 的时间不同步，则无法使用服务器，因为这两个服务器均依赖于 Cell Manager 发送的授权令牌密码和密码到期时间的验证。如果二者的时间不同步，则授权检查将失败，并显示未经授权的访问错误消息。

解决方案

确保报告服务器和 Cell Manager 中的时间同步，而不考虑其时区。

升级到 Data Protector 10.20 之后，未在 Cell Manager 中重新导入报告服务器

当 Data Protector 从早期版本升级到 Data Protector 10.20 后，不会导入报告服务器。

原因

此问题的原因未知。

解决方案

将报告服务器导入 Cell Manager 并验证密码。

导入期间，在“报告服务器信息”对话框中输入所有要求的详细信息之后，单击“验证”。如果所提供的密码不符合报告服务器的密码策略，则将密码重置为符合以下条件:

- 密码必须包含 8-20 个字符
- 密码应该包含至少一个大写字母
- 密码应该至少包含以下特殊字符之一: 星号 (*)、句点 (.)、连字符 (-) 或下划线 (_)
- 密码应该包含至少一个数值
- 密码不应包含空格。

升级到最新 DP 版本后，将取消注册 DP 2019.02 上配置的报告服务器

在报告服务器和 Cell Manager 升级到最新 DP 版本之后，将取消注册在 DP 2019.02 上配置的报告服务器。

原因

DP 2019.02 支持在 **<Any>/*** 域或组下添加用户，但在更高的 DP 版本中不支持。此外，DP 2019.08 和更高版本中的报告服务器使用有效的域或组名称与 Cell Manager 进行通信。

因此，从 DP 2019.02 升级后，Cell Manager 中添加了域名为 <Any>/* 的报告服务器用户，从报告服务器到 Cell Manager 的通信中断。

解决方案

升级到最新 DP 版本后，请按照下列步骤操作:

1. 转到“用户”上下文。
2. 在 **admin** 用户下标识报告服务器用户 (报告服务器用户将“客户机系统”字段设置为报告服务器的主机名)。右键单击“报告服务器用户”，然后从上下文菜单中选择“属性”。
3. 将“域”或“组”字段修改为针对“名称”字段输入的值 (例如，如果“名称”设置为 ADMIN，则将“域或组”也设置为 ADMIN)。
4. 单击**应用**保存更改。

在 Linux 上安装报告服务器和其他选项失败

如果要在 Linux 上安装报告服务器和其他选项，将忽略 -install 选项。

例如，如果执行 omnisetup.sh -RS -install da,ma 命令，将忽略 -install 选项。

原因

此问题的原因未知。

解决方案

安装报告服务器后，通过执行 ./omnisetup.sh -install da,ma 命令安装其他选项。

配置报告服务器时 SMTP 测试失败

配置报告服务器时 SMTP 测试失败。

原因

如果电子邮件服务器配置不正确，则可能会发生此问题。

解决方案

验证电子邮件服务器配置是否正确。

Data Protector GUI 和报告服务器中的备份会话计数不匹配

即使将已删除的备份会话从 Data Protector GUI 中删除后，这些备份会话仍会在报告服务器中显示。

原因

在计划时间运行的每日清除作业会从 Data Protector 表中移除已删除的备份会话。在那时之前，已删除的备份会话仍出现在报告服务器中。

解决方案

无需执行操作。

Data Protector 上运行的日常清除作业将从 Data Protector 表中删除备份会话，还会更新报告服务器表。

报告应用程序服务器无法运行

数据库服务停止或重新启动后，报告应用程序服务器不可用。

原因

数据库服务停止或重新启动后，需要重新启动报告服务器。

解决方案

数据库停止或重新启动后，重新启动报告服务器。

报告上下文不可见

停止或重新启动报告服务器、应用程序服务和 Cell Manager 后，报告服务器不可见。

原因

主页上下文中的“日志”选项卡提供了有关此问题原因的详细信息。

解决方案

转到“主页上下文”，然后单击“报告”。如果您无法查看导入的报告服务器，请导航至“设置”，然后单击“日志”以查看错误详细信息。

在升级之后报告应用程序服务器无法运行

在成功升级之后，报告应用程序服务器不可用。

原因

升级报告服务器后，需要重新启动应用程序服务。

解决方案

在成功升级报告服务器之后重新启动应用程序服务。

报告中出现分页错误

原因

在 GUI 或 Web 浏览器中查看报告时，如果将页面缩放的值设置为小于或大于 100%，则分页不起作用。

解决方案

为避免分页错误，请将浏览器的页面缩放设置为默认值 100%。

解决集成问题

本节包含有关集成问题的信息。以下各节包含集成过程中可能会遇到的一些问题：

DB2 UDB 集成故障诊断

This feature is available in the Premium Edition

本节列出常规检查和验证，以及在使用 Data Protector DB2 集成时可能会遇到的问题:

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 检查报告的系统错误 (位于以下目录的 debug.log 和 db2.log 文件中):

  Windows 系统： Data Protector\log

  HP-UX 和 Solaris 系统： /var/opt/omni/log

  其他 UNIX 系统： /usr/omni/log

此外，如果备份或还原失败:

- 按“预览备份会话”中所述测试备份规范。
  - 如果预览的 DB2 部分失败，请参阅 DB2 文档。
  - 如果预览的 Data Protector 部分失败，请创建 DB2 备份规范以备份为空或备份到文件设备。如果备份成功，则说明问题与设备相关。
  - Data Protector 文件系统备份和还原。对文件系统备份进行故障诊断之后，重新启动 DB2 服务器并再次启动 DB2 对象的备份。
  - 使用 DB2 工具备份和还原 DB2 对象。

此外，如果还原失败:

- 确保目标 DB2 实例处于联机状态并配置为与 Data Protector 一起使用。

问题

以下是使用 Data Protector DB2 集成时可能会遇到的一些问题：

不允许联机备份

不允许联机备份，因为未激活前滚的 logretain 或 userexit ，或者数据库的备份挂起条件生效。

原因

这是因为未激活前滚的 logretain 或 userexit ，或者数据库的备份挂起条件生效。

解决方案

在配置 DB2 数据库进行前滚恢复并将 logarchmeth1 设置为“用户退出”或“供应商”之后，必须首先对数据库进行脱机备份。如果在不进行离线备份的情况下启动了联机备份，则会报告上述错误。

脱机备份失败

执行脱机备份时会话失败，并显示类似以下错误:

[Major] From: OB2BAR_DB2BAR@ DB2ClientName InstanceName Time: DateTime
DB2 returned error: SQL1035N The database is currently in use. SQLSTATE=57019

原因

该错误意味着存在一些与数据库的连接。

解决方案

执行以下命令以断开与数据库的现有连接:

- 断开所有用户的连接并中止所有现有事务:
  db2 force application all
- 断开个人用户或应用程序的连接:
  1. 获取所有应用程序的列表:
     db2 list applications
  2. 断开使用应用程序句柄号 AppNum 标识的用户的连接:
     db2 force application AppNum

您可以创建 pre-exec 脚本来执行该命令。请注意，该命令将返回操作实际完成之前的“已完成”状态。因此，通过向脚本添加 **sleep** 命令，为完成操作提供足够的时间。

不允许脱机备份表空间

脱机备份 DB2 表空间 (而非整个数据库) 时，DB2 报告不允许脱机备份。

原因

这是因为 DB2 logretain 选项未激活，或者数据库的备份挂起条件生效。

解决方案

将 DB2 logretain 选项设置为 **ON**。

未对数据库启用增量备份

在执行完整数据库备份之前启动增量备份时，Data Protector 报告以下错误。

Incremental backup is not enabled for this database.

原因

在执行完整数据库备份之前启动增量备份时，会发生此错误。

解决方案

完成以下步骤：

1. 通过运行以下命令来激活修改跟踪:
   db2 update db cfg for database_name USING TRACKMOD ON
2. 重新启动数据库。
3. 执行完整数据库备份，然后根据需要执行增量备份。

无法访问对象

当无法访问对象时，Data Protector 报告以下错误。

以下可能是一个原因 (代码编号): 1.遇到无效的对象类型。 2.锁定对象操作失败。锁定等待可能已达到数据库配置中指定的锁定超时限制。 3.在处理数据库实用程序期间，解锁对象操作失败。 4.访问对象失败。 5.数据库中的对象已损坏。 6.被访问的对象是表空间。表空间状态欠佳，不适合操作，或者表空间的某些容器不可用。（LIST TABLESPACES 列出当前表空间状态。） 7.删除对象操作失败。 8.尝试加载/静止至此分区上未定义的表中。

原因

当对象无效、锁定或损坏时，会发生此错误。

解决方案

确保对象有效且未损坏。如果锁定对象操作失败，请确保数据库配置中的锁定超时限制足够，然后重新提交 utility 命令。请考虑使用 QUIESCE 命令将数据库置于静止状态，以确保访问。

无法列出表空间

Data Protector UI 或 CLI 无法列出表空间。

原因

数据库可能处于不适当的状态，例如已暂停。

解决方案

确保满足以下条件:

- 数据库未处于备份/还原/前滚挂起状态。
- root 用户 (仅限 UNIX) 和 DB2 用户均位于 DB2 和 Data Protector admin 组中。

从对象副本还原数据会话被阻止

从对象副本还原数据会话被阻止。

原因

IDB 中的对象副本元数据未正确更新。

解决方案

重新启动还原之前，请确保以下事项:

- 增加用于还原的设备的磁盘代理缓冲区数。
- 如果备份的所有对象都记录在 IDB 中:
  - 在 Data Protector GUI 的内部数据库上下文中，搜索备份的所有对象。对象由相同的备份 ID 标识。
  - 将单独的对象复制会话中的每个对象复制到单独的设备，例如文件库。对于每个对象，请使用具有不可追加介质策略的单独介质。
  - 为新创建的副本设置最高介质位置优先级。

还原后前滚失败

从联机备份执行前滚恢复时，还原成功完成，但前滚失败。

原因

发生此问题的原因是所有存档日志均不可用。

解决方案

确保所有存档日志可用。如果并非所有存档日志都可用，请从上次备份中还原它们。如果通过将 logarchmeth1 设置为 **vendor** 来对日志进行存档，请执行以下命令，让 DB2 数据库管理器检索日志并进行应用:

```
db2 rollforward db db_name [to time | to end of logs] [and complete]
```

在 HP-UX 环境中前滚失败

从 DB2 CLI 或 Data Protector GUI 执行 DB2 前滚命令时，HP-UX 环境中的前滚失败。

在 HP-UX 环境中执行 DB2 前滚命令 db2 rollforward db <database> to end of logs and complete 或从 Data Protector GUI 触发前滚时，您可能会遇到以下错误消息:

<SQL error code> Rollforward recovery processing has stopped because of the error <SQL error no> while retrieving log file <archive log> for database <database> on the database partition <partition number> and log stream "".

解决方案

- 对于 Data Protector GUI: 从 DB2 CLI 执行 DB2 前滚。
- 对于 DB2 CLI: 重新执行相同的命令。

示例： db2 rollforward db db_name [[stop]|[to time|to end of logs] [and complete]]

DB2 还原失败

在大型数据库上，还原挂起且失败，并显示以下超时错误消息:

```
[正常] 来自: OB2BAR_DB2LIB@<Hostname> "<Instance>" 时间: <Date> <Time> 开始 OB2BAR 还原: <HostName>:<Instance>:
<Database>#0:20151211150210:0:1 "DB2" [重大] 来自: RSM@<HostName> "" 时间: <日期> <时间> [61:1002] 主机 <主机名> 上名为 "DB2" 的
OB2BAR 还原 DA 已达到 7200 秒的静止超时。 主机上的代理即将关闭。
```

原因

DB2 甚至在数据还原开始之前就开始在磁盘上创建容器。创建这些容器所需的时间可能从几小时到几天不等。结果出现超时。

解决方案

要解决此问题，请增加 SmMaIdleTimeout 和 SmDaIdleTimeout 全局变量的值。

适用于 **Microsoft Exchange** 的 **GRE** 故障诊断

This feature is available in the Premium Edition

本节列出常规检查和验证，以及在使用适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 时可能会遇到的问题。

调试

启用调试选项：

1. 要启用调试选项，请在控制台树中单击**设置**。此时将显示“粒度恢复设置”页面。
2. 选择**启用调试日志**选项。此时将激活“调试日志文件夹名称”字段。
3. 指定文件夹的新位置，然后单击**保存**。

问题

下面是在使用适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 时可能会遇到的一些问题：

搜索条件结果页面一直空白

在“粒度恢复”向导的“邮箱搜索条件”页面中，输入要搜索的字词并单击下一步之后，“搜索结果”页面中不显示任何结果，即使多个项目符合搜索条件也是如此。

解决方案

要显示搜索结果列表，请按如下方式操作：

1. 卸载恢复数据库。
2. 使用 Granular Recovery Extension GUI 的“缓存管理”页面，确定数据库已还原到的文件夹。从此文件夹中，删除名称中具有“CatalogData”字符串的子文件夹。
3. 在 Exchange Management Shell 中，运行以下命令：
   set-mailboxDatabase DatabaseName -indexenabled $false.
4. 重新装载恢复数据库。
5. 重新启动恢复，并按照“粒度恢复”向导操作。
6. 在“邮箱搜索条件”页面中，重新输入搜索关键字并单击**下一步**。

手动删除扩展创建的临时邮箱

在恢复过程中扩展创建的临时邮箱不会在该过程完成后自动删除。

原因

这可能是由于某些例外情况，例如扩展在此过程中停止工作。

解决方案

使用前缀 DP_Recovery 或 DP_SEARCH 标识此类临时邮箱并手动将其删除。

要手动删除冗余邮箱，请使用 Exchange 管理中心或 Exchange Management Shell。

在“从备份导入”向导的列表中，一些邮箱缺失

当您单击“从备份导入”向导的“邮箱选择”页面上的“高级” 并浏览用户邮箱时，即使某些邮箱在 Exchange Server 数据库的备份映像中存在，邮箱树中也会丢失这些邮箱。

原因

此类问题可能是由许多不同的原因造成的，包括 Data Protector 单元中的时间同步问题以及检索邮箱元数据时出现的 Exchange Server 问题。

解决方案

确定所需邮箱所属的邮箱数据库，然后执行以下步骤:

1. 单击“返回”以返回向导的简介页面。
2. 选择“数据库选择”。
3. 单击“下一步”，然后按照向导完成导入过程。

装载还原的数据库失败

在 Microsoft Exchange Server 环境中，装载还原的数据库可能会以出现错误而结束。

原因

当还原的数据库处于“脏-关闭状态”时，会出现此问题。要成功安装数据库，数据库必须处于“干净-关闭状态'”。

解决方案

1. 通过执行 Microsoft Exchange Server eseutil.exe 恢复命令，将还原的数据库置于“干净-关闭状态”。
   有关 eseutil.exe 实用程序的详细信息，请参阅 Microsoft Exchange Server 文档。
2. 再次尝试装载还原的数据库。

进程间通讯错误

尝试从 Granular Recovery Extension 图形用户界面 (GUI) 触发操作后，将显示以下错误消息，并且 GUI 中的所有后续用户操作均因相同的错误而失败:
The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for communication because it is in the Faulted state.

原因

当 Granular Recovery Extension GUI 保持打开的时间段超过了 Internet 信息服务 (IIS) 回收时间段时，会显示此错误。IIS 会卸载 Exchange GRE Web 服务以及其他 Web 服务，从而导致服务和 GUI 之间通信失败。

解决方案

关闭 Granular Recovery Extension GUI，然后重新启动。

Exchange GRE 恢复操作失败

即使执行 Granular Recovery Extension (GUI 或 CLI) 的用户具有足够的权限，Granular Recovery Extension 恢复或还原操作仍因权限不足而失败

原因

发生此问题的原因是本地 SYSTEM 帐户的权限不足。此帐户需要具有适当的权限，原因如下:

- Granular Recovery Extension Web 服务在本地 SYSTEM 特权下运行。
- Granular Recovery Extension Web 服务允许 Data Protector Inet 服务（默认情况下在 Windows 本地 System 用户帐户下运行）执行或启动 Data Protector Exchange 集成代理。还原会话使用相同的用户帐户执行。

解决方案

授予本地 SYSTEM 用户帐户适当的权限以还原 Microsoft Exchange Server 数据库和创建恢复数据库：

1. 关闭当前正在运行的 Exchange Granular Recovery Extension 客户机（GUI 或 CLI）。
2. 停止 Granular Recovery Extension Web 服务。
3. 为本地 SYSTEM 帐户提供适当的权限。
4. 启动 Granular Recovery Extension 并继续执行 Granular Recovery Extension 操作。
   当请求来自 GUI 或 CLI 时，Internet 信息服务 (IIS) 会自动启动 Granular Recovery Extension Web 服务。

MMC 无法初始化管理单元

打开 Granular Recovery Extension 图形用户界面 (GUI) 时，显示消息“MMC 无法初始化管理单元” ，之后长时间显示“将管理单元添加到控制台” 消息。

“缓存管理”、“状态”和“设置”节点不会加载到 GUI 的控制台树中。

原因

如果 Internet 信息服务 (IIS) 或者其关联的服务未运行，并且 Granular Recovery Extension GUI 无法与 Exchange GREWeb 服务通信，则可能会发生此问题。

解决方案

确保 IIS 及其关联的服务已启动并且正在运行：

1. 打开 Internet 信息服务 (IIS) 管理器。
2. 要显示 Exchange GRE Web 服务主页，在控制台树中的“默认网站”下查找并选择 ExchangeGre 节点。
3. (视情况而定) 如果未显示 Exchange GRE Web 服务主页:
   a. 单击“取消” 以关闭以下消息:
      Adding snap-in to console
   b. 打开服务器管理器，选择“角色”节点。在“角色摘要”下，查找并选择 WebServer (IIS)。
   c. 此时将显示 Web Server (IIS)。在“系统服务”下，确认所有服务 (包括应用程序主机帮助程序服务、IIS 管理服务和 World Wide Web 发布服务) 是否都已启动并正在运行。
   d. 重新打开 Granular Recovery Extension GUI。
4. 右键单击 ExchangeGre 节点，单击“管理应用程序” ，然后单击“浏览” 。

管理单元将添加到 MMC。“缓存管理”、“状态”和“设置”节点显示在 GUI 中，系统不再显示该消息。

帮助不显示产品版本

当单击“帮助” 菜单，然后单击“关于适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension”时，不显示产品版本。

原因

发生此问题的原因是 Microsoft 管理控制台 (MMC) 中的一个已知问题。 升级后，由于 MUI 缓存中的字符串缓存机制，注册表不会自动更新。 MUI 缓存不会清除，产品版本不会显示在 MMC 管理单元中。

解决方案

要手动删除 MUI 缓存中的字符串并重新安装管理单元，请执行以下操作：

1. 运行 REGEDIT 命令以启动注册表编辑器。
2. 在注册表编辑器中，查找以下层次结构之一（如果它们存在）：
   HKEY_USERS\S-1-5-21-61196776-1057610366-2591919248-500_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
   HKEY_USERS\S-1-5-21-2765349584-3720068851-1520285658-500_Classes\Local Settings\MuiCache\96\52C64B7E
3. 删除适用于 Microsoft Exchange Server 的 Granular Recovery Extension 的以下注册表项：
   @C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin\GreSnapInResource.dll,-114
   @C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin\GreSnapInResource.dll,-115
   @C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin\GreSnapInResource.dll,-116
   @C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin\GreSnapInResource.dll,-117
4. 关闭注册表编辑器。
5. 运行以下命令：
   %windir%\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe "C:\Program Files\Hewlett-Packard\Exchange Granular Recovery Extension\bin\ExchangeGre.MmcGui.dll" /install
6. 单击“帮助” 菜单，然后再次单击“关于适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension”，此时将显示产品内部版本号。

无法删除邮箱还原请求

恢复项目不能从 Exchange Management Shell 自动删除。在 Exchange 2013 SP1 环境中，Exchange GRE 有时无法通过对目标邮箱使用 Remove-MailboxRestoreRequest 命令来删除邮箱还原请求 (使用 New-MailboxRestoreRequest 命令启动)，即使在邮箱还原请求处于已完成状态之后。

原因

发生此问题的原因是 Exchange 服务器无法从队列中删除已完成的请求。您不能对同一目标邮箱启动其他恢复操作，因为尚未删除或清除此先前的邮箱还原请求。

解决方案

完成以下步骤：

1. 确保不存在任何活动或运行中的 Exchange GRE 操作。
2. 通过在 Exchange Management shell 中执行以下命令来手动清理邮箱的已完成的“还原请求”，然后重试操作:
   Get-MailboxRestoreRequest -Status Completed | Remove-MailboxRestoreRequest

PowerShell 命令失败

ExchangeGRE 恢复过程将创建新的临时邮箱并将用户添加到 Active Directory (AD)。 在某些环境中，由于 AD 替换速度慢，PowerShell 命令失败。

原因

发生此问题的原因是 AD 替换速度慢。因此，PowerShell 命令必须重复几次，直到 AD sync 完成并且新用户可用为止。另外，在某些复杂域环境的情况下，最好让 Exchange 服务器决定应该在何处创建新用户，而不是使用默认情况下在 ExchangeGRE PowerShell 命令中设置的 DomainController 参数。

解决方案

- 要增加 PowerShell 命令重复的次数，请找到以下键并创建一个名为 cmdletTimeOut 的、值为 100 的新 StringValue 变量:
  HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Plugins\exchgre
- 要从 ExchangeGRE PowerShell 命令中删除默认的 DomainController 参数，请找到以下键并创建一个名为 skipDCParam 的、值为 1 的新 StringValue 变量:
  HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Plugins\exchgre

适用于 Microsoft SharePoint Server 的 GRE 故障诊断

This feature is available in the Premium Edition

本节列出常规检查和验证，以及在使用适用于 Microsoft SharePoint 的 Data Protector Granular Recovery Extension 时可能会遇到的问题。

含调试条目和日志的文件夹位于以下文件夹中：

Microsoft SharePoint Server 2010 :

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS\GranularRecovery

Microsoft SharePoint Server 2013 :

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\LOGS\GranularRecovery

此文件夹包含文件 debugs.txt 、 debugs_cliproxy.txt 、 note.txt 和 note_cliproxy.txt 。根据安装 Microsoft SharePoint Server 的位置，该文件夹位置可能有所不同。

在安装期间，将在 Data_Protector_program_data\tmp\shp_gre_setup.txt 文件中创建安装调试日志。

问题

以下是在使用适用于 Microsoft SharePoint 的 Data Protector Granular Recovery Extension 时可能会遇到的一些问题：

恢复对象 GUID 已属于其他某个对象

对象恢复期间，发生以下错误：Recovery Object GUID already belongs to some other object

原因

当备份的原始对象和恢复的对象具有相同的 GUID 时，会发生此错误。

解决方案

删除原始对象，然后重试恢复。

超过了收回作业完成的最大超时

收回 SharePoint GRE MOSS_GRE 解决方案时出现以下警告消息:

[WARNING] Maximum timeout for retraction job completion exceeded! Continue monitoring of solution deployment status at Central Administration.

原因

如果收回作业超出时间限制，则会显示此警告消息。如果先前触发的服务或配置未按预期运行，则可能导致延迟。

解决方案

在“解决方案管理”下验证收回状态。

1. 导航到:
   “中央管理员**”>>“**系统设置**”>>“**管理场解决方案**”**。
2. 重新运行卸载过程。

超过了部署作业完成的最大超时

将 SharePoint GRE MOSS_GRE 解决方案部署给中央管理员时，出现以下警告消息:

[WARNING] Maximum timeout for deployment job completion exceeded! Continue monitoring of solution deployment status at Central Administration.

原因

如果部署作业超出时间限制，则会出现此警告消息。如果先前触发的服务或配置未按预期运行，则可能导致延迟。

解决方案

在“解决方案管理”下验证部署状态。
导航到:
“中央管理员**”>>“**系统设置**”>>“**管理场解决方案**”**。
部署成功后，运行 custom_brand.ps1 将所有与 GRE 相关的品牌设置都设置为客户机。

用户 'NT AUTHORITY\SYSTEM' 不是场系统帐户

SharePoint GRE 安装期间发生以下错误:

User 'NT AUTHORITY\SYSTEM' is not a farm user account.

原因

如果在安装 SharePoint GRE 并将其推送到客户机系统时未使用场用户帐户，则会发生此错误。

解决方案

确保您使用场用户帐户来运行安装过程。要使用场凭据进行配置，请在“客户机” 上下文中右键单击虚拟机，然后选择“添加组件” 。选择要添加的组件，然后单击“配置” 以使用场凭据进行推送。

场配置操作失败

Microsoft SharePoint Server 2019 场还原会话结束，并显示以下错误:

'Farm configuration: SharePoint_Config': operation failed 'delete file system cache'. Error: [145] The directory is not empty

原因

此错误是由以下原因之一导致的:

- 前端服务器上文件系统缓存的内容比配置数据库的内容新。
- 本地服务器上的文件系统缓存正在使用中。

解决方案

执行以下操作之一：

- 通过运行 **SharePoint Management Shell** 中的以下命令来删除分布式缓存服务实例：
  “Remove-SPDistributedCacheServiceInstance”
- 停止 SharePoint Timer 服务，然后重新启动还原。
- 请按照以下文章中提供的步骤刷新前端服务器上的缓存:
  http://support.microsoft.com/kb/939308

GRE 导入作业期间出现警告符号

在 GRE 导入作业期间，“开始恢复缓存内容源爬网” 步骤会出现警告符号。

原因

恢复期间出现警告有多种原因。这些警告基于恢复时的网站集状态。

例如，如果出现另一个具有相同名称的站点已存在、站点创建过程中的端口重复等情况，则会出现警告符号。

仅在出现致命错误时，恢复执行才会发出错误。

解决方案

有关导入恢复内容时的警告和错误的详细信息，请参考 debug.logs 。

调试日志路径:

C:\Program Files\Common Files\microsoft shared\Web Server Extensions\<version>\LOGS\GranularRecovery

成功恢复会话后，子站点不链接到主页

在 Microsoft SharePoint Server 2019 上成功进行恢复会话后，子站点不链接到主页。

原因

此错误的原因未知。

解决方案

您可以在主站点的站点内容页面上的子站点部分下访问子站点。

安装过程中报告“无完全读取权限”警告

安装 MS SharePoint Granular Recovery Extension 组件时，Data Protector 报告以下警告：

Windows SharePoint Services Search service has no full read permissions for all content databases.

原因

此警告消息不是必需的，您可以忽略它。

解决方案

执行以下步骤以防止再次出现此警告消息:

1. 打开 SQL Server Management Studio。
2. 在“安全”下，展开“登录”。
3. 右键单击 Windows SharePoint Services 搜索服务运行所使用的用户帐户，然后单击“属性”。
4. 在“属性 (Properties)”对话框中，单击**用户映射 (User Mapping)**。选择所有内容数据库，并将以下两个数据库角色分配给用户：
   - db_owner
   - WSS_Content_Application_Pools
5. 单击**确定 (OK)** 应用更改。

SharePoint GRE Web 插件不反映 SharePoint Server 上的品牌自定义

在安装或升级 SharePoint GRE 组件期间，SharePoint 管理中心 Web 控制台的 Web 插件将品牌名称显示为**BC_FULL_PRODUCT_NAME Granular Recovery Extension**。即使升级完成后，此名称也可能会继续显示。

原因

如果在 SharePoint 客户机升级期间 SharePoint 服务器管理中心 Web 控制台保持打开状态，则会发生此问题。SharePoint 使用缓存内存来呈现 Web 内容，这可能会干扰其品牌自定义。

解决方案

要解决此问题，请刷新 SharePoint 管理中心网页。如果即使在刷新 SharePoint 管理中心网页后问题仍然存在，请执行以下操作:

1. 使用管理员权限打开 SharePoint Management Shell 控制台并运行以下命令:
   iisreset /noforce
2. 刷新 SharePoint 网页。

MS SharePoint GRE 组件的远程安装失败

远程安装 MS SharePoint Granular Recovery Extension 组件时，会话失败，并显示诸如以下错误:

[Critical] ClientName Post-installation script for the MS SharePoint Granular Recovery Extension failed with the output: CreateProcessWithLogonW failed, trying LogonUser/CreateProcessAsUser, GetLastError(): 1326 LogonUser failed, GetLastError(): 1326

原因

这是因为 Data Protector 尝试连接到 Microsoft SharePoint Server 系统时使用的用户帐户没有分配 “允许本地登录”策略。

解决方案

确保为 Data Protector 尝试连接到 Microsoft SharePoint Server 系统时使用的用户帐户 (例如场管理员) 分配了 “允许本地登录”策略。

要将策略分配给用户，请执行以下操作:

1. 在 Microsoft SharePoint Server 系统上，打开**管理工具 (Administrative Tools)**，然后打开**本地安全策略 (Local Security Policy)**。
2. 在“安全设置 (Security Settings)”下，展开**本地策略 (Local Policies)**，然后单击**用户权限分配 (User Rights Assignment)**。
3. 右键单击“允许本地登录”策略。
4. 单击“属性”并添加用户。
5. 单击**确定 (OK)** 应用更改。

由于用户权限不足，导入作业失败

执行“从备份导入”之后，“Granular Recovery 导入作业状态”页面将报告“还原”阶段为失败状态。

原因

这是因为没有为运行 Windows SharePoint Services 计时器服务所使用的用户帐户分配足够的权限。

解决方案

确保运行 Windows SharePoint Services 计时器服务所使用的用户帐户已分配有 Data Protector“启动还原” 和“查看私有对象” 的用户权限。例如，如果 Windows SharePoint Services 计时器服务使用 “网络服务”户运行，请执行以下操作:

1. 启动 Data Protector GUI (**Data Protector Manager**)。
2. 在“上下文”列表中，选择**用户**。
3. 右键单击已启用“启动还原” 和“查看私有对象” 用户权限的用户组。
4. 单击“添加/删除用户”，确保“网络服务” 用户帐户已配置以下属性:
   - 名称**:** Network Service
   - 域/组： NT Authority
   - 客户端系统： Any

由于磁盘空间不足，导入作业失败

执行“从备份导入”之后，“粒度恢复导入作业状态”页面将报告“可用空间不足” ，“详细信息” 列将显示“正在检查磁盘空间” 。

原因

当由于无法访问 Internet 而使 Data Protector Granular Recovery Extension 签名验证花费很长时间才能完成时，就会发生此问题。

解决方案

请执行以下操作：

- 确保拥有 Internet 访问权限。
- 禁用签名验证：
  1. 在 Microsoft SharePoint Server BIN 文件夹中查找 cliproxy.exe 和 HP.Sharepoint.GranularRecovery.CLI.exe 文件。 BIN 文件夹的默认位置:
     对于 Microsoft SharePoint Server 2010: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14
     对于 Microsoft SharePoint Server 2013: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15
  2. 在 BIN 文件夹中，创建包含以下内容的配置文件 cliproxy.exe.config 和 HP.Sharepoint.GranularRecovery.CLI.exe.config：

```
<?xml version="1.0" encoding="utf-8" ?><configuration> <runtime> <generatePublisherEvidence enabled="false"/> </runtime>
</configuration>
```

恢复会话失败

如果通过连接原始网站来启动恢复会话，则显示以下消息：

No recovery available for this site http://computer:25884/sites/User! Please contact Granular Recovery Administrator for further info!

原因

问题的根本原因在于缓存中没有内容数据库。

解决方案

执行导入作业。

无法从“我的网站”访问“粒度恢复缓存管理”链接 - 管理场功能

创建新网站集或新 Web 应用程序并备份新网站集之后，无法从“我的网站”访问“粒度恢复缓存管理”链接 (在 Microsoft SharePoint Server 2010 中，选择“网站操作”>“网站设置”>“粒度恢复”；或在 Microsoft SharePoint Server 2013 中，选择“设置”图标 >“网站设置”>“粒度恢复”)。将显示以下消息：

GR resource files are missing in site's "App_GlobalResources" folder.

解决方案

完成以下步骤：

1. 按照如下所述打开**管理中心**：
   Microsoft SharePoint Server 2010/2013：
   在“系统设置”下，选择**管理场功能**。
2. 单击 Data Protector Granular Recovery Extension 旁的“停用”。此时将显示“警告”页面，单击**停用此功能**链接。返回“管理场功能 (Manage Farm Features)”。单击 Data Protector Granular Recovery Extension 旁的“激活”。

无法从“我的网站”访问“粒度恢复缓存管理”链接 - 读取权限

创建新网站集或新 Web 应用程序并备份新网站集之后，无法从“我的网站”访问“粒度恢复缓存管理”链接 (在 Microsoft SharePoint Server 2010 中，选择“网站操作”>“网站设置”>“粒度恢复”；或在 Microsoft SharePoint Server 2013 中，选择“设置”图标 >“网站设置”>“粒度恢复”)。将显示消息“访问被拒绝。”。此时将显示以下调试条目：

[6 - Fatal] FATAL debugs - Recovery.aspx: OnPreInit: - Exception: Thread was being aborted.

解决方案

表单中各 Web 应用程序的应用程序池用户必须授予对“恢复 Web 应用程序”的读取权限。向应用程序池用户帐户授予读取权限：

1. 连接到 Microsoft SharePoint Server 管理中心系统，如下所示：
   Microsoft SharePoint Server 2010/2013：
   在“应用程序管理”下，选择“管理 Web 应用程序”，选择“恢复 Web 应用程序”，然后单击“用户策略”，此时将显示“Web 应用程序的策略”页。
2. 如果某一用户在“Web 应用程序的策略”中不存在，请单击**添加用户**。在“添加用户”页面中，选择**所有区域**，然后单击**下一步**。输入应用程序池用户，选择**完全读取 - 具有完全的只读访问权限**，然后单击**完成**。

如果用户存在于“Web 应用程序的策略”中，请选择用户并单击**编辑所选用户的权限**。在“编辑用户”页面中，选择**完全读取 - 具有完全的只读访问权限**，然后单击**保存**。

Data Protector Granular Recovery Extension 在新创建的 Web 应用程序中不可用

向已安装 Data Protector Granular Recovery Extension 的场添加新的 Web 应用程序或新的前端 Web 服务器后，网站集管理员在访问 Granular Recovery Extension 用户界面时可能会出现问题。

原因

发生此问题的原因是新创建的 Web 应用程序上的 Data Protector Granular Recovery Extension 不可用。

解决方案

停用 Data Protector Granular Recovery Extension 并再次将其重新激活:

1. 在服务器上打开“Microsoft SharePoint 管理中心”。
2. 转到“系统设置” >“管理场功能” 。
3. 单击 Data Protector Granular Recovery Extension 功能前面的“停用”。
4. 此时将显示“警告”页面，单击“停用此功能”链接。
5. 返回到“管理场功能”，并单击 Data Protector Granular Recovery Extension 功能前面的“激活”。

从备份或文件系统导入失败

从备份或文件系统导入失败，并显示以下错误:
Checking disk space — Unknown error occurred.

原因

如果场内的一个或多个系统未满足 Microsoft SQL 先决条件，则可能发生此错误。

解决方案

确保场中的每个系统安装了所有 Microsoft SQL 先决条件。如果在系统上安装任何缺少的软件包，则必须在系统上重新启动 SharePoint Timer 服务和 IIS。

无法更改默认恢复设置

开始恢复过程后，无法更改默认恢复设置，例如恢复位置。

原因

发生此问题的原因是浏览器中启用了弹出窗口阻止程序。对于包含默认配置的恢复设置的弹出窗口，弹出窗口阻止程序将进行阻止。

解决方案

禁用浏览器中的所有弹出窗口屏蔽软件。

当项目的大小超过最大允许长度时，恢复失败

恢复项目失败，并显示错误消息“发生未知错误，请联系管理员”，并且在 debug.log 文件中记录以下信息:
"System.ServiceModel.FaultException: There was an exception running the extensions specified in the config file. ---> Maximum request length exceeded."

原因

当恢复项目的大小超出了请求主体允许的最大内容长度时，会发生此情况。

解决方案

在每个远程场的 Web 前端 (WFE) 上，导航到 %ProgramFiles%\Common Files\Microsoft Shared\web server extensions\15\TEMPLATE\LAYOUTS\web.config 文件并通过添加以下代码来增加允许的最大内容长度:

```
<location path="GranularRecovery/RemoteFarm.asmx"> <system.web> <!-- maxRequestLength is in kilobytes (KB) --> <httpRuntime maxRequestLength="102400"/> </system.web> <system.webServer> <security> <requestFiltering> <!-- maxAllowedContentLength is in bytes (B) --> <requestLimits maxAllowedContentLength="104857600"/> </requestFiltering> </security> </system.webServer> </location>
```

上述代码举例说明了如何将限制设置为 100 MB。如果您希望恢复大于 100 MB 的文件，则必须在代码中相应地设置值。

命令行界面响应缓慢

您可注意到 Data Protector Granular Recovery Extension 命令行接口的响应缓慢。例如，当运行 HP.Sharepoint.GranularRecovery.CLI.exe --help 命令时，该命令需要 10 秒到几分钟时间才能显示用法。

原因

问题的根本原因是 Data Protector Granular Recovery Extension 签名验证可能需要很长一段时间才能完成。

解决方案

要禁用 Data Protector Granular Recovery Extension 签名验证，请执行以下步骤：

1. 在 Microsoft SharePoint Server BIN 文件夹中查找 cliproxy.exe 和 HP.Sharepoint.GranularRecovery.CLI.exe 文件。默认情况下，BIN 文件夹的路径为:
   Microsoft SharePoint Server 2010：
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN
   Microsoft SharePoint Server 2013：
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN
2. 在 BIN 文件夹中，创建包含以下内容的配置文件 cliproxy.exe.config 和 HP.Sharepoint.GranularRecovery.CLI.exe.config：

```
<?xml version="1.0" encoding="utf-8" ?><configuration><runtime><generatePublisherEvidence enabled="false"/></runtime>
</configuration>
```

图形用户界面响应缓慢

您可注意到 Data Protector Granular Recovery Extension GUI 的响应缓慢。例如，从备份或从文件系统导入内容数据库时。导入作业可能会因超时而失败。

原因

问题的根本原因是 Data Protector Granular Recovery Extension 签名验证可能需要很长时间才能完成。

解决方案

要禁用 Data Protector Granular Recovery Extension 签名验证，请执行以下步骤。

1. 在 Microsoft SharePoint Server BIN 文件夹中查找 cliproxy.exe 和 HP.Sharepoint.GranularRecovery.CLI.exe 文件。默认情况下，BIN 文件夹的路径为:
   Microsoft SharePoint Server 2010：
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN
   Microsoft SharePoint Server 2013：
   C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN
2. 在 BIN 文件夹中，创建包含以下内容的配置文件 cliproxy.exe.config 和 HP.Sharepoint.GranularRecovery.CLI.exe.config：

```
<?xml version="1.0" encoding="utf-8" ?><configuration> <runtime> <generatePublisherEvidence enabled="false"/> </runtime>
</configuration>
```

Data Protector 服务未运行

从文件系统会话中执行导入时，显示以下消息：Required Data Protector service is not running!

原因

这是因为必需的 Data Protector 服务未运行。

解决方案

完成以下步骤：

1. 打开控制面板，双击**管理工具**，然后双击**服务**。
   查找 Data Protector 服务，右键单击已禁用的服务，然后单击**启动**以启用该服务。
2. 在“备份版本选择”页面上，单击**返回**完成会话。

“还原 - 装载请求挂起”状态

执行从备份导入会话时，“粒度恢复导入作业状态”页面上会显示**还原 - 装载请求挂起**状态。

解决方案

1. 启动 Data Protector GUI (Data Protector Manager)。
2. 在“监视”上下文中检查是否有任何装载请求。确认装载请求，然后重新启动备份会话。
3. 备份会话完成后，再次执行“从备份导入”会话。

子文件夹不会恢复到原始位置

在恢复包含子文件夹的文件夹时，将恢复父文件夹，但不恢复子文件夹。

原因

在您删除文件夹后，Microsoft SharePoint Server 会将此文件夹置于网站集回收站中。

解决方案

要使用 Granular Recovery Extension 将您的文件夹及其子文件夹恢复到原始位置，请执行以下步骤:

1. 在“网站集回收站”中，选择该文件夹，然后单击“删除所选项目”。
2. 再次执行文件夹的恢复会话。

Granular Recovery Extension 组件安装失败

安装已启用 Data Protector Granular Recovery Extension 组件的 Data Protector 失败。

解决方案

要手动安装 Data Protector Granular Recovery Extension，而不使用标准 Data Protector 安装过程，请执行以下操作:

1. 使用 Microsoft SharePoint Server **场管理员**用户帐户登录到 Microsoft SharePoint Server 管理中心系统。
2. 在“开始”菜单中，右键单击**命令提示符**，并选择**以管理员身份运行**。
3. 将当前目录更改为在产品安装过程期间从中提取自提取存档中文件的 Data_Protector_home\bin 目录。
4. 运行 grm_install.bat 安装 Data Protector Granular Recovery Extension 解决方案。

Granular Recovery Extension 删除失败

卸载 Data Protector 之后，不会将 Data Protector Granular Recovery Extension 从系统中删除。

原因

原因未知。

解决方案

要手动删除 Data Protector Granular Recovery Extension，而不使用标准 Data Protector 删除过程，请执行以下操作:

1. 使用 SharePoint 系统帐户启动 SharePoint Management Shell。
2. 从 Data_Protector_home\bin 目录中运行:
   grm_check.ps1

在 SharePoint 管理中心上具有多个服务器的服务器场中，GRE 的安装意外结束

在包含 SharePoint 管理中心的多个服务器的场上，安装 Data Protector Granular Recovery Extension 可能意外停止。

原因

发生此问题的原因是在 SharePoint 管理中心上禁用了 Microsoft SharePoint Foundation Web Application 服务。

解决方案

在 Microsoft SharePoint 管理中心上启用 Microsoft SharePoint Foundation Web Application 服务。

适用于 VMware 的 GRE 故障诊断

本主题列出常规检查和验证，以及在使用适用于 VMware vSphere 的 Data Protector Granular Recovery Extension 时可能会遇到的问题。

问题

下面是您可能会遇到的一些问题：

找不到分区

浏览具有 VMware GRE 用户快照的 Windows 装载代理 VM 时出现以下消息:

```
Partition not found
```

从 Data Protector 2020.08 版开始，会出现此错误。

原因

在以下情况下可能会发生此错误:

- 磁盘配置低
- 启用了 CBT
- 分区表为 GPT，并且
- 存在用户快照

解决方案

完成以下步骤来解决此问题:

1. 终止 Windows 装载代理中运行的所有 VMware GRE 进程，或等待 30 分钟以使 VMware GRE 代理进程自动关闭。
2. 将 omnirc 文件中的以下 omnirc 变量更新为 1:
   OB2_USE_VMDK_MOUNTER
3. 重新启动 inet 进程。

在链接模式配置中，并非在所有 vCenter 上都能使用 HTML5 VMware GRE 插件

在链接模式配置中，并非在所有 vCenter 上都能使用 HTML5 VMware GRE 插件。

原因

该插件未在所有 vCenter 上注册。

解决方案

要在所有 vCenter 上查看 HTML5 VMware GRE 插件，必须在所有 vCenter 上注册该插件。

注册后无法使用 VMWare Granular Recovery 插件

成功安装和注册插件后，VMware Granular Recovery 插件在 vCenter Manager 用户界面上不可用。

原因

如果尚未从 vCenter Server 中正确清除较旧版本的插件，则可能会发生此问题。

解决方案

执行以下操作之一以重新启动 vCenter 服务，然后在 vCenter Manager 中检查 Granular Recovery 插件:

- **Windows vCenter:** 转到 *<vmware-install-dir>*\VMware\vCenter Server\bin 并运行以下命令:
  service-control --restart vsphere-ui
- **Linux vCenter (VCSA):** 在命令 shell 中，将目录更改为 /bin 并运行以下命令:
  service-control --restart vsphere-ui

升级后无法浏览在旧版本中创建的恢复请求

从旧版本的 Data Protector 升级后，您可以查看在旧版本中创建的恢复请求列表，但无法浏览缓存的和非缓存的恢复请求。

原因

此问题的原因可能是清除了装载代理主机上的装载点。

解决方案

创建新请求以能够浏览缓存的和非缓存的请求。

与装载虚拟机磁盘有关的问题

执行文件恢复时，选择分区后显示以下消息：

[EXCEPTION] boost: filesystem: status: The volume does not contain a recognized file system. Please make sure that all required file system drivers are loaded and that the volume is not corrupted: "\\?\M:\" ProxyGetAllNodesForPath.

手动装载虚拟磁盘后，在命令行界面中显示以下消息：

The volume does not contain a recognized file system. Please make sure that all required file system drivers are loaded and that the volume is not corrupted

原因

您的配置不受支持。扩展和 VMware VDDK 不支持动态磁盘。这是已知的 VMware 装载限制。分区未包含任何文件系统时，或者包含其他不受支持的文件系统时，可能会出现此问题。

解决方案

- 对于 Windows 虚拟机磁盘，使用受支持的文件系统之一。例如，NTFS 或 FAT 系统格式。
- 对于 Linux 虚拟机磁盘，使用受支持的 Linux 文件系统之一。

有关受支持的文件系统列表，请参阅最新的支持矩阵。

删除扩展后出现问题

如果先前无法成功从服务器上删除 VMware GRE 代理组件和脚本，则在 Windows 服务器上重新安装 VMware GRE 代理时可能遇到问题。

原因

适用于 VMware 的 Granular Recovery Extension 的删除命令尝试删除 VMDK 驱动程序。如果删除失败，则即使重复执行安装过程，驱动程序也会保持“已停止” / “等待下次引导时删除”状态。尝试重新安装 VMware Granular Recovery Extension 代理组件时，Data Protector Manager 安装会话日志中显示类似于以下内容的消息：

> **注意** 这是一个错误消息示例，可能因情况而异。

[Critical] computer.company.com 运行 VMware Granular Recovery Extension Agent 的安装后脚本失败，并且具有以下输出

Data_Protector_home\bin

perl -I "..\lib\perl" vmwgre_ag.pl -install

Cannot start vstor2-mntapi20-shared: The service is starting or stopping. Please try again later.

Delete of vstor2-mntapi20-shared driver failed: [SC] DeleteService FAILED 1072:

The specified service has been marked for deletion.

解决方案

重新启动系统以完成 VMware GRE 代理的安装。

> **注意**如果 VMDK 驱动程序已经安装在 Data Protector 之外的系统上并且已启动并正在运行，则将使用该驱动程序。既不删除也不重新安装它，升级过程成功。

密钥长度小于 1024 位的 RSA 证书被阻止

安装 Microsoft Security Advisory 更新 (KB2661254) 后，与 vCenter Server VMware GRE 插件的连接可能会失败。

原因

之所以发生此情况，是因为 VMware vCenter Server 默认情况下使用 512 位的 RSA 证书，但 Microsoft Security Advisory kb2661254 中的更新会阻止使用长度小于 1024 位的 RSA 证书。

解决方案

Microsoft Security Advisory 2661254。

在 Linux 上浏览 VMware GRE 时装载 LVM 逻辑卷失败

尝试浏览 LVM 逻辑卷时，操作失败并显示以下错误消息：

There are no partitions on selected disk.

原因

这是由于 GRE 操作只能在分区类型 ID 设置为 **8E** 的 LVM 卷上执行。

解决方案

执行以下步骤创建新的 LVM 分区/组/卷:

1. 在支持 LVM 的 Linux 系统上运行以下命令：

   fdisk /dev/<device_name>

2. 通过按 n 创建新分区并配置此分区的设置。
3. 创建分区后，按 t 并将分区类型设置为 8e 。
4. 按 w 以编写分区表。
5. 在新创建的分区上创建物理卷：pvcreate /dev/<partition_name> .
6. 在物理卷上创建卷组：vgcreate <VGNAME> /dev/<partition_name> .
7. 在卷组中创建逻辑卷：lvcreate -l <Total PE> -n <LVNAME> /dev/<VGNAME> .

   > **注意** <Total PE> 是指卷组的大小。您可以使用 vgdisplay -v <VGNAME> 获取该信息。

8. 在新创建的逻辑卷上创建文件系统：mkfs -t ext3 /dev/<VGNAME>/<LVNAME> .
9. 将逻辑卷装载到您所选的任何位置。

   > **注意**如果运行 fdisk -l over /dev/<partition_name> 命令，您会看到磁盘中有一个 LVM 分区。因此，VDDK VIX 装载会查找所选磁盘上的分区并装载它们。

vmwaregre-agent.exe 使用 lvscan、vgscan 和 pvscan 收集有关 LVM 分区的具体信息。为了使 vmwaregre-agent.exe 可以按预期方式工作，您必须在 lvm.conf 文件中将 log silent 属性设置为 0 。

一般来说，silent 属性设置为 0 ，但在某些情况下 (例如 SLES 12)，它设置为 1 。如果该属性设置为 1 ，则 lvscan、vgscan 和 pvscan 不显示输出，并且 vmwaregre-agent.exe 无法装载 lvm 分区。

VMware Granular Recovery Extension 选项卡缺失

您使用 vSphere Web Client 登录到了 vCenter 服务器。在“VM 和模板”视图中选择虚拟机时，没有 Data Protector 选项卡，扩展缺失。

原因

如果防火墙不允许通信，则会出现此问题。

解决方案

在 vCenter 服务器上，配置 Windows 防火墙。选择“例外”选项卡并**添加端口**以将 VMware vCenter Server-Web 服务 HTTPS 的端口（默认为 8443）添加到例外列表，并重新启动 vSphere 客户机界面。

VMware Granular Recovery Extension 选项卡缺失并且 vCenter Server 插件被禁用

您使用 vSphere Web Client 登录到了 vCenter 服务器。在“VM 和模板”视图中选择虚拟机时，没有 Data Protector 选项卡，并且扩展缺失。

原因

根本原因是安装异常结束。

解决方案

完成以下步骤：

1. 在 vCenter 服务器上，从系统中删除扩展。
2. 重新远程安装扩展。有关导入过程的详细信息，请参阅《*Data Protector 集成指南*》中的“配置集成”一节。
3. 通过 vSphere 客户机界面连接到 vCenter Server 系统。此时将显示 VMware vSphere Web 客户机主页。默认情况下，**主页**选项卡已选中。单击**管理**选项卡，然后单击**客户机插件**。此时将显示“客户机插件”窗口。
4. 在“客户机插件名称”列中，找到 VMwareGRE，右键单击，然后单击**启用**。

文件被覆盖问题

在选择了**覆盖**选项的情况下恢复项目时会显示与以下内容类似的消息：

\ 表示命令行的延续。

[Failed] c:\vix_27-2\incremental-21-2\incremental\ \

Username \CheckVix\vixlibs\arp.ico

Source:\incremental-21-2\incremental\Username\CheckVix\ \

vixlibs\arp.ico

You do not have access rights to this file.

[Failed] c:\overwrite_incr-21-2\incr24-2\incremental-21-2\ \

incremental\Username\CheckVix\vixlibs\vix.h

Source:\incr24-2\incremental-21-2\incremental\Username\ \

CheckVix\vixlibs\vix.h

[5] Access is denied.

原因

项目在目标系统上已存在。由于文件安全选项，无法覆盖此项目。如果源位置包含 NTFS 文件系统，并且目标虚拟机磁盘位于网络上，则适用于 VMware 的 Granular Recovery Extension 会恢复与项目关联的所有安全信息。无法覆盖这些信息。

解决方案

如果项目在目标位置中已存在，请执行以下操作之一：

- 将这些项目恢复到另一位置。
- 选择**跳过**恢复选项。
- 选择**重命名**恢复选项。
- 先手动更改目标位置中的文件权限，然后再启动恢复。

呈现失败

缓存恢复涉及在智能缓存设备主机上创建共享，并将其呈现给装载代理主机。呈现任务失败可能会导致恢复失败并显示以下消息：

- 在缓存呈现操作期间显示的消息:
  Unable to present shared disk ()
- 在相应的 Data Protector 会话报告中显示的消息:
  Presentation failed ()

原因

凭据不匹配时可能会发生此错误。

解决方案

- 确认配置智能缓存设备时提供的用户/管理员凭据。
- 使用 Data Protector GUI (在 IDB 上下文中) 或者使用 HTML5 GRE Web 插件 GUI (监视请求) 确认会话报告中的详细信息。
- 使用创建设备时存储在 Data Protector 中的凭据直接访问共享。

如果问题仍然存在，请与 Data Protector 管理员联系。

Vmware 文件的缓存恢复失败

在缓存恢复期间恢复 VMware 文件失败并显示以下错误：

Cannot access the file. Access is denied.

原因

与服务器或者共享资源存在多个连接时，可能会发生此错误。

解决方案

在每个介质代理主机中，必须确保只使用一个操作系统用户凭据来创建智能缓存设备。建议您断开与服务器或共享资源的所有先前连接，并重新引导系统。

还原会话在一段时间后停止

执行还原时，会话在某一特定的时间段后停止，RSM 停止响应。

原因

此问题可能是由于防火墙关闭不活动的连接所导致。

解决方案

确保连接保持活动状态，以便防火墙不会将其关闭。在 Cell Manager 系统上设置以下 omnirc 选项:

选项	描述	值
OB2IPCKEEPALIVE		1
OB2IPCKEEPALIVETIME	指定在发送第一个保持活动数据包之前连接保持不活动状态的时间。	number_of_seconds
OB2IPCKEEPALIVEINTERVAL	如果没有收到确认，则指定发送连续的保持活动数据包的时间间隔	number_of_seconds

VMware GRE 会话无响应

当装载代理主机具有 Linux 环境时，浏览或恢复操作会使 GRE 会话无响应。

原因

如果浏览磁盘或者从磁盘恢复后会话空闲超过 10 分钟，则下次浏览或恢复操作会使 GRE 会话变得无响应。

解决方案

在装载代理上查找正在运行的 VMware GRE 代理进程（vmwaregre-agent.exe）并手动结束该进程。

VMware GRE 文件恢复无法访问网络共享

VMware GRE 中的文件恢复无法访问 Windows 装载代理上的网络共享，并显示以下错误消息:

Could not start Recovery.
“无法访问目标 VMError 信息上的网络共享: 系统错误 [2250]。找不到网络连接。”

原因

之所以出现此问题，是因为 Windows 2008 R2 SP1 环境中缺少更新。

解决方案

确保在系统上应用了 Microsoft 支持的修补程序来解决此问题。有关此修补程序的更多详细信息，请参阅 http://support.microsoft.com/kb/2807716。

调整使用 HTML5 GRE Web 插件打开的浏览器窗口的大小时出错

调整使用 HTML5 GRE Web 插件打开的浏览器窗口的大小会引发错误并且会重新加载页面。

原因

这是 VMware 的已知问题。

解决方案

请参阅 https://communities.vmware.com/message/2434421#2434421。

浏览恢复显示错误

当您使用 HTML5 GRE Web 插件浏览恢复时，该插件可能显示以下错误消息:
Failure of REST call to getPartitionsForDisks:status =500 error.

原因

如果您在“可用文件”部分中选择了未格式化的磁盘，则可能会发生此问题，因为 HTML5 GRE Web 插件不支持恢复未格式化的磁盘。

解决方案

格式化磁盘。

VMware GRE GUI 无法在装载代理系统上启动代理

VMware GRE GUI 无法在装载代理系统上启动代理，并显示以下错误消息:

Error! Connection to agent ended (final repeat).

原因

装载代理系统使用与多个域共享的 IP。但是，VMware GRE 不支持使用共享 IP 托管的装载代理系统。

解决方案

在 Data Protector Cell Manager 中，使用装载代理系统客户机的 IP (而不是主机名) 来添加装载代理系统客户机，然后重试 GRE 操作。

Data Protector GUI 与 vSphere Web Client 之间的备份会话存在时间差异

所有备份会话的 Data Protector GUI 与 vSphere Web 客户机之间存在 1 分钟的时差。

原因

一个备份会话可能有多个 VM。

解决方案

不要比较会话时间，而是执行以下步骤比较对象版本，因为 IDB 具有每个 VM 的对象版本:

1. 启动 Data Protector GUI，并选择“内部 IDB”。
2. 单击**会话**。
3. 在左侧展开要确认的会话 (格式 <date>-<number> 例如: 2014-09-22-1)
4. 单击 vCenter。在右侧，您会看到**备份对象版本**
5. 选择“开始时间”，观察时间戳是否相同。

无法展开文件夹进行浏览

尝试浏览文件以进行恢复时，无法展开文件夹以浏览文件。

原因

如果您在浏览屏幕中已空闲了 10 分钟或更长时间，则会发生此情况，因为装载代理已关闭。

解决方案

单击**取消**，然后单击**浏览**以浏览并展开文件夹。

展开分区以进行浏览时引发错误

尝试展开分区时，显示以下错误:
"Error trying to mount the restored disk(s). Exception occurred while mounting the disk”

原因

这可能是由于一些问题而导致的，例如因为浏览屏幕闲置 10 分钟或更久而关闭了装载代理。

解决方案

单击**取消**，然后单击**浏览**以浏览并展开分区。

vSphere Web 界面灰显

如果具有 HTML5 GRE Web 插件的 VM 关闭，则 vSphere Web 界面将被部分禁用 (显示为灰色)。这不会影响 HTML5 GRE Web 插件的外观。

原因

托管 HTML5 GRE Web 插件的 VM 已关闭。

解决方案:

执行以下操作:

- 使用来宾主机上的插件时，避免关闭该主机。
- 选择另一个 VM。

浏览 LVM 磁盘时出现错误消息

浏览 LVM 磁盘时，VMware HTML5 GRE Web 插件显示以下错误消息:
"Something went wrong while searching for logical volumes. Check if you backed up and restored all the disks that are a part of the same volume group and try again".

原因

此问题可能是以下原因引起的:

- 如果创建的 LVM 具有超过 8 个磁盘，并且所有 8 个环路设备都可用，则浏览分区会失败并显示以下错误消息:
  This is because the additional loop devices are using all the disks that are part of the LVM.
- 如果创建的 LVM 具有 X 个磁盘，并且可用环路设备数小于 LVM 磁盘数，则浏览分区会失败并显示以下错误消息:
  This is also because the additional loop devices are using all the disks that are part of the LVM.
- 由于格式不正确，GRE 无法解析 pvscan 命令的执行输出。

解决方案

如果是前两个原因，请配置环路设备限制，然后重试浏览操作。有关更改受支持的环路设备数量的信息，请参阅 http://www.tldp.org/HOWTO/CDServer-HOWTO/。

如果是第三个原因，请检查 lvm.conf 文件中的 filter 参数。确保它看起来不像 filter = ["a|/dev/disk/by-id/scsi-.*|", "r|.*|"]。

在装载代理主机上启动 VMware GRE 代理时出现错误消息

如果您在装载代理主机上启动 VMware GRE 代理并且 Cell Manager 身份验证令牌已过期，则会显示以下错误消息

Authentication token expired. Please select 'Change Cell Manager' tab in GRE menu to authenticate with cell manager.

原因

Cell Manager 身份验证令牌过期时，会发生此问题。

解决方案

您必须通过选择同一虚拟机来再次执行 Cell Manager 身份验证。要重新选择同一虚拟机，请在 GRE 菜单中选择“更改 Cell Manager”选项卡，然后选择之前选择的同一 Cell Manager。

如果无法访问装载代理，则 GRE 插件会报告错误

当具有多个装载代理的安装程序在其 cell_info 文件中包含不可访问或无响应的代理作为第一个条目时，GRE 插件报告以下错误。

```
Connection to agent ended (final repeat)
```

原因

不可访问或无响应的代理作为安装程序 cell_info 文件中的第一个条目列出。

解决方案

当 Cell Server 上存在多个装载代理时，必须将可从 vCenter 访问的装载代理作为 Cell Manager 的 cell_info 文件 *<Dp-install-dir>*\Config\Server\cell\cell_info) 的第一个条目列出。

在介质代理主机系统上创建的共享文件夹或目录未被删除

在介质代理主机系统上创建的共享文件夹或目录是缓存 (智能缓存设备备份) 请求创建过程的一部分，不会被删除。

原因

这是因为该请求即使在过期之前也没有被浏览或恢复。

解决方案

执行以下步骤，手动删除介质代理主机上的共享文件夹或目录。

在 Windows 环境中

要删除共享，请以介质代理系统的本地管理员用户身份执行以下步骤。

1. 右键单击共享文件夹，然后单击属性。
2. 单击“共享” 选项卡，然后取消选中“共享此文件夹”复选框。
3. 单击“应用”并关闭“属性”对话框。

在 Linux 环境中：

要删除共享，请以 root 用户身份执行以下步骤:

1. 通过选择未浏览请求并获取会话报告，记下请求的共享文件夹名称。会话报告包含共享文件夹名称。
2. 登录介质代理主机系统并转到 file /etc/samba/smb.conf
3. 在 smb.conf 文件中，检查与共享文件夹名称匹配的条目。
4. 共享文件夹条目的格式如下：

   ```
   [dp_share_12435]

   comment = dp share

   path = /blob_store/blobShare/12435

   writeable = yes

   valid users = dp_user2

   create mask = 0755
   ```

5. 从 smb.conf 文件中删除匹配的条目。
6. 在命令提示符下，执行以下命令以通过 Samba 守护程序重新加载配置:
   killall -HUP smbd

在 HTML5 GRE Web 插件中浏览智能缓存时出现装载错误

在 HTML5 GRE Web 插件中浏览智能缓存时，如果代理超时，则可能会显示装载错误。

原因

浏览磁盘但未启动恢复操作时，可能会发生此问题。在所有 GRE 代理进程停止之前，您无法再次浏览同一磁盘。不得手动停止进程，因为代理可能正在为其他 vCenter 运行。

解决方案

等待 GRE 代理进程正常退出，然后再次尝试浏览。这可能需要大约 15 分钟。

与包含特殊字符的文件夹有关的浏览和恢复问题

在 HTML5 GRE Web 插件中，无法浏览名称中具有多字节字符的文件夹。浏览具有多字节字符的文件夹不会返回任何内容。

解决方案

尽管无法浏览文件夹，但如果选择它们进行恢复，可以成功恢复文件夹。

与包含特殊字符的文件夹有关的恢复问题

在 HTML5 GRE Web 插件中，恢复名称中具有特殊字符的文件夹或文件在 Linux 上不受支持。

无法恢复具有以下特殊字符的文件夹或文件。您将在会话报告中看到“无法复制”错误。

- "\" (反斜杠):
- “`”（重音符）
- "\" (反斜杠):

解决方案

通过使用 Data Protector GUI 恢复整个 VM，而不是使用 GRE 进行恢复，可以解决此问题。

无法浏览磁盘

浏览磁盘时，如果装载代理主机系统花费较多时间扫描新呈现的复本磁盘，则会显示以下错误消息:

Discovery of the newly presented replica disk(s) on the mount proxy host *<mount proxy hostname>* is still in progress.
Retry the operation after sometime.

原因

出现此情况的可能原因如下:

- 无论多路径服务是否正在装载代理系统上运行，装载代理操作系统都无法识别呈现的复本。
- 装载代理操作系统需要更多时间才能识别呈现的复本磁盘。

解决方案

检查操作系统上是否存在与多路径服务或者识别阵列中的复本有关的任何问题，然后重试操作。

无法浏览 SLES 12 装载代理主机上的 LVM 磁盘

在 SLES 12 装载代理主机上浏览 LVM 磁盘时，代理失败并显示以下错误消息:
"Something went wrong while searching for logical volumes. Check that you backed up and restored all disks that are part of same volume group and try again."

原因

发生此问题的原因是 lvscan 输出中出现问题。

解决方案

检查 lvscan 输出。要获取 lvscan 命令的输出，请在 /etc/lvm/lvm.conf 文件中设置以下行:

log silent = 0

从 Smart Cache 设备进行大容量的粒度恢复失败

智能缓存设备托管于 Windows Server 2008 R2 系统上时，智能缓存设备中的大型卷的粒度恢复可能会失败。

原因

这可能是由于 Windows 服务器操作系统中的内存碎片问题。

解决方案

将智能缓存设备托管于比 Windows 2008 R2 版本更高的 Windows 服务器上，然后执行备份和粒度恢复操作。

不可访问的 VM 上的文件或文件夹恢复失败

在目标虚拟机上恢复文件或文件夹失败并显示以下错误消息:

```
Error while trying to do recovery
Could not start recovery:
Details: Cannot access to network share on target VM
Error info: System Error[2] No such file or directory
```

原因

当目标虚拟机无法从装载代理系统访问时，会发生此情况。

解决方案

确保目标虚拟机可访问。将目标虚拟机配置为与装载代理系统的 DNS 具有相同的主机名。

对 StoreOnce Catalyst 或数据域的 VMware GRE 操作失败

在 VMware GRE 操作执行到 StoreOnce Catalyst 或数据域设备的备份期间，Data Protector dpfs 进程无法初始化， OB2DBG__DBGLOG_ClientInterface 调试日志中显示以下错误消息:

"Files are not available at mount path".

原因

发生此问题的原因是 fuse 库无法初始化。

解决方案

通过在装载代理主机上执行以下命令来初始化 fuse 库:

<hostname>/: # modprobe fuse

使用“无日志”选项执行的备份会话不符合 GRE 的条件

使用“无日志”选项执行的 Data Protector 备份会话无资格进行 GRE 或实时迁移和从 StoreOnce Catalyst 或数据域设备中启动。在备份期间显示以下错误消息:

[Major] From: BSM@hostname.com <VMname> Time: <Timestamp>

[61:4039] Following error occurred while storing detail catalog

information for device <Catalyst_device>

with loaded medium <Catalyst_medium> to Data Protector Internal Database:

There is no more space available in any of the Detail Catalog directories.

From this point on, all objects on this medium will have logging switched to "No Log".

原因

发生此问题的原因是任一详细编目目录中没有可用空间。

解决方案

在 Cell Manager 的 IDB 驱动器上创建空间，并针对另一设备执行单一会话复制。确保针对另一 StoreOnce Catalyst 或数据域设备执行单一会话复制时未选择替换选项。

缓存 GRE 操作期间出现数据一致性问题

在缓存 GRE 运行期间，数据可能会不一致。

原因

由于以下原因，在缓存 GRE 运行期间数据可能不一致:

- 选择的会话是对象复制的结果。
- 多个备份会话聚合到一个对象复制会话中，以执行对象复制。

解决方案

要执行对象复制，请选择一个单独的会话。

在源 VM 上启用了重复数据删除服务时，VMware GRE 恢复无法正常工作

当源 VM 启用了“重复数据删除”服务时，恢复将无法进行。

原因

这是因为在装载代理计算机上未启用“重复数据删除”。

解决方案

在装载代理计算机上启用“重复数据删除”。

用于 VMware GRE 装载的 Linux 装载代理上缺少环回设备

VMware GRE 浏览失败，并在 Linux 装载代理上显示以下错误消息:

Error while trying to mount the restored disk(s)

Exception occured while mounting disk

原因

发生此问题的原因是装载代理上缺少环回设备。

解决方案

要启用环回功能，请加载循环内核模块或使用以下 shell 命令手动创建环回设备:

```
for i in `seq 0 8`; do mknod -m660 /dev/loop$i b 7 $i; done
```

有关此问题的详细信息，请参阅虚拟磁盘开发套件 6.0 发行说明。

在 Linux 安装代理主机上扩展分区时出错

在 Linux 装载代理主机上扩展分区时显示以下错误:

Error while trying to mount the restored disk(s)

Exception occured while mounting disk

原因

此问题是由于以下原因之一导致:

- 环回设备不可用。
- 没有空闲的可用环回设备，因为所有设备都在使用中。

解决方案

根据需要执行以下任务，然后重试该操作:

- 通过释放使用设备的进程或应用程序，使占用的环回设备变为空闲。
- 通过执行以下命令来创建环回设备:
  for i in `seq 0 7`; do mknod -m660 /dev/loop$i b 7 $i; done.

当 Cell Manager 与装载代理主机相同时，无法访问装载代理主机

在选择 Cell Manager 和装载代理主机并单击“确定”后，VMware GRE 插件显示以下错误:

Mount proxy host is not reachable

原因

当 Cell Manager 和装载代理主机相同时，会发生这种情况。

解决方案

如果端口 **7116** 正在使用中，请在 **Windows** 主机上执行以下步骤**:**

1. 停止 **Cell server** 和 **filterListener** 服务，然后再次重新启动服务。
2. 重试该操作。

在 **Linux** 上执行以下步骤**:**

1. 停止并重新启动 Data Protector 服务。
2. 重试该操作。

GRE 操作失败

GRE 操作失败，并显示以下错误消息:
Error while trying to get the partitions for the disk(s). Object locked: The VM <*VM Name*> could be locked by another process for recovery/power on /live migrate. Please retry after the process is either done or cancelled.

原因

当某些其他进程锁定您要恢复的对象时，会发生此错误。

解决方案

确保满足以下条件:

- 显示“浏览” 选项的“恢复文件”窗口已关闭。
- 虚拟机没有正在从 StoreOnce Catalyst 或数据域设备执行的还原操作 (对象复制、还原、启动、实时迁移或 GRE)。
- 检查是否有其他任何启动、实时迁移或 GRE 操作使用同一备份对象。 如果使用，则清除请求并重试该操作。
- 您可以使用以下强制清理命令:
  ./vmwaregre-agent.exe -force_cleanup 0010 -vcenter xyz.hpeswlab.net

REST API 调用获取 Cell Manager 失败

升级 Data Protector 后，REST GET API 调用无法使所有客户机注册到 Cell Manager。

解决方案

要解决此问题，请完成以下步骤:

1. 在 vCenter Server 上取消注册插件。
2. 从以下路径手动删除任何 com.MicroFocus.DataProtector.VMwareGREAng.WebClient-10 插件:
   - **Windows**： C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity
   - **Linux**: /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
3. 在 vCenter Server 或设备上重新启动 Web 服务客户机。
4. 在 Data Protector 上重新注册插件。
5. 在 vCenter Server 或设备上重新启动 Web 服务客户机。
6. 确认插件位于 mob https://vcenter_name/mob 中。
7. 登录 vCenter GRE。

VMware GRE 失败

VMware GRE 失败，并显示以下错误：

[4] [MARK 2] in VMware::vCenter::Configuration::BuildSessionFactory:188

Code: 17101

原因

当您使用 Internet Explorer 浏览器时，浏览数据的缓存可能导致发生此问题。

解决方案

清除 Internet Explorer 浏览数据。

尝试获取 LVM 的装载点时出错

当尝试获取 LVM 的装载点时，会显示以下错误:

Something went wrong while searching for logical volumes. Check that you backed up and restored all disks that are part of same volume group and try again

原因

如果在备份过程中未选择所有磁盘，则会发生此错误。

解决方案

执行以下操作之一：

- 选择所有与 LVM 相关的磁盘。
- 检查 /tmp/vmware-root/vmware-vix-*.log 以确定端口 902 是否打开。

装载代理主机不可访问

将 Data Protector 的版本升级到 10.*x* 时，会出现以下错误消息:

Mount proxy host not reachable

原因

当 GRE 插件未使用 Web 服务器上的 REST API 连接到 Cell Manager 时，会发生此错误。

解决方案

执行以下检查:

- 安装了磁盘代理、介质代理、HPE P6000/HPE 3PAR SMI-S 代理、虚拟环境集成和 VMware Granular Recovery Extension 代理组件。
- /etc/hosts 文件包含所有主机条目。
- 检查证书:

  omnicc -secure_comm -configure_peer <*hostname*>.hpeswlab.net
  omnicc -secure_comm -configure_peer <*hostname*>.hpeswlab.net
  omnisv –stop (CM)
  omnisv –start (CM)

- 检查在 MP 上运行的 GRE 进程数。终止这些进程，然后重试 GRE 操作。
- 确保 cell_info 文件包含添加为客户机的 vCenter IP 地址:

  ```
  vcenter.domain.com={ encryption={ exception=1; }; }; xxx.xxx.xxx.xxx={ encryption={ exception=1; }; };
  ```

  cell_info 文件的位置:
  - **Windows**： C:\ProgramData\OmniBack\Config\Server\cell\cell_info
  - **Linux**： /etc/opt/omni/server/cell/cell_info
- 确保 ssconfig 文件包含 vCenter 主机名和 MP 主机名。另外，检查权限:

  DP CM err - CmnGetFile] open(/etc/opt/omni/client/ssconfig) failed, errno=[13] Permission denied

  /etc/opt/omni/client/ssconfig
  [root@hostname~]# ll /etc/opt/omni/client/ssconfig

  -rw-r--r-- 1 root root 1436 Nov 10 14:20 /etc/opt/omni/client/ssconfig

  [root@hostname~]#

  禁用 MP unset http_proxy 中的代理

  omnisv -stop

  omnisv –start

- 启用调试，并检查以下目录的 CM 中的应用程序服务器日志:
  - 应用程序服务器 **(Windows):** C:\ProgramData\OmniBack\Config\Server\AppServer
  - 应用程序服务器 **(Linux):** /etc/opt/omni/config/server/Appserver
  - **Linux** 日志**:** /var/opt/omni/log/AppServer
  - **Windows** 日志**:** C:\ProgramData\OmniBack\log\AppServe

  在 standalone.xml 文件中，将 <level name ="INFO"> 更改为 <level name ="DEBUG">。对于设备和 MP，请禁用 selinux、防火墙和代理。
- 任何添加的用户。
- 配置了多少个网卡? 如果配置了多个网卡，则使用 omnicc –secure 命令添加所有 DNS 条目。

Cell Manager 身份验证期间出错

尝试获取磁盘分区时发生以下错误：

Object Locked: The VM RHEL_7.3_iwf1114243 could be locked by another process for recovery/power on/Live Migrate. Please retry after the other process is either done or cancelled.

原因

如果装载代理未连接到 Cell Manager，则会发生此错误。

解决方案

重新启动装载代理。

GRE 无法浏览文件系统或装载代理无法扩展已还原 VM 的装载点

系统显示以下错误消息：

[exception] message: Insufficient permissions. Access denied.

[30] [exception] details: Unable to get request files from cell server

原因

如果未添加 <Any> <Any> 用户，则会发生此错误。

解决方案

添加 <Any> <Any> 用户。执行以下命令：

omniusers -add -type W -usergroup admin -name administrator -group "*" -client xyz.hpeswlab.net -pass *<Password>*

安装了无效的插件

vCenter GUI 中将显示以下错误消息:

getCellManagers;textStatus=error,errorThrown=

原因

当您安装无效的插件或未正确安装插件时，会发生此错误。

解决方案

完成以下步骤：

1. 从 vCenter 客户机卸载插件。
2. 从 vCenter 中的以下路径中手动删除 com.MicroFocus.DataProtector.VMwareGREAng.WebClient- 插件：
   - *Linux*: /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity
   - *Windows*: C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity
3. 重新启动 vSphere 客户机。设备：/usr/lib/vmware-vmon/vmon-cli -r vsphere-client vCenter: C:\Program Files\VMware\vCenter Server\vmon \vmon-cli --start vsphere-client C:\Program Files\VMware\vCenter Server\vmon\vmon-cli --stop vsphere-client
4. 使用 Data Protector 重新注册插件。
5. 重新启动 vSphere 客户机。
   设备：/usr/lib/vmware-vmon/vmon-cli -r vsphere-client Vcenter à vmon-cli -start vsphere-client vmon-cli -stop vsphere-client
6. 确保您在 mob https://vcenter_name/mob 中看到了该插件。
7. 登录 vCentre GRE。

无法注册 VMware Granular Recovery Extension Web 插件

This page is still under development. No published version is available at this time.

指定的 Dba 函数参数无效

浏览 GRE 时，显示以下错误消息:

message: Internal error: Invalid Dba function parameters specified

解决方案

执行以下检查:

- 检查设备是否在设备列表中。
- 检查执行 GRE 时是否对 vCenter 使用了单一登录以及用户名。

在 VMware 数据的粒度恢复期间尝试装载已还原的磁盘时出错

尝试装载还原的磁盘时出现以下错误:

Agent Process on mount proxy ended because vmwaregre-agent.exe did not send response in expected time frame of 10 minutes.

原因

出现此错误的原因是 vmwaregre-agent.exe 在预期的 10 分钟时间范围内未发送响应。

解决方案

在防病毒排除列表中包括以下目录和文件:

< DP 安装目录>\ OmniBack\

< DP 数据目录>\OmniBack\tmp\

< DP 安装目录>\OmniBack\bin\vepa_bar.exe

< DP 安装目录>\OmniBack\bin\vepa_util.exe

< DP 安装目录>\OmniBack\bin\vmwaregre-agent.exe

< DP 安装目录>\OmniBack\bin\FilterListener.exe

For example:
< DP 安装目录> = C:\Program Files
< DP 数据目录>= C:\ProgramData

HpeDpHsm 未加载

因为过滤侦听程序驱动器无效，HpeDpHsm 无法加载。

原因

发生此问题是由于过滤侦听程序驱动器无效。

解决方案

执行以下命令卸载 HpeDpHsm，然后再次加载:

```
fltmc unload hpedphsm
fltmc load hpedphsm
```

无法注册 VMware Granular Recovery Extension Web 插件

尝试注册 VMware GRE Web 插件时可能显示以下错误消息:

[exception] message: Could not register VMware Granular Recovery Extension web plug-in in VMware vCenter. [exception] details: Web service error: A specified parameter was not correct: extension.key

原因

这是因为指定了错误的注册参数。

解决方案

执行以下步骤：

1. 从 vCenter 客户机卸载插件。
2. 从 vCenter 服务器的以下路径中手动删除 com.MicroFocus.DataProtector.VMwareGREAng.WebClient- 插件:
   - **Linux:** /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity
   - **Windows:** C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity
3. 使用以下信息重新启动 vSphere 客户机 (如果适用):

在设备中:	运行以下命令以停止和启动 vSphere 客户机: `# service vsphere-client stop rm -rf /etc/vmware-vsphere-client/SerenityDB/serenity/* # service vsphere-client start`
在 vSphere 6.5 和更高版本中	运行以下命令以停止和启动 vSphere 客户机: `# service-control --stop vsphere-client rm -rf /etc/vmware-vsphere-client/SerenityDB/serenity/* # service-control --start vsphere-client`
在 Windows 中	1. 运行以下命令以停止 vSphere 客户机: `# cd <C:\Program Files\VMware\vCenter Server\bin> # service-control --stop vspherewebclientsvc` 2. 在 Data Protector 上重新注册插件。 3. 重新启动 vSphere 客户机。

4. 转到 vSphere 托管对象 URL (https://<vcenter_name>/mob)，并确保您可以在 mob 中查看插件。
5. 登录 vCenter GRE。

装载代理无法连接到磁盘存储设备

如果您没有访问磁盘所需的权限，则尝试获取磁盘分区时或在虚拟磁盘恢复期间会发生以下错误:

Mount proxy is unable to connect to disk storage device

原因

当您没有访问磁盘所需的权限时，会发生此问题。

解决方案

您必须根据启动 inet 和过滤侦听程序进程时使用的帐户来授予所需的权限:

- 对于本地系统帐户，不需要其他权限。
- 对于域帐户，向该帐户授予“域管理员”权限。
- 对于本地帐户 (本地系统帐户除外)，向该帐户添加“管理员”权限。

要提供“企业管理员”或“域管理员”权限，请执行以下步骤:

1. 登录 Active Directory 服务器。
2. 从“服务器管理器”的左窗格中，选择“AD DS”。
3. 单击服务器名称，转到屏幕右上角的“工具”>“Active Directory 用户和计算机”。
4. 选择域，然后单击“用户”。
5. 双击 Active Directory 用户。
6. 在“属性”页中，转到“成员所属”选项卡，单击“添加”。
7. 单击“高级”。
8. 在“选择组”对话框中，单击“立即查找”。从搜索结果中选择“企业管理员”或“域管理员” ，然后单击“确定” 。

Informix Server 集成故障诊断

This feature is available in the Premium Edition

本节列出常规检查和验证，以及在使用 Data Protector Informix Server 集成时可能会遇到的问题。从问题开始，如果找不到解决方案，请执行常规检查和验证。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 在 Informix Server 系统上，检查报告的系统错误 (位于以下目录的 debug.log 和 informix.log 文件中):

  Windows 系统： Data_Protector_home\log

  HP-UX 和 Solaris 系统： /var/opt/omni/log

  其他 UNIX 系统： /usr/omni/log
- 在有问题的客户机上进行测试备份和还原任意文件系统。
- ***Windows 系统：***确保使用帐户 informix 运行 Data Protector Inet 服务。
- ***UNIX 系统：***验证 onbar_d 命令是否已设置交换机所有权位，并且它由 Informix Server 用户拥有，例如 informix:informix 或 root:informix 。

  验证此用户是否也是备份规范的所有者，或者在还原失败的情况下，验证是否为还原会话指定此用户，以及它是否位于 Data Protector operator 或 admin 组中。

  如果此用户位于 Data Protector operator 组中，请确保选定此组的“查看私有对象”用户权限。

  现在测试此用户 (例如用户 *informix*) 是否在 Data Protector 中具有相应的权限。以用户 informix 登录 Informix Server 系统。从以下目录中:

  HP-UX 和 Solaris 系统： /opt/omni/bin/utilns

  其他 UNIX 系统： /usr/omni/bin/utilns

  执行:

  ```
  testbar -type:informix -perform:checkuser -bar: backup_specification_name
  ```

  检查 Informix Server 用户的示例

  在此示例中，用户具有名为 InformixWhole 的备份规范的所有必需权限。

  如果用户 informix 在 Informix Server 系统上 computer.hp.com 没有必需权限，则将显示类似以下的错误:

  ```
  [严重] 来自: OB2BAR@computer.hp.com "" 时间: 08/06/2011 17:51:41[131:53] 不允许用户 "informix.users@computer.hp.com" 执行还原。
  ```
- 在群集环境中，请确保在从 Data Protector CLI 执行过程之前将环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称。使用 Data Protector GUI 时，不需要此步骤。

此外，如果配置或备份失败:

- 确保 Informix 实例处于联机状态。

此外，如果您的备份失败:

- 检查 Informix 实例的配置，如“检查配置”中所述。
- 按“预览备份会话”中所述测试备份规范。
  - 如果此操作失败，请检查测试的 Informix Server 部分是否失败:

执行 onbar -b -F 命令。如果测试失败，请参阅 Informix Server 文档以获取进一步说明。

- 如果测试的 Data Protector 部分失败，请创建 Informix Server 备份规范以备份为空或备份到文件设备。

  如果备份成功，则问题可能与设备有关。

- 如果测试成功，请使用 Informix Server 命令直接从 Informix Server 系统启动备份。有关信息，请参阅“使用 Informix Server 命令”。

  如果此备份成功，则问题可能是运行 Data Protector 用户界面的客户机内存、磁盘空间或其他操作系统资源不足。

此外，如果备份或还原失败:

- 使用 testbar 实用程序测试 Data Protector 数据传输。以用户 informix 登录 Informix Server 系统。从以下目录中:

  Windows 系统： Data_Protector_home\bin

  HP-UX 和 Solaris 系统： /opt/omni/bin/utilns

  其他 UNIX 系统： /usr/omni/bin/utilns

  - 如果备份失败，请执行以下操作:

    testbar -type:Informix -appname:INFORMIXSERVER -bar: backup_specification_name -perform:backup

    其中 INFORMIXSERVER 是 Informix 实例的名称。

  - 如果还原失败，请执行以下操作:

    testbar -type:Informix -appname:INFORMIXSERVER -bar:backup_specification_name -perform:restore -object:OBJECT_NAME -version:OBJECT_VERSION

    其中 INFORMIXSERVER 是 Informix 实例的名称，OBJECT_NAME 是要还原的对象的名称，OBJECT_VERSION 是对象版本。

  如果测试失败:

  1. 使用位于以下位置中的 Cell Manager 上的 Data Protector 故障诊断文件对 testbar 实用程序报告的错误进行故障诊断:

     Windows 系统： Data_Protector_home\help\enu\Trouble.txt

     UNIX 系统： /opt/omni/gui/help/C/Trouble.txt

  2. 在 Informix Server 系统上，检查文件中报告的系统错误:

     Windows 系统： Data_Protector_home\log\debug.log

     HP-UX 和 Solaris 系统： /var/opt/omni/log/debug.log

     其他 UNIX 系统： /usr/omni/log/debug.log

此外，如果还原失败:

- 确保正确配置用于抢救逻辑日志的备份规范。

检查 Informix Server 端

以下检查可以帮助您解决一些与 Informix Server 相关的问题。

如果备份或还原失败:

- 检查以下 Informix Server 文件以获取错误说明:

  bar_act.log

  bar_dbg.log

  online.log

  这些文件的位置在 Informix Server ONCONFIG 文件中指定。

此外，如果您的备份失败:

- 开始备份，而不是使用 Data Protector:

1. 将 BAR_BSALIB_PATH shell 变量设置为:

   Windows 系统： ISMDIR\bin\libbsa.dll

   其中 ISMDIR 是指向 ISM 的路径。

   UNIX 系统： INFORMIXDIR/lib/ibsad001.sl

   其中 INFORMIXDIR 是 Informix Server 的主目录。

2. 使用 onbar 命令以启动备份。

此外，如果还原失败:

- 对于冷还原，请验证要还原的 dbspace 是否处于脱机状态:
  1. 以用户 informix 登录 Informix Server 系统。
  2. 执行以下命令：

     Windows 系统： INFORMIXDIR\bin\onstat -d

     UNIX 系统： INFORMIXDIR/bin/onstat -d

     其中 INFORMIXDIR 是 Informix Server 的主目录。
- 确保 Informix Server 配置文件 (ONCONFIG 、紧急引导文件、 oncfg_INFORMIXSERVER.SERVERNUM 以及 UNIX 上的 sqlhosts 文件) 均未损坏。如果它们损坏，请手动进行还原。

问题

下面是使用 Data Protector Informix 服务器集成时可能遇到的问题。

还原到另一个客户机失败

如果已将数据备份到一个客户机，导出介质，然后将它们导入到另一个单元中的另一个客户机，则可以在 IDB 中更改备份会话的 Data Protector 会话 ID。但是，会话 ID 不会在 Informix Server 紧急引导文件 (ixbar.server_id ，其中 server_id 是 SERVERNUM 配置参数的值) 中自动更改。因此，此类对象的还原可能会失败。

解决方案

编辑紧急引导文件以反映已更改的 Data Protector 会话 ID。在导入过程中列出已更改的会话 ID。

有关备份对象的信息按以下格式存储在紧急引导文件中:

```
ODS730 rootdbs R 1 7 0 9 2011008018 2011-08-18 18:10:25 1
```

条目 7 和 9 组成 Data Protector 会话 ID。条目 9 是日期，条目 7 是唯一的会话编号。

此处，会话 ID 是 2011/08/18-9 。请注意，日期字段中的分隔符在紧急引导文件中为 "-"，在 Data Protector 会话 ID 中为 "/"。

SERVERNUM 配置参数的值在条目 4 中给出。

由于紧急引导文件太大，还原失败

解决方案

使用 ON-Bar onsmsync 实用程序以从 Informix Server sysutils 数据库和紧急引导文件中删除已过期备份。

备份或还原失败并显示 131 ISAM 错误

备份或还原会话失败，并显示以下 131 ISAM 错误: 无可用磁盘空间。

解决方案

将数据块空间添加到 rootdbs ，或者添加 temp dbs。默认情况下，如果磁盘空间不可用于 dbobject，且未配置 temp dbs ，则从 rootdbs 获取空间。

示例: 要将具有 2048 页大小的 500MB 的数据块空间添加到 rootdbs ，请使用以下命令: *onspaces -a rootdbs -p /opt/IBM/informix/ol_informix1170/dbspaces/Chunk2_rootdbs -o 2048 -s 500000*。

Lotus Notes/Domino Server 集成故障诊断

This feature is available in the Premium Edition

本节列出了 Lotus Notes/Domino Server 检查、常规检查和验证，以及使用 Data Protector Lotus Notes/Domino Server 集成时可能遇到的问题。从问题开始，如果找不到解决方案，请执行检查和验证。

开始之前

- 确已安装最新的正式补丁。

检查 Lotus Notes/Domino Server 端 如果执行以下检查时遇到错误，请联系 Lotus Notes/Domino Server 支持人员。***Windows 系统：***

- 检查 nNotes.dll 库是否已链接。执行：

  ```
  Data_Protector_home\bin\util_notes.exe -chkconf
  ```

检查和验证

如果配置、备份、还原或恢复失败:

- 查看 Lotus Notes/Domino Server 系统中 debug.log 文件中报告的系统错误，该文件位于以下目录中:

  Windows 系统： Data_Protector_home\log

  Solaris 系统： /var/opt/omni/log/

  AIX 系统： /usr/omni/log/
- 验证 Data Protector 软件是否已正确安装。
- 检查系统上是否已安装 Data Protector Lotus 集成代理 ldbar.exe 。
- ***Windows 系统：***验证 Lotus Notes/Domino Server 系统上的 Inet 启动参数。

  确保 Data Protector Inet 服务在运行时所用的用户是 Data Protector admin 用户组成员。
- 检查 omnirc 环境设置。
- 检查备份或还原会话期间的错误。

  与 Lotus Notes/Domino Server 相关的错误采用以下形式:

  ```
  Lotus ERROR [error #]: Error description
  ```

  检查错误描述并采取相应的操作。

此外，如果您的备份失败:

- 按照“检查配置”中所述检查 Lotus Notes/Domino Server 配置。
- 执行 Lotus Notes/Domino Server 系统的文件系统备份。

  查看会话消息并检查以下位置的 debug.log 文件中报告的系统错误
  - Data Protector Lotus Notes/Domino Server 客户机 (如果文件系统备份的 Lotus Notes/Domino Server 部分失败)。
  - Data Protector Cell Manager 系统 (如果文件系统备份的 Data Protector 部分失败)。
- 使用 testbar 实用程序验证 Data Protector 内部数据传输。
  1. 从以下目录中:

     Windows 系统： Data_Protector_home\bin

     Solaris 系统： /opt/omni/bin/utilns

     AIX 系统： /usr/omni/bin/utilns

     执行:

     ```
     testbar -type:Lotus -appname:SRV_NAME -bar:backup_specification_name -perform:backup
     ```
  2. 创建 Lotus Notes/Domino Server 备份规范，以备份到 null 设备或文件。如果备份成功，则问题可能与备份设备有关。
- 使用 ldbar.exe 启动备份会话。

通过将备份选项指定为 ldbar.exe 命令行选项，您可以使用 Data Protector CLI 启动单个数据库的备份。

在 Data Protector Lotus Notes/Domino Server 客户机上，从以下目录中:

Windows 系统： Data_Protector_home\bin

Solaris 系统： /opt/omni/bin

AIX 系统： /usr/omni/bin

执行:

Windows 系统：

ldbar.exe -perform:backup -db: DB_NAME -server: SRV_NAME [-ini:Path_to_notes.ini_file] -bar: backup_specification_name

UNIX 系统：

ldbar.exe -perform:backup -db:DB_NAME -server:SRV_NAME [-ini:Path_to_Notes.ini_file] -bar:backup_specification_name [-homedir:PathToLotus Home] [-datadir:path to Domino data] [-execdir:PathToDominoExecutables]

-bar 选项是必需的，因为 ldbar.exe 读取备份规范中的设备选项，而不是备份规范中的其他选项 (将被忽略)。改为使用命令行选项。

对于其他 ldbar.exe 参数，执行 ldbar.exe -help 。

- ***Windows 系统：*** 如果 Lotus Notes/Domino Server 和 Windows 终端服务共存于同一系统上，且从终端客户机程序启动 Lotus Notes/Domino Server，则无法执行 Lotus Notes/Domino Server 备份。

  不应使用 Windows 终端服务来管理 Lotus Notes/Domino Server。但是，如果使用终端服务客户机程序在运行 Lotus Notes/Domino Server 的系统上启动 GUI，则可执行 Lotus Notes/Domino Server 备份。可以在本地或使用 VNC 程序对 Lotus Notes/Domino Server 进行管理。

此外，如果还原失败:

- 在有问题的客户机上进行测试还原任何文件系统。
- 在 Lotus Notes/Domino Server 系统上使用 ldbar.exe 命令测试还原会话。从以下目录中:

  Windows 系统： Data_Protector_home\bin

  Solaris 系统： /opt/omni/bin

  AIX 系统： /usr/omni/bin

  执行:

  ldbar.exe -perform:restore -db:DB_NAME -server:SRV_NAME -ini:Path_to_notes.ini_file

  对于其他 ldbar.exe 参数，执行 ldbar.exe -help.

此外，如果您的恢复失败:

- 请检查恢复时间参数是否以 24 小时格式设置:

  yyyy/mm/dd.hh:mm:ss

  示例

  2011/08/26.18:15:00

问题

以下是使用 Data Protector Lotus Notes/Domino Server 集成时可能遇到的一些问题：

- 脚本失败错误
- 具有大量数据库的增量备份速度很慢
- Lotus Notes/Domino Server 在备份期间冻结
- 还原到另一个客户机失败
- 数据库还原失败
- 恢复已还原的 Lotus Notes/Domino 服务器 NSF 数据库失败

脚本失败错误

使用 Data Protector GUI 配置或启动备份时，会显示以下错误:

```
Script failed. Cannot get information from remote host.
```

解决方案

有关如何解决此问题的信息，请参阅“检查 Lotus Notes/Domino Server 端”。

具有大量数据库的增量备份速度很慢

对大量含已设置事物日志的数据库进行备份且使用增量备份类型时，备份速度减慢。

解决方案

将 omnirc 文件选项 OB2_LOTUS_NODBIID 设置为 1 。

Lotus Notes/Domino Server 在备份期间冻结

Lotus Notes/Domino Server 冻结并显示以下错误:

```
Fatal Error signal = 0x0000000b PID/TID = xxxx/l

Freezing all server threads ...
```

原因

在以下情况下可能发生此问题：

- Lotus C API 初始化失败。
- ***UNIX 系统：***如果 Lotus Notes/Domino 服务器未联机且 Lotus Notes/Domino 服务器后台程序 logasio 未运行，则在 Lotus Integration Agent 初始化 Lotus C API 时， logasio 后台程序将自动启动。用户 notes 的环境因未执行 .profile 而未进行设置，因此 logasio 服务器可能无法启动。

解决方案

终止 ldbar.exe 或 logasio 进程:

1. ***UNIX 系统：***以用户 root 登录 Lotus Notes/Domino Server 系统。
2. ***Windows 系统：***使用 Task Manager 终止所有 ldbar.exe 进程。
3. ***UNIX 系统：***终止所有 ldbar.exe 和 logasio 进程。
4. 如果 Lotus Notes/Domino Server 正在运行，请重新启动它。在重新启动之前，请确保所有 Lotus Notes/Domino Server 进程均未运行。
5. 以用户 notes 身份登录，然后检查 Lotus Notes/Domino Server 是否已恢复。从以下目录中:

   Windows 系统： Data_Protector_home\bin

   Solaris 系统： /opt/omni/lbin

   AIX 系统： /usr/omni/bin

   执行: util_notes.exe -box -ini:path_to_notes.ini

   如果所有均正常，则会显示 *RETVAL*0 消息。

> **注意**在 UNIX 上，需要在重新启动 Lotus Notes/Domino Server 之前清理共享内存和信号。

还原到另一个客户机失败

解决方案

确保 Lotus Notes/Domino Server 已安装在目标系统上，且它与要还原其备份的 Lotus Notes/Domino Server 系统具有相同的非数据库文件。必须先从文件系统备份还原这些文件。

数据库还原失败

在还原会话期间，某些选定 Lotus/Notes Domino Server 数据库未还原，对于这些数据库，Data Protector 会报告类似如下所示的错误:

```
[重要] 来自：OB2BAR@ice.company.com "BLUE" 时间: 8/22/2011 4:07:09 PM Lotus Notes C API 'NSFTakeDatabaseOffline' 返回错误 5098: 服务器正在使用中，不能脱机。
```

解决方案

1. 断开正在访问要还原数据库的所有用户。
2. 重新启动还原。

恢复已还原的 Lotus Notes/Domino 服务器 NSF 数据库失败

在恢复过程中，会显示以下错误消息： [Critical] From: OB2BAR@ice.company.com "BLUE" Time: 19.10.11 17:24:23 Lotus Notes C API 'NSFGetTransLogStyle' returned error 5114:Recovery Manager: Recovery only supported for Backup Files. 这表示在恢复结束之前，Lotus Notes/Domino Server、用户或进程将至少访问还原列表中的一个数据库。

解决方案

1. 重新启动 Lotus Notes/Domino Server 系统并再次执行还原。
2. 将发生故障的数据库还原到备份位置以外的位置。

Microsoft 365 集成故障诊断

本主题介绍使用 Data Protector Microsoft 365 集成时的常规检查和验证操作以及可能会遇到的问题。

调试日志

如果在使用 Microsoft 365 集成时遇到问题，则以下日志文件中的信息可以帮助您确定该问题:

Data Protector Web GUI 日志文件

“主页”上下文 >“设置”>“日志”

应用程序服务器日志

- <ProgramData>\Omniback\log\AppServer\server.log
- <ProgramData>\Omniback\log\AppServer\DPServer.log

边缘服务日志

- <ProgramData>\Omniback\log\edgeservice\edgeservice.log - 此日志文件包含与边缘服务操作相关的日志。
- <ProgramData>\Omniback\log\edgeservice\edgeservice_accesslog.log - 此日志文件包含 HTTP 访问日志。您可以使用这些日志来识别 HTTP 请求的状态并审核哪些客户机通过边缘服务发出了这些请求。

您可以使用位于以下位置的 log_config.xml 配置文件来配置两个边缘服务日志文件:

<ProgramData>\Omniback\Config\client\modules\edgeservice

您可以为两个日志文件配置以下参数:

- maxFileSize - 这是最大日志文件大小。一旦日志文件达到最大文件大小，将对其进行存档并在同一位置创建一个具有相同名称的新日志文件。该参数的默认值为 10 MB。
- maxHistory - 这是保留存档日志的持续时间 (天数)。该参数的默认值为 30。
- totalSizeCap - 这是日志存档的最大大小。该参数的默认值为 1 GB。

按照以下步骤进行更新 log_config.xml:

1. 停止 Edge Service 。打开 Windows 服务管理器，选择“Data Protector 边缘服务”，然后单击“停止”。
2. 在 log_config.xml 文件中更新所需的参数。
3. *可选*。更改日志级别。可用选项为 TRACE、DEBUG、INFO、WARN、ERROR。
   示例: 要从 Edge Service 查看调试日志，必须按如下所示配置日志级别:
   ```
   <logger name="com.mf.dp.edgeservice" level="DEBUG" additivity="false">
     <appender-ref ref="ROLLING"/>
   </logger>
   ```
4. *可选*。要启用 HTTP 访问日志，请在 edgeservice.properties 文件中将 properties.wireTap 设置为 true 。该文件可从以下位置获取: <ProgramData>\Omniback\Config\client\modules\edgeservice\edgeservice.properties
5. 启动“边缘服务”。打开 Windows 服务管理器，选择“Data Protector 边缘服务”，然后单击“启动”。

Microsoft 365 代理日志

- <ProgramData>\Omniback\log\m365.log
- <ProgramData>\Omniback\tmp\ (如果启用了调试，则可用)

从系统中删除 M365 组件时 AppServer 和 IDB 出现问题

当您从系统中删除 Office 365 组件时， **AppServer** 和 **IDB** 无法启动。

原因

出现此问题的原因是在您卸载 Office 365 组件时系统中保留了一些配置文件。

变通方法

要解决此问题，请删除以下配置文件:

1. 从 *<PROGRAMDATA>|Config|client|components|registry* **:**
   - CDpO365DataMoverComponent.librarytype
   - DpSessionLogger.librarytype
   - O365ExchangeProtector.librarytype
   - O365OnedriveProtector.librarytype
2. 从 *<PROGRAMDATA>|Config|client|components:*
   - ExchangeO365Composite.xml
   - OnedriveO365Composite.xml

Azure 应用程序已成功从 Cell Manager 中删除，但无法从 Azure 中删除

当您尝试删除通过 Data Protector 注册的 Azure 应用程序时，会显示以下错误消息:

Azure application successfully deleted from cell manager but could not be deleted from Azure.

解决方案

要从 Azure 中删除应用程序，请执行以下步骤:

1. 登录 Azure Active Directory 门户。
2. 导航到所需的应用程序并将其删除。有关详细信息，请参阅 Microsoft Azure 文档。

连接到边缘服务失败

Microsoft 365 集成代理无法连接到边缘服务。错误消息类似如下所示:

[Major] From: O365LIB_EXCHANGE@cellmanager.mydomain.net "M365" Time: 2/12/2021 6:36:58 PM
[183:34] Could not connect to the Data Protector Edge Service on host 'm365client.mydomain.net' and port '3612'.

原因

此问题是由于网络连接问题所致。

解决方案

要解决此问题，请修改以下 omnirc 变量:

1. 通过修改变量 OB2_REST_CLIENT_SESSION_TIMEOUT 来增加连接超时时间。例如， OB2_REST_CLIENT_SESSION_TIMEOUT=360.
2. 通过修改变量 OB2_O365_REST_RETRY_COUNT 增加 Microsoft 365 代理与边缘服务之间的连接尝试次数。例如， OB2_O365_REST_RETRY_COUNT=6.
3. 通过修改变量 OB2_O365_REST_RETRY_INTERVAL 增加失败的 REST API 调用之间的重试间隔。例如， OB2_O365_REST_RETRY_INTERVAL=30000.
4. 重试运行会话。

如果问题仍然存在，请通过将变量 OB2_O365AGENT_THREADED_BACKUP 设置为 FALSE 禁用并发会话。

相关主题

Microsoft 365 omnirc 选项

边缘服务器导入失败

边缘服务导入到 Cell Manager 失败。

原因

如果边缘服务无法解析 Cell Manager 主机名，则会出现此问题。

解决方案

要解决此问题，请按照下列步骤操作:

1. 触发 Cell Manager 的反向 DNS 查找。运行以下命令:
   nslookup IPAddress
2. 如果仍然无法解析 Cell Manager 主机名，请在 hosts 文件中添加 Cell Manager 主机条目。该文件可从以下位置获取:
   Windows 系统: %SystemRoot%\system32\drivers\etc\
   Linux 系统: /etc/hosts
3. 重新启动 edgeservice 。

services.msc 中缺少边缘服务

在 Cell Manager 上添加 Office 365 组件后，Edge Service 不会出现在以下位置的服务列表中：service.msc.

解决方案

要解决此问题，请运行以下命令：

"<DP_Home>\OmniBack\bin\edgeservice\install_dp_edge_service.bat" "Data Protector Edge Service" "[Micro Focus Data Protector] - Edge Service" "Domain\Username" "password"

非英语区域设置中的 **esgencert** 脚本错误

在非英语区域设置中运行 esgencert 脚本时会显示以下错误消息:

ERROR: 'Failed to create master encryption key in windows credential manager.
ErrorMsg:
Name Version Source Summary
---- ------- ------ -------

nuget 2.8.5.208 https://onege... NuGet provider for the OneGet meta-package manager

ERROR The property'ValidAuthenticodeSignatureInFile' cannot be found on this object. Make sure the property exists.

原因

发生此问题的原因是操作系统上缺少 Windows 更新。

解决方案

要解决此问题，请按照下列步骤操作:

1. 打开 Windows 设置。选择“开始” 按钮，然后单击“设置” 。
2. 单击“更新和安全” >“Windows 更新” 。
3. 更新完成后，重新启动操作系统。

找不到有效的认证路径

原因

此问题是以下原因之一导致的:

- jreNG 的默认密钥库中缺少 cacert.pem
- edgeservice.jar 未与位于以下位置的 java.exe 一起运行: <DP_Home>\OmniBack\jreNG\bin\java.exe

解决方案

通过运行以下命令导入 CA 证书:

```
keytool -import -alias edgeserverhost.net -file cacert.pem -keystore "<DP_Home>\OmniBack\jreNG\lib\security\cacerts" -storepass <password>
```

分页文件太小，无法完成操作

边缘服务失败，并显示以下错误:
OpenJDK 64-Bit Server VM warning: INFO: os::commit_memory(0x0000000600000000, 8589934592, 0) failed; error='The paging file is too small for this operation to complete' (DOS error/errno=1455)

解决方案

按照以下步骤解决此问题:

1. 打开“运行” 对话框，键入 sysdm.cpl ,3 或 SystemPropertiesAdvanced ，然后单击“确定” 以弹出“系统属性 - 高级” 窗口。
2. 在“性能”下，单击“设置” 。
3. 在“高级” 选项卡中，单击“更改” 。
4. 取消选择“自动管理所有驱动器的分页文件大小” 。
5. 选择“自定义大小” 。将“初始大小” 指定为 4000 MB，将“最大大小” 指定为 6000 MB。
6. 重新引导系统。

远程服务器证书出现问题

备份会话失败，并显示以下错误:

[Normal] From: O365LIB_EXCHANGE@hostname.domain "M365" Time: 2/18/2021 11:58:09 AM
Problem encountered with remote server certificate:
[Critical] From: O365LIB_EXCHANGE@hostname.domain "M365" Time: 2/18/2021 11:58:09 AM
No objects to backup.

certificate is not yet valid

原因

如果在 Cell Manager 和 Microsoft 365 客户机之间未进行时间同步，则会出现此问题。

解决方案

要解决此问题，请在 Microsoft 365 客户机上按照以下步骤操作:

1. 停止边缘服务。打开 Windows 服务管理器，选择“Data Protector 边缘服务”，然后单击“停止”。
2. 运行以下 Perl 脚本:

   <Data_Protector_Home>\bin\perl <Data_Protector_Home>\bin\esgencert.pl

   > 注意: 必须以边缘服务登录用户身份运行 Perl 脚本。如果边缘服务登录用户属于管理员组但不是管理员用户，则通过以管理员身份打开命令提示符来运行上述脚本 (单击“开始”按钮，键入 cmd，右键单击“命令提示符”图块，然后单击“以管理员身份运行”)。

3. 再次运行备份会话。

Microsoft Exchange Server 集成故障诊断

This feature is available in the Premium Edition

本节列出了常规检查和验证以及在使用 Data Protector Microsoft Exchange Server 集成时可能会遇到的问题。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果浏览、备份或还原操作失败:

- 检查 debug.log 文件中报告的系统错误。
- 检查您是否可以在有问题的客户机上执行文件系统备份和还原。

问题

下面是使用 Data Protector Microsoft Exchange Server 2010 集成时可能会遇到的一些问题：

无法连接到系统上的介质代理

运行 Microsoft Exchange 服务器还原时发生以下错误:

[Critical] From: OB2BAR_VSSBAR_COMP@mediaserver.domain "MS Exchange 2010+ Server" Time: 7/30/2021 7:28:12 PM
Cannot connect to Media Agent on system.domain, port 12345 (IPC Cannot Connect
System error: [10061] Connection refused
) => aborting.

原因

如果您使用源端重复数据删除网关来备份 Exchange DAG 配置，则会发生此错误。如果目标服务器与原始数据源不同，则还原可能失败。

解决方案

执行以下操作之一：

- 在写入重复数据删除设备的 DAG 配置中配置 Exchange 备份时，请使用源端类型以外的网关。
- 如果您已经使用源端网关备份到重复数据删除目标，并且必须将数据还原到与原始源不匹配的目标服务器，请使用“更改设备”功能来选择非源端类型的网关。

无法将数据库添加到卷影副本集

运行 Microsoft Exchange 2010+ Server 备份时发生以下错误:

```
[Major] From: OB2BAR_VSSBAR@exchange01.domain.tld "MS Exchange 2010+ Server"  Time: 9/17/2015 12:34:09 PM
        Could not add 'C:\ExchDBs\DB09\' to Shadow Copy Set.
```

原因

此错误发生在使用 **AutoReseed** 的 Exchange **JBOD** 部署中。在这种配置中，具有多个装载点的系统可以访问同一个物理磁盘。使用不同装载点访问的同一物理磁盘上的多个 Exchange 邮箱数据库的备份失败。这是因为此唯一磁盘的 VSS 快照无法多次添加到同一个备份会话。

解决方案

有两种选项可以解决这个问题:

1. 确保同一 Microsoft Exchange 2010+ Server 备份规范中仅包含驻留在不同物理磁盘上的数据库。可以同时创建和执行多个备份规范。
2. 重新配置 Microsoft Exchange 2010+ Server，使每个数据库都驻留在一个唯一的磁盘 (驱动器号或装载点) 上，以便有一个唯一的卷来获取 VSS 快照。

在 Data Protector GUI 中显示 Microsoft Exchange Server 拓扑时出现滞后

打开 Data Protector GUI 并尝试显示源页面时，无论是处于“备份”还是“还原”上下文，您都必须等待很长时间。

原因

如果同一个域中存在无响应的系统 (例如，关闭的系统)，则可能发生这种情况。即使无响应的系统不是备份环境的一部分，也会出现此问题。这是由于执行 Microsoft Exchange Server Shell 命令时 Microsoft Exchange Server 出现了问题。

解决方案

从域中删除系统或修复该问题。

无法执行数据库备份

启动数据库的备份会话时，即使当前未运行其他备份会话，数据库也不进行备份，似乎被其他会话锁定。显示的消息如下所示:

```
[轻微] 来自: OB2BAR_E2010_BAR@exch03.e2010.company.com "MS Exchange Server" 时间: 1/17/2013 3:07:13 PM [170:313] 已在不同的会话中备份数据库 DEMAR 的一个或多个副本。
```

原因

如果在上一个备份会话进行中时，集成代理 (e2010_bar.exe) 因 Microsoft Exchange Server 系统重新启动或某些其他原因而被强制终止，会话则保持锁定状态，因而便会发生这种情况。

解决方案

请执行以下命令：

```
omnidbutil –free_cell_resources
```

> **注意**此命令行将删除现有的全部锁定，因此，请确保不需要现有锁定中的任何一个。

还原失败

尝试还原数据库时，会话失败。

原因

如果数据库之前已还原 (可能不成功)，并且在上一个还原会话期间，Microsoft Exchange Server 在数据库目录中创建了 .env 文件，则可能发生这种情况。此文件现在会阻止数据库再次还原。

解决方案

删除 .env 文件并启动新的还原会话。

在 DAG 环境中从对象副本还原失败

从在对象复制会话中创建的介质集还原数据库时，由于在原始备份会话中创建的介质集不再存在，会话将失败，并显示如下所示的错误:

[Critical] From: OB2BAR_E2010_BAR@computer1.company.com "MS Exchange 2010 Server" Time: 28/02/2013 16:08:12 No mailbox database copy can be selected for restore/instant recovery.

解决方案

1. 验证在对象复制会话中创建的介质集是否仍存在。
2. 在所有 Microsoft Exchange Server 系统节点上，将环境变量 OB2BARHOSTNAME 设置为 DAG 虚拟系统的名称，然后重新启动 Data Protector Inet 服务。
3. 启动新的还原会话。

还原到最新状态失败

在使用还原方法“还原到最新状态”并选中“执行数据库恢复”选项的情况下，尝试还原丢失了所有日志文件的数据库时，数据库恢复失败。

原因

如果从完整备份还原数据库 (即，还原链仅包含完整备份会话)，可能会发生这种情况。由于在“还原到最新状态”会话中，只有 .edb 文件会从完整备份中还原，因此在启动数据库恢复时，不会对数据库文件应用任何日志，数据库恢复因而失败。

解决方案

使用还原方法“还原到时间点”来还原数据库。

在即时恢复后，被动副本仍处于“失败”状态

使用还原方法“还原到时间点”在 DAG 环境中启动即时恢复会话来还原同一个数据库的活动副本和被动副本时，数据还原成功，但活动副本与被动副本之间的同步失败，从而使被动副本处于 Failed 状态。

原因

如果在数据还原后，被动副本具有额外的日志文件 (活动副本端不存在该文件) 而无法建立同步，则会出现此问题。如果在完整备份会话期间选择多个数据库副本进行备份，则会发生这种情况。Data Protector 会先对应用于数据库文件的日志最少的被动副本执行完整备份，然后再对所有其他副本执行复制备份，最后再备份活动副本。备份会话正在进行中时，可能会在活动副本端创建一个新日志，因此，在备份活动副本时，也会备份新创建的日志。如果将来发生故障转移 (其中一个被动副本成为活动副本) 且您执行“还原到时间点”即时恢复，则每个副本都将从其自己的复本存储卷进行还原。这会导致活动副本 (在备份时处于被动状态) 的日志数量比被动副本 (在备份时处于主动状态) 少。因此，无法建立同步。

解决方案

对处于“失败”状态的所有被动副本执行完整种子重新设定。

Exchange 备份或还原失败

Exchange 备份或还原失败，并显示以下 VSS API 错误:

[正常] 来自: OB2BAR_E2010_BAR@exch03.e2010.company.com "MS Exchange 2010+ Server" 时间: 8/29/2016 2:10:55 PM 正在初始化 DP VSS 接口。 [正常] 来自: OB2BAR_E2010_BAR@exch03.e2010.company.com "MS Exchange 2010+ Server" 时间: 8/29/2016 2:10:55 PM 正在通过 DP VSS 接口启动备份。 [严重] 来自: OB2BAR_E2010_BAR@exch03.e2010.company.com "MS Exchange 2010+ Server" 时间: 8/29/2016 2:10:55 PM 从 DP VSS API 返回错误 3。 [正常] 来自: BSM@as-backup-01.jenoptik.corp "mx_test_db40" 时间: 8/29/2016 2:12:01 PM "exch03.e2010.company.com" 上的 OB2BAR 应用程序已断开。

解决方案

如果客户机不受保护，则从未能执行备份或还原操作的 Exchange 数据库服务器中删除文件 C:\ProgramData\OmniBack\config\client\allow_hosts 。如果客户机受保护，除了将 Cell Manager FQDN 添加到 Exchange 数据库服务器上的 allow_hosts 文件之外，还要添加 Exchange 数据库服务器 FQDN。

集合已经包含使用方案 **http** 的地址

首次安装或对 IIS 服务器进行任何更改时，Exchange GRE 无法打开。它因管理单元错误而失败，并且当您尝试打开管理单元页面时，将显示以下内容：

This collection already contains an address with scheme http. There can be at most one address per scheme in this collection. If your service is being hosted in IIS you can fix the problem by setting 'system.serviceModel/serviceHostingEnvironment/multipleSiteBindingsEnabled' to true or specifying 'system.serviceModel/serviceHostingEnvironment/baseAddressPrefixFilters'."

原因

发生此错误的原因是，http 端口号 443 已被另一个应用程序使用，并且 IIS 服务器未配置为处理对同一端口的多次绑定。

解决方案

配置 IIS 服务器以处理多个端口绑定。与供应商 (Microsoft) 联系以对其进行配置。

Microsoft Exchange Single Mailbox 集成故障诊断

This feature is available in the Premium Edition

本节列出了常规检查和验证以及在使用 Data Protector Exchange Single Mailbox 集成时可能会遇到的问题。从问题开始。如果在这里找不到解决方案，请执行常规检查和验证。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 确保 Data Protector Cell Manager 上存在以下目录:

  Data_Protector_program_data\config\server\barlists\Mailbox

  Data_Protector_program_data\config\server\barschedules\Mailbox

- 检查 Exchange Server 系统上默认 Data Protector 日志文件目录下 debug.log 文件中报告的错误。

此外，如果备份或还原失败:

- 确保在 Exchange Server 系统上正确指定 Cell Manager: 确保密钥下存在名为 CellServer 且值为 "Cell Manager" 的值条目:

  HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack II\Site

- 检查 Windows 事件日志中记录的错误。

此外，如果您的备份失败:

- 预览 Data Protector Exchange Single Mailbox 备份。

  如果预览的 Exchange Server 部分失败，请确保 Exchange Server 处于联机状态。

  如果预览的 Data Protector 部分失败:

  - 请确保已将 Exchange Server 配置为用于 Data Protector。
  - 创建 Exchange Single Mailbox 备份规范以备份到空设备或文件设备。

    如果备份成功，则问题可能与设备有关。

问题

以下是使用 Data Protector Exchange 单邮箱集成时可能遇到的一些问题：

您无权登录系统

debug.log（位于 Exchange Server 上）包含以下消息之一：

```
错误 = 596 登录失败: 尚未对用户 授予此计算机的请求登录类型。
```

或：

[MBX_ImpersonateUser] A required privilege is not held by the client.

解决方案

检查域控制器系统是否已定义域级别策略设置。转到：

Start >“设置”>“控制面板” >“管理工具” > “域安全策略”> “本地策略”> User Rights Assignment

然后，检查“用作操作系统的一部分”和“作为服务登录”用户权限是否均设置为“已定义”。

如果定义了域级别策略设置:

1. 在域控制器系统上:
   a. 转到：
      Start >“设置” >“控制面板” >“管理工具” >“域安全策略” >“本地策略” >“用户权利分配” 。
   b. 为 Exchange Server 管理员设置“用作操作系统的一部分”和“作为服务登录”用户权限。
   c. 执行：
      secedit /refreshpolicy machine_policy /enforce
2. 在 Exchange Server 系统上:
   a. 从系统注销，然后使用同一用户帐户重新登录。
   b. 转到：
      Start >“设置” >“控制面板” >“管理工具” >“本地安全策略” >“本地策略” >“用户权利分配” 。
   c. 确保在“本地设置”和“有效设置”列中为 Exchange Server 管理员设置了“用作操作系统的一部分”和“作为服务登录”用户权限。
   d. 重新启动 Data Protector Inet 服务。

如果未定义域级别策略设置:

1. 登录 Exchange Server 系统。
2. 转到：
   Start >“设置” >“控制面板” >“管理工具” >“本地安全策略” >“本地策略” >“用户权利分配” 。
3. 为 Exchange Server 管理员设置“用作操作系统的一部分”和“作为服务登录”用户权限。
4. 从系统注销，然后使用同一用户帐户重新登录。
5. 重新启动 Data Protector Inet 服务。

Exchange Server 配置失败

debug.log（位于 Exchange Server 系统上）包含以下消息：

An error has occurred while creating a profile administration object.

解决方案

1. 登录 Exchange Server 系统。
2. 删除不正确的管理员配置文件：

   mbx_bar.exe delete
3. 手动新建配置文件：

   mbx_bar.exe create
4. 在“选择配置文件”页中，单击“新建”。
5. 按照设置向导操作。输入 $$$Data Protector 作为配置文件名称。指定 Exchange Server 系统和 Exchange Server 管理员邮箱的名称。

还原到另一个客户机失败

解决方案

确保在要还原到的目标系统上安装并配置了 Exchange Server 和 Data Protector **MS Exchange 集成**组件。

还原到其他邮箱失败

解决方案

确保目标 Exchange Server 系统上存在目标邮箱。

Microsoft Exchange Single Mailbox 备份失败

从 Data Protector 10.xx 成功升级到 10.40 及更高版本后，现有的 MS Exchange 2010 Single Mailbox 备份将失败，并且无法创建或集成新的备份。

原因

此错误的原因未知。

解决方案

在 MS Exchange 2010 客户机上，替换以下文件并重命名原始文件 (可选)。

- 从 Data Protector 安装仓库服务器位置，将文件 **vcruntime140.dll** 复制到 MS Exchange 2010 客户机邮箱路径 *C:\Program Files\OmniBack\bin*。
- 从 MS Exchange 2010 邮箱客户机，将文件 **omnilibeay32.dll** 从 *C:\Program Files\OmniBack\lib\i386* 复制到 *C:\Program Files\OmniBack\bin*。
- 从 MS Exchange 2010 邮箱客户机，将文件 **omnissleay32.dll** 从 *C:\Program Files\OmniBack\lib\i386* 复制到 *C:\Program Files\OmniBack\bin*。

Microsoft SharePoint Server 集成故障诊断

本节列出了常规检查和验证以及在使用 Data Protector Microsoft SharePoint Server 集成时可能会遇到的问题。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 在客户机系统上，检查 debug.log 文件中报告的系统错误，该文件位于默认 Data Protector 日志文件目录中。
- 检查您是否可以在有问题的客户机上执行文件系统备份和还原。
- 检查是否已正确设置环境。要列出可用系统和服务，可执行 sharepoint_bar.exe -farmtree 命令，该命令将列出具有可备份的持久数据的所有服务器。不会列出不支持的服务 (FAST 搜索、前端 Web 服务器系统等)。

此外，如果配置或备份失败:

- 确保 Microsoft SharePoint Server 和 Microsoft SQL Server 实例处于联机状态。

问题

下面是使用 Data Protector Microsoft SharePoint Server 集成时可能遇到的一些问题。

不支持单服务器场还原

当为 SharePoint Central Administrator 服务器配置了单个服务器场角色时，场还原将失败。

原因

发生这种情况是因为单个服务器场角色不允许重新配置 SharePoint_configdb 。

解决方案

配置多服务器场角色。

要使用 Microsoft SharePoint Server 2016 配置多服务器场角色，请安装并应用以下于 2019 年 11 月发布的 minrole 补丁:

- https://www.microsoft.com/en-us/download/details.aspx?id=54210(KB3127942)
- https://www.microsoft.com/en-us/download/details.aspx?id=54205(KB3127940)

对于 Microsoft SharePoint Server 2019，安装程序随附 minroles。

要在中央管理员中更改角色，请转至“系统设置”>> 在场中转换服务器角色 。

从下拉列表中选择一个用户角色。例如：带有搜索的应用程序。

更改角色时，请按照屏幕上的说明进行操作。

在内容数据库上备份和还原期间的权限问题

在内容数据库的备份和还原期间，发生与权限相关的警告和错误。

原因

如果配置的用户权限存在问题，则会发生这些警告和错误。

解决方案

验证用于创建、执行或还原数据库的用户角色权限。还要验证在 NTAuthority 和其他场用户中分配的角色。

发生抓取状态错误

在 Microsoft SharePoint Server 环境中还原配置数据库后，发生爬网状态错误。

显示以下消息：

503 Service unavailable.

原因

发生这种情况的原因如下: 在还原配置数据库之前断开所有 Microsoft SharePoint Server 客户机之后，会从 IIS (Internet Information Services 虚拟目录/IIS 数据库) 中删除 Search Service 应用程序应用程序池。

解决方案

转至“管理中心”页中的“管理服务应用程序”，然后将新的应用程序池 (搜索管理 Web 服务的应用程序池以及搜索查询和站点设置 Web 服务的应用程序池) 分配给 Search Service 应用程序。

共享服务提供程序 (SSP) 的还原失败

在还原多个 SSP 期间，还原会话管理器会在 10 分钟后中止会话。

删除 SSP 需要的时间可能比会话管理器等待与客户机建立连接的时间 (默认为 10 分钟) 更长。

解决方案

将全局选项 SmWaitForFirstRestoreClient 设置为适当的值，或者升级场客户机的资源。

备份失败，并显示错误“未安装 MS SQL 集成”

如果 Microsoft SQL Server 系统配置了别名，并且 Microsoft SharePoint Server 配置使用 SQL Server 系统别名，则备份会话将失败，并显示类似于以下内容的错误:

[Critical] From: OB2BAR_SHAREPOINT@Domain Database Time: Date Time 'MS SQL' integration not installed on.

解决方案

1. 确保每个 Microsoft SharePoint Server 系统上都安装了 Microsoft SQL Server 管理对象 (SMO)。
2. 在每个 Microsoft SharePoint Server 系统上安装 Data Protector Microsoft SharePoint Server 集成 DPWIN_00574 或更高版本的补丁。

备份失败，并显示错误“客户机没有所需的特权”

备份会话失败，并显示类似于以下内容的错误:

[70:24] A system error occurred when starting the target script or an agent module. The system error code reported is 1314 and the message resolves to '[1314] A required privilege is not held by the client.'.

解决方案

1. 转到：

   “控制面板”>“管理工具”>“本地安全策略”

2. 展开“本地政策”，然后选择“用户权限分配”。
3. 必须向 Data Protector Inet 服务启动备份时使用的 Windows 域用户 (即场管理员) 授予“替换进程级别令牌”用户权限。

无法浏览实例

在 SharePoint 备份配置期间，将显示类似于以下内容的错误:

Unable to browse instances

原因

如果在 Data Protector 安装期间缺少 **sharepoint_bar.exe.config.tmpl** 文件，则会出现此问题。要复制 sharepoint_bar.exe.config.tmpl 文件，请完成以下步骤:

解决方案

1. 导航到 Data Protector bin 目录，然后验证是否缺少 **sharepoint_bar.exe.config** 文件。
2. 在所有 SharePoint 服务器上手动将 **sharepoint_bar.exe.config.tmpl** 文件复制到 **sharepoint_bar.exe.config**，然后重试该操作。例如， C:\Program Files\OmniBack\bin>copy sharepoint_bar.exe.Config.tmpl sharepoint_bar.exe.config

如果可用性组侦听器将默认端口与命名实例复本结合使用，则备份将失败

如果可用性组侦听器端口设置为默认值 (1433) 并且使用命名实例配置了 SQL Server 复本，则备份将失败并显示以下错误消息:

[严重] 来自: OB2BAR_SQLBAR@server.domain“数据库” 时间: 日期时间

虚拟设备接口报告的错误:

对象未打开。

有关详细信息，另请参阅 debug.log 和 SQL Server 错误日志。

解决方案

在开始备份之前，必须在每个 SharePoint 系统上设置服务器别名。必须满足以下先决条件:

- 服务器别名必须与实际的可用性组侦听器名称完全匹配。
- 网络库必须设置为 TCP/IP。
- 服务器名称必须设置为实际的侦听器名称。
- 端口号必须设置为 **1433** - SQL Server 默认端口号。

基于 Microsoft SharePoint Server VSS 的解决方案集成故障诊断

This feature is available in the Premium Edition

本节列出常规检查和验证以及在使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案时可能会遇到的问题。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果浏览、备份或还原操作失败:

- 检查 debug.log 文件中报告的系统错误。
- 检查您是否可以在有问题的客户机上执行文件系统备份和还原。

问题

以下是使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案时可能遇到的一些问题：

还原后无法连接到管理中心网页

还原后，在尝试连接到 Microsoft SharePoint 管理中心网页时，Web 浏览器中将显示类似于以下内容的错误:

Windows Internet Explorer :

Retrieving the COM class factory for component with CLSID (BDEADEE2–C265–11D0–BCED-00A0C90AB50F) failed due to the following error 800703fa.

Mozilla Firefox:

An unexpected error has occurred.

解决方案

1. 在场中的所有客户机上重新启动 Microsoft SharePoint Server 服务。
2. 打开 Internet Information Services (IIS) 管理器，然后重新启动所有应用程序池。
3. 如果应用程序池无法重新启动，并显示以下错误:

   Cannot Restore Application Pool. There was an error while performing this operation.

   等待几秒钟，然后重新启动该操作。
4. 在 Web 浏览器中删除浏览历史记录。
5. 登录管理中心网页。

无法恢复服务 Windows SharePoint Services 帮助搜索

启动备份会话时，将显示类似于以下内容的错误:

Service Windows SharePoint Services Help Search on host

MOSS07-INDEX

-> Resuming background activity ...

ERROR: Failed to resume Service Windows SharePoint Services Help Search

on host MOSS07-INDEX

Web site URL: http://moss07-web:2001

Root title: as

-> Resuming background activity

解决方案

执行：

SharePoint_VSS_backup.ps1–resumefarm

还原后静默操作失败

还原配置数据库并执行 SharePoint_VSS_backup.ps1–resumefarm 后，前端 Web Server 系统上 Microsoft SharePoint Server 文件系统缓存中的数据将与刚刚还原的配置数据库数据不一致。如果尝试静默场，则该操作将失败并显示以下错误:

用户界面中发生未处理的异常。异常 信息: 发生了更新冲突，必须重试 此操作。对象 SessionStateService Parent=SPFarm Name=< farm_config_database_name > 正在由 < domain\username > 在计算机 < servername > 上的 w3wp 进程中进行更新。有关冲突的详细信息， 请查看跟踪日志。

解决方案

清除场中所有服务器系统上的 Microsoft Office SharePoint Server 文件系统缓存。

还原后无法连接到 **FAST Search** 服务器

还原后，当尝试连接到适用于 SharePoint 的 Microsoft FAST Search Server 2010 系统时，操作失败。

FAST Query SSA 搜索操作将显示类似于以下内容的错误:

```
The search request was unable to connect to the Search Service.
```

解决方案

执行：

```
SharePoint_VSS_backup.ps1 -resumecert
```

> **注意**基于 VSS 的解决方案会将 FAST Search 证书 FASTSearchCert.pfx 从 FAST Admin Server 系统复制到 SharePoint Server 系统并进行安装。此外，还会复制 SharePoint 证书并将其安装到所有 FAST Search Server 系统。

SharePoint_VSS_backup.ps1 脚本停止响应

启动备份时， SharePoint_VSS_backup.ps1 脚本在执行 Microsoft SharePoint Server 爬网时停止响应。SSA 索引损坏、需要手动重新颁发证书等外部条件可能导致此问题。

因此，场将保持只读模式。

解决方案

通常，爬网应在 15 分钟后自动中止。如果没有中止:

1. 通过按 **Ctrl**+**C** 中止脚本。
2. 手动恢复场。

可以指定其他超时，在此超时之后，将使用 -timeout 选项中止爬网并恢复场。

还原后，SharePoint 搜索服务应用程序无法运行

还原 SharePoint 搜索服务应用程序 (SSA) 并恢复 SharePoint Server 2013 场后，SSA 状态将读为暂停: 外部请求而不是正在运行，表示 SSA 无法运行。

解决方案

执行以下步骤：

1. 使用 SharePoint Online Server 命令管理程序，导出 SharePoint 搜索服务应用程序 (SSA) 拓扑:

   ```
   $ssa = Get-SpenterpriseSearchServiceApplication -Identity "NameOfSSA"

   Export-SPEnterpriseSearchTopology -SearchApplication $ssa -Filename "TopologyFilename.xml"
   ```

2. 记录 SSA 应用程序池标识 (如果存在):

   ```
   $ssaAppPool = $ssa.ApplicationPool
   ```

   如果不存在，则通过执行以下命令进行创建:

   ```
   $ssaAppPool = New-SPServiceApplicationPool -name "ApplicationPoolName" -account "Domain\Username"
   ```

3. 执行以下命令删除 SSA:

   ```
   $ssa = Get-SPEnterpriseSearchServiceApplication -Identity "NameOfSSA"

   Remove-SPEnterpriseSearchServiceApplication -Identity $ssa -RemoveData

   Remove-SPEnterpriseSearchServiceApplicationProxy -Identity "NameOfSSAProxy"
   ```

4. 通过 Data Protector Microsoft 卷影复制服务集成，使用 Microsoft SQL Server VSS 写入程序还原 SSA 数据库。确保数据库名称以 SSA 的名称开头。
5. 使用 SharePoint Online Server 命令管理程序，通过执行以下命令还原 SSA 本身:

   ```
   Restore-SPEnterpriseSearchServiceApplication -Name "NameOfSSA" -ApplicationPool $ssaAppPool -TopologyFile "TopologyFilename.xml" -KeepId
   ```

6. 通过执行以下命令创建 SSA 代理:

   ```
   $ssa = Get-SPEnterpriseSearchServiceApplication -Identity "NameOfSSA"

   New-SPEnterpriseSearchServiceApplicationProxy -Name "NameOfSSAProxy" -SearchApplication $ssa
   ```

7. 在安装了 SSA 索引组件的所有系统上停止 SharePoint 搜索主控制器服务。执行以下命令:

   ```
   Stop-Service SPSearchHostController
   ```

8. 通过 Data Protector Microsoft 卷影复制服务集成，使用 OSearch VSS 写入程序还原 SSA 索引文件。
9. 使用 SharePoint Online Server 命令管理程序，在安装了 SSA 索引组件的所有系统上启动 SharePoint 搜索主控制器服务:

   ```
   Start-Service SPSearchHostController
   ```

10. 通过执行以下命令恢复 SSA:

    ```
    $ssa = Get-SpenterpriseSearchServiceApplication -Identity "NameOfSSA"

    Resume-SPEnterpriseSearchServiceApplication $ssa
    ```

Microsoft SQL Server 集成故障诊断

This feature is available in the Premium Edition

本节列出了常规检查和验证以及在使用 Data Protector SQL Server 集成时可能会遇到的问题。从问题开始。如果在这里找不到解决方案，请执行常规检查和验证。

开始之前

- 确保已安装最新的 Data Protector 官方修补程序。

检查和验证

如果配置、备份或还原失败:

- 检查 SQL Server 服务是否正在运行。
- 检查在 SQL Server 客户机的 debug.log 中报告的系统错误。

  此外，检查 MSSQL\log 目录中的 errorlog 和 VDI.log 文件。
- 对有问题的客户机进行测试文件系统备份和还原。
- 检查与 Data Protector 一起使用的每个 SQL Server 是否都安装了“MS SQL 集成”组件。
- 使用与 Data Protector“配置”对话框中指定的登录 ID 相同的登录 ID，通过 SQL Server 企业管理器连接到 SQL Server。
- 使用 SQL Server 企业管理器执行数据库备份。如果备份失败，则修复任何 SQL Server 问题，然后使用 Data Protector 执行备份。

此外，如果您的备份失败:

- 验证配置文件以检查是否在 SQL Server 上正确设置了 Cell Manager。
- 如果在创建备份规范时您未将 SQL Server 实例视为应用程序数据库，则输入实例名称。如果未显示“未命名的实例”，则插入 DEFAULT 字符串。
- 如果 Data Protector 报告已正确配置集成，则验证 SQL Server 用户是否具有访问所需数据库的适当权限。

在主数据库还原期间，执行 SQL 语句时会发生以下错误:

```
执行 SQL 语句时发生错误。 错误消息: 'SQLSTATE:[42000] CODE:(3108) MESSAGE:[Microsoft] [ODBC SQL Server Driver][SQL Server] 要还原主数据库，服务器必须以单用户模式运行。有关 以单用户模式开始的信息，请参阅“如何: 启动 SQL Server 实例 (sqlservr.exe)”(在“联机丛书”中)。
```

请注意，未在单用户模式下还原主数据库时，预计会出现此行为。

问题

下面是使用 Data Protector SQL Server 集成时可能遇到的一些问题。

超时后数据库备份失败

- 显示类似下面的错误:

  ```
  [警告] 来自：OB2BAR@computer.company.com "SQLSRV" 时间: 7/29/2011 8:19:22 PM 执行 SQL 语句时发生错误。 [Microsoft][ODBC SQL Server Driver][SQL Server] 备份或还原 操作异常终止。' [严重] 来自: OB2BAR@computer.company.com "SQLSRV" 时间: 7/29/11 8:19:24 PM 从 SM 接收到“中止”请求 => 正在中止
  ```

- SQL Server 错误日志包含类似于下面的条目:

  ```
  2011-07-29 20:19:21.62 kernel BackupVirtualDeviceSet::初始化: 打开备份 设备 'Data_Protector_master' 失败。 Operating system error - 2147024891(Access is denied.).
  ```

- SQL Server VDI.LOG 文件包含类似于下面的条目:

  ```
  2011/07/30 13:19:31 pid(2112) BuildSecurityAttributes 错误: SetSecurityDescriptorDacl 状态代码: 1338, x53A Explanation: 安全描述符 结构无效。
  ```

SQL Server 服务和 Data Protector Inet 在不同的帐户下运行。由于安全问题，集成无法访问 SQL Server。

解决方案

在 SQL Server 服务运行的同一帐户下重新启动 Data Protector Inet 服务。

备份失败并显示“对象未打开”错误

备份 Microsoft SQL Server 数据库时会话失败，并显示类似于以下的错误:

[Critical]From : OB2BAR_Main@wemaoldb2dr "Aolins" Time:11/12/2011 02:01:34 AM Microsoft SQL Server reported the following error during login : The object was not open

原因

如果 SQL Server Browser 服务未运行，则可能会出现此错误。

解决方案

请执行以下操作：

1. 启动 SQL Server Browser 服务。
2. 启动新的备份会话。

如果并发设置为多个，则备份失败

如果并发设置为多于一个并且其中一个设备出现故障或根本未启动，则备份将失败。

原因

这可能是介质错误导致的。

解决方案

将设备并发数设置为 1 或替换无效介质。

从对象复制还原失败

当尝试从对象复制会话还原 SQL Server 数据库时，还原失败。

使用多个流备份的 SQL Server 数据库 (“并发流”选项设置为大于 1) 只有在流创建的备份对象驻留在单独的介质上时才能还原。在 Data Protector Microsoft SQL Server 备份期间，每个流始终备份到单独的介质。但是，如果使用对象复制功能在同一介质上复制这些备份对象，并从对象复制会话启动还原，则还原将失败。

原因

如果使用对象复制功能在同一介质上复制这些备份对象，并从对象复制会话启动还原，则会发生此问题。

解决方案

在重新启动还原之前:

1. 增加设备的磁盘代理缓冲区数量。
2. 在“内部数据库”上下文中，查找属于同一备份的对象 (由相同的备份 ID 标识)。
3. 将单独的对象复制会话中的每个对象复制到单独的设备，例如文件库。对于每个对象，请使用具有不可追加介质策略的单独介质。
4. 为新创建的副本设置最高介质位置优先级。

还原 SQL 数据库时会话失败

还原 SQL 数据库时会话失败，并显示以下错误消息:

```
[正常] 来自: OB2BAR_<dbname>_0@<Hostname> "<Instance>" 时间: <Date> <Time>
```

```
[152:9209] 清零操作前的数据库文件。
```

```
[重大] 来自: RSM@<Hostname> "" 时间: <Date> <Time>
```

```
[61:1002] 在主机 <Hostname> 上的名为 "MSSQL" 的 OB2BAR 还原 DA
```

```
已达到其闲置超时时间 14400 秒。
```

主机上的代理即将关闭。

原因

发生此错误的原因是 DA 闲置超时。

解决方案

要成功还原 SQL 数据库，请增加 Da 和 Ma 空闲超时时间 (SmDaIdleTimeout 和 SmMaIdleTimeout)。

差异备份的还原失败

如果差异备份驻留在一个以上的磁带上，使得完整备份位于一个磁带上，而差异备份位于另一磁带上，则差异备份的还原将失败。

原因

如果差异备份驻留在多个磁带上，则会发生此问题。

解决方案

请执行以下操作：

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开“还原对象”、“MS SQL Server”，然后选择要从中还原的 Microsoft SQL Server。此时将在“结果区域”中显示备份对象的列表。
3. 在“设备”选项卡中，选择选项“原始设备选择”。
4. 单击“还原”以启动还原操作。

数据库处于未恢复状态

数据库保持未恢复状态，就像在“不对数据库执行任何操作”情况下运行“还原日志”操作一样。

解决方案

使用 SQL 查询分析器将数据库恢复到最新时间点:

RESTORE DATABASE *database_name* WITH RECOVERY

恢复后，无法应用其他事务日志。

还原成功完成后，数据库留置于未恢复状态

如果将“停止于”时间设置为超出“还原日志”操作的结束时间，则数据库保持未恢复状态，就像在“不对数据库执行任何操作”情况下运行“还原日志”操作一样。

解决方案

使用 SQL 查询分析器将数据库恢复到最新时间点:

```
RESTORE DATABASE database_name WITH RECOVERY
```

恢复后，无法应用其他事务日志。

还原到另一个客户机失败

还原到未配置为使用 SQL Server 的 Data Protector 单元中的另一客户机失败。

原因

如果未在客户机上配置 SQL Server 集成，则会发生此问题。

解决方案

在此客户机上配置 SQL 集成。

数据库还原失败

还原会话中止，并显示类似于下面的主要错误: 尚未备份数据库 "test2" 的日志结尾。

Error has occurred while executing a SQL statement.Error message: 'SQLSTATE:[42000] CODE:(3159) MESSAGE:[Microsoft][ODBC SQL Server Driver][SQL Server]The tail of the log for the database "test2" has not been backed up. Use BACKUP LOG WITH NORECOVERY to backup the log if it contains work you do not want to lose. Use the WITH REPLACE or WITH STOPAT clause of the RESTORE statement to just overwrite the contents of the log. SQL STATE:[42000] CODE:(3013) MESSAGE:[Microsoft][ODBC SQL Server Driver][SQL Server]RESTORE DATABASE is terminating abnormally.

原因

发生此错误的原因是尚未备份数据库 "test2" 的日志结尾。

解决方案

要解决问题，请在重新启动还原会话之前执行以下操作之一:

- 选择还原选项“启用结尾日志备份”(推荐)。
- 执行事务日志备份以获取最新的事务日志。

在启用结尾日志备份的日志传送配置中还原数据库失败

在 Microsoft SQL Server 日志传送配置中，运行 Data Protector 时它将执行差异数据库备份而非事务日志备份。进行自动备份类型切换时还进行结尾日志备份。在这些情况下，数据库备份链不包含来自日志尾部的最新事务。如果尚未备份目标数据库的日志尾部，则 Microsoft SQL Server 不允许通过此数据库还原。

解决方案

执行以下某个操作后重新启动还原会话:

- 禁用 Microsoft SQL Server 日志传送。
- 为所有涉及的数据库启用选项“通过现有数据库进行强制还原”。

> **警告**
>
> 涉及的所有数据库的日志尾部都将丢失。

Microsoft SQL Server ZDB 集成故障诊断

This feature is available in the Premium Edition

本节列出了常规检查和验证以及在使用 Data Protector SQL Server ZDB 集成时可能会遇到的问题。从问题开始。如果在这里找不到解决方案，请执行常规检查和验证。

开始之前

- 确保已安装最新的 Data Protector 官方修补程序。

检查和验证

如果配置、备份或还原失败:

- 检查 SQL Server 服务是否正在运行。
- 检查在 SQL Server 客户机的 debug.log 中报告的系统错误。

  此外，检查 MSSQL\log 目录中的 errorlog 和 VDI.log 文件。
- 对有问题的客户机进行测试文件系统备份和还原。
- 检查与 Data Protector 一起使用的每个 SQL Server 是否都安装了“MS SQL 集成”组件。
- 使用与 Data Protector“配置”对话框中指定的登录 ID 相同的登录 ID，通过 SQL Server 企业管理器连接到 SQL Server。
- 使用 SQL Server 企业管理器执行数据库备份。如果备份失败，则修复任何 SQL Server 问题，然后使用 Data Protector 执行备份。

此外，如果您的备份失败:

- 验证配置文件以检查是否在 SQL Server 上正确设置了 Cell Manager。
- 如果在创建备份规范时您未将 SQL Server 实例视为应用程序数据库，则输入实例名称。如果未显示“未命名的实例”，则插入 DEFAULT 字符串。
- 如果 Data Protector 报告已正确配置集成，则验证 SQL Server 用户是否具有访问所需数据库的适当权限。

在主数据库还原期间，执行 SQL 语句时会发生以下错误:

```
执行 SQL 语句时发生错误。 错误消息: 'SQLSTATE:[42000] CODE:(3108) MESSAGE:[Microsoft] [ODBC SQL Server Driver][SQL Server] 要还原主数据库，服务器必须以单用户模式运行。有关 以单用户模式开始的信息，请参阅“如何: 启动 SQL Server 实例 (sqlservr.exe)”(在“联机丛书”中)。
```

请注意，未在单用户模式下还原主数据库时，预计会出现此行为。

问题

下面是使用 Data Protector SQL Server ZDB 集成时可能遇到的一些问题。

超时后数据库备份失败

- 显示类似下面的错误:

  ```
  [警告] 来自：OB2BAR@computer.company.com "SQLSRV" 时间: 7/29/2011 8:19:22 PM 执行 SQL 语句时发生错误。 [Microsoft][ODBC SQL Server Driver][SQL Server] 备份或还原 操作异常终止。' [严重] 来自: OB2BAR@computer.company.com "SQLSRV" 时间: 7/29/11 8:19:24 PM 从 SM 接收到“中止”请求 => 正在中止
  ```

- SQL Server 错误日志包含类似于下面的条目:

  ```
  2011-07-29 20:19:21.62 kernel BackupVirtualDeviceSet::初始化: 打开备份 设备 'Data_Protector_master' 失败。 Operating system error - 2147024891(Access is denied.).
  ```

- SQL Server VDI.LOG 文件包含类似于下面的条目:

  ```
  2011/07/30 13:19:31 pid(2112) BuildSecurityAttributes 错误: SetSecurityDescriptorDacl 状态代码: 1338, x53A Explanation: 安全描述符 结构无效。
  ```

SQL Server 服务和 Data Protector Inet 在不同的帐户下运行。由于安全问题，集成无法访问 SQL Server。

解决方案

在 SQL Server 服务运行的同一帐户下重新启动 Data Protector Inet 服务。

备份失败并显示“对象未打开”错误

备份 Microsoft SQL Server 数据库时会话失败，并显示类似于以下的错误:

[Critical]From : OB2BAR_Main@wemaoldb2dr "Aolins" Time:11/12/2011 02:01:34 AM Microsoft SQL Server reported the following error during login : The object was not open

原因

如果 SQL Server Browser 服务未运行，则可能会出现此错误。

解决方案

请执行以下操作：

1. 启动 SQL Server Browser 服务。
2. 启动新的备份会话。

如果备份系统上的相应驱动器号不存在，则备份将失败

备份失败并显示类似于下面的错误:

```
[重大] 来自: SSEA@computer1.com "" 时间: 02-Feb-11 14:07:54 文件系统 \\.\Volume{ef58fe0e-b2b8-11db-aa08-000802804af6} 无法装载 到
Q:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\。 ([87] 参数不正确。）。
```

原因

备份失败，因为 SSE 代理尝试将文件系统装载到备份系统上不存在的驱动器号上。驱动器号必须与应用程序系统中的相同。SSE 或 SMI-S 代理始终将文件系统装载到备份系统上的相同驱动器号上，就像 ZDB_PRESERVE_MOUNTPOINTS omnirc 选项设置为 1 一样。

解决方案

要成功复制源卷，请在备份系统上创建与在应用程序系统上装载源卷所用驱动器号相同的驱动器号。

在报告“为 STOPAT 参数指定了无效值”之后，数据库留置于未恢复状态

数据库保持未恢复状态，就像在“不对数据库执行任何操作”情况下运行“还原日志”操作一样。

解决方案

使用 SQL 查询分析器将数据库恢复到最新时间点:

RESTORE DATABASE *database_name* WITH RECOVERY

恢复后，无法应用其他事务日志。

无法从磁带还原事务日志

恢复成功完成，且数据库处于 norecovery 状态，但无法从磁带还原事务日志。

解决方案

使用 SQL 查询分析器将数据库恢复为 ZDB 到磁盘的状态:

```
RESTORE DATABASE database name WITH RECOVERY
```

恢复后，无法应用其他事务日志。

SQL Server 数据库的即时恢复失败

SQL Server 数据库的即时恢复失败。

显示以下错误:

```
[严重] 自: computer@company.com "(默认)" 时间: 4/9/2011 7:01:42 PM Microsoft SQL Server 在登录期间报告了以下错误: 对象未打开。 [警告] 自: computer@company.com "(默认)" 时间: 4/9/2011 7:01:42 PM [152:9208] Data Protector 可能未配置为用于此主机上的 SQL Server。
```

原因

如果 SQL Server 服务在即时恢复之前脱机，则会发生此错误。

解决方案

执行以下某个操作：

- 将 Data Protector omnirc 选项 OB2_SQLRESTORE_STARTSRV 设置为 1 ，该选项在恢复 SQL 数据库之前启动 SQL Server 服务。

  在主数据库还原期间，显示以下错误:

  ```
  不支持带有快照的还原主数据库。
  ```

  请注意，此行为在预期中。即时恢复之后无需进一步的步骤。

- 即时恢复完成后重新启动 SQL Server 实例服务。如果重新启动服务未自动启动所有系统数据库的恢复，请以单用户模式启动 SQL Server 实例并手动启动主数据库的恢复。对其他系统数据库执行相同的过程。最后，重新启动 SQL Server 实例服务。

还原到另一个客户机失败

还原到未配置为使用 SQL Server 的 Data Protector 单元中的另一客户机失败。

原因

如果未在客户机上配置 SQL Server 集成，则会发生此问题。

解决方案

在此客户机上配置 SQL Server 集成。

还原成功完成后，数据库留置于未恢复状态

数据库保持未恢复状态，就像在“不对数据库执行任何操作”情况下运行“还原日志”操作一样。

原因

如果您将“停止于” 时间设置为超出 “还原日志”操作的结束时间，则会发生此问题。

解决方案

使用 SQL 查询分析器将数据库恢复到最新时间点:

```
RESTORE DATABASE database_name WITH RECOVERY
```

恢复后，无法应用其他事务日志。

Microsoft SQL Server 数据库的即时恢复失败

在 Microsoft 群集服务器系统上的 Business Copy 配置中即时恢复 Microsoft SQL Server 数据失败，并显示以下错误:

[Microsoft][ODBC SQL Server Driver][SQL Server]Device activation error.

The physical file name '< Data/Log filename>' may be incorrect.

解决方案

执行以下步骤：

1. 使用 Microsoft SQL Server 企业管理器分离要恢复的 Microsoft SQL Server 数据库。
2. 使用群集管理器使 Microsoft SQL Server 磁盘资源脱机。
3. 在应用程序系统上，配置 ZDB_TAKE_CLUSRES_ONLINE omnirc 选项。
4. 启动即时恢复。
5. 当 Data Protector GUI 中出现消息“请使 MS SQL 群集资源联机”时，使用群集管理器使 Microsoft SQL Server 群集资源联机。

数据库还原失败

还原会话中止，并显示类似于下面的主要错误:

Error has occurred while executing a SQL statement.Error message: 'SQLSTATE:[42000] CODE:(3159) MESSAGE:[Microsoft][ODBC SQL Server Driver][SQL Server]The tail of the log for the database "test2" has not been backed up. Use BACKUP LOG WITH NORECOVERY to backup the log if it contains work you do not want to lose. Use the WITH REPLACE or WITH STOPAT clause of the RESTORE statement to just overwrite the contents of the log. SQL STATE:[42000] CODE:(3013) MESSAGE:[Microsoft][ODBC SQL Server Driver][SQL Server]RESTORE DATABASE is terminating abnormally.

解决方案

要解决问题，执行事务日志备份以获取最新的事务日志。

Microsoft 卷影复制服务集成故障诊断

This feature is available in the Premium Edition

本主题列出使用 Data Protector Microsoft 卷影复制服务集成时可能遇到的问题。

开始之前

- 确已安装最新的正式补丁。

检查和验证

- 在应用程序和备份系统上，检查 debug.log 文件中报告的系统错误。
- 通过 P9000 XP 阵列集成，确保 RAID 管理器库已正确安装在应用程序和备份系统上。此外，检查 *RMLIB_home* 目录中是否存在 libsvrrm.dll 文件。
- Data Protector 单元中所有客户机的名称必须与 DNS 条目和 Data Protector cell_server 文件条目相匹配。如果名称不匹配，则显示警告消息。在这种情况下，请不要使用 VSS 集成，因为它的行为可能会变得无法预测。首先在客户机上重置网络设置，然后重新导入客户机。

问题

下面是使用 Data Protector Microsoft 卷影复制服务集成时可能遇到的一些问题：

Microsoft Exchange Server 写入程序备份失败

启动 Microsoft Exchange Server 写入程序的备份时，显示以下错误:

```
[重大]: 写入程序 'Microsoft Exchange Writer' 无法准备 要备份的文件。
```

原因

原因可能是由于 Microsoft Exchange Server 问题导致先前的备份失败，Exchange Server Writer 无法执行正确的清理。

解决方案

重新启动信息存储。

Microsoft Exchange Server 中止备份

如果卷影副本创建时间超过 20 秒，则 Microsoft Exchange Server 将中止备份

如果正在备份 Exchange Server 写入程序，则会话可能会失败，并且 VSSBAR 报告：

```
无法创建快照。
```

在应用程序系统上的应用程序事件日志中，记录以下事件：

```
事件类型：错误 事件来源: ESE 事件 类别: (16) 事件 ID: 2004 Information Store (4916) 卷影副本 3 超时 (20000 毫秒)。
```

解决方案

以下方法可以帮助解决问题：

- 限制同时访问管理系统的用户数。
- 减少快照集中的卷数。创建专用于每个存储组的备份规范而不是用于整个服务器的一个规范。请参阅“备份”。

备份 Microsoft Exchange Server CCR 数据库副本失败

在 Microsoft Exchange Server CCR 环境中的数据库副本的备份会话期间，Data Protector 会报告一个主要错误，通知备份会话已失败。

原因

由于 Microsoft Exchange Server 在 Exchange 管理控制台中显示错误的数据库副本状态，因此在 CCR 环境中可能会出现此问题。在这种情况下，处于“故障”状态的数据库副本可以显示为“正常”。

解决方案

要使 Exchange 管理控制台显示数据库副本的真实状态，请执行以下操作之一:

- 使用 Service Pack 1 更新 Microsoft Exchange Server。
- 如下执行重新设置种子过程:

  1. 在被动节点上，通过使用 Suspend-StorageGroupCopy cmdlet 暂挂复制。
  2. 从数据库副本的 Logs 目录删除所有日志文件。
  3. 使用 Update-StorageGroupCopy cmdlet 为数据库副本设置种子或重新同步原始数据库及其副本。
  4. 使用 Resume-StorageGroupCopy cmdlet 恢复数据库副本。
  5. 在被动节点上，通过使用 vssadmin list writers 命令检查 Exchange 复制服务的状态。如果状态不是 stable ，则重新启动 Microsoft Exchange 复制服务。

LCR 环境中的 Exchange 复制服务写入程序实例未显示在 Data Protector GUI 中

在 Data Protector GUI 中，在创建备份规范时， Microsoft Exchange Writer(Exchange Replication Service) 对象不会显示在窗格上以选择备份对象。

原因

由于 Microsoft Exchange Server 在 Exchange 管理控制台中显示错误的数据库副本状态，因此在 LCR 环境中可能会出现此问题。在这种情况下，处于“故障”状态的数据库副本可以显示为“正常”。

解决方案

要使 Exchange 管理控制台显示数据库副本的实际状态并启用备份对象的选择，请重新启动 Microsoft Exchange 复制服务。

重新启动时 Windows 操作系统损坏

如果某些系统写入程序 (例如 System Writer) 的还原因任何原因 (硬件或软件故障、手动中止等) 而中止，则 Windows 操作系统可能在重新启动后损坏 (例如，GUI 或某些系统服务无法启动等)。

解决方案

根据损坏的本质，从 Windows 安装 CD-ROM 修复或重新安装操作系统。

Microsoft Exchange Server 数据库的时间点还原过程中的数据丢失

尽管时间点还原会话成功完成，但某些数据未还原，因为现有日志可能会干扰装载过程。

解决方案

在运行时间点还原之前手动删除日志文件。

RSG 创建失败

当您使用 Restore to a non-Exchange location and create RSG选项启动 Microsoft Exchange Server 写入程序的标准还原或即时恢复时，显示以下错误:

```
[重大] 应用程序特定函数 'PostRestoreEndExt' 失败，错误为: '您指定的邮箱数据库已与恢复 邮箱数据库关联。
```

原因

如果已在某些其他系统上创建还原的存储组或邮箱数据库的 RSG，则会显示此错误。

解决方案

由于同一存储组只能存在一个 RSG，且 Data Protector 只能删除目标还原位置上存在的 RSG，因此需要手动删除另一个系统上的 RSG 并重新启动还原。

备份之后 VSS 写入程序最终处于“故障”状态

执行备份会话之后，VSS 应用程序写入程序可能始终处于“故障”状态。

例如，在使用 SQL 写入程序备份 Microsoft SQL Server 期间，写入程序失败。重新启动写入程序之后，写入程序处于良好状态。但在下一个备份会话期间，写入程序再次失败。

对于 SQL 写入程序，已发现该问题，但也可能适用于其他写入程序。

使用 vssadmin list writer 命令检查写入程序的状态。例如，在备份会话之前运行命令时:

```
vssadmin 列表写入程序 vssadmin 1.1 - 卷影复制服务管理命令行 (C) 版权所有 2001-2005 Microsoft Corp. 写入程序名称: 'SqlServerWriter' 写入程序 Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a} 写入程序实例 Id: {c249df3c-f9d5-4f4a-8797-03724a60771c} 状态: [1] 稳定 上一个错误: 无错误
```

备份会话之后:

```
C:\Program Files>vssadmin 列表写入程序 vssadmin 1.1 - 卷影复制服务管理命令行 (C) 版权所有 2001-2005 Microsoft Corp. 写入程序名称: 'SqlServerWriter' 写入程序 Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a} 写入程序实例 Id: {e3d115c5-9c1a-47f6-8404-bfdba4c37890} 状态: [8] 失败 上一个错误: 不可重试的错误
```

原因

此类行为的原因通常包括错误配置或过期的用户帐户、过期的密码以及应用程序和卷影复制服务之间的其他连接问题。

解决方案

确保帐户设置正确。

备份或还原失败

针对 SQL Server 2008 使用 FILESTREAM 提供程序的远程 BLOB 存储 (RBS) 时备份或还原失败备份会话意外结束，并显示以下错误消息:

```
[重大] 来自: OB2BAR_VSSBAR@computer.company.com <mailto:OB2BAR_VSSBAR@computer.company.com> "MSVSSW" 时间: 2/3/2011 3:42:06 PM [145:575] 写入程序 'SqlServerWriter' 无法准备要备份 的文件: 报告的状态: VSS_WS_FAILED_AT_PREPARE_SNAPSHOT 预期状态: VSS_WS_WAITING_FOR_BACKUP_COMPLETE 故障代码: VSS_E_WRITERERROR_NONRETRYABLE [重大] 来自: OB2BAR_VSSBAR@computer.company.com <mailto:OB2BAR_VSSBAR@computer.company.com> "MSVSSW" 时间: 2/3/2011 3:42:06 PM 无法执行备份: '/SqlServerWriter(SQL Server 2008:SQLWriter)/BELMAVM20/SHAREPOINT/ FileStreamDB'，它包含数据: C:\temp\FileStreamDB\FileStreamDB.mdf C:\temp\FileStreamDB\FileStreamDB_log.ldf C:\temp\FileStreamDB\FileStreamData\*
```

同样，还原会话意外结束，并显示以下错误消息:

```
[重大] 来自: OB2BAR_VSSBAR@computer.company.com <mailto:OB2BAR_VSSBAR@computer.company.com> "MSVSSW" 时间: 12/8/2010 3:23:16 PM [145:298] 写入程序 'SqlServerWriter(SQL Server 2008 R2:SQLWriter)' 无法准备要还原的文件: 报告的状态: VSS_WS_FAILED_AT_PRE_RESTORE 预期状态: VSS_WS_STABLE 故障代码: VSS_E_WRITERERROR_NONRETRYABLE
```

原因

如果 FILESTREAM 访问级别设置为“已禁用”，则会显示这些问题。

解决方案

确保将 FILESTREAM 访问级别设置为“已启用完全访问”或“已启用 Transact-SQL 访问”。

Microsoft Exchange Server 还原或即时恢复失败

Microsoft Exchange Server 还原或即时恢复会话失败，并显示类似以下的消息:

[重大] 来自: OB2BAR_VSSBAR@tpc202.company.com "MSVSSW" 时间: 19.02.2011 21:02:37 备份 '2011/02/19-1' 的后还原操作失败。

原因

如果 Microsoft Exchange Server 数据库的恢复持续时间超过后还原操作的超时 (默认为两小时)，则可能会发生这种情况。达到超时后，Data Protector 将中止会话。

解决方案

使用 OB2VSS_WAIT_TIMEOUT omnirc 选项增加超时并重新启动会话。

VSS 集成只使用 5 个并发线程进行备份或还原

在备份或还原会话期间，即使设备和应用程序系统都能够同时处理更多线程，VSS 集成也始终仅使用 5 个并发线程。无论设备并发设置如何，都会显示此限制。

解决方案

通过将 omnirc 选项 OB2VSS_MAX_CONCURRENT_WORKER_THREADS 设置为更高的数字来修改该限制。最大并发线程数为 64。

由于 VDS 问题，备份或即时恢复中止

备份或即时恢复会话中止，并显示以下错误:

```
无法加载 VDS 服务。
```

原因

可能由于 VDS 服务的异常终止而显示此错误。

解决方案

1. 停止虚拟磁盘服务 (VDS):
   - 检查是否已启动虚拟磁盘服务，如果是，则使用命令 `net stop vds` 或通过控制面板停止该服务。
   - 如果上面的步骤没有帮助，则通过使用任务管理器终止进程 `vds.exe` 来停止虚拟磁盘服务。VDS 将根据需要自动启动。
   - 另外，您还可以再次登录到系统，并检查系统是否请求您确认停止异常终止的 VDS。如果是，则将调试器重新配置为自动启动以避免未来的相似问题。这可以通过将 `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug` 值 `Auto` 设置为 `1` 来完成此操作。
2. 检查您的配置。

   Data Protector 备份或还原的成功完成受许多非 Data Protector 组件因素的影响，包括 Microsoft Exchange Server 和 VSS。其中一个因素就是计时，而计时又会受环境条件影响，比如 I/O 负载、存储设备活动和并发 Data Protector 操作。

   为消除潜在问题，建议均衡 Data Protector 跨可用活动或维护窗口的活动。如果遇到问题，请“检查并可以减少并发 Data Protector 活动数”(如并发备份数或还原数)。

由于注册表中空间不足，无法导入卷影副本卷，因此备份失败

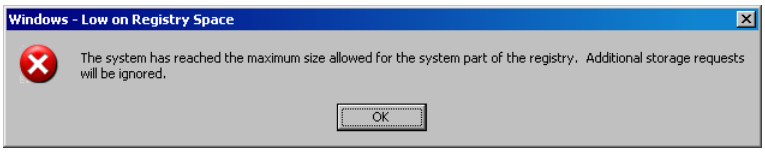
在 Windows 系统上，在 ZDB 会话期间报告以下错误之一:

- 按 Data Protector:

  ```
  [严重] 不可能从应用程序主机导入卷影 副本。
  ```

- 按操作系统:

  Windows 注册表报告的错误

原因

这些现象指明 Windows 注册表包含太多项并且空间不足。

这种情况导致 Data Protector ZDB 会话失败。尽管 Data Protector 不直接向注册表写入任何内容，但注册表包含有关曾经呈现在系统上的所有卷的项。这些项由存储设备驱动程序写入。

解决方案

通过执行以下命令清理 Windows 注册表。必须定期执行此清理任务，以防止注册表运行空间不足和 Data Protector ZDB 会话失败。但是，任务应在监督下运行，不应自动执行。

mountvol /R 。

Data Protector 报告未删除卷

在备份会话中，会报告以下错误:

```
未删除卷 'StorageID'，该卷是备份 'backupID' 的一部分。
```

原因

如果删除磁盘阵列上的复本，但保留 VSS 数据库 (VSSDB) 中的条目，则可能出现此错误。

如果备份会话在未创建复本的情况下失败，则可能会发生这种情况，但由于网络问题，无法删除为其创建的引用。

解决方案

要从 VSSDB 删除错误条目，请执行以下操作：

1. 在错误消息中，查找无法删除目标卷的会话 ID。
2. 执行以下命令，其中 *SessionID* 是无法删除目标卷的会话:

   omnidbvss -remove session SessionID -reference

   成功删除之后，命令应该显示确认消息“正在从 VSSDB 中删除会话 SessionID 的引用”。

Microsoft Exchange Server 写入程序的即时恢复失败

Microsoft Exchange Server 写入程序的即时恢复失败。

原因

如果 Microsoft Exchange 写入程序不处在稳定状态中，可能发生此问题。通过从命令提示符执行 VSSadmin list writers 检查此情况。

解决方案

通过重新启动 Microsoft Exchange 信息存储，使 Exchange Server 写入程序处于稳定状态。

系统重新启动错误

还原之后，将显示系统重新启动错误。

原因

在某些情况下，如果在应用程序系统上已更改 HBA，则先期 HBA 的软件驱动程序可能会在还原之后导致此错误。

解决方案

从应用程序系统中删除已卸载的 HBA 的较旧驱动程序。

重新启动 SQLServer 写入程序即时恢复后，数据库无法联机

如果 SQLServer 写入程序的即时恢复中止或失败，则可以重新启动会话。但是，SQLServer 写入程序可能报告错误，指示在即时恢复期间无法准备文件，会话完成并出现错误。

原因

如果在中止会话之前卸载磁盘并且文件对写入程序不可见，可能会出现此问题。因此，会报告错误，并且在还原之后无法将数据库联机。

解决方案

要在此类会话之后恢复数据库:

1. 从数据库分离。
2. 重新附加到数据库。

VSS 系统提供程序无法创建卷影副本

将 VSS 系统提供程序用于硬件 LUN 磁盘时，卷影副本创建将失败。

解决方案

安装最新的供应商驱动程序及其支持包，包括 HBA 适配器和 MPIO 驱动程序。

在备份会话期间，将导入卷，然后立即删除卷

使用硬件提供程序执行备份时，将导入正在备份的卷，然后立即删除，并显示以下错误:

[Normal] From: OB2BAR_VSSBAR@comp.company.com "MSVSSW" Time: 9/4/2010 1:37:41 PM Imported Volume Shadow Copy with the properties: ...

[Normal] From: OB2BAR_VSSBAR@comp.company.com "MSVSSW" Time: 9/4/2010 1:37:41 PM Deleting Volume Shadow Copies and releasing the volumes.

[Critical] From: OB2BAR_VSSBAR@comp.company.com "MSVSSW" Time: 9/4/2010 1:37:51 PM Backup failed.

原因

如果客户机安全设置未正确更新，则会发生此错误。

解决方案

确保客户机安全设置正确。如果单元安全，则 allow_hosts 文件中必须列出以下系统:

- 对于本地或网络备份，为应用程序系统
- 对于可传输备份，为应用程序和备份系统

如果没有 P9000 XP 阵列 VDS 硬件提供程序，则无法执行即时恢复

即时恢复会话异常结束，并显示消息:

To perform VDS Swap Instant Recovery, the source and target LUNS need to be resolved with VDS Hardware Providers.

原因

当 VDS 硬件提供程序无法解析源和目标 LUNS 时，会发生此错误。

解决方案

1. 在应用程序和备份系统上安装 VDS 硬件提供程序。
2. 解析应用程序系统 (源卷):

   omnidbvss -resolve -apphost AppSystem
3. 解析备份系统 (在备份会话中创建的目标卷):

   omnidbvss -resolve -session SessionID
4. 重新启动会话。

更新 3PAR StoreServ Storage 固件之后，零宕机时间备份会话失败

更新 3PAR StoreServ Storage 系列的存储系统上的固件并在此系统上调用零宕机时间备份会话之后，会话将失败，并显示类似以下的错误:

[Critical] From: SMISA@appsys.company.com "SMISA" Time: 06/15/2012 2:23:28 PM Replicator aborted with exception "No CIMOM found for ID 2FF70002AC000B6C".

原因

导致问题的原因是存储系统固件更新之后有关 VSS 数据库中源卷的信息已过时。

解决方案

要解决该问题，通过针对问题应用程序系统执行以下命令来更新 VSS 数据库:

```
omnidbvss -resolve -apphost ApplicationSystem
```

MySQL 集成故障诊断

This feature is available in the Premium Edition

本节列出在使用 Data Protector MySQL 集成时可能遇到的问题的常规检查、验证以及症状。

开始之前

- 确保已安装 Data Protector 最新补丁。

问题

下面是使用 Data Protector MySQL 集成时可能会遇到的一些问题。

无法在 **Data Protector** 中配置 **MySQL** 实例

解决方案

1. 请验证是否已在要备份的所有 MySQL 主机上安装 Data Protector MySQL 集成组件。
2. 检查在 MySQL 主机上的 Data Protector debug.log 文件中记录的错误。
3. 对存储 MySQL 数据的卷执行文件系统备份和还原。

备份会话失败 - 无法配置集成

备份会话失败

- 无法配置集成
- 无法连接到主机名=<主机>，用户=<用户>，端口=<端口>

解决方案

- 检查在操作系统事件日志中记录的错误。
- 检查 MySQL 实例的配置是否已按照备份 MySQL 集成主题中的说明进行配置。
- 检查 MySQL 服务器是否处于活动状态并处于运行状态。
- 检查 MEB 版本和数据库版本。（仅支持 MYSQL56/MEB 3.12 或更高版本。）

还原会话失败 - 还原链不包含有效的备份映像

解决方案

检查是否向 Data Protector 用户组分配了“查看私有对象”用户权限。

备份会话因新代理而失败

与新代理的备份会话失败，并显示以下消息：

```
[严重] 来自: BSM@server.domain.com "MySQL" 时间：18.09.2019 19:43:37 所有磁带客户机均无法成功完成。 会话失败。
```

解决方案

尝试使用旧代理进行备份。要切换到旧代理，请设置以下全局选项：

EnableLegacyMySQLAgent = 1

这些选项存储在 global 中，这是 Cell Manager 中的一个纯文本文件，位置如下:

Windows: <PROGRAMDATA>\Config\Server\Options

Linux: /etc/opt/omni/server/options

您无需重新启动服务。

备份会话因旧代理而失败

解决方案

1. 验证实例文件是否已编码密码。打开实例文件，并检查 password = “encoded password“ 在实例文件中是否可用。
2. 使用旧代理创建新的实例文件，然后重试进行备份。

备份会话失败 - 无法获取 MySQL 二进制日志路径

执行 MySQL 备份时，备份会话可能会因缺少 MySQL 二进制日志路径而失败。

原因

会话失败的原因可能是:

- 未启用二进制日志和 MySQL 二进制日志。
- 用户帐户没有备份权限。

解决方案

- 检查是否启用了二进制日志，还检查是否启用了 MySQL 二进制日志。
- 检查用户帐户是否具有备份权限。

备份会话失败

解决方案

- 在 my.cnf 或 my.ini 文件中启用 log-bin 参数，然后重新启动服务器。
- 通过使用 show binary logs 查询来启用二进制日志。

NDMP 服务器集成故障诊断

This feature is available in the Premium Edition

本主题列出使用 Data Protector NDMP 服务器集成时可能遇到的问题。

开始之前

- 确保已安装 Data Protector 的最新正式补丁。

问题

下面是使用 Data Protector NDMP 服务器集成时可能遇到的一些问题。

介质末尾

在编写编目的过程中，可能会发生“介质末尾”错误。

原因

编目大小随备份文件数量的增加而增加。由于 Data Protector 无法控制介质上剩余的可用空间，因此在写入编目期间可能会出现介质末尾错误。这对未来的还原没有影响，因为编目仍然存储在 IDB 中。但是，介质不能再导入。

设备和文件系统不在本地；正在切换到三向操作

如果为备份选择的卷和驱动器不是群集节点的本地卷，则 Data Protector 会在会话输出中显示以下错误消息:

[Warning] From: BMA-NDMP@hostname.com "netappCAB_drive1" Time: 5.4.2016 15:35:10

Device and the filesystem are not local, switching to 3-way operation.

原因

这意味着将使用三向 NDMP 模式备份选定卷，因为该卷不是选定磁带驱动器所连接的节点的本地卷。

解决方案

确保所选卷在所选磁带驱动器连接到的节点本地。

三向直接访问还原 (DAR) 还原问题

在三向配置中使用 DAR 还原时，性能可能会降低。

解决方案

切换到本地 DAR 还原。

或

禁用 DAR 用于三向还原。

导入 NDMP 介质失败

导入 NDMP 介质失败。

原因

如果用于导入 NMDP 介质的驱动器未连接到 NDMP 系统，则会发生此问题。

解决方案

确保用于导入 NMDP 介质的驱动器已连接到 NDMP 服务器系统。

三向群集感知备份 (CAB) 或正常模式下的备份或还原失败

在 3 向 CAB 或正常模式下，备份或还原失败，并显示以下错误消息:

[Warning] From: BMA-NDMP@hostname.com "CAB_drive2" Time: 4/26/2016 10:14:31 AM

Device and the filesystem are not local, switching to 3-way operation.

[Warning] From: BMA-NDMP@hostname.com "CAB_drive2" Time: 4/26/2016 10:14:31 AM

BMA-NDMP: Catalog not loaded, message #-1 in set 242

[Normal] From: BMA-NDMP@hostname.com "CAB_drive2" Time: 4/26/2016 10:14:34 AM

Ejecting medium '1'.

（或）

[Normal] From: BMA-NDMP@hostname.com "NDMP_drive1" Time: 4/26/2016 11:25:14 AM

ABORTED Media Agent.

[Normal] From: BMA-NDMP@hostname.com " NDMP_drive1" Time: 4/26/2016 11:25:18 AM

Ejecting medium '1'.

原因

如果文件管理器上没有足够的 NDMP 会话，则会发生此错误。

解决方案

要了解所支持的 NDMP 会话数并相应地进行规划，请参考文件管理器文档。介质代理在正常模式或 CAB 模式下使用两个 NDMP 会话，但在三向正常或 CAB 模式备份期间使用 3 个会话。

而在正常或 CAB 模式下，一个介质代理 (MA) 使用两个 NDMP 会话；在三向正常或 CAB 模式下，使用三个 NDMP 会话。

驱动器扫描成功后，磁带仍保留在驱动器中

解决方案

手动弹出磁带，然后将 NDMP 客户机上的 OB2SCTLMOVETIMEOUT omnirc 选项设置为更高的值 (例如，等于或大于 360000)。

Data Protector 无法设置 NDMP 记录大小

Data Protector 报告:

Data Protector was unable to set NDMP record size. Reason for this might be that NDMP server doesn't support specified record size. Please check th e release notes in order to determine which record size is supported for your NDMP server.

原因

当您指定不支持的记录大小时，会发生此错误。

解决方案

检查块大小。

Oracle Server 集成故障诊断

This feature is available in the Premium Edition

本主题包含常规检查和验证的列表，以及使用 Data Protector Oracle 集成时可能遇到的问题列表。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 验证您可以访问 Oracle 目标数据库且其处于打开状态:
  1. 请执行以下操作：

     Windows 系统： 设置 ORACLE_HOME 变量。

     UNIX 系统： 导出 ORACLE_HOME 变量，如下所示:
     - 如果您使用的是类似于 sh 的 shell，请输入以下命令:

       ORACLE_HOME="ORACLE_HOME"

       export ORACLE_HOME
     - 如果您使用的是类似于 csh 的 shell，请输入以下命令:

       setenv ORACLE_HOME "ORACLE_HOME"
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog
  3. 启动 SQL*Plus 并键入:

     connect user_name/password@service as sysdba';'

     select * from dba_tablespaces;

     exit

     > **注意**
     >
     > 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

     如果失败，请打开 Oracle 目标数据库。
- 验证您是否可以访问恢复编目 (如已使用) 并且其按如下方式打开:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog
  3. 启动 SQL*Plus 并键入:

     connect Recovery_Catalog_Login

     select * from rcver;

     exit

  如果失败，请打开恢复编目。
- 验证是否为 Oracle 目标数据库和恢复编目数据库正确配置了侦听程序。这是正确建立网络连接所必需的:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。

2. 从 ORACLE_HOME 目录中的 bin 目录启动侦听程序:
3. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

   sqlplus /nolog
4. 启动 SQL*Plus 并键入:

   connect Target_Database_Login

   exit

   然后

   connect Recovery_Catalog_Login

   exit

   如果失败，请参阅 Oracle 文档以获取有关如何创建配置文件 (NAMES.ORA) 的说明。

- 验证是否已将 Oracle 目标数据库和恢复编目数据库配置为允许使用系统特权进行远程连接:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog
  3. 启动 SQL*Plus 并键入:

     connect Target_Database_Login as SYSDBA

     exit

     和

     sqlplus connect Recovery_Catalog_Login as SYSDBA

     exit

  使用 SYSOPER 代替 SYSDBA 重复此过程。

  > **注意**
  >
  > 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。
  >
  > 恢复目录服务器应仅属于一个从中配置备份的 Cell Manager。如果它属于多个 Cell Manager，则 configure_peer 命令将失败，并且恢复目录数据库的备份也将失败。

  如果失败，请参阅 Oracle 文档中有关在 initDB_NAME.ora 文件中设置密码文件和相关参数的说明。
- 在应用程序系统中，验证目标数据库和恢复编目数据库是否已配置为允许使用系统特权进行远程连接并允许备份:
  - 如果使用恢复编目数据库:

    按步骤 1 所述，导出或设置 ORACLE_HOME 和 DB_NAME 变量。

    SQL> connect login_to_recovery_catalog_or_target_database as sysdba;

    > exit

    ORACLE_HOME /bin/rman target login_to_target database catalog login_to_Recovery_Catalog
- 如果不使用恢复编目数据库:

  按步骤 1 所述，导出或设置 ORACLE_HOME 和 DB_NAME 变量。

  ORACLE_HOME /bin/rman target login_to_target_database nocatalog

  有关如何在 initDB_NAME.ora 文件中设置密码文件和参数以及如何为用户添加系统特权的信息，请参阅 Oracle 文档。
- 如果使用恢复编目数据库，请验证目标数据库是否已在恢复编目中注册:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME; 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog
  3. 启动 SQL*Plus 并键入:

     connect Recovery_Catalog_Login;

select * from rc_database;

exit

如果失败，请使用 Data Protector 启动配置，或参阅 Oracle 文档中有关如何在恢复编目数据库中注册 Oracle 目标数据库的信息。

- 验证备份并使用 RMAN 通道类型磁盘直接还原到磁盘:

  如果使用恢复编目:

  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 RMAN:

     rman target Target_Database_Login catalog Recovery_Catalog_Login cmd_file=rman_script

  如果不使用恢复编目:

  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 RMAN:

     rman target Target_Database_Login nocatalog cmd_file=rman_script

  RMAN 备份脚本的示例如下所示:

  ```
  run { allocate channel 'dev0' type disk; backup tablespace tablespace_name format 'ORACLE_HOME/tmp/datafile_name'; }
  ```

  成功备份后，请尝试执行以下还原脚本，还原备份的表空间:

  ```
  run { allocate channel 'dev0' type disk; sql 'alter tablespace tablespace_name offline immediate'; restore tablespace tablespace_name;
  recover tablespace tablespace_name; sql 'alter tablespace tablespace_name online';release channel 'dev0'; }
  ```

  如果失败，请参阅 Oracle 文档中有关如何执行备份和使用 RMAN 直接还原到磁盘的详细信息。

此外，如果配置或备份失败:

- 验证 Data Protector 软件是否已正确安装。
- 检查是否为 Oracle 管理员授予了 SYSDBA/SYSBACKUP 特权。
- 如果有特殊的 Oracle 环境设置，请确保在 Cell Manager 中将其输入 Data Protector Oracle 配置文件中。
- 执行 Oracle Server 系统的文件系统备份，以便消除 Oracle Server 和 Data Protector Cell Manager 系统之间潜在的通信问题。

  确保备份规范中定义为要备份的系统的主机名是应用程序系统的名称。
- ***Windows 系统：*** 检查 Oracle Server 系统上的 Data Protector Inet 服务启动参数:

  转到“控制面板”>“管理工具”>“服务”>“Data Protector Inet”。

  该服务必须在指定的用户帐户下运行。确保同一用户也添加到 Data Protector admin 或 user 组。
- 检查 Oracle Server 系统中在以下 debug.log 文件中报告的系统错误。

此外，如果备份或还原失败:

- 使用 testbar2 实用程序测试 Data Protector 内部数据传输:
  1. 验证是否在 Oracle Server 系统中正确定义了 Cell Manager 名称。检查位于默认 Data Protector 客户机配置目录中的 cell_server 文件，该目录包含 Cell Manager 系统的名称。
  2. 从 ORACLE_HOME 目录中的 bin 目录中，执行:

     如果备份失败:

     testbar2 -type:Oracle8 -appname:DB_NAME-perform:backup -bar:backup_specification_name

     如果还原失败:

     testbar2 -type:Oracle8 -appname:DB_NAME-perform:restore -object:object_name -version:object_version-bar:backup_specification_name

     主机名不应在 object 选项中指定。而是由 testbar2 自动提供。

3. 您应看到屏幕上仅显示 NORMAL 消息，否则请单击 Data Protector 的“监视器”上下文中的“详细信息”按钮，检查 testbar2 实用程序报告的错误。

如果消息指示集成的 Data Protector 端存在问题，请继续执行以下步骤:

- 检查启动备份或还原会话的用户是否具有相应的 Oracle 权限 (例如，属于 DBA 组)。此用户还必须位于 Data Protector operator 或 admin 用户组中。
- 检查各个 Data Protector 用户组是否已启用“查看私有对象”用户权限。
- ***如果备份失败:*** 创建 Oracle 备份规范以备份到空设备或文件。如果备份成功，则问题可能与备份设备有关。
- ***如果还原失败:*** 执行 omnidb 命令，查看数据库中的对象。

如果测试再次失败，请致电支持代表寻求帮助。

此外，如果还原失败:

- 验证备份介质上是否存在对象。

  可以在 Oracle Server 系统 ORACLE_HOME; 目录中的 bin 目录执行以下命令来完成此操作:

  ```
  omnidb -oracle8 "object_name" -session "Session_ID" -media
  ```

  该命令的输出列出了有关指定的 Oracle 对象的详细信息、包含此对象的备份会话的会话 ID 以及所使用介质的列表。有关 omnidb 命令的详细语法，请参阅手册页。
- 确保数据库处于正确的状态。

  如果您尝试使用 Data Protector GUI 还原数据库项，而 GUI 停止响应，请尝试以下操作之一:

  - 如果要还原控制文件，则数据库应处于 NoMount 状态。

    打开命令窗口并输入以下内容:

    ```
    sqlplus/nolog
    SQL>connect user/password@service as sysdba
    SQL>shutdown immediate
    SQL>startup nomount
    ```
  - 如果要还原数据文件，则数据库应处于 Mount 状态。

    打开命令窗口并输入以下内容:

    ```
    sqlplus/nolog
    SQL>connect user/password@service as sysdba
    SQL>shutdown immediate
    SQL>startup mount
    ```
- 如果在尝试使用 Data Protector GUI 还原数据库项时出现无法解决的问题，请尝试使用 RMAN CLI 还原数据库项。
- 在使用 Data Protector GUI 恢复和还原备份会话后，尝试手动将数据库置于“打开”状态。

  如果已使用 Data Protector GUI 来恢复和还原备份会话，则会看到以下错误消息:

  ```
  Oracle Error: ORA-1589: must use RESETLOGS or NORESETLOGS option for database open.
  ```

  打开 SQLplus 窗口并使用以下命令:

  ```
  sqlplus/nolog
  SQL>connect user/password@service as sysdba
  SQL>alter database open noresetlogs;
  ```

  如果不起作用，请尝试使用以下命令:

  ```
  SQL>alter database open resetlogs;
  ```

> **注意**
>
> 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

问题

下面是使用 Data Protector Oracle 集成时可能会遇到的一些问题。

遇到 ORACLE 错误 6550

在 Oracle 备份期间调用 SYS.LT_EXPORT_PKG.schema_inf_exp 时 Data Protector 报告错误。

Data Protector 监视器中列出了以下错误:

```
EXP-00008: 遇到 ORACLE 错误 6550 ORA-06550: 第 1 行第 13 列: PLS-00201: 必须声明标识符 'SYS.LT_EXPORT_PKG' ORA-06550: 第 1 行第 7 列:
PL/SQL: 声明被忽略 EXP-00083: 调用 SYS.LT_EXPORT_PKG.schema_info_exp 时发生前一个问题 。导出统计信息 导出已成功终止，但出现警告。 [重大] 来自:
ob2rman.pl@machine "MAKI" 时间: 10/01/01 16:07:53 导出恢复编目数据库失败。
```

解决方案

启动 SQL*Plus 并授予 LT_EXPORT_PKG 执行权限，如下所示 (确保事先为用户 sys 授予了 SYSDBA 特权):

```
sqlplus 'sys/password@CDB as sysdba'
```

```
SQL> grant execute on sys.lt_export_pkg to public;
```

重新启动失败的备份会话。

无法分配/附加共享内存

备份失败，并显示以下错误消息:

```
无法分配/附加共享
```

```
内存 (IPC 无法分配共享内存段) 系统错误: [13] 权限被拒绝）=> 正在中止
```

解决方案

将 OB2SHMEM_IPCGLOBAL omnirc 选项设置为 1 以正确使用内存窗口，然后重新启动失败的备份会话。

在时间点还原和恢复之后备份失败

显示以下错误：

RMAN-06004: ORACLE error from recovery catalog database: RMAN-20003: target database incarnation not found in recovery catalog

原因

发生此错误的原因是数据库的新版本未在恢复编目中注册。

解决方案

使用 RMAN 连接到目标和恢复编目数据库并重置数据库，以在恢复编目中注册数据库的新对应物:

rman target Target_Database_Login catalog Recovery_Catalog_Login

RMAN> RESET DATABASE;

RMAN> exit

Oracle 联机备份失败

Oracle 联机备份失败，并显示以下错误:

RMAN-06004: ORACLE error from recovery catalog database: RMAN-20220: controlfile copy not found in the recovery catalog

原因

运行联机备份时，Data Protector 会将 *controlfilecopy* 的文件名添加到 RMAN 备份脚本中。必须在备份命令之前将此文件名归入 RMAN 编目。发生此错误的原因是 *controlfilecopy* 文件未编目。

解决方案

要将 *controlfilecopy* 归入 RMAN 编目，请执行以下操作:

1. 在应用程序系统上连接到 RMAN。
2. 请执行以下命令：

   RMAN> catalog controlfilecopy 'CONTROL_FILE_LOCATION/ctrlDB_NAME.ctl'

无法在 **RAC** 上备份存档日志

在 RAC 上，无法备份存档日志。

原因

装载 NFS 的磁盘上未安装存档日志。

解决方案

编辑存档日志备份规范:

- 为“每个”节点添加一个额外的 allocate channel 命令。
- 添加命令以连接到每个实例。应采用 username / passwd @ INSTANCE 格式指定连接参数。

例如，如果您使用两个节点，则备份规范可能如下所示:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)' connect username/passwd@INSTANCE_1; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)' connect username/passwd@INSTANCE_2; backup format
'RAC_arch<QU_%s:%t:%p>.dbf' archivelog all; }
```

无法从托管备份还原控制文件

未使用恢复编目，未使用 RMAN 自动备份功能，并且无法从 Data Protector 托管备份还原控制文件。磁带上存在有效的控制文件备份。

解决方案

从 RMAN 备份集还原控制文件，装载和还原数据库，并执行数据库恢复:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML'; restore controlfile from 'backup piece handle';
sql 'alter database mount'; set until time 'MMM DD YY HH24:MM:SS'; restore database; recover database; sql 'alter database open resetlogs';
release channel 'dev_0'; }
```

此时，您必须手动注册在还原控制文件备份之后所做的任何备份。然后再继续执行还原过程。

对于 *backup piece handle*，请搜索 Data Protector 内部数据库和先前备份会话的会话输出。

如何修改 RMAN 还原脚本

开始使用 Data Protector GUI 或 CLI 还原 Oracle 数据库时，会创建一个 RMAN 还原脚本，该脚本会立即运行，因此您无法先对其进行编辑。

原因

omnirc 选项 OB2RMANSAVE 不指向保存 RMAN 还原脚本的位置。

解决方案

要在脚本运行之前编辑脚本，请将 Data Protector omnirc 选项 OB2RMANSAVE 设置为指向现有目录。设置变量并开始还原后，在运行时创建的 RMAN 还原脚本将以名称 RMAN_restore_backup_specification_name.rman 保存到指定位置，并跳过实际还原。然后，便可编辑脚本，再手动运行。

要再次使用 Data Protector 启动还原，请清除 OB2RMANSAVE 选项，方法是删除其内容或者注释或删除整个选项。如果您在 Windows 系统上注释或删除此选项，请重新启动 Data Protector Inet 服务以使设置生效。

即时恢复 Oracle 数据库失败

Oracle 数据库的即时恢复会话失败，并显示类似如下的消息:

```
[正常] 来自: ob2rman@x64-node1.x64ring.com "testdb" 时间: 2/7/2008 10:48:19 AM 正在启动目标数据库即时恢复。 网络服务名称: testdb。 实例状态: . 实例名称: . 数据库 DBID = 。 数据库控制文件类型: . 数据库日志模式: . [重大] 来自: ob2rman@x64-node1.x64ring.com "testdb" 时间: 2/7/2008 10:48:20 AM 执行请求的操作时，数据库报告错误。
```

请注意，数据库参数为空，Data Protector 无法连接到 Oracle 数据库时会出现此状况。

原因

Data Protector 未连接到 Oracle 数据库。

解决方案

即使数据库处于 Mount 或 Nomount 状态，Data Protector 也必须能够连接到 Oracle 数据库。实现此目标的一种方法是为 Oracle 侦听程序配置静态服务信息。

以下示例显示如何使用 Oracle Net Manager 配置静态服务信息。

假设您有以下环境:

侦听程序名称: LISTENER
全局数据库名称: orcl
Oracle SID: ORCL

要为侦听程序配置静态服务信息，请打开 Oracle Net Manager，选择侦听程序，转到 **Database Services** 上下文，添加数据库并指定 Oracle 数据库参数。

此后， listener.ora 文件将更新 SID_LIST_LISTENER 部分。

```
SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (GLOBAL_DBNAME = orcl) (SID_NAME = ORCL) ) )
```

最后，重新启动 Oracle 侦听程序服务以应用更改。

IPC 主机名或 IP 地址无效

在 Data Protector GUI 还原上下文中浏览 Oracle 数据库的还原会话时，显示以下错误消息:

IPC Invalid Hostname or IP Address

原因

发生此问题的原因是:

- 将数据库项还原到其他客户机时。
- 从另一个 Data Protector 单元导入包含 Oracle 数据库备份的 Data Protector 介质时。

解决方案

要成功将数据库项还原到其他客户机，请确保将启动 Data Protector Oracle 集成代理的系统配置为 Data Protector Oracle 数据库实例 ("ORACLE_SID")。

要进行验证，请检查它是否列在“选项”页面中的“客户机”下拉列表中。

选择系统并继续执行还原 Oracle 数据库对象过程的步骤 7。

显示 RMAN 备份脚本错误

在 Data Protector GUI 中，当您编辑 Data Protector 备份规范的 RMAN 脚本部分时，将显示以下错误消息:

```
Cannot proceed, invalid RMAN backup script.
```

原因

如果指定了 Oracle RMAN 参数，但 Data Protector 分析程序未能识别或发生分析错误，则会显示此错误。

解决方案

将 Data Protector `NoGUIRMANScriptParsing` 全局选项设置为 `1` ，在 Data Protector GUI 中禁用 Oracle RMAN 脚本分析。

恢复管理器中的致命错误

Oracle RMAN 失败，并显示以下错误消息:

RMAN-06900: 警告: 无法生成 V$RMAN_STATUS 或 V$RMAN_OUTPUT 行

RMAN-06901: 警告: 正在禁用 V$RMAN_STATUS 和 V$RMAN_OUTPUT 行更新

RMAN-06003: 目标数据库发生 ORACLE 错误:

ORA-03113: 通信信道上出现文件结尾

进程 ID: 4222

会话 ID : 29 序列号: 51

..

RMAN-00569: ========== 继续列出错误消息 ==========

RMAN-00571: ===

RMAN-00601: Recovery Manager 中发生致命错误

RMAN-03004: 执行命令时发生致命错误

原因

发生此错误是因为恢复过程超时。

解决方案

在 sqlnet.ora 文件中，增加 SQLNET.RECV_TIMEOUT 值。

Oracle Server ZDB 集成故障诊断

This feature is available in the Premium Edition

本节包含常规检查和验证的列表，以及使用 Data Protector Oracle Server ZDB 集成时可能遇到的问题列表。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果配置、备份或还原失败:

- 在应用程序系统上，验证是否可以访问 Oracle 目标数据库并将其打开:
  1. 请执行以下操作：

     Windows 系统： 设置 ORACLE_HOME 变量。

     UNIX 系统： 导出 ORACLE_HOME 变量，如下所示:

     - 如果您使用的是类似于 sh 的 shell，请输入以下命令:

       ORACLE_HOME="ORACLE_HOME"

       export ORACLE_HOME

     - 如果您使用的是类似于 csh 的 shell，请输入以下命令:

       setenv ORACLE_HOME "ORACLE_HOME"

  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog

  3. 启动 SQL*Plus 并键入:

     connect user_name/password@service as sysdba';'

     select * from dba_tablespaces;

     exit

     > **注意**
     >
     > 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba。

     如果失败，请打开 Oracle 目标数据库。
- 在应用程序系统上，验证是否可以访问恢复编目 (如果已使用) 并按照如下所示将其打开:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog

  3. 启动 SQL*Plus 并键入:

     connect Recovery_Catalog_Login

     select * from rcver;

     exit

  如果失败，请打开恢复编目。
- 验证是否为 Oracle 目标数据库和恢复编目数据库正确配置了侦听程序。这是正确建立网络连接所必需的:
  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动侦听程序:
  3. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog

4. 启动 SQL*Plus 并键入:

   connect Target_Database_Login

   exit

   然后

   connect Recovery_Catalog_Login

   exit

   如果失败，请参阅 Oracle 文档以获取有关如何创建配置文件 (NAMES.ORA) 的说明。

- 验证是否已将 Oracle 目标数据库和恢复编目数据库配置为允许使用系统特权进行远程连接:

  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog

  3. 启动 SQL*Plus 并键入:

     connect Target_Database_Login as SYSDBA

     exit

     和

     sqlplus connect Recovery_Catalog_Login as SYSDBA

     exit

  使用 SYSOPER 代替 SYSDBA 重复此过程。

  > **注意**
  > 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

  如果失败，请参阅 Oracle 文档中有关在 initDB_NAME.ora 文件中设置密码文件和相关参数的说明。

- 在应用程序系统中，验证目标数据库和恢复编目数据库是否已配置为允许使用系统特权进行远程连接并允许备份:
  - 如果使用恢复编目数据库:

    按步骤 1 所述，导出或设置 ORACLE_HOME 和 DB_NAME 变量。

    SQL> connect login_to_recovery_catalog_or_target_database as sysdba;

    > exit

    ORACLE_HOME /bin/rman target login_to_target database catalog login_to_Recovery_Catalog

- 如果不使用恢复编目数据库:

  按步骤 1 所述，导出或设置 ORACLE_HOME 和 DB_NAME 变量。

  ORACLE_HOME /bin/rman target login_to_target_database nocatalog

  有关如何在 initDB_NAME.ora 文件中设置密码文件和参数以及如何为用户添加系统特权的信息，请参阅 Oracle 文档。

- 如果使用恢复编目数据库，请验证目标数据库是否已在恢复编目中注册:

  1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
  2. 从 ORACLE_HOME; 目录中的 bin 目录启动 SQL*Plus:

     sqlplus /nolog

  3. 启动 SQL*Plus 并键入:

     connect Recovery_Catalog_Login;

     select * from rc_database;

     exit

  如果此操作失败，请在应用程序系统上使用 Data Protector 启动配置，或参阅 Oracle 文档以获取有关如何在恢复编目数据库中注册 Oracle 目标数据库的信息。

- 在应用程序系统上，验证是否使用 RMAN 通道类型磁盘直接备份并还原到磁盘:

  如果使用恢复编目:

1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
2. 从 ORACLE_HOME 目录中的 bin 目录启动 RMAN:

   rman target Target_Database_Login catalog Recovery_Catalog_Login cmd_file=rman_script

如果不使用恢复编目:

1. 按步骤 1 所述，导出或设置 ORACLE_HOME 变量。
2. 从 ORACLE_HOME 目录中的 bin 目录启动 RMAN:

   rman target Target_Database_Login nocatalog cmd_file=rman_script

RMAN 备份脚本的示例如下所示:

```
run { allocate channel 'dev0' type disk; backup tablespace tablespace_name format 'ORACLE_HOME/tmp/datafile_name'; }
```

成功备份后，请尝试执行以下还原脚本，还原备份的表空间:

```
run { allocate channel 'dev0' type disk; sql 'alter tablespace tablespace_name offline immediate'; restore tablespace tablespace_name;
recover tablespace tablespace_name; sql 'alter tablespace tablespace_name online';release channel 'dev0'; }
```

如果失败，请参阅 Oracle 文档中有关如何执行备份和使用 RMAN 直接还原到磁盘的详细信息。

此外，如果配置或备份失败:

- 验证 Data Protector 软件是否已正确安装。
- 检查是否为 Oracle 管理员授予了 SYSDBA/SYSBACKUP 特权。
- 如果有特殊的 Oracle 环境设置，请确保在 Cell Manager 中将其输入 Data Protector Oracle 配置文件中。
- 执行 Oracle Server 系统的文件系统备份 (非 ZDB)，以便消除 Oracle Server 和 Data Protector Cell Manager 系统之间的所有潜在通信问题。

  确保备份规范中定义为要备份的系统的主机名是应用程序系统的名称。
- ***Windows 系统：*** 检查 Oracle Server 系统上的 Data Protector Inet 服务启动参数:

  转到“控制面板”>“管理工具”>“服务”>“Data Protector Inet”。

  该服务必须在指定的用户帐户下运行。确保同一用户也添加到 Data Protector admin 或 user 组。
- 检查 Oracle Server 系统应用程序系统 (Oracle proxy-copy ZDB 方法) 中以下文件报告的系统错误，或者将系统 (Oracle 备份集 ZDB 方法) 备份到 debug.log 文件。

此外，如果备份或还原失败:

- 使用 testbar2 实用程序测试 Data Protector 内部数据传输:
  1. 验证是否在 Oracle Server 系统中正确定义了 Cell Manager 名称。检查位于默认 Data Protector 客户机配置目录中的 cell_server 文件，该目录包含 Cell Manager 系统的名称。
  2. 从 ORACLE_HOME 目录中的 bin 目录中，执行:

     如果备份失败:

     testbar2 -type:Oracle8 -appname:DB_NAME-perform:backup -bar:backup_specification_name

     如果还原失败:

     testbar2 -type:Oracle8 -appname:DB_NAME-perform:restore -object:object_name -version:object_version-bar:backup_specification_name

     主机名不应在 object 选项中指定。而是由 testbar2 自动提供。
  3. 您应看到屏幕上仅显示 NORMAL 消息，否则请单击 Data Protector 的“监视器”上下文中的“详细信息”按钮，检查 testbar2 实用程序报告的错误。

  如果消息指示集成的 Data Protector 端存在问题，请继续执行以下步骤:

  - 检查启动备份或还原会话的用户是否具有相应的 Oracle 权限 (例如，属于 DBA 组)。此用户还必须位于 Data Protector operator 或 admin 用户组中。
  - 检查各个 Data Protector 用户组是否已启用“查看私有对象”用户权限。
  - ***如果备份失败:*** 创建 Oracle 备份规范以备份到空设备或文件。如果备份成功，则问题可能与备份设备有关。
  - ***如果还原失败:*** 执行 omnidb 命令，查看数据库中的对象。

  如果测试再次失败，请致电支持代表寻求帮助。

此外，如果还原失败:

- 验证备份介质上是否存在对象。

  可以在 Oracle Server 系统 ORACLE_HOME; 目录中的 bin 目录执行以下命令来完成此操作:

  ```
  omnidb -oracle8 "object_name" -session "Session_ID" -media
  ```

  该命令的输出列出了有关指定的 Oracle 对象的详细信息、包含此对象的备份会话的会话 ID 以及所使用介质的列表。有关 omnidb 命令的详细语法，请参阅手册页。

- 确保数据库处于正确的状态。

  如果您尝试使用 Data Protector GUI 还原数据库项，而 GUI 停止响应，请尝试以下操作之一:

  - 如果要还原控制文件，则数据库应处于 NoMount 状态。

    打开命令窗口并输入以下内容:

    ```
    sqlplus/nolog

    SQL>connect user/password@service as sysdba

    SQL>shutdown immediate

    SQL>startup nomount
    ```

  - 如果要还原数据文件，则数据库应处于 Mount 状态。

    打开命令窗口并输入以下内容:

    ```
    sqlplus/nolog

    SQL>connect user/password@service as sysdba

    SQL>shutdown immediate

    SQL>startup mount
    ```

- 如果在尝试使用 Data Protector GUI 还原数据库项时出现无法解决的问题，请尝试使用 RMAN CLI 还原数据库项。
- 在使用 Data Protector GUI 恢复和还原备份会话后，尝试手动将数据库置于“打开”状态。

  如果已使用 Data Protector GUI 来恢复和还原备份会话，则会看到以下错误消息:

  ```
  Oracle Error: ORA-1589: must use RESETLOGS or NORESETLOGS option for database open.
  ```

  打开 SQLplus 窗口并使用以下命令:

  ```
  sqlplus/nolog

  SQL>connect user/password@service as sysdba

  SQL>alter database open noresetlogs;
  ```

  如果不起作用，请尝试使用以下命令:

  ```
  SQL>alter database open resetlogs;
  ```

  > **注意**
  >
  > 对于 Oracle 12c 版本，如果用户具有 SYSBACKUP 特权，必须使用 as sysbackup 代替 as sysdba 。

问题

下面是使用 Data Protector Oracle Server ZDB 集成时可能会遇到的一些问题。

- 恢复管理器中的致命错误

SQL*Plus 无法连接到目标

解决方案

检查 Oracle 侦听程序是否已启动且正在运行。检查是否需要输入任何环境变量 (例如， TNS_ADMIN)。在 Cell Manager 的 Data Protector Oracle 配置文件中输入这些变量。

ORA-12532：：无效参数

显示以下错误:

ORA-12532: : invalid argument

原因

如果 Data Protector 监视器中的 SQL*Plus 报告此错误，则应用程序系统可能资源 (CPU、内存等) 较少。

解决方案

尝试配置应用程序系统，确保尽可能减少资源消耗。通过在应用程序系统上启动 SQL*Plus 并连接到应用程序系统中的目标数据库，无需使用 Data Protector 即可重现此错误。

备份集 ZDB 在 10 分钟后中止

执行备份集 ZDB 时，对每个数据库的数据文件都显示以下警告:

RMAN-06554: WARNING: file n is in backup mode

然后，ZDB 会话将中止并显示以下消息:

Bar backup session was started but no client connected in 600 seconds.

原因

如果客户机在启动备份会话后的 600 秒内未连接，则会发生此错误。

解决方案

增大以下全局选项的值 (默认情况下，这些选项设置为 10):

- 如果从以前版本的 Data Protector 升级 Data Protector:

  SmWaitForFirstClient=minutes

- 如果您执行了全新安装:

  SmWaitForFirstBackupClient=minutes

更改数据库的物理模式后，备份集 ZDB 失败

修改数据库的物理模式 (例如，添加或删除表空间、添加新数据文件、添加或删除回滚段) 后，备份失败。根据执行的修改，将显示不同的错误消息，例如:

RMAN-06056: could not access datafile datafile

原因

发生该问题是由于恢复编目中未更新目标数据库的物理模式。

解决方案

手动重新同步恢复编目数据库与当前控制文件。

在 UNIX 系统上，备份集 ZDB 到磁盘磁带会话失败

执行备份集“ZDB 到磁盘 + 磁带”时，如果 Oracle Server 尝试在备份系统上启动实例，则会话失败并显示以下错误:

[Major] From: ob2rman@computer.company.com DB_NAME Time: Date Time

The database reported error while performing requested operation.

原因

当应用程序和备份系统上的 Oracle 操作系统用户帐户的用户 ID 或组 ID 编号不匹配时，将发生此问题。在这种情况下，由于缺少特权，Oracle Server 无法在备份系统上启动实例。

解决方案

如“配置 Oracle 操作系统用户帐户”所示配置用户帐户，然后重新启动会话。

代理副本还原失败

代理副本还原失败并显示以下错误:

```
RMAN-10035: exception raised in RPC: ORA-27197: skgfprs: sbtpcrestore returned error

RMAN-10031: ORA-27197 occurred during call to DBMS_BACKUP_RESTORE.PROXYRESTOREDATAFILE
```

解决方案

检查会话 IDB 和最新备份对象。您可以检查恢复编目中是否存在更新的会话。连接到 RMAN 提示符:

```
rman target user/password@TGT_DB catalog user/password@CDB
```

在 RMAN> 提示符下，输入

```
list backup;
```

显示恢复编目中的对象列表。检查列在最后的代理复制会话列表。

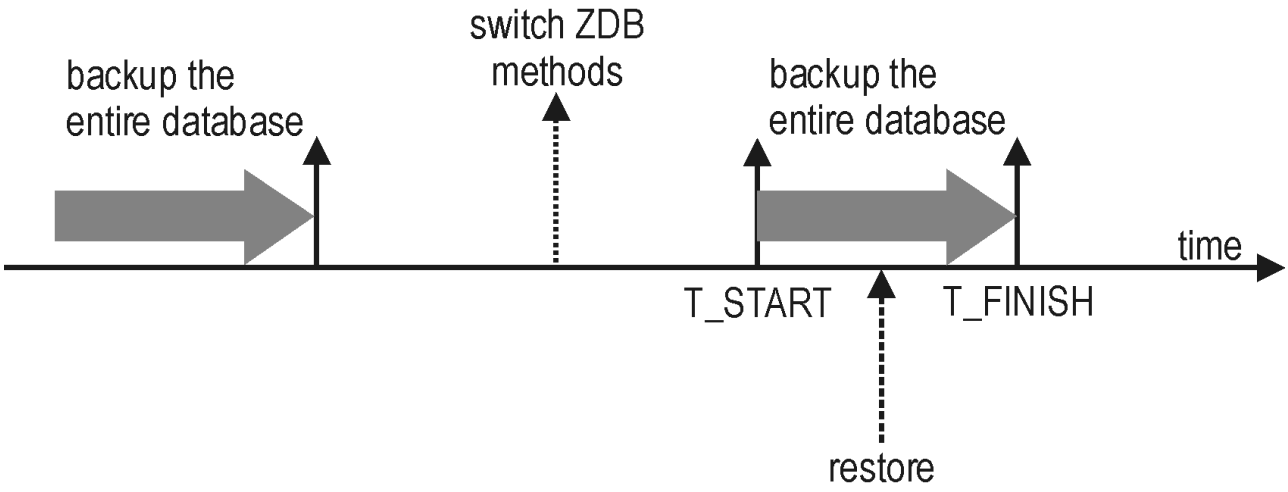
要同步恢复编目和 IDB，请执行 RMAN 命令:

```
resync catalog;
```

执行同步后，应该可以执行还原。

切换 ZDB 方法失败后还原

切换 ZDB 方法失败后还原



原因

如果还原到特定时间间隔的指定时间 (T_RESTORE) (即，使用新方法 (T_START) 开始第一次备份整个数据库之后及完成此备份之前 (T_FINISH))，RMAN 可能尝试使用为使用前一方法生成的备份文件分配的通道来还原使用新方法生成的备份文件。结果，还原过程失败。

解决方案

使用 RMAN 脚本手动还原备份会话。将所需的参数添加到已分配的通道，即此通道的 OB2PROXYCOPY=1 ，该参数将用于还原使用 proxy-copy ZDB 方法进行的备份。然后，使用正确的通道还原备份文件。

例如，如果已从备份集切换到 proxy-copy ZDB 方法，则脚本可能类似于以下内容:

```
run { ALOCATE CHANNEL 'dev_0' TYPE 'sbt_tape' PARMS 'SBT_LIBRARY=Path_to_Data_Protector_MML,
ENV(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)'; ALOCATE CHANNEL 'dev_1' TYPE 'sbt_tape' PARMS
'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)'; RESTORE DATAFILE
list_of_backup_set_backups UNTIL T_RESTORE CHANNEL 'dev_0'; RESTORE DATAFILE list_of_proxy-copy_backups UNTIL T_RESTORE CHANNEL
'dev_1'; RELEASE 'dev_0'; RECOVER DATABASE UNTIL T_RECOVER ... RELEASE 'dev_1'; }
```

其中：

T_RESTORE 指定还原时间，*T_RECOVER* 指定应用事务的时间。

list_of_backup_set_backups 是使用备份集 ZDB 方法的整个数据库的备份列表。

list_of_proxy_copy_backups 是在开始备份整个数据库 (T_START) 之后及 *T_RESTORE* 之前完成的数据文件备份列表。

遇到 ORACLE 错误 6550

在 Oracle 备份期间调用 SYS.LT_EXPORT_PKG.schema_inf_exp 时 Data Protector 报告错误。

Data Protector 监视器中列出了以下错误:

```
EXP-00008: 遇到 ORACLE 错误 6550 ORA-06550: 第 1 行第 13 列: PLS-00201: 必须声明标识符 'SYS.LT_EXPORT_PKG' ORA-06550: 第 1 行第 7 列:
PL/SQL: 声明被忽略 EXP-00083: 调用 SYS.LT_EXPORT_PKG.schema_info_exp 时发生前一个问题 。导出统计信息 导出已成功终止，但出现警告。 [重大] 来自:
ob2rman.pl@machine "MAKI" 时间: 10/01/01 16:07:53 导出恢复编目数据库失败。
```

解决方案

启动 SQL*Plus 并授予 LT_EXPORT_PKG 执行权限，如下所示 (确保事先为用户 sys 授予了 SYSDBA 特权):

```
sqlplus 'sys/password@CDB as sysdba'
```

```
SQL> grant execute on sys.lt_export_pkg to public;
```

重新启动失败的备份会话。

无法分配/附加共享内存

备份失败，并显示以下错误消息:

```
无法分配/附加共享
```

```
内存 (IPC 无法分配共享内存段) 系统错误: [13] 权限被拒绝）=> 正在中止
```

解决方案

将 OB2SHMEM_IPCGLOBAL omnirc 选项设置为 1 以正确使用内存窗口，然后重新启动失败的备份会话。

在时间点还原和恢复之后备份失败

显示以下错误：

RMAN-06004: ORACLE error from recovery catalog database: RMAN-20003: target database incarnation not found in recovery catalog

原因

发生此错误的原因是数据库的新版本未在恢复编目中注册。

解决方案

使用 RMAN 连接到目标和恢复编目数据库并重置数据库，以在恢复编目中注册数据库的新对应物:

rman target Target_Database_Login catalog Recovery_Catalog_Login

RMAN> RESET DATABASE;

RMAN> exit

Oracle 联机备份失败

Oracle 联机备份失败，并显示以下错误:

RMAN-06004: ORACLE error from recovery catalog database: RMAN-20220: controlfile copy not found in the recovery catalog

原因

运行联机备份时，Data Protector 会将 *controlfilecopy* 的文件名添加到 RMAN 备份脚本中。必须在备份命令之前将此文件名归入 RMAN 编目。发生此错误的原因是 *controlfilecopy* 文件未编目。

解决方案

要将 *controlfilecopy* 归入 RMAN 编目，请执行以下操作:

1. 在应用程序系统上连接到 RMAN。
2. 请执行以下命令：

   RMAN> catalog controlfilecopy 'CONTROL_FILE_LOCATION/ctrlDB_NAME.ctl'

无法在 **RAC** 上备份存档日志

在 RAC 上，无法备份存档日志。

原因

装载 NFS 的磁盘上未安装存档日志。

解决方案

编辑存档日志备份规范:

- 为“每个”节点添加一个额外的 allocate channel 命令。
- 添加命令以连接到每个实例。应采用 username / passwd @ INSTANCE 格式指定连接参数。

例如，如果您使用两个节点，则备份规范可能如下所示:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)' connect username/passwd@INSTANCE_1; allocate channel 'dev_2'
type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML, ENV=
(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)' connect username/passwd@INSTANCE_2; backup format
'RAC_arch<QU_%s:%t:%p>.dbf' archivelog all; }
```

无法从托管备份还原控制文件

未使用恢复编目，未使用 RMAN 自动备份功能，并且无法从 Data Protector 托管备份还原控制文件。磁带上存在有效的控制文件备份。

解决方案

从 RMAN 备份集还原控制文件，装载和还原数据库，并执行数据库恢复:

```
run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=Path_to_Data_Protector_MML'; restore controlfile from 'backup piece handle';
sql 'alter database mount'; set until time 'MMM DD YY HH24:MM:SS'; restore database; recover database; sql 'alter database open resetlogs';
release channel 'dev_0'; }
```

此时，您必须手动注册在还原控制文件备份之后所做的任何备份。然后再继续执行还原过程。

对于 *backup piece handle*，请搜索 Data Protector 内部数据库和先前备份会话的会话输出。

如何修改 RMAN 还原脚本

开始使用 Data Protector GUI 或 CLI 还原 Oracle 数据库时，会创建一个 RMAN 还原脚本，该脚本会立即运行，因此您无法先对其进行编辑。

原因

omnirc 选项 OB2RMANSAVE 不指向保存 RMAN 还原脚本的位置。

解决方案

要在脚本运行之前编辑脚本，请将 Data Protector omnirc 选项 OB2RMANSAVE 设置为指向现有目录。设置变量并开始还原后，在运行时创建的 RMAN 还原脚本将以名称 RMAN_restore_backup_specification_name.rman 保存到指定位置，并跳过实际还原。然后，便可编辑脚本，再手动运行。

要再次使用 Data Protector 启动还原，请清除 OB2RMANSAVE 选项，方法是删除其内容或者注释或删除整个选项。如果您在 Windows 系统上注释或删除此选项，请重新启动 Data Protector Inet 服务以使设置生效。

即时恢复 Oracle 数据库失败

Oracle 数据库的即时恢复会话失败，并显示类似如下的消息:

```
[正常] 来自: ob2rman@x64-node1.x64ring.com "testdb" 时间: 2/7/2008 10:48:19 AM 正在启动目标数据库即时恢复。 网络服务名称: testdb。 实例状态: . 实例名称: . 数据库 DBID = 。 数据库控制文件类型: . 数据库日志模式: . [重大] 来自: ob2rman@x64-node1.x64ring.com "testdb" 时间: 2/7/2008 10:48:20 AM 执行请求的操作时，数据库报告错误。
```

请注意，数据库参数为空，Data Protector 无法连接到 Oracle 数据库时会出现此状况。

原因

Data Protector 未连接到 Oracle 数据库。

解决方案

即使数据库处于 Mount 或 Nomount 状态，Data Protector 也必须能够连接到 Oracle 数据库。实现此目标的一种方法是为 Oracle 侦听程序配置静态服务信息。

以下示例显示如何使用 Oracle Net Manager 配置静态服务信息。

假设您有以下环境:

侦听程序名称: LISTENER
全局数据库名称: orcl
Oracle SID: ORCL

要为侦听程序配置静态服务信息，请打开 Oracle Net Manager，选择侦听程序，转到 **Database Services** 上下文，添加数据库并指定 Oracle 数据库参数。

此后， listener.ora 文件将更新 SID_LIST_LISTENER 部分。

```
SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (GLOBAL_DBNAME = orcl) (SID_NAME = ORCL) ) )
```

最后，重新启动 Oracle 侦听程序服务以应用更改。

IPC 主机名或 IP 地址无效

在 Data Protector GUI 还原上下文中浏览 Oracle 数据库的还原会话时，显示以下错误消息:

IPC Invalid Hostname or IP Address

原因

发生此问题的原因是:

- 将数据库项还原到其他客户机时。
- 从另一个 Data Protector 单元导入包含 Oracle 数据库备份的 Data Protector 介质时。

解决方案

要成功将数据库项还原到其他客户机，请确保将启动 Data Protector Oracle 集成代理的系统配置为 Data Protector Oracle 数据库实例 ("ORACLE_SID")。

要进行验证，请检查它是否列在“选项”页面中的“客户机”下拉列表中。

选择系统并继续执行还原 Oracle 数据库对象过程的步骤 7。

显示 **RMAN** 备份脚本错误

在 Data Protector GUI 中，当您编辑 Data Protector 备份规范的 RMAN 脚本部分时，将显示以下错误消息:

```
Cannot proceed, invalid RMAN backup script.
```

原因

如果指定了 Oracle RMAN 参数，但 Data Protector 分析程序未能识别或发生分析错误，则会显示此错误。

解决方案

将 Data Protector `NoGUIRMANScriptParsing` 全局选项设置为 `1` ，在 Data Protector GUI 中禁用 Oracle RMAN 脚本分析。

恢复管理器中的致命错误

Oracle RMAN 失败，并显示以下错误消息:

RMAN-06900: 警告: 无法生成 V$RMAN_STATUS 或 V$RMAN_OUTPUT 行

RMAN-06901: 警告: 正在禁用 V$RMAN_STATUS 和 V$RMAN_OUTPUT 行更新

RMAN-06003: 目标数据库发生 ORACLE 错误:

ORA-03113: 通信信道上出现文件结尾

进程 ID: 4222

会话 ID : 29 序列号: 51

..

RMAN-00569: ========== 继续列出错误消息 ==========

RMAN-00571: ===

RMAN-00601: Recovery Manager 中发生致命错误

RMAN-03004: 执行命令时发生致命错误

原因

发生此错误是因为恢复过程超时。

解决方案

在 sqlnet.ora 文件中，增加 SQLNET.RECV_TIMEOUT 值。

PostgreSQL 集成故障诊断

This feature is available in the Express Edition

本主题列出了使用 Data Protector PostgreSQL 集成时所需的常规检查和验证操作。

开始之前

- 确保已安装最新补丁。

检查和验证

- 如果无法在 Data Protector 中配置 PostgreSQL 实例，或者备份或还原会话失败:
  - 确认是否在用于备份和还原的每台 PostgreSQL 主机上安装了 Data Protector“PostgreSQL 集成”组件。
  - 检查 PostgreSQL 主机上 Data Protector debug.log 文件中记录的错误。
  - 对存储 PostgreSQL 数据的卷执行系统文件备份和还原。
- 如果备份或还原会话失败:
  - 检查在操作系统事件日志中记录的错误。
- 如果备份会话失败:
  - 如第 1 页的“配置集成”中所述，检查涉及到的 PostgreSQL 实例的配置。
- 如果还原会话失败:
  - 检查是否向 Data Protector operator 用户组分配了查看私有对象用户权限。
  - 检查正在使用的备份版本是否由用于还原的同一代理创建 (备份)。

SAP HANA 集成故障诊断

This feature is available in the Premium Edition

本主题列出了使用 Data Protector SAP HANA 集成时可能会遇到的问题。

开始之前

- 确保已安装最新的 Data Protector 补丁。

问题

下面是使用 Data Protector SAP HANA 集成时可能会遇到的一些问题：

分布式 SAP HANA 环境中备份会话失败

在分布式 SAP HANA 环境中从 SAP HANA Studio 调用会话来备份数据库或对应的重做日志时，该会话失败并报告以下错误:

Backup of system InstanceID failed.

Backup could not be completed, Backint cannot execute PathnameOfSymbolicLinkToBackintAgent, No such file or directory (2)

原因

故障原因可能是某些 SAP HANA 系统上缺少 Data Protector“SAP HANA 集成”组件。

解决方案

在缺少 Data Protector“SAP HANA 集成”组件的所有 SAP HANA 系统上安装该组件，然后重新启动会话。

恢复会话失败，且出现日志错误

SAP HANA 在恢复期间报告以下错误:

```
RECOVER DATA 完成，但出现以下错误: 恢复无法完成，卷 <volumeID>，到达日志位置 <LSN>， 服务 '<serviceName>' 在 '<backupID>' 的日志备份的日志段找不到，卷 id '<volumeID>'，状态 '到达日志结尾'
```

原因

此故障的原因可能是还原链断开。

解决方案

可以执行以下操作之一：

- 使用“清除日志”功能。它确保仅恢复日志备份中的日志条目。
- 还原到前述错误消息中的 LSN 指出的特定日志位置。

SAP HANA Studio 中的 SAP HANA 备份或还原失败

从 SAP HANA Studio 启动 SAP HANA 备份或还原时，备份或还原立即失败。由于 Data Protector 会话未启动，因此无法排查该故障。

解决方案

可以执行以下操作：

- 在“备份”>“配置”>“Backint 设置”上下文中检查“Backint 代理”选项，以确认是否已在 SAP HANA Studio 中正确链接 backint 代理。
- 确认执行 SAP HANA 备份或还原的用户是否已添加到 Data Protector 用户列表。

Data Protector SAP HANA 并行备份会话可能会失败

Data Protector SAP HANA 并行备份会话失败，并显示以下错误消息:

|Major| From: OB2BAR_SAPHANA_BACKINT@<hostname> "" Time:<Date >>Time>

Aborting connection to BSM. Abort code -2.

解决方案

在 global.ini 文件中将 SAP HANA 变量 max_log_backup_group_size 设置为 1。

SAP HANA hdbbackint 异常终止并显示错误消息

升级到 Data Protector 9.03 后，hdbbackint 异常终止，并导致会话推迟且日志中记录了以下错误消息:

[Major] From: OB2BAR_SAPHANA_BACKINT@<hostname> "" Time: <Date><Time> Aborting connection to BSM. Abort code 2.

或

[Major] From: BSM@<hostname> "" Time: <Date><Time> |61:1005| Got unexpected close from OB2BAR Backup DA on <ip_address>.

解决方案

将 backint_response_timeout SAP HANA 参数设置为 600 秒 (10 分钟)。这是默认超时。

> 注意您可以通过编辑 global.ini 文件中的 backint_response_timeout 参数来调整该超时。

SAP HANA 中出现错误

SAP HANA 中出现错误

未找到任何数据备份

DP 中出现错误

#NOTFOUND "/usr/sap/HAN/SYS/global/hdb/backint/log_backup_0_0_0_0"

解决方案

在参数文件中确认主机名 **OB2BARHOSTNAME** 是否正确。

SAP HANA 还原失败

适用于 SAP HANA 的 Data Protector 无法定位租户 MDC 数据库还原对象。

尝试检索对象 /usr/sap/DEV/SYS/global/hdb/backint/COMPLETE_DATA_BACKUP_DEV_databackup_0_1 时， hdbbackint 失败，并显示 #NOTFOUND 。

Data Protector IDB 上现有的对象命名为 /usr/sap/DEV/SYS/global/hdb/backint/DB_DEV/COMPLETE_DATA_BACKUP_DEV_databackup_0_1 。此名称包括 DB_DEV 数据库名称。

原因

SAP HANA 应用程序格式化对象名称，按 SID、备份前缀和提供用于还原的数据库备份信息进行检索。

解决方案

在 MDC 环境中还原租户数据库时，需要使用 SID 上的 DB 名称指定还原的数据库。SAP 管理手册中进行了相关说明。请参阅 https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.02/en-US/39dc3f370efe4f2983a8be5e6dfeda8c.html

SAP MaxDB 集成故障诊断

This feature is available in the Premium Edition

本主题列出了使用 Data Protector SAP MaxDB 集成时可能会遇到的问题。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。请参阅索引: 有关如何执行此验证的“修补程序”。

与 SAP MaxDB 群集相关的故障诊断

在群集环境中，在客户机上从命令行执行某些过程之前，必须将环境变量 OB2BARHOSTNAME 定义为群集虚拟系统的名称。 OB2BARHOSTNAME 变量设置如下:

Windows 系统

```
set OB2BARHOSTNAME=VirtualSystemName
```

UNIX 系统

```
export OB2BARHOSTNAME=VirtualSystemName
```

问题

下面是使用 Data Protector SAP MaxDB 集成时可能会遇到的一些问题：

Data Protector 在备份或还原期间报告错误

报告了以下错误：

```
[严重] 来自: OB2BAR_SAPDBBAR@machine.company.com "INSTANCE" 时间: 02/06/04 18:17:18 错误: SAPDB 响应以下内容: -24920,ERR_BACKUPOP: 备份操作不成功 数据库无法满足请求 (-2025，备份设备数量无效)。
```

解决方案

将 SAP MaxDB MAXBACKUPDEVS 参数的值增加到大于或等于 Data Protector“并行性”选项的值，或者减小 Data Protector“并行性”选项的值。

还原后无法启动 SAP MaxDB 实例

解决方案

使用 SAP MaxDB db_restartinfo 命令检查是否可以重新启动实例。

- 如果无法重新启动实例，则现有日志卷很可能没有足够的数据以从数据卷重新启动实例。所需的差异备份或事务备份可能尚未还原。
- 如果可以重新启动实例，请检查 SAP MaxDB 实例内核错误文件以查找错误。

  如果某些时间点的 SAP MaxDB 日志空间不足，则日志可能已损坏。此时请删除日志 (使用 dbmcli util_execute clear log 命令) 或联系 SAP MaxDB 或 Data Protector 支持人员。

用于从对象副本还原数据的还原会话被阻止

解决方案

在重新启动还原之前:

- 增加用于还原的设备的磁盘代理缓冲区数。
- 如果备份的所有对象都记录在 IDB 中，请执行以下步骤:
  1. 在 Data Protector GUI 的内部数据库上下文中，搜索属于同一备份的所有对象。对象由相同的备份 ID 标识。
  2. 将单独的对象复制会话中的每个对象复制到单独的设备，例如文件库。对于每个对象，请使用具有不可追加介质策略的单独介质。
  3. 为新创建的副本设置最高介质位置优先级。

SAP MaxDB 数据库处于 histlost 状态

初始化日志卷时 (例如在还原或恢复后)，数据库处于 histlost 状态。因此，在此状态下无法成功执行还原或恢复。例如，恢复失败并显示以下错误:

```
错误: SAPDB 响应以下内容: -24920,ERR_BACKUPOP: 备份操作不成功 数据库无法满足请求 (-9407，系统错误: 意外错误)。
```

解决方案

还原或恢复后，执行完整备份以启动新的备份历史记录。如果在还原或恢复期间发生此错误，请执行 `db_execute clear log` 命令并重复还原或恢复操作。

未能与数据库群集的节点 (本地) 建立连接

报告了以下错误：

```
错误: SAPDB 响应以下内容: 错误! 未能与数据库群集的节点 (本地) 建立连接: 连接被拒绝: x_server 未运行。
```

解决方案

启动 SAP MaxDB x_server。有关详细信息，请参阅 SAP MaxDB 文档。

数据库未运行

报告了以下错误：

```
错误: SAPDB 响应以下内容: -24988，ERR_SQL: sql 错误 1，数据库未运行。
```

解决方案

启动 SAP MaxDB 实例。有关详细信息，请参阅 SAP MaxDB 文档。

实用程序会话已在使用中

Data Protector 报告以下错误:

```
错误: SAPDB 响应以下内容: -24988，ERR_SQL: sql error1，实用程序会话已在使用中。
```

原因

发生此错误的原因是，其他用户已连接到 SAP MaxDB 实例并正在执行管理任务 (实用程序会话)。

解决方案

此类 SAP MaxDB 任务属于“实用程序”类型，可以使用 dbmcli show task 命令显示。在运行新任务之前，请确保正在运行的任务已完成。

用户身份验证失败

Data Protector 报告以下错误:

```
错误: SAPDB 响应以下内容: -24950，ERR_USRFAIL: 用户身份验证失败。
```

原因

用户授权失败时，会发生此错误。

解决方案

按照“配置 SAP MaxDB 实例”一节中的说明重新配置 SAP MaxDB 实例。

备份操作失败

Data Protector 在备份或还原期间报告以下错误:

```
错误: SAPDB 响应以下内容: -24920,ERR_BACKUPOP: 备份操作不成功 备份工具被终止，且退出代码总和为 -1。 数据库请求终止且显示代码 0。
```

解决方案

通过执行以下命令在 Cell Manager 上设置 TimeoutSuccess 环境变量:

> 必须在 Cell Manager 上执行命令 util_cmd 。要使用它，必须在运行命令之前定义环境变量 OB2BARHOSTNAME 。
>
> 设置 OB2BARHOSTNAME=client_name (Windows) 或 OB2BARHOSTNAME=client_name (Linux)

```
util_cmd -putopt SAPDB SAPDB_instance TimeoutSuccess 1000 -sublist Environment
```

有关详细信息，请参阅 util_cmd 手册页。

还可以使用 Data Protector GUI 设置 TimeoutSuccess 环境变量。在“范围窗格”中选择备份规范，然后在“源”选项卡下的“结果窗格”中右键单击 SAP MaxDB 实例对象，并从弹出菜单中选择“设置环境变量”。

SAP R/3 集成故障诊断

This feature is available in the Premium Edition

本主题列出了使用 Data Protector SAP R/3 时的常规检查和验证操作以及可能会遇到的问题。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。请参阅索引: 有关如何执行此验证的“修补程序”。
- 请参阅发行说明了解一般限制以及已知问题和解决方法。

Windows 系统上的故障诊断

集成中 Oracle 方面的先决条件

故障诊断时有必要执行以下步骤，验证是否已按要求安装 Oracle 以使集成正常工作。这些步骤不包括验证 Data Protector 组件。

1. **验证能否访问 Oracle 目标数据库并打开它，具体步骤如下:**

   设置 ORACLE_HOME 和 ORACLE_SID 变量。

   从 ORACLE_HOME 目录启动 SQL Plus:

   bin\sqlplus

   在 SQL 提示符下，键入:

   connect user/passwd@service

   select * from dba_tablespaces;

   exit

   如果失败，请打开 Oracle 目标数据库。

2. **验证是否为 Oracle 目标数据库正确配置了 TNS 侦听程序。这是正确建立网络连接所必需的:**

   从 ORACLE_HOME 目录启动该侦听程序:

   bin\lsnrctl status service

   quit

   如果失败，请启动 TNS 侦听程序进程，并查看 Oracle 文档以了解有关如何创建 TNS 配置文件 (LISTENER.ORA) 的说明。

   该侦听程序进程可以从 Windows 桌面启动。在“控制面板”中，转到“管理工具”、“服务”。

   1. “服务”窗口中相应侦听程序服务的状态应为“已启动”，否则必须手动启动相应的侦听程序。
   2. 从 ORACLE_HOME 目录启动 SQL Plus:

      在 SQL 提示符下，键入:

      connect Target_Database_Login

      exit

      如果失败，请参阅 Oracle 文档以了解有关如何创建 TNS 配置文件 (TNSNAMES.ORA) 的说明。

3. **如果在 RMAN 模式下运行备份，请验证 Oracle 目标数据库是否配置为允许具有系统特权的远程连接:**

   按照步骤 1 所述设置 ORACLE_HOME ，然后从 ORACLE_HOME 目录启动 Server Manager:

   bin\svrmgrl

   在 wSVRMGR 提示符下，键入

   connect Target_Database_Login as SYSDBA;

   exit

   使用 SYSOPER 而不是 SYSDBA. 重复此过程。设置 ORACLE_HOME 目录

   如果正在使用恢复编目:

   bin\rman target Target_Database_Login rcvcat Recovery_Catalog_Login

   如果未在使用恢复编目:

   bin\rman target Target_Database_Login nocatalog

   如果失败，请参阅 Oracle 文档以了解有关如何在 initORACLE_SID.ora 文件中设置密码文件和任何相关参数的说明。

集成中 SAP 方面的先决条件

故障诊断时有必要执行以下验证步骤，验证是否已按要求安装 SAP 以使集成正常工作。这些步骤不包括验证 Data Protector 组件。

1. **验证能否直接备份到磁盘，如下所示:**

   brbackup -d disk -u user/password

   如果失败，请在继续之前检查错误消息并解决可能的问题。

2. **验证能否直接还原到磁盘，如下所示:**

   brrestore -d disk -u user/password

   如果失败，请在继续之前检查错误消息并解决可能的问题。

3. **如果在 RMAN 模式下运行备份，请使用 Recovery Manager 通道类型磁盘验证能否直接备份和还原到磁盘，如下所示:**

   a. 必须在初始化文件 init ORACLE_SID. ora 中定义参数 init 。执行以下命令：

      brrestore -d pipe -u user/password -t online -m all

      brrestore -d disk -u user/password

   b. 如果失败，请参阅《SAP 联机帮助》，了解如何使用 SAP 备份实用程序直接备份和还原到磁盘。

   在继续之前，请检查错误消息并解决这些问题。

4. **验证 SAP 备份工具能否正确启动 backint (由 Data Protector 提供):**

   移动原始 backint 并在 SAP 备份实用程序所在的目录中创建含有以下条目的测试脚本 namedbackint.bat:

   ```
   echo "Test backint called as follows:" echo "%0%1%2%3%4%5%6%7%8%9" exit
   ```

   然后启动以下命令:

   brbackup -t offline -d util_file -u user/password -c

如果收到 backint 参数，这意味着 SAP 已正确配置为使用 backint 进行备份；否则必须重新配置 SAP。

请参阅“配置 SAP R/3 数据库”。

配置问题

> **重要说明**开始检查 Data Protector 配置之前，必须执行前一节中所述的步骤。

1. **验证 Data Protector 软件是否已正确安装。**

   有关详细信息，请参阅“安装”。

2. **对 SAP 数据库服务器执行文件系统备份。**

   对 SAP 数据库服务器系统执行文件系统备份，以便消除 SAP 数据库服务器与 Data Protector Cell Manager 系统之间的任何潜在通信问题。

   除非已成功完成 SAP 数据库服务器系统的文件系统备份，否则不要开始对联机数据库备份进行故障诊断。

   有关如何执行文件系统备份的详细信息，请参阅“标准备份过程”索引。

3. **如果 SAP 备份实用程序安装在共享目录中，则必须按步骤 4 中所述指定 inet 启动参数，否则必须正确设置 Windows 权限。**

   执行以下命令 (如果使用默认目录):

   dir \\client_name\sapmnt\ORACLE_SID\SYS\exe\run\brbackup

   或

   dir \\client_name\SAPEXE\brbackup

   如果失败，请设置 inet 启动参数，或设置正确的访问权限以访问 Windows 网络目录。

4. **如果使用命令行启动 Data Protector 命令，请验证 inet 启动参数。**

   检查 SAP 数据库服务器系统上的 Data Protector Inet 服务启动参数。请执行以下操作：

   a. 在“控制面板”中，转到“管理工具”、“服务”。

b. 选择 Select Data Protector **Inet**。

在“服务”窗口中，选择 Data Protector“Inet，启动”。

该服务必须在指定的用户帐户下运行。确保同一用户也已经添加到 admin 用户组。

5. **检查环境变量。**

如果需要在启动 Oracle Server Manager、TNS 侦听程序或其他 Oracle 实用程序之前导出某些变量，必须在 Cell Manager 上 Data Protector SAP 配置文件的 Environment 部分中定义这些变量。请参阅“SAP R/3 配置文件”。

6. **检查系统错误。**

SAP Server 上的 debug.log 文件中会报告系统错误。

备份问题

在此阶段，您应该已执行前面几节中说明的所有验证步骤。如果备份仍然失败，请继续执行以下步骤:

1. **检查 SAP Server 配置:**

要检查配置，请在 SAP Server 系统上启动以下命令:

```
Data_Protector_home\bin\util_sap.exe -CHKCONF ORACLE_SID
```

消息 *RETVAL*0 表示配置成功。

2. **使用 testbar2 实用程序验证 Data Protector 内部数据传输。**

运行 testbar2 实用程序之前，请验证是否在 SAP 数据库服务器上正确定义了 Cell Manager 名称。在默认的 Data Protector 客户机配置目录中，检查 cell_server 文件，其中包含 Cell Manager 系统的名称。然后执行以下命令:

```
Data_Protector_home\bin\testbar2 -type:SAP -appname:ORACLE_SID -bar:backup_specification_name -perform:backup
```

在 Data Protector“监视器”上下文中单击“详细信息”按钮，检查 testbar2 实用程序报告的错误。

如果消息指示集成中 Data Protector 方面出现问题，请创建一个 SAP 备份规范来备份到空设备或文件设备。如果备份成功，则问题可能与备份设备有关。如果测试再次失败，请致电支持部门。

3. **验证使用 backint 的备份**

```
export OB2BARLIST=barlist_name
```

```
export OB2APPNAME=ORACLE_SID
```

```
Data_Protector_home\bin\backint.exe -f backup -t file -u ORACLE_SID -i input_file
```

其中 input_file 是包含备份的完整路径名列表的文件。

Backint 需要使用以下格式的文件列表: pathName_1 pathName_2 pathName_3

还原问题

在此阶段，您应该已执行前面几节中说明的所有验证步骤。然后请继续执行以下步骤:

1. **验证备份介质和 IDB 中是否存在备份对象:**

为此，可以在 SAP 数据库服务器系统上执行以下命令:

```
omnidb -sap "object_name" -session "Session_ID" -media
```

。

该命令的输出会列出有关指定备份对象的详细信息、包含此对象的备份会话的会话 ID 以及所用介质的列表。

有关 omnidb 命令的详细语法，请执行:

```
omnidb -help
```

也可以使用 SAP 工具执行此操作:

使用 backint，以便 SAP 工具也使用此命令来查询:

```
Data_Protector_home\bin\backint.exe -f inquiry -u ORACLE_SID -i input_file
```

这时会查询指定的 input_file 。

如果失败，请检查备份会话是否已成功执行以及是否在相应的用户帐户下启动了查询。

Backint 需要使用以下格式的文件列表:

backup_ID_1 pathName_1 [targetDirectory_1]

backup_ID_2 pathName_2 [targetDirectory_2]

backup_ID_3 pathName_3 [targetDirectory_3]

要检索 backup_ID 编号，请输入以下命令:

```
echo #NULL #NULL | backint –f inquiry –u ORACLE_SID
```

或者，也可以在 input_file 中为 backup_ID_1 指定 #NULL。在这种情况下，该文件的最新备份会话会用于还原。

2. **验证使用 Data Protector 用户界面的还原**

   如果对象已由 backint 备份，则可以执行此测试。

   如果失败，请检查备份会话是否已成功执行以及是否在相应的用户帐户下启动了查询。

3. **模拟还原会话**

   了解有关要还原的对象的信息后，可以使用 Data Protector testbar2 实用程序模拟还原。

   执行 testbar2 之前，请验证是否在 SAP 数据库服务器上正确定义了 Cell Manager 名称。

   在默认 Data Protector 客户机配置目录中，检查 cell_server 文件，其中包含 Cell Manager 系统的名称。

   然后，使用 testbar2 实用程序测试 Data Protector 内部数据传输:

   ```
   Data_Protector_home\bin\testbar2 -type:SAP
   -appname:ORACLE_SID
   -perform:restore
   -object:object_name
   -version:object_version
   -bar:backup_specification_name
   ```

   这时应该只看到屏幕上显示 NORMAL 消息。否则，请在 Data Protector“监视器”上下文中单击“详细信息”按钮，检查 testbar2 实用程序报告的错误。

4. **验证使用 backint 的还原**

   请执行以下命令：

   ```
   Data_Protector_home\bin\backint.exe -f restore -u ORACLE_SID -i input_file
   ```

   这时会还原 input_file 的内容。

   如果失败，请检查会话是否已成功执行以及是否在相应的用户帐户下启动了还原。

   Backint 需要使用以下格式的文件列表: backup_ID_1 pathName_1 [targetDirectory_1]backup_ID_2pathName_2 [targetDirectory_2]backup_ID_3pathName_3 [targetDirectory_3]

   要检索 backup_ID 编号，请输入以下命令:

   ```
   echo "#NULL #NULL" | backint –f inquiry –u ORACLE_SID
   ```

UNIX 系统上的安装故障诊断

集成中 Oracle 方面的先决条件

故障诊断时有必要执行以下步骤，验证是否已按要求安装 Oracle 以使集成正常工作。这些步骤不包括验证 Data Protector 组件。

1. **验证能否访问 Oracle 目标数据库并打开它，具体步骤如下:**

   按照如下方式导出 ORACLE_HOME 和 ORACLE_SID：

   - 如果使用 SH 类 shell，请输入以下命令:

     ```
     ORACLE_HOME="ORACLE_HOME"
     export ORACLE_HOME
     ORACLE_SID ="ORACLE_SID"
     export ORACLE_SID
     ```

   - 如果使用 CSH 类 shell，请输入以下命令:

     ```
     setenv ORACLE_HOME "ORACLE_HOME"
     setenv ORACLE_SID "ORACLE_SID"
     ```

   从 ORACLE_HOME 目录启动 SQL Plus:

   ```
   bin\sqlplus
   ```

   在 SQL 提示符下，键入:

   ```
   connect user/passwd@service
   select * from dba_tablespaces;
   ```

exit

如果失败，请打开 Oracle 目标数据库。

2. **验证是否为 Oracle 目标数据库正确配置了 TNS 侦听程序。这是正确建立网络连接所必需的:**

   按步骤 1 中所述导出 ORACLE_HOME 并从 ORACLE_HOME 目录启动侦听程序:

   bin/lsnrctl start service

   exit

   如果失败，请启动 TNS 侦听程序进程，并查看 Oracle 文档以了解有关如何创建 TNS 配置文件（LISTENER.ORA）的说明。

   按步骤 1 中所述导出 ORACLE_HOME 并从 ORACLE_HOME 目录启动 SQL Plus:

   bin\sqlplus

   在 SQL 提示符下，键入:

   connect Target_Database_Login

   exit

   如果失败，请参阅 Oracle 文档以了解有关如何创建 TNS 配置文件（TNSNAMES.ORA）的说明。

3. **如果在 RMAN 模式下运行备份，请验证 Oracle 目标数据库是否配置为允许具有系统特权的远程连接:**

   按步骤 1 中所述导出 ORACLE_HOME 并从 ORACLE_HOME 目录启动 SQL Plus:

   bin/svrmgrl

   在 SQL 提示符下，键入:

   connect Target_Database_Login as SYSDBA;

   exit

   使用 SYSOPER 而不是 SYSDBA. 重复此过程。设置 ORACLE_HOME 目录

   如果使用恢复编目:

   bin/rman target Target_Database_Login rcvcat Recovery_Catalog_Login

   如果未使用恢复编目:

   bin/rman target Target_Database_Login nocatalog

   如果失败，请参阅 Oracle 文档以了解有关如何在 initORACLE_SID.ora 文件中设置密码文件和任何相关参数的说明。

4. **如果在 RMAN 模式下运行备份，请使用 Recovery Manager 通道类型磁盘验证能否直接备份和还原到磁盘。**

   如果使用恢复编目:

   按步骤 1 中所述导出 ORACLE_HOME 并启动 Recovery Manager:

   bin/rman target Target_Database_Login rcvcat Recovery_Catalog_Login cmd_file=rman_script

   如果未使用恢复编目:

   按步骤 1 所述导出 ORACLE_HOME 并启动 Recovery Manager:

   bin/rman target Target_Database_Login nocatalog cmd_file=rman_script

   下面列出了 rman_script 的示例:

   ```
   run { allocate channel 'dev0' type disk; backup (tablespace tablespace_nameformat '
   ```

   ```
   ORACLE_HOME /tmp/datafile_name'); }
   ```

   成功备份后，请尝试执行以下还原脚本，还原备份的表空间:

   ```
   run { allocate channel 'dev0' type disk; sql 'alter tablespace tablespace_name offline immediate'; restore tablespace tablespace_name;
   recover tablespace tablespace_name; sql 'alter tablespace tablespace_name online'release channel 'dev0'; }
   ```

   如果上述过程之一失败，请参阅 Oracle 文档以了解如何使用 Recovery Manager 直接备份和还原到磁盘。

集成中 SAP 方面的先决条件

故障诊断时有必要执行以下验证步骤，验证是否已按要求安装 SAP 以使集成正常工作。这些步骤不包括验证 Data Protector 组件。

1. **验证能否直接备份到磁盘，如下所示:**

   brbackup -d disk -u user/password

如果失败，请在继续之前检查错误消息并解决可能的问题。

2. **验证能否直接还原到磁盘，如下所示：**

   brrestore -d disk -u user/password

   如果失败，请在继续之前检查错误消息并解决可能的问题。

3. **如果在 RMAN 模式下运行备份，请使用 Recovery Manager 通道类型磁盘验证能否直接备份和还原到磁盘，如下所示：**
   __COMMENT_Obsolete 符号链接，Gordana_COMMENT__

   a. 将 Oracle Server 与 SAP 提供的数据库例程库 (libobk.sl) 重新链接起来。

      对于每个 RMAN 通道，将 SBT_LIBRARY 参数设置为指向 libobk.sl 文件。

      > **重要说明**
      >
      > 在 RMAN 模式下再次使用 Data Protector 前，必须再次将 Oracle 与 Data Protector 数据库例程库重新链接起来。

   b. 您必须在初始化文件 init ORACLE_SID . ora 中定义参数 init 。

      执行以下命令：

      brrestore -d pipe -u user/password -t online -m all

      brrestore -d disk -u user/password

      如果失败，请参阅《SAP 联机帮助》，了解如何使用 SAP 备份实用程序直接备份和还原到磁盘。在继续之前，请检查错误消息并解决此问题。

4. **验证 SAP 备份工具能否正确启动 backint (由 Data Protector 提供)：**

   移动原始 backint 并在 SAP 备份实用程序所在的目录中创建含有以下条目的测试脚本 backint :

   ```
   #!/usr/bin/sh echo "Test backint called as follows:" echo "$0 $*" echo "exiting 3 for a failure" exit 3
   ```

   然后，按“配置用户帐户”中所述，以 Oracle 数据库用户的身份启动以下命令:

   brbackup -t offline -d util_file -u user/password -c

如果收到 backint 参数，这意味着 SAP 已正确配置为使用 backint 进行备份；否则必须重新配置 SAP。

配置问题

> **重要说明**开始检查 Data Protector 配置之前，必须执行前一节中所述的步骤。

1. **验证 Data Protector 软件是否已正确安装。**

   有关详细信息，请参阅“安装”。

2. **对 SAP R/3 数据库服务器执行文件系统备份：**

   对 SAP 数据库服务器系统执行文件系统备份，以便消除 SAP 数据库服务器与 Data Protector Cell Manager 系统之间的任何潜在通信问题。

   除非已成功完成 SAP 数据库服务器系统的文件系统备份，否则不要开始对联机数据库备份进行故障诊断。

3. **检查环境变量：**

   如果需要在启动 Oracle Server Manager、TNS 侦听程序或其他 Oracle 实用程序之前导出某些变量，必须在 Cell Manager 上 Data Protector SAP 配置文件的 Environment 部分中定义这些变量。

4. **验证当前使用的用户帐户的权限：**

   您的用户帐户必须具有足够权限，可以使用 Data Protector 执行备份或还原。使用 testbar2 实用程序检查权限:

   /opt/omni/bin/utilns/testbar2 -perform:checkuser

   如果用户帐户拥有所有必需的权限，您只会看到屏幕上显示 NORMAL 消息。

   另请参阅“配置用户帐户”。

5. **检查系统错误：**

   系统错误在 SAP 服务器上的 /var/opt/omni/log/debug.log 文件 (HP-UX、Solaris 和 Linux 系统) 或 /usr/omni/log/debug.log 文件 (其他 UNIX 系统) 中报告。

备份问题

在此阶段，您应该已执行前面几节中说明的所有验证步骤。如果备份仍然失败，请继续执行以下步骤:

1. **检查 SAP Server 配置:**

   要检查配置，请在 SAP Server 系统上启动以下命令:

   /opt/omni/lbin/util_sap.exe -CHKCONF ORACLE_SID (HP-UX、Solaris 和 Linux 系统) 或

   /usr/omni/bin/util_sap.exe -CHKCONF ORACLE_SID (其他 UNIX 系统)

   如果出现错误，错误编号将以 *RETVAL*Error_number 格式显示。

   要获取错误说明，请启动以下命令:

   /opt/omni/lbin/omnigetmsg 12 Error_number (HP-UX、Solaris 和 Linux 系统) 或

   /usr/omni/bin/omnigetmsg 12 Error_number (其他 UNIX 系统)

   消息 *RETVAL*0 表示配置成功。

2. **使用 testbar2 实用程序验证 Data Protector 内部数据传输。**

   运行 testbar2 实用程序之前，请验证是否在 SAP 数据库服务器上正确定义了 Cell Manager 名称。检查 /etc/opt/omni/client/cell_server 文件 (HP-UX、Solaris 和 Linux 系统) 或 /usr/omni/config/cell/cell_server 文件 (其他 UNIX 系统)，其中包含 Cell Manager 系统的名称。然后执行以下命令:

   /opt/omni/bin/utilns/testbar2 -type:SAP -appname:ORACLE_SID -bar:backup_specification_name -perform:backup (HP-UX、Solaris 和 Linux 系统)

   /usr/omni/bin/utilns/testbar2 -type:SAP -appname:ORACLE_SID -bar:backup_specification_name -perform:backup (其他 UNIX 系统)

   在 Data Protector“监视器”上下文中单击“详细信息”按钮，检查 testbar2 实用程序报告的错误。

   如果消息指示集成的 Data Protector 方面出现问题，请继续执行以下步骤:

   a. 检查备份规范的所有者是否为“配置用户帐户”中所述的 Oracle OS 用户
   b. 检查各个 Data Protector 用户组是否已启用“查看私有对象”用户权限。
   c. 创建用于备份到空设备或文件设备的 SAP 备份规范。如果备份成功，则问题可能与备份设备有关。

      如果测试再次失败，请致电支持部门。

3. **验证使用 backint 的备份**

   export OB2BARLIST=barlist_name

   export OB2APPNAME=ORACLE_SID

   /opt/omni/lbin/backint -f backup -t file -u ORACLE_SID -i input_file(HP-UX、Solaris 和 Linux 系统)

   /usr/omni/bin/backint -f backup -t file -u ORACLE_SID -i input_file(其他 UNIX 系统)

   其中 input_file 是包含备份的完整路径名列表的文件。

   Backint 需要使用以下格式的文件列表: pathName_1pathName_2pathName_3

还原问题

在此阶段，您应该已执行前面几节中说明的所有验证步骤。然后请继续执行以下步骤:

1. **验证为还原指定的用户:**

   验证为还原会话指定的用户是否为备份会话的用户以及他们是否为 Data Protector operator 或 admin 组的成员。

   请参阅“配置用户帐户”。

2. **验证备份介质和 IDB 中是否存在备份对象:**

   为此，可以在 SAP 数据库服务器系统上执行以下命令:

   omnidb -sap "object_name" -session "Session_ID" -media (HP-UX、Solaris 和 Linux 系统) 或

   omnidb -sap "object_name" -session "Session_ID" -media (其他 UNIX 系统)

   。

   该命令的输出会列出有关指定备份对象的详细信息、包含此对象的备份会话的会话 ID 以及所用介质的列表。

   有关 omnidb 命令的详细语法，请执行:

   omnidb -help (HP-UX、Solaris 和 Linux 系统)

   omnidb -help (其他 UNIX 系统)

也可以使用 SAP 工具执行此操作:

使用 backint，以便 SAP 工具也使用此命令来查询:

/opt/omni/lbin/backint -f inquiry -u ORACLE_SID -i input_file (HP-UX、Solaris 和 Linux 系统)

/usr/omni/bin/backint -f inquiry -u ORACLE_SID -i input_file(其他 UNIX 系统)

这时会查询指定的 input_file 。

如果失败，请检查备份会话是否已成功执行以及是否在相应的用户帐户下启动了查询。

Backint 需要使用以下格式的文件列表:

backup_ID_1 pathName_1 [*targetDirectory_1*]

backup_ID_2 pathName_2 [*targetDirectory_2*]

backup_ID_3 pathName_3 [*targetDirectory_3*]

要检索 backup_ID 编号，请输入以下命令:

echo "#NULL #NULL" | backint –f inquiry –u ORACLE_SID

或者，也可以在 input_file 中为 backup_ID_1 指定 #NULL 。在这种情况下，该文件的最新备份会话会用于还原。

3. **验证使用 Data Protector 用户界面的还原**

   如果对象已由 backint 备份，则可以执行此测试。

   如果失败，请检查备份会话是否已成功执行以及是否在相应的用户帐户下启动了查询。

4. **模拟还原会话**

   了解有关要还原的对象的信息后，可以使用 Data Protector testbar2 实用程序模拟还原。

   运行 testbar2 前，请验证是否在 SAP 数据库服务器上正确定义了 Cell Manager 名称。

   检查 /etc/opt/omni/client/cell_server 文件 (HP-UX、Solaris 和 Linux 系统) 或 /usr/omni/config/cell/cell_server 文件 (其他 UNIX 系统)，其中包含 Cell Manager 系统的名称。

   然后，使用 testbar2 实用程序测试 Data Protector 内部数据传输:

   /opt/omni/bin/utilns/testbar2 -type:SAP

   -appname:ORACLE_SID

   -perform:restore

   -object:object_name

   -version:object_version

   -bar:backup_specification_name (HP-UX、Solaris 和 Linux 系统) 或

   /usr/omni/bin/utilns/testbar2 -type:SAP

   -appname:ORACLE_SID

   -perform:restore

   -object:object_name

   -version:object_version

   -bar:backup_specification_name (其他 UNIX 系统)

   您应看到屏幕上仅显示 NORMAL 消息，否则请单击 Data Protector 的“监视器”上下文中的“详细信息”按钮，检查 testbar2 实用程序报告的错误。

5. **验证使用 backint 的还原**

   请执行以下命令：

   HP-UX、Solaris 和 Linux 系统： /opt/omni/lbin/backint -f restore -u ORACLE_SID -i input_file

   其他 UNIX 系统： /usr/omni/bin/backint -f restore -u ORACLE_SID -i input_file

   这时会还原 input_file 的内容。

   如果失败，请检查会话是否已成功执行以及是否在相应的用户帐户下启动了还原。

   Backint 需要使用以下格式的文件列表: backup_ID_1 *pathName_1* [*targetDirectory_1*]*backup_ID_2pathName_2* [*targetDirectory_2*]*backup_ID_3pathName_3* [*targetDirectory_3*]

   要检索 backup_ID 编号，请输入以下命令:

   echo #NULL #NULL | backint –f inquiry –u ORACLE_SID

验证先决条件 (Oracle 方面)

按数字顺序执行以下验证步骤，以验证是否已正确安装了 Oracle:

1. ***UNIX 系统：***

   export ORACLE_SID=Oracle_SID

   export ORACLE_HOME=Oracle_home_path

   $ORACLE_HOME/bin/sqlplus

   Windows 系统：

   set ORACLE_SID=Oracle_SID

   set ORACLE_HOME=Oracle_home_path

   %ORACLE_HOME%\bin\ sqlplus

   在 SQLPlus 提示符下，键入:

   connect user/passwd@service

   select * from dba_tablespaces

   exit;

   尝试启动目标数据库。

2. 要建立 TNS 网络连接，请按照以下方式验证是否为目标数据库正确配置了 Net8 软件:
   - 在应用程序系统上，执行以下操作:

     UNIX 系统：

     $ORACLE_HOME/bin/lsnrctl status service

     Windows 系统：

     %ORACLE_HOME%\bin\lsnrctl status service

     如果失败，请启动 TNS 侦听程序进程，或查看 Oracle 文档以了解如何创建 TNS 配置文件 (LISTENER.ORA)。
   - 在应用程序系统上，执行以下步骤。使用 sqlplus：

     UNIX 系统：

     export ORACLE_SID=Oracle_SID

     export ORACLE_HOME=Oracle_home_path

     $ORACLE_HOME/bin/sqlplus

     Windows 系统：

     set ORACLE_SID=Oracle_SID

     set ORACLE_HOME=Oracle_home_path

     %ORACLE_HOME%\bin\ sqlplus

     在 SQLPlus 提示符下，键入:

     connect user/passwd@service；

     exit;

     如果失败，请参阅 Oracle 文档，了解如何创建 TNS 配置文件 (TSNAMES.ORA)。

验证先决条件 (SAP 方面)

开始执行本节中的步骤前，请确保已完成“验证先决条件 (Oracle 方面)”中的所有步骤。

按数字顺序执行以下验证步骤，以验证是否已正确安装了 SAP:

1. 在应用程序系统上，按照以下方式验证能否直接备份到磁盘:

   brbackup -d disk -u user/password

   如果失败，请参阅《SAP 联机帮助》，了解如何使用 SAP 备份实用程序备份到磁盘。
2. 在应用程序系统上，按照以下方式验证能否从磁盘还原:

   brrestore -d disk -u user/password

   如果失败，请参阅《SAP 联机帮助》，了解如何使用 SAP 还原实用程序还原到磁盘。

3. 在应用程序系统上，按照以下方式验证 SAP 是否已正确配置:

   移动原始 backint 。使用 SAP 备份实用程序在目录中创建名为 backint 并含有以下条目的测试脚本:

   ```
   #!/usr/bin/sh echo "Test backint called as follows:" echo "$0 $*" echo "exiting 3 for a failure" exit 3
   ```

   导出 SAP 所需的所有环境变量 (SAPDATA_HOME、SAPBACKUP ...)，然后以备份所有者用户的身份启动以下命令:

   ```
   brbackup -t offline_split -d util_file -u user/password -c
   ```

   或者，如果 Data Protector 使用 splitint :

   ```
   brbackup -t offline_mirror -d util_file -u user/password -c
   ```

   如果从 backint 收到参数，则表示 SAP 已正确配置为使用 backint 执行备份。否则，您应该重新配置 SAP。

验证配置

开始本节所述的操作前，请确保已完成“验证先决条件 (Oracle 方面)”和“验证先决条件 (SAP 方面)”中提供的所有步骤。

按数字顺序执行以下验证步骤，以验证是否正确配置了 Data Protector:

1. 在应用程序系统上，验证能否使用 Data Protector 对 SAP 数据库服务器执行文件系统备份:

   执行 Oracle Server 系统的文件系统备份，以便消除 Oracle Server 和 Data Protector Cell Manager 系统之间潜在的通信问题。

2. 验证应用程序系统上的环境变量:

   如果在启动 SAP 备份实用程序、Oracle Server Manager 或 TNS 侦听程序之前需要导出某些变量，请使用 Data Protector GUI 设置这些环境变量。

3. 验证 SAP 用户在应用程序系统上的权限:

   SAP 用户权限必须设置为有能力使用 Data Protector 执行 SAP 备份或还原。

   - 以 SAP 用户身份登录
   - 执行 /opt/omni/bin/testbar2 -perform:checkuser

   如果用户帐户拥有所有必需的权限，您只会看到屏幕上显示正常消息。

4. 检查系统错误:

   Oracle Server 上的以下文件中会报告系统错误:

   /var/opt/omni/log/debug.log

验证备份配置

开始本节所述的操作前，请确保已完成“验证先决条件 (Oracle 方面)”和“验证先决条件 (SAP 方面)”中提供的所有步骤。

按数字顺序执行以下验证步骤，以验证是否正确配置了 Data Protector:

1. 验证应用程序系统上的 Data Protector SAP ZDB 配置:

   请执行以下命令：

   HP-UX 和 Solaris 系统: /opt/omni/lbin/util_sap –CHKCONF ORACLE_SID

   Windows 系统： Data_Protector_home\bin\util_sap.exe –CHKCONF ORACLE_SID

   如果发生错误，错误编号将以 *RETVAL*error_number 的形式显示。

   要获取错误描述，请在 Cell Manager 上执行:

   Windows 系统： Data_Protector_home\bin\omnigetmsg 12 error_number

   该文件位于 Cell Manager 上。

   HP-UX 和 Linux 系统： /opt/omni/lbin/omnigetmsg 12 error_number

2. 验证 SAP 用户。

   检查相应的用户组是否已选择 See Private Objects 用户权限。另请参阅“配置用户帐户”。

3. 在应用程序系统上，使用 testbar2 验证备份:

   执行以下操作以确保在 Data Protector 中建立通信:

   - 在应用程序系统上创建非 ZDB 备份规范。
   - 执行：

/opt/omni/bin/testbar2 –type:SAP –appname:ORACLE_SID \ –perform:backup –file:file_name -bar barlist_name

如果失败，请检查错误并尝试修复它们或致电支持代表寻求帮助。

4. 在应用程序系统上，使用 backint 验证备份:

   执行以下命令以确保在 Data Protector 内建立通信并确保可以执行文件备份:

   - 在备份系统上创建非 ZDB 备份规范。
   - export OB2BARLIST=barlist_name

     export OB2APPNAME=ORACLE_SID

     /opt/omni/lbin/backint –f backup –t file –u ORACLE_SID -i \ input_file

     其中 input_file 是包含备份的完整路径名的文件。

   如果失败，请检查错误并尝试修复它们或致电支持代表寻求帮助。

验证还原

开始本节所述的操作前，请确保已完成“验证先决条件 (Oracle 方面)”和“验证先决条件 (SAP 方面)”中提供的所有步骤。

按数字顺序执行以下验证步骤，以验证是否正确配置了 Data Protector:

1. 验证为还原指定的用户

   验证为还原会话指定的用户是否为备份会话的用户以及他们是否为 Data Protector operator 或 admin 组的成员。检查相应的用户组是否已选择 See private objects 用户权限。

2. 验证文件是否已备份且位于 Data Protector 数据库中:

   - 使用 omnidb 命令；

     有关使用 omnidb 命令的信息，请参阅相应的手册页。

   - 使用 backint ；

     SAP 工具也使用此命令执行查询。

     /opt/omni/lbin/backint –f inquiry –u ORACLE_SID -i input_file

     其中 input_file 是查询的内容。 Backint 需要使用以下格式的文件列表:

     ```
     backint_ID_1 pathName_1 backint_ID_2 pathName_2 backint_ID_3 pathName_3
     ```

     要检索 backint_ID 编号，请输入以下命令:

     echo "#NULL #NULL" | backint –f inquiry –u ORACLE_SID

     或者，也可以在 input_file 中将 backint_ID_1 指定为 #NULL 。在这种情况下，该文件的最新备份会话会用于还原。

   如果失败，请继续执行以下步骤:

   - 检查备份会话 - 是否成功执行?
   - 检查用户权限。是否在正确的 SAP 用户帐户下启动了查询?
   - 致电支持代表寻求帮助。

3. 使用 Data Protector 或 CLI 验证还原:

   如果失败，请继续执行以下步骤:

   - 检查备份会话 - 是否成功执行?
   - 检查文件是否在 Data Protector 数据库中。
   - 检查用户权限。是否在正确的 SAP 用户帐户下启动了还原?
   - 致电支持代表寻求帮助。

4. 使用 testbar2 验证还原:

   执行以下操作以确保可以执行还原:

   /opt/omni/bin/testbar2 –type:SAP –appname:ORACLE_SID \ –perform:restore –file:file_name -bar barlist_name -object objectName

   如果失败，请继续执行以下步骤:

   - 检查备份会话 - 是否成功执行?
   - 检查文件是否在 Data Protector 数据库中。
   - 检查用户权限。是否在正确的 SAP 用户帐户下启动了还原

- 致电支持代表寻求帮助。

5. 使用 backint 验证还原:

   backint 与 SAP 备份实用程序使用的命令相同。

   /opt/omni/lbin/backint –f restore –u ORACLE_SID -i input_file

   其中，input_file 指定要还原的内容； backint 需要使用以下格式的文件列表:

   ```
   backint_ID_1 pathName_1 [targetDirectory_1] backint_ID_2pathName_2 [targetDirectory_2] backint_ID_3pathName_3 [targetDirectory_3]
   ```

   要检索 backint_ID 编号，请输入以下命令:

   echo "#NULL #NULL" | backint –f inquiry –u ORACLE_SID

   或者，也可以在 input_file 中为 backint_ID_1 指定 #NULL 。在这种情况下，该文件的最新备份会话会用于还原。

   如果失败，请继续执行以下步骤:

   - 检查备份会话 - 是否成功执行?
   - 检查文件是否在 Data Protector 数据库中。
   - 检查用户权限。是否在正确的 SAP 用户帐户下启动了还原?
   - 致电支持代表寻求帮助。

配置和备份问题

以下列表说明了问题以及解决这些问题的措施:

- **服务器管理器无法连接到目标**

  检查 Oracle TNS 侦听程序进程是否已启动并正在运行。检查是否需要任何环境变量才能成功与目标数据库建立远程连接；例如 TNS_ADMIN 和 SHLIB_PATH。请使用 Data Protector GUI 设置这些环境变量。

- **配置过程失败**

  检查 Oracle Server 是否已启动并正在运行。

  使用 Oracle Server Manager 从应用程序系统检查目标的登录信息。如果无法登录，请执行以下操作:

  检查是否为 Oracle 管理员用户设置了 sysoper 和 sysdba 权限。

  检查位于默认 Data Protector 日志文件目录中的 debug.log 、 sap.log 和 oracle8.log 文件中报告的系统错误。

  如果具有特殊的 Oracle 环境设置，请确保它们已在 Data Protector SAP 配置文件的 Environment 子列表中注册:

  /etc/opt/omni/server/integ/config/SAP/ *client_name* % *ORACLE_SID* (Linux Cell Manager) 或 '**Data_Protector_program_data\Config\server\integ\config\ sap\ *client_name*% *ORACLE_SID* (Windows Cell Manager)**。

- **启动备份失败**

  在 UNIX 系统上，检查应用程序系统上以下命令的输出:

  /opt/omni/lbin/util_sap.exe -CHKCONF ORACLE_SID

  如果出现错误，错误编号将按以下格式显示:

  *RETVAL*Error_number

  要获取错误说明，请在应用程序系统上启动以下命令:

  /opt/omni/lbin/omnigetmsg 12 Error_number

  在 Windows 系统上，使用 Data Protector GUI 执行以下过程:

  1. 在上下文列表中，选择“备份”。
  2. 在“范围窗格”中，依次展开“备份”、“备份规范”和“SAP R/3”。此时将显示 SAP 备份规范列表。
  3. 在“范围窗格”中，选择失败的备份规范，然后右键单击“结果窗格”中的 SAP R/3 服务器项以显示弹出菜单。
  4. 从弹出菜单中，选择“检查配置”。

  此时将显示简短说明来描述问题及如何解决这些问题。

- **备份不起作用**

  - 检查是否在应用程序系统中正确设置了 Cell Manager。文件 /etc/opt/omni/client/cell_server (UNIX 系统) 或
  - 检查应用程序系统上 initORACLE_SID.sap 文件中的 primary_db 参数是否设置为 LOCAL 。
  - 在 UNIX 系统上，检查是否在用户组中正确配置了用户。UNIX Oracle 管理员 (ora ORACLE_SID) 和 UNIX SAP 管理员 (ORACLE_SID adm) 都必须在 operator 类中。

- 在 UNIX 系统上，检查 SAPDATA_HOME/sapbackup/ 目录的权限是否设置为 755。
- 在 Windows 系统上，检查启动 Data Protector Inet 服务的用户帐户是否已添加到 Data Protector operator 类中。

- **备份失败并显示“连接到数据库实例失败”**

  在数据库实例处于“卸除”或“装载”模式的情况下启动备份时，会话失败并显示类似于以下内容的消息:

  BR0301E SQL error -1033 at location BrDbConnect-2

  ORA-01033: ORACLE initialization or shutdown in progress

  BR0310E Connect to database instance HOOHOO failed

  开始备份前，请确保数据库实例处于 open 或 shutdown 模式。

问题

下面是使用 Data Protector SAP R/3 集成时可能会遇到的一些问题。

数据库操作失败导致配置失败

配置 SAP R/3 数据库期间，Data Protector 报告以下错误:

Integration cannot be configured.

The database reported error while performing requested operation.

解决方案

查看 Oracle 数据库访问身份验证中使用的用户帐户的用户组成员身份。有关详细信息，请参阅“配置用户帐户”。

使用对象副本的还原会话失败

Data Protector SAP R/3 备份对象跨越多个备份介质时，针对此类备份对象的还原会话失败，并报告以下错误:

[Major] From: RSM@CMSystemName "" Time: DateTime

[61:9001] Could not find the object ObjectName named "SAP" in the database. Database error reported is: "Object version not found."

原因

仅当 SAP R/3 备份对象为复制的对象，而且会话前并未回收和导出所有原始介质时才会出现此问题。对于此类还原会话，Data Protector 会选择原始介质，而不是存储备份对象副本的介质。由于无法再使用原始介质集中的某些介质，因此会话失败。

解决方案

请遵循以下步骤：

1. 回收并导出存储原始 SAP R/3 备份对象的其余介质。
2. 重新启动还原会话。

每次针对 SAP R/3 备份对象执行对象复制，然后开始回收和导出原始介质时，都要确保回收并导出所有原始介质，这是成功完成还原会话的前提条件。

脚本失败导致配置失败

配置 SAP R/3 数据库期间，Data Protector 会报告以下错误:

Integration cannot be configured.

Script failed. Cannot get information from remote host.

原因

如果用户帐户没有所需的特权，则可能会发生此错误。

解决方案

检查环境设置并确保 Data Protector Inet 在具有所需权限的用户帐户下运行。

连接数据库实例失败

会话失败，并显示类似于以下内容的消息:

BR0301E SQL error -1033 at location BrDbConnect-2

ORA-01033: ORACLE initialization or shutdown in progress

BR0310E Connect to database instance HOOHOO failed

原因

如果在数据库实例处于 unmount 或 mount 模式时启动备份，则会发生此错误。

解决方案

开始备份前，请确保数据库实例处于“打开”或“关闭”模式。

由于文件名中的字符无效，还原会话失败

在 Windows 系统上，如果 Oracle 数据库字符集 (DBCS) 的设置值与系统为非 Unicode 程序设置的默认 Windows 字符集不同，而且使用了 SAP 工具来创建 Oracle 数据文件，则还原将失败。

原因

如果数据文件包含非 ASCII 或非拉丁语 1 字符，则会发生此错误。

解决方案

使用以下任一解决方法:

- 对于新的 Oracle 安装，请将 DBCS 设置为 UTF-8。
- 如果不使用其他非 Unicode 程序，请将非 Unicode 程序的语言设置为与 DBCS 相同的值。
- 不要在文件名中使用非 ASCII 或非拉丁语 1 字符。

Util_File_Online SAP 备份失败，并显示“设备上没有剩余空间”错误

多个 sapback 代理失败，并出现以下错误:

[28] No space left on device.

原因

将 util_file_online 选项与 BRBACKUP 一起使用时 (例如选择 Brbackup_Util_File_Online 模板)，表空间将单独切入/切出备份模式。由于只能有一个进程与 BRBACKUP 通信，因此若干 sapback 进程会使用信号来同步它们与 BRBACKUP 的交互。

sapback 进程的数量等于用于备份的所有设备的并发数之和。使用大量 sapback 进程时，撤消操作在系统的任何给定 IPC 信号上挂起的进程数可能会超出最大值。

解决方案

执行以下任意操作以解决此问题:

- 减少备份设备的数量或其并发数。
- 增加 semmnu 内核参数的值。增加该值后，重建内核并重新启动系统。

还原位于原始分区上的 SAP R/3 表空间失败

还原 SAP 表空间时，还原失败并显示类似如下消息:

```
[重要] 来自：VRDA@joca.company.com "SAP" 时间: 5/9/06 3:33:51 PM /dev/sapdata/rsapdata 无法还原 -> 原始磁盘分区! [警告] 来自：VRDA@joca.company.com "SAP" 时间: 5/9/06 3:42:45 PM 未还原任何内容。
```

原因

使用 Data Protector GUI 还原原始分区上的 SAP 表空间时，会发生此错误。

解决方案

使用 SAP 命令 (例如 brrestore) 还原这些表空间。

服务器管理器无法连接到目标

解决方案

检查 Oracle TNS 侦听程序进程是否已启动并正在运行。检查是否需要任何环境变量才能成功与目标数据库建立远程连接；例如 TNS_ADMIN 和 SHLIB_PATH。请使用 Data Protector GUI 设置这些环境变量。

配置过程失败

解决方案

检查 Oracle Server 是否已启动并正在运行。

使用 Oracle Server Manager 从应用程序系统检查目标的登录信息。如果无法登录，请执行以下操作:

检查是否为 Oracle 管理员用户设置了 sysoper 和 sysdba 权限。

检查位于默认 Data Protector 日志文件目录中的 debug.log 、 sap.log 和 oracle8.log 文件中报告的系统错误。

如果具有特殊的 Oracle 环境设置，请确保它们已在 Data Protector SAP 配置文件的 Environment 子列表中注册:

/etc/opt/omni/server/integ/config/SAP/ *client_name* % *ORACLE_SID* (Linux Cell Manager) 或 '**Data_Protector_program_data\Config\server\integ\config\ sap\ *client_name*% *ORACLE_SID* (Windows Cell Manager)**。

启动备份失败

解决方案

在 UNIX 系统上，检查应用程序系统上以下命令的输出:

/opt/omni/lbin/util_sap.exe -CHKCONF ORACLE_SID

如果出现错误，错误编号将按以下格式显示:

*RETVAL*Error_number

要获取错误说明，请在应用程序系统上启动以下命令:

/opt/omni/lbin/omnigetmsg 12 Error_number

在 Windows 系统上，使用 Data Protector GUI 执行以下过程:

1. 在上下文列表中，选择“备份”。
2. 在“范围窗格”中，依次展开“备份”、“备份规范”和“SAP R/3”。此时将显示 SAP 备份规范列表。
3. 在“范围窗格”中，选择失败的备份规范，然后右键单击“结果窗格”中的 SAP R/3 服务器项以显示弹出菜单。
4. 从弹出菜单中，选择“检查配置”。

此时将显示简短说明来描述问题及如何解决这些问题。

备份不起作用

解决方案

- 检查是否在应用程序系统中正确设置了 Cell Manager。文件 /etc/opt/omni/client/cell_server (UNIX 系统) 或
- 检查应用程序系统上 initORACLE_SID.sap 文件中的 primary_db 参数是否设置为 LOCAL。
- 在 UNIX 系统上，检查是否在用户组中正确配置了用户。UNIX Oracle 管理员 (ora ORACLE_SID) 和 UNIX SAP 管理员 (ORACLE_SIDadm) 都必须在 operator 类中。
- 在 UNIX 系统上，检查 SAPDATA_HOME/sapbackup/ 目录的权限是否设置为 755。
- 在 Windows 系统上，检查启动 Data Protector Inet 服务的用户帐户是否已添加到 Data Protector operator 类中。

在 Solaris 和 HP-UX 上使用 backint 进行备份失败

在 Solaris 和 HP-UX 系统上使用 backint 进行备份失败，并出现以下错误:

[Major] From: OB2BAR_DMA@computer.company.com "SAP" Time: 4/29/09 3:55:52 PM Cannot open file '/saphome/SAP/sapbackup/cntrlSAP.dbf'. Error: 13

解决方案

使用 root 权限并通过 NFS 共享应用程序系统上的目录。

在应用程序系统上，将以下几行添加到 /etc/dfs/dfstab 文件中:

Solaris 系统：

share -F nfs -o anon=0 /usr/src

share -F nfs -o anon=0,rw -d "" SAPHOME

在应用程序系统上，将以下几行添加到 /etc/exports 文件中:

RHEL/SUSE 系统:

SAPHOME backuphost(rw,sync)

报告连接错误后，ZDB 会话失败

ZDB 会话报告以下严重错误且未能成功完成:

Connection with DMA was reset

Signal SIGABRT (6) received from BRtools

解决方案

在应用程序系统上的 SAP 参数文件中，将参数 primary_db 设置为 LOCAL 并重新启动会话。

由于文件名中的字符无效，ZDB、还原或即时恢复会话失败

原因

在 Windows 系统上，如果 Oracle 数据库字符集 (DBCS) 的设置值与系统为非 Unicode 程序设置的默认 Windows 字符集不同，而且使用了 SAP 工具来创建 Oracle 数据文件，则数据文件含有非 ASCII 或非拉丁语 1 字符时 ZDB 还原和即时恢复将失败。

解决方案

使用以下任一解决方法:

- 对于新的 Oracle 安装，请将 DBCS 设置为 UTF-8。
- 如果不使用其他非 Unicode 程序，请将非 Unicode 程序的语言设置为与 DBCS 相同的值。
- 不要在文件名中使用非 ASCII 或非拉丁语 1 字符。

Sybase Server 集成故障诊断

This feature is available in the Premium Edition

本主题列出了常规检查和验证操作。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。请参阅索引: 有关如何执行此验证的“修补程序”。

检查和验证

如果配置、备份或还原失败:

- 检查写入 debug.log 的系统错误，该日志位于默认 Data Protector 日志文件目录中的 Sybase Server 系统上。
- 在有问题的客户机上进行测试备份和还原任意文件系统。
- 在群集环境中，在通过 Data Protector CLI 执行过程之前，请确保将环境变量 OB2BARHOSTNAME 设置为虚拟服务器名称。使用 Data Protector GUI 时，不需要此步骤。
- 确保 Sybase 实例及其默认 Sybase Backup Server 处于联机状态。
- ***UNIX 系统：*** 如果 Sybase Server 系统使用网络加密导出，则需要在 omnirc 文件中添加以下变量:

  LC_ALL = <value_from_env>

  SHLIB_PATH = <value_from_env>

  LD_LIBRARY_PATH = <value_from_env>

  其中， <value_from_env> 需要使用从环境中检索的变量的值进行更改。

此外，如果配置或备份失败:

- 如果使用非默认 Sybase 设置，请确保它们已在以下位置注册:

  Windows 系统： “系统属性”对话框，可通过双击“控制面板”中的“系统”访问。

  UNIX 系统： Data Protector Sybase 配置文件。

此外，如果您的备份失败:

- 检查“检查配置”中描述的 Sybase 实例的配置。
- 按“预览备份会话”中所述测试备份规范。

  如果测试的 Data Protector 部分失败:

  1. ***UNIX 系统：*** 确保备份规范的所有者是用户 sybase ，且其已添加到 Data Protector operator 或 admin 用户组。
  2. 创建 Sybase 备份规范以备份到 null 或文件设备。如果备份成功，则问题可能与设备有关。

  如果测试成功，则直接从 Sybase Server 启动备份。请参阅“使用 Sybase 命令”。

此外，如果备份或还原失败:

- 使用 testbar 实用程序测试 Data Protector 数据传输。以用户 sybase 身份登录 Sybase Server 系统并执行:
  - 如果备份失败:

    testbar -type:Sybase -appname:Sybase_instance_name \ -bar:backup_specification_name -perform:backup
  - 如果还原失败:

    testbar -type:Sybase -appname:Sybase_instance_name \ -bar:backup_specification_name -perform:restore \ -object:object_name -version

:object_version

其中， object_name 是要还原的对象的名称。

如果测试失败:

- 错误故障诊断。请参阅位于 Cell Manager 上的文本文件 Trouble.txt ，位置:

  Windows 系统： Data_Protector_home\help\enu

  UNIX 系统： /opt/omni/gui/help/C

- 在 Sybase Server 系统上，检查位于默认 Data Protector 日志文件目录中的 debug.log 文件中报告的系统错误。

此外，如果还原失败:

- 确保 Data Protector operator 用户组已选择“查看私有对象”用户权限。

问题

下面是使用 Sybase Server 集成时可能遇到的一些问题：

- 还原到另一个客户机系统
- 在 SLES 10 或更高版本的操作系统版本中配置 Sybase 集成失败
- 在 Windows 操作系统中备份 Sybase 集成失败

无法加载库

在 HPUX OS 上配置 Sybase 16sp3 时发生以下错误:

The database reported error while performing requested operation.

CS-LIBRARY error:

comn_cryptolib_load(): user api layer: internal common library error: Failed to load library '%1!'.

原因

无法从服务器检索 SHLIB_PATH 时，会发生此错误。

解决方案

将 SHLIB_PATH 添加到 Sybase 客户机的 omnirc 文件中。

将值设置如下:

SHLIB_PATH = $SYBASE/$SYBASE_ASE/lib:$SYBASE/DataAccess64/ODBC/lib:/$SYBASE/DataAccess64/ODBC/lib:/$SYBASE/$SYBASE_OCS/lib:$SYBASE/$SYBASE_OCS/lib3p:$SYBASE/$SYBASE_OCS/lib3p64: $SHLIB_PATH

Restore to another client system fails

When you start a restore of a database to the original Sybase instance, the session finishes successfully. However, when you start a restore of the database to a different Sybase instance on another client, your restore session fails with a message similar to the following:

```
Mar 11 18:16:13 2010: Backup Server: 4.124.2.1: Archive API error for device='ob2syb::2010/03/11-19::test_db: :incprod::00': Vendor application name=Data Protector A.06.10 , Library version=221, API routine=syb_read(), Message=Object version not found.ar 11 18:16:13 2010: Backup Server: 6.32.2.3: ob2syb:: 2010/03/11-19::test_db::incprod::00: volume not valid or not requested (server: , session id: 62.) Mar 11 18:20:07 2010: Backup Server: 4.132.1.1: Attempting to open byte stream device: 'ob2syb:: 2010/03/11-19::test_db::incprod::00'
```

Cause

The problem is that the IDB uses the name of the destination client instead of the name of the client from which the database was backed up.

Solution

Complete the following steps:

1. Set the `OB2HOSTNAME` variable on the target client: add the `OB2HOSTNAME=BackupClient.company.com` variable entry to the `Sybase_TargetInstance.cfg` configuration file, located in the default Data Protector temporary files directory.
2. Restart the restore of the database.

在 SLES 10 或更高版本的操作系统版本中配置 Sybase 集成失败

在 SLES 10 或更高版本的操作系统版本中配置 Sybase 集成失败，并显示以下错误:

```
尝试加载本地化文件时上下文分配例程失败!!，
```

```
一个或多个以下问题可能会导致失败，
```

```
您的 sybase 主目录是 <HOME_DIRECTORY_PATH>。如果环境变量 SYBASE 不是您想要的变量，请进行检查该变量!，
```

```
使用环境变量 LC_ALL 中定义的区域设置名称 "POSIX"，
```

```
您的 <HOME_DIRECTORY_PATH>/locales/locales.dat 文件中不存在区域设置名称 "POSIX"，
```

```
尝试分配与本地化相关的结构时发生错误。，
```

原因

在 SLES 10 或更高版本的环境中可以看到此错误，其中默认区域设置设置为 POSIX 。

解决方案

将 POSIX 本地化相关的结构添加到 Sybase 安装或使用其他区域设置。

在 Windows 操作系统中备份 Sybase 集成失败

在 Windows 操作系统中备份 Sybase 集成失败并出现错误。

原因

如果 Sybase 代理 **ob2sybase.exe** 找不到共享的 Sybase 库，则会发生此错误。Sybase 代理 **ob2sybase.exe** 使用 Sybase API 调用，这些调用又使用 Sybase 共享库运行。

解决方案

安装 Sybase ASE 之后，重新启动 Windows 操作系统。Sybase 代理在 LocalSystem 帐户下运行，且当 Windows 操作系统引导时会加载 LocalSystem 的环境变量。如果在安装 Sybase ASE 后未重新启动 Windows 操作系统，则这些变量对 LocalSystem 帐户不可见。

如果即使在重新启动后备份仍然失败，请将以下路径手动添加到 PATH 变量:

- <SYBASEHOMEDIR>\ASE-16_0\bin
- <SYBASEHOMEDIR>\OCS-16_0\bin
- <SYBASEHOMEDIR>\OCS-16_0\lib3p64
- <SYBASEHOMEDIR>\OCS-16_0\lib3p (同样适用于 Sybase ASE 15.7)

此外，导出以下 Sybase 环境变量:

- SYBASE
- SYBASE_ASE
- SYBASE_OCS
- SYBROOT
- LIB
- INCLUDE

H3C CAS 集成故障诊断

This feature is available in the Express and Premium Editions

本主题列出常规检查和验证，以及在使用适用于 H3C CAS 的虚拟环境集成时可能会遇到的问题。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。

问题

以下是将虚拟环境集成用于 H3C CAS 时可能会遇到的一些问题：

H3C CAS 非缓存还原失败

从 Data Protector 版本 2019.12、2020.05 和 2020.08 升级到 2020.11 后，H3C CAS 非缓存还原失败。

原因

发生此错误的原因是 cell_info 文件中缺少暂存详细信息。

解决方案

升级后重新配置备份规范。

使用不同的备份主机时，还原会话失败

执行还原时，如果所选备份主机不同于在备份期间选择的备份主机，则会显示以下错误消息:

```
[严重] 来自: VEPALIB H3CCAS@backuphost.company.com "hostpool"  时间: <日期时间> 指定的备份主机无效: ‘backuphost.company.com’
```

原因

原因是在执行还原时，H3C CAS REST API 也需要选择备份期间使用的备份主机。

解决方案

选择备份期间使用的备份主机。

还原客户机不同于原始 CAS 服务器时，还原会话失败

执行还原时，如果还原客户机不同于原始 CAS 服务器，还原将失败并显示以下错误消息:

```
[严重] 来自: VEPALIB H3CCAS@backuphost.company.com "hostpool"  时间: <日期时间> 指定的 H3C CAS 主机无效: ‘host.company.com'
```

原因

原因是 H3C CAS REST API 仅支持还原到原始 CAS 服务器。

解决方案

选择 H3CAS 服务器作为备份期间使用的还原客户机。

如果在原始主机池中找不到虚拟机，还原会话失败

执行还原时，如果虚拟机被迁移到其他主机池或删除，还原将失败并显示以下错误消息:

```
[重大] 来自: VEPALIB H3CCAS@backuphost.company.com "hostpool"  时间: <日期时间> 虚拟机: 在主机池 'hostpool' 中找不到 'VM'。正在跳过...
```

原因

原因是仅当虚拟机在相同的主机池中可用时，H3C CAS REST API 才支持还原虚拟机。

解决方案

如果虚拟机已迁移，则将其复制或移动到相同的主机池。如果已删除，则手动还原虚拟机。

可以通过下列方式将虚拟机手动还原到 H3C CAS:

将备份文件还原到同一虚拟机

1. 通过在 REST 浏览器客户机 (例如 POSTMAN) 中执行以下 REST API 提取 backupID :
   - 获取 hostpoolID - 使用 /cas/casrs/hostpool/all
   - 获取 vm ID - 使用 /cas/casrs/vm/vmList?hpId={hostpoolID}
   - 获取 backupfiletree - 使用 /cas/casrs/backupStrategy/backupFileTree?domainId={vm ID}
   - 在还原文件中，复制 specified_name 文件中提供的 backupName 并在 backupfiletree 中搜索 backupName 。您将获得相应 backupName 的 backupID 。
2. 还原备份文件 - 使用 PUT /cas/casrs/vm/v2/restore?backupId={backupID}&tmpDir=/vms/&isForce=true

将备份文件还原到另一个虚拟机

如果已删除虚拟机的备份可用，则执行以下步骤手动还原已删除的虚拟机。

1. 创建虚拟机 (没有 OS) 并对其进行备份。
2. 使用“还原到目录”选项还原新创建的虚拟机的备份映像。
3. 将新创建的虚拟机中的以下文件替换为已删除虚拟机的文件:
   - {VMhostName}_0
   - {VMhostName}_0.sum
4. 使用以下项的新大小更新信息文件:
   - {VMhostName}_0
   - {VMhostName}_0.sum
5. 通过在任何 REST 浏览器客户机 (例如 POSTMAN) 中执行以下 REST API 提取 backupID :
   i. 获取 hostpoolID - 使用 /cas/casrs/hostpool/all
   ii. 获取 vm ID - 使用 /cas/casrs/vm/vmList?hpId={hostpoolID}
   iii. 获取 backupfiletree - 使用 /cas/casrs/backupStrategy/backupFileTree?domainId={vm ID}
   iv. 在还原文件中，复制 specified_name 文件中提供的 backupName 并在 backupfiletree 中搜索 backupName 。您将获得相应 backupName 的 backupID 。
6. 还原备份文件 - 使用 PUT /cas/casrs/vm/v2/restore?backupId={backupID}&tmpDir=/vms/&isForce=true

如果从虚拟机中删除了新添加的磁盘，还原会话失败

备份之后，如果删除新添加到虚拟机的磁盘，则在还原期间可能无法恢复这些磁盘。将显示以下错误消息：

[重大] 来自: VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <日期时间> 在 CAS 服务器上执行任务时发生错误 错误: 还原已终止! 根据备份文件 "<file name>" 还原 VM "vm_test" 失败。原因: 要还原的目标文件已存在 (错误代码: 4531)。 [重大] 来自: VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <Date Time> 还原失败。

原因

原因是 H3C CAS REST API 不支持还原已删除磁盘的虚拟机。

解决方案

执行备份后不删除磁盘。

如果输入的凭据无效，预览备份会话将失败

如果在创建备份规范时输入的 CAS 管理服务器凭据和备份主机凭据无效，预览备份会话将失败。将显示以下错误消息：

```
[重大] 来自: VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <日期时间> 备份主机 <备份主机名> 的暂存凭据无效
```

原因

原因是在使用“预览备份”选项时，将验证所选备份规范的 CAS 管理服务器凭据和备份主机凭据。

解决方案

请在创建备份规范时输入有效的 CAS 管理服务器凭据和备份主机凭据。

将在最新版本 (E0526) 的 H3C CAS 上备份的文件还原到较低版本的 H3C CAS 失败

还原文件失败，并显示以下错误:

```
对于低于 E0526 的 CAS 服务器，在 CAS 服务器中未找到虚拟机 <vm>，应在 CAS 基础架构中找到虚拟机。
```

原因

当您尝试将在 H3C CAS 新版本 (E0526) 上备份的文件还原到旧版本时，会发生此错误。

解决方案

升级到新版本的 CAS 后，运行还原操作。

没有为还原操作提供主机池名称

还原失败并显示以下错误消息:

```
[警告] 来自：VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <日期时间> 没有为还原操作提供主机池名称...
```

原因

未指定主机池名称或主机名时，会发生此错误。

解决方案

运行还原操作时，指定主机池名称和主机名。

尝试在并行还原会话中还原同一 VM 时，还原失败

尝试在并行还原会话中还原同一 VM 时，还原失败，并出现以下错误:

[重大] 来自: VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <日期时间> 无法在此会话中获取虚拟机 <vm> 的锁定。 请稍后再试。

原因

在多个并行还原会话中还原同一 VM 时，其中一个会话会获取使用 VM 的 UUID 创建的互斥，然后继续还原操作。其他会话将等待，直到释放互斥为止。如果设置为 8 分钟的锁定超时 (OB2_H3CCAS_MULTIPLE_SESSION_VM_TIMEOUT) 在第二个会话的还原开始之前到期，则还原将失败。

解决方案

尝试过一段时间后运行还原。如果问题仍然存在，请通过运行以下命令清除会话锁定:

vepa_util.exe command --virtual-environment h3ccas --host <CAS_HOST> --clear-vm-lock --vm-uuid <UUID>.

在启用 **CBT** 的情况下运行差异备份会话时，备份失败

在启用 CBT 的情况下运行差异备份时，将显示以下错误消息:

```
[严重] 来自: VEPALIB_H3CCAS@VEPALIB H3CCAS@backuphost.company.com "/Hostpool1" 时间: <日期时间> 差异备份不支持更改后的块跟踪 (CBT)。
```

原因

还原失败的原因是不支持从新版本的 H3C CAS (V5.0 (E0526H02)) 到早期版本 (低于 (V5.0 (E0522))) 的备份文件非缓存还原。

解决方案

运行差异备份时，禁用 CBT 选项。H3C CAS 不支持在启用 CBT 的情况下使用差异备份。

Hyper-V 集成故障诊断

This feature is available in the Express and Premium Editions

本主题列出常规检查和验证，以及在使用 Data Protector 虚拟环境集成时可能会遇到的问题。

开始之前

- 确已安装最新的正式补丁。

检查和验证

如果浏览操作或者备份或还原会话失败:

- 检查位于默认 Data Protector 日志文件目录下的 debug.log 中报告的系统错误。
- 检查您是否可以在有问题的客户机上执行文件系统备份和还原。

问题

下面是一些使用 Data Protector 虚拟环境集成时可能会遇到的问题：

删除虚拟机磁盘资源时出错

将 VM 从其他虚拟机监控程序主机还原到原始 SMB 位置时，还原会话失败并显示以下错误:

[Major] From: VEPALIB_HYPERV@<hostname> “/HyperV” Time: <date_time>

Virtual Machine ''<vm_name>'': Error while removing the virtual machine disk resources...

原因

。在还原操作期间，Data Protector 尝试将磁盘文件还原到源 VM 使用的原始网络共享位置。这会导致任何 VM 操作都无法访问该磁盘文件。

解决方案

在还原期间将目标选择为“还原到目标存储路径”，并指定与源不同的路径。

找不到虚拟磁盘的更改跟踪 ID

Hyper-V RCT 增量备份会话期间发生以下错误:

Virtual Machine 'VMName: Could not find change tracking ID for the virtual disk 'DiskName'

原因

发生此错误的原因是缺失更改跟踪 ID。

解决方案

在这种情况下，建议执行完整备份。

虚拟机 (GUID): 配置不受支持

Hyper-V RCT 还原期间发生以下错误:

[Critical] From: VEPALIB_HYPERV@hyperv.hypervdomain.local "" Time: 10/24/2020 7:06:09 AM

[172:184] Virtual Machine 'VM' (GUID)': Configuration not supported.

原因

如果虚拟机包含 UI 快照，则会发生此错误。如果磁盘上存在快照，则不支持单磁盘还原。

解决方案

删除磁盘上的用户快照，然后重新启动还原。

Hyper-V RCT 还原: 还原项目时出错

Hyper-V RCT 还原期间发生以下错误:

Error:[Critical] From: VEPA_HYPERV@abc.hpeswlab.net "" Time: 11/20/2020 12:05:21 PM
Virtual Machine ''TestVm1'': Error restoring item: <diskName>

原因

发生此错误的原因是，Data Protector Hyper-V RCT 还原在还原时使用新的 UUID 创建虚拟机。

解决方案

备份虚拟机后，请手动删除原始虚拟机及其资源，然后再开始还原会话。

快照合并或磁盘合并超时

备份会话失败，并显示以下错误:

[Critical] From: VEPALIB_HYPERV@hostname "" Time: <date_time>
[172:11611] Virtual Machine 'VM': Snapshot merge or disk consolidation timed out.

原因

此错误可能是由于以下任一原因造成的:

- 如果备份会话突然结束，它将留下旧快照。触发后续备份会话时，Data Protector 会尝试合并快照。在某些情况下，合并会花费很长时间，并导致备份因该错误而结束。
- 在某些情况下，由于 Microsoft 的限制，尽管在 Hyper-V 管理器中没有看到快照或检查点，但旧的差异磁盘会留在文件系统上。此情况以及差异磁盘的巨大变化可能导致备份失败。

解决方案

执行以下操作之一：

- 等待一段时间，然后再次重新触发备份。
- 检查 Hyper-V 管理器的合并状态，然后重新触发备份。
- 在触发下一个备份会话之前，使用以下 omnirc 变量增加超时时间。
  OB2_VEAGENT_MERGE_SNAPSHOTS_TIMEOUT=<seconds>

Microsoft Hyper-V VSS 写入程序无法为备份中的某些组件准备文件

在 Hyper-V VM 上进行 Linux VM 备份时，Microsoft Hyper-V VSS 写入程序无法为备份中的某些组件准备文件。显示以下错误：

```
[重大] 来自: [[OB2BAR VSSBAR@myserver.net "HyperV"  时间: MM/DD/YYYY HH:MM:SS PM [145:575]  写入程序 'Microsoft Hyper-V VSS 写入程序' 无法准备用于备份的文件:              报告的状态:     VSS_WS_FAILED_AT_PREPARE_SNAPSHOT              预期状态:     VSS_WS_WAITING_FOR_BACKUP_COMPLETE              故障代码:       VSS_E_WRITERERROR_NONRETRYABLE
```

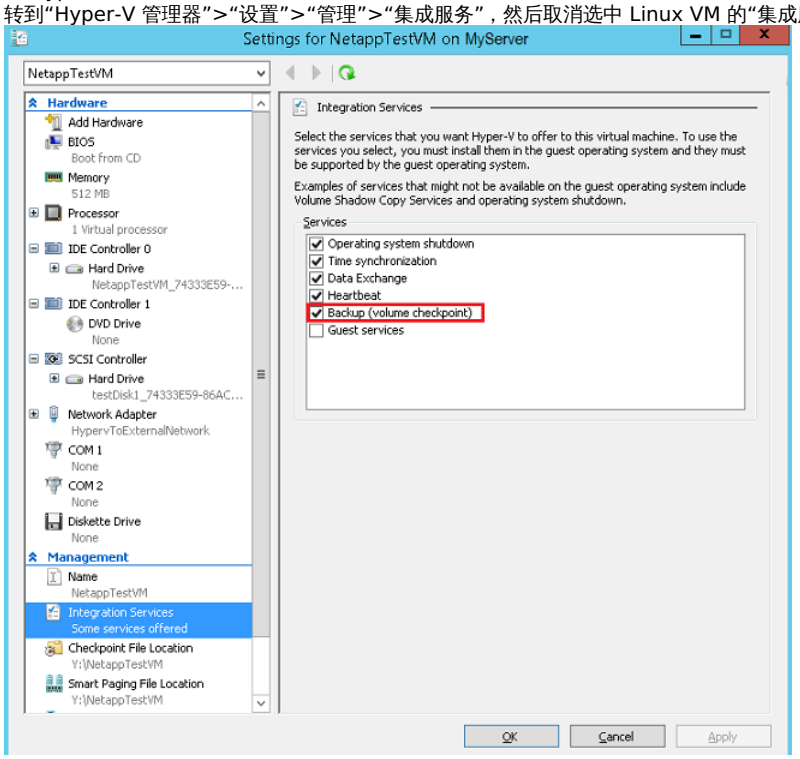
原因

Linux 操作系统没有 VSS 写入程序，默认情况下，Hyper-V 会尝试连接到来宾。如果集成服务没有响应，则 Microsoft Hyper-V VSS 写入程序会将其解释为 VSS 错误。

解决方案

要解决此问题，请按照下列步骤操作:

1. 执行以下某个操作：
   - 在 Hyper-V VM 上安装 Linux 集成服务，然后继续备份以确保与 Windows 系统中的 VSS 写入程序兼容。
   - 转到“Hyper-V 管理器”>“设置”>“管理”>“集成服务”，然后取消选中 Linux VM 的“集成服务”中的“备份 (卷检查点)”选项。



2. 运行备份。

Microsoft Hyper-V 虚拟机的备份会话失败

备份 Microsoft Hyper-V 虚拟机时，会话意外结束，出现与下面类似的错误:

```
[重大] 来自: OB2BAR_VSSBAR@computer.company.com "MSVSSW" 时间: YYYY/MM/DD HH:MM:SS AM [145:575] 写入程序 'Microsoft Hyper-V VSS Writer' 无法准备 用于备份的文件: 报告的状态: VSS_WS_FAILED_AT_POST_SNAPSHOT 预期状态: VSS_WS_WAITING_FOR_BACKUP_COMPLETE 故障代码: VSS_E_WRITERERROR_NONRETRYABLE
```

原因

可能的原因如下:

- 在 Microsoft Hyper-V 系统上禁用了自动装载新卷。
- 虚拟机内部存在问题，例如卷影复制的存储空间不足、使用了非 NTFS 文件系统等等。

解决方案

检查是否在 Microsoft Hyper-V 系统上启用了自动装载新卷。例如：

```
diskpart.exe Microsoft DiskPart 版本 6.1.7600 版权所有 (C) 1999-2008 Microsoft Corporation。 在计算机上: TPC021 DISKPART> automount 已启用自动装载新卷。
```

如果禁用自动装载，请通过执行以下命令启用:

```
MOUNTVOL /E
```

如果该问题在启用了自动装载后仍然存在，请检查虚拟机内的应用程序日志文件以确定原因。

在 CSV 环境中备份会话失败

使用位于群集共享卷上的文件备份虚拟机时，会话失败，出现与下面类似的错误:

```
[重大] 来自: OB2BAR_VSSBAR@tpc049.company.com "HyperV" 时间: YYYY/MM/DD HH:MM:SS PM 无法执行以下项的备份: /Microsoft Hyper-V VSS Writer/虚拟机/使用子分区快照备份\vmw39192', 该备份在以下位置包含数据: C:\ClusterStorage\Volume3\vmw39192\Virtual Machines\1FC08961-08B8-4AC5-BDE8-AF4E2AAA07E8.xml C:\ClusterStorage\Volume3\vmw39192\Virtual Machines\1FC08961-08B8-4AC5-BDE8-AF4E2AAA07E8\* C:\ClusterStorage\Volume3\vmw39192\vmw39192.vhd [重大] 来自: OB2BAR_VSSBAR@tpc049.company.com "HyperV" 时间: YYYY/MM/DD HH:MM:SS PM 没有要备份的数据。
```

原因

如果两个会话尝试同时从同一 CSV 备份虚拟机，则会出现此问题。由于第一个会话锁定了 CSV，第二个会话无法访问 CSV 并因此失败。

解决方案

逐一运行会话。

由于密码错误，浏览操作或者备份或还原会话失败

当应用程序系统和备份主机是同一系统时，不执行用户名和密码的配置检查。实际上，在此类设置中，即使凭据无效，配置检查也总是会成功，并且后续的浏览、备份和还原操作将起作用。但在建立非本地连接时，例如，使用不同的备份主机，由于密码错误，操作将失败。

解决方案

同时配置不是应用程序系统的备份主机。

Data Protector Inet 服务配置缺失

在还原会话期间，会话输出中将报告与下面类似的消息:

[警告] 来自：INET_thread_vepa_bar.exe@tpc040.company.com "tpc040.company.com" 时间: YYYY/MM/DD HH:MM:SS PM Inet 的模拟配置中没有用户 ADMINISTRATOR@DOMAIN 的数据。

解决方案

您可以安全地忽略此信息。

无法还原磁盘。磁盘正在由另一个磁盘使用

会话输出中将报告与下面类似的消息:

[严重] 来自: VEPALIB_HYPERV@tpc040.company.com "" 时间: MM/DD/YYYY HH:MM:SS PM

虚拟机 'vm2 (GUID: 1911B13E-9BD4-4DB2-B678-F1327810AE1C)':

无法还原磁盘。磁盘 (控制器: '393A6E0D-BE4B-4EDC-81F0-86035A277160'，驱动器位置:'0') 正在由其他磁盘使用。

原因

如果控制器可用，但磁盘驱动器位置由其他磁盘使用，则会发生此问题。

解决方案

使用 omnirc 变量 OB2_VEAGENT_FORCE_DISK_RESTORE =1 覆盖此方案。

（或）

导航到 Hyper-V 管理器上的 VM 设置，并使驱动器位置可用于磁盘还原。

无法还原磁盘。找不到控制器

如果从 VM 中手动删除了控制器，则会话输出中将报告与下面类似的消息:

```
[严重] 来自: VEPALIB_HYPERV@tpc040.company.com "" 时间: MM/DD/YYYY HH:MM:SS PM 虚拟机 'vm2 (GUID: 1911B13E-9BD4-4DB2-B678-F1327810AE1C)': 无法还原磁盘。未找到控制器 '393A6E0D-BE4B-4EDC-81F0-86035A277160'
```

原因

如果从 VM 中手动删除了控制器，则会发生此错误。

解决方案

如果该控制器与备份的控制器截然不同，则执行虚拟机还原。

配置不受支持

如果在磁盘还原期间找到快照，则会显示一个弹出窗口，其中包含以下错误消息、说明和操作:

[严重] 来自: VEPALIB_HYPERV@tpc040.company.com "" 时间: MM/DD/YYYY HH:MM:SS PM 虚拟机 'vm2 (GUID: 1911B13E-9BD4-4DB2-B678-F1327810AE1C)': 配置不受支持 描述: 虚拟机中含有用户的快照。不支持恢复单个磁盘。 操作: 删除用户快照，然后再次重新启动恢复。

原因

在包含用户快照的 VM 上还原单个磁盘时，会发生此问题。

解决方案

在 Hyper-V 主机上使用以下 PowerShell 命令:

```
Get-vmsnapshot -vmname <vmname> | remove-vmsnapshots
```

（或）

使用 Data Protector“还原”上下文中的“还原前合并快照”选项。

无法初始化 Hyper-V 远程环境

初始化 Hyper-V 远程环境时，将显示以下错误消息:

```
[严重] 来自: VEPALIB_HYPERV@tpc040.company.com "" 时间: MM/DD/YYYY HH:MM:SS PM 节点 'iwf1114072.hyperv.net': 初始化 Hyper-V 远程环境失败...
```

原因

在以下情况下会发生此错误:

- 未正确配置 SSL 证书和 HTTPS 端口。
- 您使用的不是端口 5986。

解决方案

请执行以下操作：

1. 创建 SSL 证书。
2. 使用创建的 SSL 证书配置 HTTPS。
3. 如果使用的 HTTPS 端口不是 5986 (默认端口)，请使用 omnirc 变量 OB2_VEAGENT_HTTPS_PORT 。

无法还原磁盘。已启用复制

显示以下错误:

```
[重大] 来自: VEPALIB_HYPERV@computer.company.com "/HyperV" 时间: MM/DD/YYYY HH:MM:SS AM [172:2047] 虚拟机 'testvm (GUID: FA019E3E-207A-4B14-AD19-F3B675645D86)': 无法还原磁盘。已启用复制。
```

原因

如果在磁盘还原期间替换了虚拟机，则可能发生此错误。

解决方案

从主虚拟机和复本虚拟机中删除复制。

无法进行磁盘还原

将显示以下错误消息：

[严重] 来自: VEPALIB_HYPERV@ computer.company.com "/HyperV" 时间: MM/DD/YYYY HH:MM:SS AM [172:2031] 虚拟机 'testvm (GUID: FA019E3E-207A-4B14-AD19-F3B675645D86)': 磁盘 (控制器: '7016CBD1-EF2C-40F7-A248-9C687FB44CD5'，驱动器位置:'0') 不能进行还原。

原因

由于以下原因，无法进行磁盘还原:

- 如果另一个磁盘连接到控制器和驱动器位置。
- 如果复本虚拟机中的磁盘正在还原到主服务器，反之亦然。

解决方案

请执行以下操作：

1. 验证驱动器位置是否正在由另一个磁盘使用或者不是来自虚拟机设置。
2. 如果正在还原复本虚拟机中的磁盘，请选择复本服务器或群集作为还原客户机。
3. 如果正在还原主虚拟机中的磁盘，请选择主服务器或群集作为还原客户机。

Data Protector 无法还原文件

在还原会话期间，将显示与下面类似的消息:

[重大] 来自: OB2BAR_VSSBAR_COMP@tpc021.company.com "HyperV" 时间: MM/DD/YYYY HH:MM:SS PM 无法还原文件 'C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines \8F74F8EE-E93A-4CD3-998F-3324784ED932.xml'. 失败，错误为: '[33] 进程无法访问文件，因为 另一个进程已锁定了文件的一部分。' [重大] 来自: OB2BAR_VSSBAR_COMP@tpc021.company.com "HyperV" 时间: YYYY/MM/DD HH:MM:SS PM [145:221] 还原组件 '/Microsoft Hyper-V VSS Writer/虚拟机/ 无法使用子分区快照备份\VM_name' 失败。

原因

如果无法访问虚拟机的配置文件，则会发生此问题。

解决方案

重新启动还原，而不清除已还原的文件。

还原期间，CSV 数据通过 LAN 而不是 SAN 发送

由于 Microsoft 限制，在还原群集共享卷 (CSV) 上的虚拟机文件期间，在某些情况下，数据通过 LAN 而不是 SAN 发送，这可能会增加还原时间。

原因

使用除协调器节点外的节点进行数据传输时，会发生这种情况。

解决方案

在开始还原之前，确保使用协调器节点进行还原。执行以下操作之一：

- 在 Windows Server Manager 中，检查当前哪个节点是协调器节点，并在 Data Protector 中选择该节点进行还原。
- 在 Windows Server Manager 中，手动将协调切换到要用于还原的节点。

Windows 应用程序事件日志中记录了警告事件 ID 5605

Windows 应用程序事件日志中记录了警告事件 ID 5605。尽管如此，会话仍然成功完成。

原因

当 Microsoft Hyper-V 虚拟环境集成连接到群集命名空间时，会出现该警告。

解决方案

您可以安全地忽略此警告。

备份会话后，VM 复制状态为“错误”，运行状况为“严重”

在 Data Protector 备份会话期间，Hyper-V 服务会锁定虚拟机以防止出现不一致。在主 Hyper-V 服务器上，它在 Windows 事件日志中记录错误和警告:

Hyper-V failed to replicate changes for virtual machine 'vmw38078' (Virtual Machine ID FBCDBFDF-ACBD-4A01-BA8D-A4A9CF597651). Hyper-V will retry replication after 5 minute(s).

在复制服务器端，Hyper-V 服务在 Windows 事件日志中记录多个错误:

Hyper-V failed to apply replication logs for 'vmw38078': Operation aborted (0x80004004). (Virtual Machine ID FBCDBFDF-ACBD-4A01-BA8D-A4A9CF597651)

原因

默认情况下，Hyper-V 服务每五分钟重试一次复制，最多不超过一小时。如果由于 VM 的备份时间过长而无法在此时间范围内成功执行复制，则复制将保持在“错误”状态，且运行状况设置为“严重”，Hyper-V 服务不再尝试自动重新同步 VM。

解决方案

更改允许 Hyper-V 自动重新同步复本 VM 的时间间隔。

例如，要将间隔更改为五小时，请执行以下 PowerShell 命令:

Set-VMReplication –VMName VMName -AutoResynchronizeEnabled $true -AutoResynchronizeIntervalStart 00:00:00 -AutoResynchronizeIntervalEnd 05:00:00

在涉及还原链的还原会话后触发备份会话失败

启动从增量备份映像还原数据的 Data Protector 会话后，如果在会话输出中报告与下面类似的错误，则后续备份会话将失败:

```
[重大] 来自: OB2BAR_VSSBAR@computer.company.com "HyperV" 时间: YYYY/MM/DD HH:MM:SS AM [145:575] 写入程序 'Microsoft Hyper-V VSS Writer' 无法准备用于备份的文件: 报告的状态: VSS_WS_FAILED_AT_POST_SNAPSHOT 预期状态: VSS_WS_WAITING_FOR_BACKUP_COMPLETE 故障代码: 0x80042336
```

当您检查操作系统的事件日志时，会发现其中记录了一个 ID 为 `10145` 的 Windows 日志类别事件。

原因

失败的根本原因可能是 Data Protector 防止备份不一致的数据。当 Data Protector 处理 Microsoft Hyper-V 还原链 (即一个或多个增量备份映像) 时，来自每个此类映像的数据将合并到基本备份映像中。自动合并过程由 Microsoft Hyper-V 执行，与 Data Protector 还原会话异步。会话完成后，它可能继续在后台运行。在合并完成之前调用所涉及虚拟机的备份会话时，Data Protector 会检测到该会话并中止此过程，以避免备份映像中出现不一致。

解决方案

稍后重新启动有问题的备份会话或相应地调整会话计划。

还原到 SMB 文件共享时，还原会话失败

还原到 SMB 文件共享时，不允许 Data Protector 代理修改所有者，并且会报告类似于以下内容的错误:

[Major] From: OB2BAR_VSSBAR_COMP@hyperv.example.com "HyperV" Time: MM/DD/YYYY HH:MM:SS PM

Cannot restore file '\\fileserver.example.com\share4vms\local_vm\Virtual Machines\A9321AEE-EC69-4F79-BB34-59BA97D83CAC.xml'.

Failed with error: '[1307] This security ID may not be assigned as the owner of this object.'

原因

Data Protector 需要足够的权限才能更改文件服务器上的文件所有者。

解决方案

使用具有足够权限的域用户在 Hyper-V 主机上运行 Data Protector Inet 服务，或将 Hyper-V 主机的计算机帐户添加到文件服务器的 Administrators 组。

尝试使用相同的备份规范备份两个 VM 时，备份失败

尝试使用相同的备份规范备份两个虚拟机时，备份失败。

原因

尝试使用相同的备份规范备份两个虚拟机时备份失败，其中一个虚拟机使用 IP 地址指定快照位置主机，另一个虚拟机使用主机名指定 VM 快照位置主机。

解决方案

创建两个 barlist:

- 第一个 barlist 用于按 IP 地址指定快照位置的虚拟机。
- 第二个 barlist 用于按主机名指定快照位置的虚拟机。

Hyper-V 虚拟机还原到原始位置失败

将显示以下错误消息:

[Warning] From: VEPALIB_HYPERV@hyperv.example.net "/HyperV" Time: MM/DD/YYYY HH:MM:SS PM

Host 'hyperv.example.net':

Cannot connect through WMI using Hyper-V credentials.

[Major] From: VEPALIB_HYPERV@hyperv.example.net "/HyperV" Time: MM/DD/YYYY HH:MM:SS PM

Virtual Machine 'Test_VM_7022_Test_VM_0466 (GUID: 14A23703-4D30-4A55-9A82-C80AFB79C611)': Cannot be deleted.

原因

为了检查虚拟机是否存在，将连接到所有 Hyper-V 主机。如果其中一个节点出现故障，则会显示上述错误。

解决方案

可以执行以下操作之一:

- 确保系统处于联机状态或从群集中删除该节点，然后重试还原操作。
- 启用“还原到目录”选项，然后从 Hyper-V 设置中导入虚拟机。
- 还原到所有主机均联机的群集。

VMware 集成故障诊断

This feature is available in the Express and Premium Editions

本主题列出了使用适用于 VMware 的虚拟环境集成时的常规检查和验证操作以及可能会遇到的问题。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。

检查和验证

如果配置、备份或还原失败:

- 检查备份主机上的 debug.log 中报告的系统错误。
- 检查您是否可以在有问题的客户机上执行文件系统备份和还原。

此外，如果您的备份失败:

- 按照“检查 VMware 客户机的配置”中所述，检查 vCenter Server 或独立 ESX(i) Server 系统的配置。

其他操作:

- 在来宾 VM 中执行文件删除操作后，完整 CBT 备份会话与先前的完整 CBT 备份会话具有类似的备份数据。原因是在来宾 VM 中执行文件删除操作后，VMware 不会回收磁盘空间。

  变通方法 1:

  1. 在 ESXi/ESX 4.1 或更高版本中回收虚拟磁盘的未用空间。
  2. 禁用 CBT，然后重新启用。

  变通方法 2:

  对虚拟机或 VMDK 执行 Storage vMotion，以迁移到使用不同块大小格式化的数据存储。例如，如果 VMDK 位于使用 2 MB 块格式化的数据存储上，请使用 1 MB、4 MB 或 8 MB 块大小格式化目标 VMFS 数据存储。完成此操作后，必须重置 CBT。

- 在启用 CBT 并运行备份之前，请确保虚拟机中没有用户创建的快照可用。否则会显示以下错误消息：

  [Warning] From: VEPALIB_VMWARE@hostname “<DataCenter>" Time: Date Time

  [172:390] Virtual Machine 'VM': User Snapshot(s) found. Changed Block Tracking cannot be enabled.

  变通方法：

  - 在启用 CBT 之前，删除与虚拟机关联的所有用户创建的快照。
  - 如果需要使用 CBT 备份快照中的更改，请合并更改。

- 在使用 VMware Storage VMotion 进行虚拟磁盘迁移后执行增量或差异 CBT 备份会话时，增量或差异 CBT 备份会话将回退到完整 CBT 备份会话，备份将回退到完整 CBT 会话。

  变通方法：

  ESX 5.5 Update 2 解决了该问题。原因是在使用 Storage VMotion 进行虚拟磁盘迁移后会重置 CBT。

问题

下面是将虚拟环境 ZDB 集成用于 VMware 时可能会遇到的一些问题：

VEPA 不清理以前连接的磁盘

VEPA 集成无法清除 VMware 备份主机上以前连接的磁盘。

原因

如果在 Hotadd 模式下虚拟机的 VEPA 备份突然结束，则同一虚拟机的后续备份会话可能无法清除备份主机上以前连接的磁盘。

解决方案

根据 VMware，必须在 vepa_vddk.config 文件中设置 tmpDirectory 。此问题已在 Data Protector 2020.11 发布中修复。有关详细信息，请参阅 https://vdc-download.vmware.com/vmwb-repository/dcr-public/91cc8936-cbd5-4f61-9a24-6b9b9e8cd63a/07ff0eec-8401-485e-bab3-5ca4db49905f/VDDK-701-ReleaseNotes.html。

备份对象失败

Data Protector VMware 虚拟机备份失败，并显示以下错误:

[Major] From: VEPALIB_VMWARE@<backup-proxy-name> "/<Datacenter-name>" Time: <Time>

Backup of object failed.

Name: <virtual-machine-name>

Path: /<Datacenter-name>/vm/Discovered virtual machine/<virtualmachine-name>

InstanceUUID : <instance-uuid-of-virtual-machine>

原因

如果 VEPA 备份代理主机上的 VDDK 临时目录路径名包含非 ASCII 字符，则会发生此错误。

解决方案

完成以下步骤：

1. 创建 Data Protector 进程可以访问的目录。例如 "C:\ProgramData\tmp "。目录路径应仅包含标准美国英语 ASCII 字符。
2. 将以下行添加到 VEPA 备份主机上的文件 "vepa_vddk.config "

   tmpDirectory="<path_to_temp_directory>".
   例如， tmpDirectory="<C:\ProgramData\tmp>" 。

   您可以在以下位置找到 vepa_vddk.config 文件:
   - Windows 备份主机 -
   - Linux 备份主机 - "/etc/opt/omni/client/vepa_vddk.config"

有关详细信息，请参考以下链接:

- https://vdc-download.vmware.com/vmwb-repository/dcr-public/8f96698a-0e7b-4d67-bb6c-d18a1d101540/ef536a47-27cd-481a-90ef-76b38e75353c/vsphere-vddk-671-programming-guide.pdf
- https://vdc-repo.vmware.com/vmwb-repository/dcr-public/8f96698a-0e7b-4d67-bb6c-d18a1d101540/ef536a47-27cd-481a-90ef-76b38e75353c/doc/GUID-EAC428A4-E110-4F03-83D0-4FE5D09F355A.html

卸载时出错 - IPC 读取错误

从 Data Protector 2019.12 升级到 Data Protector 2020.08 后，浏览在 2019.12 版本中创建的请求时，浏览结果中没有文件或文件夹。有时会出现以下错误:

Error while unmounting
IPC Read Error
Access denied

原因

此错误的原因未知。

解决方案

完成以下步骤：

1。删除旧请求。执行：
vmwaregre-agent.exe -force_cleanup <request_id> -vcenter <vcenter hostname>

2。使用相同的 Data Protector 2019.12 备份会话创建新请求。

3。执行浏览和恢复。

无法将标记附加到虚拟机

在还原期间，将标记附加到还原的 VM 时，会显示以下警告消息:
[Warning] From: VEPALIB_VMWARE@<hostname> "<DataCenter>" Time: <Date> <Time>
Failed to attach tags to virtual machines ..

原因

当不满足标记基数或您没有适当的标记特权时，会显示此警告消息。

解决方案

- 检查标记基数。
- vSphere 备份用户帐户应具有适当的附加和读取特权。

增量或差异 CBT 备份会话失败

在启用“使用更改后的块跟踪”选项的情况下执行增量或差异备份会话时，会话会失败并显示类似以下内容的错误:

```
[严重] 来自: OB2BAR_VEPA_BAR@droid.company.com "/New Datacenter 4.1" 时间: 2/10/2011 11:14:52 AM 虚拟机 'ddd': 无法在磁盘 scsi0:0 上收集更改后的块...
```

原因

原因可能是您执行了还原会话，但忘记运行完整备份会话以启动新的备份链。

要确保更改后的块跟踪正常工作，需要满足某些要求。

解决方案

完成以下步骤：

1. 运行完整备份会话。
2. 运行增量或差异备份会话。

还原或移动到其他文件夹后，无法正确执行备份

将虚拟机还原或移动到其他文件夹后，未正确备份虚拟机。例如，执行完整备份，而不是增量备份。

原因

原因是数据中心配置文件已更新。因此，它包含两个具有相同 UUID 的虚拟机部分；这是出现不一致的地方。

解决方案

重新配置虚拟机:

1. 打开备份规范。
2. 在“源”页面中，右键单击 VMware 客户机，然后选择“配置虚拟机”。
3. 单击**确定**。

还原会话使用 LAN 传输模式进行还原

还原会话使用 LAN 传输模式而不是 SAN 进行还原。

原因

如果用于控制还原会话的备份主机是虚拟机，则 Data Protector 会自动切换到 LAN 传输模式。

解决方案

要使用 SAN 传输模式进行还原，请在物理系统上配置备份主机 (即，在物理系统上安装“虚拟环境集成”组件)，并选择此系统作为还原会话的备份主机。

无法执行还原。找到附加到 **Nova** 实例的新磁盘

当您尝试还原备份的 Nova 实例时，显示以下错误消息:

```
错误: 虚拟机 '9d28cd95-c158-45ec-b606-53f7c63a2a78': 无法执行还原。找到附加到 Nova 实例的新磁盘。
```

原因

如果在执行备份后将磁盘添加到 Nova 实例，则会发生此错误。

解决方案

当需要进行时间点还原，且在备份中的该时间点之后添加了新磁盘时，还原将失败。必须从 OpenStack 中分离附加到实例的新卷，然后再次执行还原。

添加新磁盘后，需要执行完整备份。

使用 SAN 传输模式的还原会话失败

使用 SAN 传输模式的还原会话失败，并显示类似于以下内容的消息:

```
[严重] 来自: OB2BAR_VEAgent@dpi00019.company.com "/BlrVirtual01_ESX401" 时间: 13-03-2011 12:22:57 虚拟机 'Win2k3_x64_dpi00002': 还原项目时出错 \a1f9f4e3-482d-4b7f-afcb-cb16babe1980\%2FBlrVirtual01_ESX401\vms\%2FBlrVirtual01_ESX401%2Fhost%2FClus01%2FWin2k3_x64_dpi00002\ images\3\scsi2:15。
```

原因

如果备份主机与 ESX(i) Server 系统之间共享的存储卷为只读，则可能会发生这种情况。

解决方案

1. 登录备份主机，并打开命令提示符。
2. 执行 diskpart 。

   ```
   C:\Users\Administrator>diskpart Microsoft DiskPart 版本 6.1.7600 版权所有 (C) 1999-2008 Microsoft Corporation。 在计算机上: TPC134
   ```

3. 将 SAN 策略设置为 onlineAll 。

   ```
   DISKPART> san policy=onlineAll DiskPart 成功更改了当前 操作系统的 SAN 策略。
   ```

4. 选择应用于还原的磁盘 (存储卷)。

   ```
   DISKPART> list disk 磁盘 ### 状态 大小 可用大小 Dyn Gpt -------- ------------- ------- ------- --- --- 磁盘 0 联机 136 GB 1024 KB 磁盘 1 脱机 14 GB 14 GB 磁盘 2 脱机 14 GB 14 GB 磁盘 3 脱机 14 GB 14 GB 磁盘 4 脱机 14 GB 14 GB 磁盘 5 脱机 50 GB 50 GB 磁盘 6 脱机 14 GB 14 GB 磁盘 7 脱机 14 GB 14 GB DISKPART> select disk 1
   ```

5. 将磁盘联机。

   ```
   DISKPART> online disk DiskPart 已将选定磁盘成功联机。
   ```

6. 确保磁盘不是只读。

   列出磁盘属性。

   ```
   DISKPART> detail disk HP OPEN-V SCSI 磁盘设备 磁盘 ID: 00000000 类型 : FIBRE 状态: 联机 路径 : 0 目标: 0 LUN ID: 0 位置路径: 不可用 当前只读状态: 是 只读 : 是 引导磁盘 : 否 页面文件磁盘 : 否 休眠文件磁盘 : 否 崩溃转储磁盘 : 否 群集磁盘 : 否 没有卷。
   ```

   清除只读属性。

   ```
   DISKPART> attribute disk clear readonly 磁盘属性已成功清除。
   ```

   再次列出磁盘属性。

   ```
   DISKPART> detail disk HP OPEN-V SCSI 磁盘设备 磁盘 ID: 00000000 类型 : FIBRE 状态: 联机 路径 : 0 目标: 0 LUN ID: 0 位置路径: 不可用 当前只读状态: 否 只读 : 否 引导磁盘 : 否 页面文件磁盘 : 否 休眠文件磁盘 : 否 崩溃转储磁盘 : 否 群集磁盘 : 否 没有卷。
   ```

   退出会话。

   ```
   DISKPART> exit
   ```

7. 重新启动还原会话。

vepa_util.exe 浏览命令在更高的 Red Hat Enterprise Linux (RHEL) 版本上性能下降

在更高的 RHEL 版本上执行 vepa_util.exe browse 命令时，其性能比在其他操作系统上明显下降。

原因

问题的根本原因是，在更高版本的 RHEL 系统上，默认情况下不启用名称服务缓存后台程序。

解决方案

通过调用以下命令启动名称服务缓存后台程序：/etc/init.d/nscd start .要在系统启动期间启用自动后台程序启动，请执行：chkconfig nscd on .

将虚拟机还原到由 vCenter Server 5.x 或更高版本管理的 ESX(i) 主机时，还原作业失败

将虚拟机还原到由 vCenter Server 5.x 或更高版本管理的 ESX(i) 主机时，还原作业将失败，并且虚拟机无法成功还原。

原因

从 ESX(i) 5.0 开始，VMware 已阻止将虚拟机还原到由 vCenter 管理的 ESX(i) 主机的能力。

解决方案

要解决此问题，请通过 vCenter Server 还原虚拟机，或者在从 vCenter Server 更改主机管理后通过 ESX/ESX(i) 还原虚拟机。

使用 ESX(i) Server 系统还原虚拟机以 VM 来宾操作系统损坏结束

在 vSphere 环境中，当使用 ESX(i) 5.0 Server 系统或更高版本作为还原客户机将虚拟机还原到 /ha-datacenter 时，还原会话成功结束，但虚拟机上的客户机操作系统损坏。

原因

如果您选择 ESX(i) 服务器作为还原客户机，则会发生此问题。

解决方案

选择要还原的对象时，在“目标”页面中的“还原客户机”下拉列表中，选择一个 vCenter Server，而不是 ESX(i) Server 系统。

栏备份会话已开始，但在 600 秒内无客户机连接。正在中止会话!

在某些情况下，启动备份且备份规范包含多个虚拟机时，将显示以下消息:

[重大] 来自: BSM@company.name.com "backup_spec_name" 时间: 4/10/2014 2:55:07 PM [61:2052] BAR 备份会话已启动，但在 600 秒内无客户机连接。正在中止会话!

在启动备份过程之前，VEAgent 会收集所有虚拟机的元数据信息。当 VEAgent 忙于收集信息时，BSM 会等待 10 分钟 (默认超时) 以使 VEAgent 连接。在超过默认时间后，BSM 超时并显示上面显示的消息。

解决方案

提高 Data Protector 全局选项中可用的超时变量的值。

SmWaitForFirstBackupClient=WaitForInMinutes

SmWaitForFirstBackupClientSec=WaitForInSeconds

创建 VM 快照时发生异常。备份对象失败

虚拟环境的备份可能会失败，并显示以下错误消息:

- Exception occurred while creating VM snapshot
- Backup of object failed

原因

如果 vCenter 和 ESX 主机上的超时值较低，则可能会发生这些错误。

解决方案

提高 vCenter 配置文件（vpxd.cfg）和 ESX 主机配置文件（vpxa.cfg）中的超时值。

> **注意**您可以根据需求更改此处建议的值。

此外，请检查 vCenter 中的超时值和操作超时值:

提高 vCenter 中的操作超时值。

1. 使用管理员凭据登录 vCenter Server。
2. 转至以下位置:

   vCenter Server 设置 > 超时设置。

3. 在“客户机连接超时”下，设置以下值:
   - Normal Operations timeout：600
   - Long Operations timeout：2000

提高 vCenter 中的超时值

要增加 ESX 与 vCenter 主机之间的空闲连接数，请在 vpxd.cfg 文件中的 <config> 和 </config> 标记内添加以下值:

```
<vpxd>

<maxHostPooledConnections>20000</maxHostPooledConnections>

</vpxd>
```

> **注意**这将减少主机同步期间创建与代理的其他 TCP 连接。

未找到要备份的对象

升级之后，如果备份规范是使用 Data Protector、7.01 或早期版本创建的，则 VEAgent 备份将会失败，并显示以下错误:

[Critical] From: VEPALIB_VMWARE@<hostname> "<Datacenter>" Time: <Date Time>

No Objects found for backup

解决方案

升级之后，请执行以下步骤:

1. 使用与之前相同的 VM 选择和选项重新创建备份规范。
2. 再次运行备份。

虚拟环境集成代理 (VEPA) 和会话管理器在等待超过超时值时停止

运行多个并行 VEPA 备份会话时，您可能会遇到一种情况，其中一小部分 (1 个或 2 个) 会话可能会停止，这样 VEPA 和 BSM 无法响应，直到达到超时期限。

这些会话的 VEPA 和 BSM 停止进程可能最终会超时，并显示以下消息：

[Major] From: BSM@machineName "barlist7" Time: 6/13/2014 2:05:41 AM

[61:1002] The OB2BAR Backup DA named "/Datacenter" on host machineName reached its inactivity timeout of xxxx seconds. The agent on host will be shutdown .

原因

这可能是由于 vCenter 是通过 VEPA 代理 (来自并行 VM 备份会话) 发出的多个并发连接请求加载的。

解决方案

在超时期限后：

1. 手动停止 vepa_bar 进程并等待与其关联的 BSM 进程也关闭。(BSM 在 vepa_bar 退出后关闭。)
2. 重新启动包含该失败 VM 对象的备份规范。

注意: 如果超时期限在备份启动之前 (正在解析对象时) 便已结束，则在“内部数据库”->“全局选项”中提高 SmWaitForFirstBackupClient 参数值。

并行备份会话失败

并行运行的备份会话失败。

原因

如果备份规范中的 VM 属于同一 LUN (已备份)，并且用于备份的装载代理主机相同，则对于并行备份，第二个备份会话将失败。

解决方案

为第二个备份会话使用另一个装载代理主机。

从 3PAR 副本进行的虚拟机零宕机时间备份失败

零宕机时间备份失败，并显示以下错误消息:

```
[重大] 来自: BSM@hostname.com "New2" 时间: MM/DD/YYYY HH:MM:SS AM
```

```
[61:2052] BAR 备份会话已启动，但
```

```
在 XX 秒内无客户机连接。
```

```
正在中止会话!
```

原因

如果备份规范包含大量虚拟机，或者虚拟中心或 ESX 服务器上的负载很高，则会发生此错误。

解决方案

通过重置 Data Protector SmWaitForFirstBackupClient 全局选项变量来扩展超时值。

配置的 IP 丢失

对 Linux 虚拟机执行还原操作后，配置的 IP 丢失。

原因

以下情况下可能会出现这种问题:

在执行还原操作之前，如果在还原工作流中单击“保留以用于取证”或“还原后删除”选项，则还原的 VM 会将新的 NIC 设置为 DHCP ，且其原始 NIC 隐藏。

解决方案

这是已知 VMware/Linux 限制。对于运行 Linux 客户机操作系统的虚拟机，在还原该虚拟机时，ESX 服务器可以为虚拟机分配新的 (虚拟) MAC 地址。重新启动虚拟机后，您可能必须配置其 MAC 地址。例如，虚拟机的原始 MAC 地址可能位于必须按以下知识库文章中所述进行更新的配置文件中。

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2002767

和

http://www.uptimemadeeasy.com/vmware/fixing-eth0-mac-address-vmware-clone-restore/

虚拟机还原: 在虚拟环境中的三个磁盘上找不到对象

在还原虚拟机时，在虚拟环境中的三个磁盘上找不到该对象。

原因

如果虚拟机在数据存储中不再可用，则会发生此问题。

解决方案

要启用数据存储上不再可用的虚拟机的部分还原，请继续执行以下步骤:

1. 使用与原始备份相同的 UUID 创建临时虚拟机。
2. 将部分数据从备份还原到临时虚拟机。

使用备份到磁盘 (B2D) 网关的 Data Protector 虚拟环境集成 (VEPA) 备份会话可能会失败

在使用 B2D 网关的虚拟环境备份中，当用于服务器端重复数据删除的 Cell Manager、VEPA 代理、介质代理网关位于同一台计算机上时，备份可能会失败。

原因

当虚拟环境备份使用 B2D 网关，以及当服务器端重复数据删除的 Cell Manager、VEPA 代理，介质代理网关在同一台计算机上时，会发生此错误。

解决方案

您可以执行以下任务来解决此问题:

- 将介质代理和 VEPA 代理移动到另一个主机。
- 减少介质代理中的并发流数。
- 将 omnirc 变量 OB2BMAUPDT 设置为 10000。
- 提高备份会话管理器的进程优先级。
- 切换到源端重复数据删除。
- 将 VEPA 备份从 SAN 模式切换到 NBD 模式。
- 避免在 Data Protector GUI 中监视会话。

VMware 虚拟机磁盘的备份可能会失败

VMware 虚拟机磁盘的备份可能会失败，并显示以下错误消息:

[20] [VddkUtil::diskLibWarning] VixDiskLib: Failed to load vixDiskLibVim.dll : ErrorCode = 0x7f.

原因

这是已知 VMware 问题。

解决方案

要解决此问题，请执行以下任务:

1. 在单独的服务器上安装 vCenter 和 VDDK。
2. 将 libldap_r.dll 和 liblber.dll 从 \Program Files\OmniBack\lib\vddk\AMD64 复制到 \Program Files\OmniBack\bin 。
3. 将 libcurl.dll 从 \Program Files\OmniBack\lib\x8664 复制到 \Program Files\OmniBack\bin 。

还原后，Windows 虚拟机的引导失败

当在还原操作后引导 Windows 虚拟机时，引导过程会失败，并显示以下错误：No operating system found.

原因

这是已知 VMware 问题。如果操作系统磁盘和数据磁盘来自不同的控制器类型 (如 SCSI 和 IDE)，则可能会出现此错误。有关更多详细信息，请参阅 http://kb.vmware.com/kb/1023592。

解决方案

您必须使用选项 bios.bootOrder 和 bios.hddOrder 更改虚拟机的引导顺序。有关详细过程，请参阅 http://kb.vmware.com/kb/2011654。

VMware ZDB 备份、启动和实时迁移可能会失败

有时，VMware ZDB 备份会话、启动和实时迁移会话可能会失败，并显示以下错误消息:

```
[严重] 来自: VEPALIB_VMWARE@<HostName> "<AppName>" 时间: <Timestamp>
```

```
装载数据存储时出错
```

原因

出现此错误可能是因为源 ESX 主机或装载 ESX 可能包含一些无法解析到数据存储的错误的未解析磁盘卷。

解决方案

您必须在源 ESX 服务器或装载代理 ESX 服务器主机上标识此类卷，并从主机中删除这些卷的呈现。

启动和实时迁移期间显示错误消息

启动和实时迁移会话期间显示以下错误消息:

Failed to install/start NFS service.

解决方案

在装载代理主机上打开 Windows PowerShell 窗口，然后运行以下命令:

```
PS C:\Program Files\OmniBack\bin> .\nfsServiceCheck.ps1
```

```
True
```

```
PS C:\Program Files\OmniBack\bin>
```

创建虚拟机快照和对象备份失败时出错

创建虚拟机的快照时发生错误:

[严重] 来自: VEPALIB_VMWARE@<HostName> "<AppName>" 时间: <Timestamp>

装载数据存储时出错

[正常] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/DATACENTERNAME"

虚拟机 'VMNAME': 正在创建快照...

[重大] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/DATACENTERNAME "

虚拟机 'VMNAME': 删除快照时出错

[严重] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/CPD2" 时间: 19/03/2016 8:01:48

备份对象失败。

名称: VMNAME

路径: / DATACENTERNAME /DATASTORE/ VMNAME

InstanceUUID: IUUIDOFVM

原因

当虚拟机位于 Site Recovery Manager (SRM) 中时，会出现此问题。对 SRM 中的虚拟机禁用创建快照 API，因此不支持备份操作。

解决方案

由于不支持位于 SRM 中的虚拟机快照，因此没有针对该问题的解决方案。

还原到数据中心后，虚拟硬件版本为 4 的虚拟机无法启动

当虚拟机从 Data Protector GUI 还原到数据中心时，虽然还原成功，但虚拟机无法启动。

原因

在具有虚拟硬件版本 4 的 VM 中，会间歇性地看到此问题。

解决方案

1. 从 Data Protector GUI，将虚拟机还原到备份主机上的某个文件夹。
2. 在 vCenter 中，创建一个没有附加任何磁盘的新虚拟机。
3. 转到 vCenter 数据存储浏览器，然后从步骤 1 中创建的文件夹上载 vmdk 文件。
4. 从 vCenter 编辑 VM 设置并附加上载的 vmdk 文件。
5. 重新启动虚拟机。

GRE、启动和实时迁移操作失败

GRE、启动和实时迁移操作失败，并显示以下错误消息:

Object locked: The VM <*VM Name*> could be locked by another process for recovery/power on/live migrate.

Please retry after the process is either done or cancelled.

原因

如果正在进行的还原操作在 VM 上运行，则会发生此错误。

解决方案

确保满足以下条件:

- 虚拟机没有正在从 StoreOnce Catalyst 或数据域设备执行的还原操作 (对象复制、还原、启动、实时迁移或 GRE)。
- 检查是否在任何其他启动、实时迁移或 GRE 操作中使用相同的备份对象。如果使用，则清除请求并重试该操作。

由于相关卷影 VM 已附加到另一个 Nova 实例，因此无法执行还原

还原时，会话日志中将显示以下错误消息:

Virtual machine '9d28cd95-c158-45ec-b606-53f7c63a2a78': Can not perform restore, as the related shadow VM is attached to another Nov Instance '8d28ad65-c158-45ec-b606-53f7c63a4578

原因

如果作为备份 Nova 实例一部分的卷影 VM 附加到另一个 Nova 实例，则会发生此错误。

解决方案

从新实例中分离卷影 VM 并开始还原。

OpenStack 仪表板中的已还原实例未反映正确状态并仍处于错误状态

解决方案

还原完成后，重新启动 Compute Nova 代理服务，并手动将错误状态重置为“活动”。有关详细信息，请参阅“还原使用 vStorage 映像 + Openstack 方法备份的 Nova 实例和卷影 VM”。

还原或对象操作可能失败

Data Protector 对象复制会话中将显示以下错误:

[Major] From: RMA@hostname <DataCenter> Time: <Timestamp>

Cannot open device (StoreOnce error: The object is already locked and multiple open sessions not supported, or the server is unable to lock any more objects due to resource constraints)

原因

如果正在对与 StoreOnce Catalyst 或数据域设备相同的 VEPA 备份会话执行 GRE、启动或实时迁移操作，则还原或对象操作可能会失败。

如果正在为在会话 “X” 中备份的同一对象执行 GRE，则对象操作 (对象复制) 将因备份会话 “X” 失败。

解决方案

请执行以下操作：

- 确保虚拟机没有正在从 StoreOnce Catalyst 或数据域设备执行的还原操作 (对象复制、还原、启动、实时迁移或 GRE)。
- 清理已启动的虚拟机。
- 完成活动的 GRE、启动或实时迁移操作后重试。

在任何详细信息编目目录中均没有更多可用空间。从这一点开始，此介质上的所有对象都将日志记录切换为“无日志”

如果出现以下情况，则 StoreOnce Catalyst 或数据域设备的备份会话无资格进行启动和实时迁移:

- 在备份规范中选择了“无日志”选项或
- 备份会话报告中显示以下错误消息:

  [Major] From: BSM@hostname.com <VMname> Time: <Timestamp>

  [61:4039] Following error occurred while storing detail catalog

  information for device <Catalyst_device>

  with loaded medium <Catalyst_medium> to Data Protector Internal Database:

  There is no more space available in any of the Detail Catalog directories.

  From this point on, all objects on this medium will have logging switched to "No Log".

原因

如果选择了 无日志选项，或者在详细编目目录中没有更多可用空间，则会发生此错误。

解决方案

可以采取以下操作:

- 删除“无日志”选项或
- 在 Cell Manager 的 IDB 驱动器上创建一个空间，并针对另一设备执行单一会话复制。确保针对另一 StoreOnce Catalyst 或数据域设备执行单一会话复制时未选择复制选项。

启动和实时迁移操作期间出现数据一致性问题

启动和实时迁移操作期间出现数据一致性问题。

原因

发生此问题的原因如下:

1. 您选择的会话是对象复制的结果。
2. 对象复制通过将许多备份会话聚合为单个对象复制会话来执行。

解决方案

执行对象复制时选择单个会话。

Linux 虚拟机的还原成功完成，但 ifconfig 显示缺少 NIC

启动和实时迁移操作期间出现数据一致性问题。

原因

发生此问题的原因如下:

1. 您选择的会话是对象复制的结果。
2. 对象复制通过将许多备份会话聚合为单个对象复制会话来执行。

解决方案

执行对象复制时选择单个会话。

磁盘描述符文件 (<disk_vmdk_file_name>) 下载失败

在虚拟机备份期间，将显示以下错误消息:

[Warning] From: VEPALIB_VMWARE@<backup_host> <datacenter> Time: <date> <time>

Virtual Machine <virtual_machine_name>: Download of disk descriptor file (<disk_vmdk_file_name>) failed.

原因

如果在 vCenter 配置文件中禁用了 **vpxd.enableHttpDatastoreAccess** 和 **vpxd.enableDebugBrowse**，则会发生此错误。

解决方案

检查 vCenter 配置文件中是否启用 **vpxd.enableHttpDatastoreAccess** 和 **vpxd.enableDebugBrowse**，

因为出于安全原因可能会禁用这些设置。

VCenter 中存在 MAC 地址冲突

为虚拟机分配 MAC 地址时，VCenter 有时可能会分配重复的 MAC 地址。

原因

有关此问题的原因的详细信息，请参阅 https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.troubleshooting.doc/GUID-8D7D0126-8E8A-470F-A61E-4197EE32D08F.html。

解决方案

使用非源 VCenter 启动虚拟机。

启动/实时迁移失败

启动/实时迁移失败，并显示以下错误:

NFS share creation failed

原因

在 Windows 备份代理上，如果 Data Protector INET 服务最近从“本地系统”更改为某个服务帐户以允许介质代理或磁盘代理访问网络资源 (例如 CIFS 共享或网络共享备份上的文件库)，则会发生此失败。

解决方案

停止 Data Protector 过滤侦听程序服务 (FilterListenerService)，将其重新配置为使用与 Data Protector INET (omniinet) 服务相同的帐户，而不是使用“本地系统”帐户。启动服务，重试操作。

VEPA 备份无响应

在从数据域或 StoreOnce 存储设备执行 VEPA 备份的还原操作期间，VEPA 备份无限挂起并显示以下警告消息。

Device "<*device_name*>" is occupied. Waiting for device to get free.

原因

如果最初使用的介质代理不再属于 Cell Manager 且最初使用的设备配置仍然存在于 MMD 数据库中，则会发生这种情况。

解决方案

要成功还原备份，请执行以下步骤:

1. 手动中止挂起的会话。
2. 导航到“设备和介质”上下文。
   i. 展开“设备”树。
   ii. 右键单击“DD_boost”并选择“属性”。
   iii. 选择“存储单元和网关”选项卡。
   iv. 从“网关”下拉列表中添加新的介质代理主机用作新网关。单击**添加**。
   v. 将新介质代理主机的块大小设置为与旧介质代理主机的块大小设置相同。
      如果块大小未知，则从旧介质代理主机复制相应值。完成以下步骤:
      1. 从“网关”下拉列表中选择旧介质代理网关，然后单击“属性”。
      2. 在网关属性页中选择“设置”选项卡。
      3. 选择“高级”选项卡和“大小”选项卡。记下此选项卡中的值并将其添加到新介质代理网关。
   vi. 单击**检查**。检查完毕后，“状态”显示为“正常”。
   vii. 删除旧介质代理主机网关。选择该网关，然后单击“删除”。
   viii. 单击**应用**保存更改。
3. 使用新添加的介质代理主机网关重试还原操作。

正在中止与 **BSM** 的连接。中止代码 **-2**

在 VMware 并行备份会话期间，某些对象无法备份，并且显示以下错误消息：

```
[重大] 来自: OB2BAR_VEPA_BAR@<主机名> 时间：<<日期>><<时间>> 中止与 BSM 的连接。中止代码 2。
```

原因

当两个或多个 VMDK 文件具有相同的 UUID 时，将发生此错误。

解决方案

确保要备份的所有 VMDK 文件都具有唯一的 UUID。

启用 vSAN HOTADD 传输模式时备份失败

在备份以 HOTADD 传输模式配置的 VM 期间：

- **vSAN 数据存储 6.6**：备份过程不一致会导致备份失败。
- **vSAN 数据存储 6.7**：传输模式回退到 NBDSSL，相应的备份操作成功。

原因

当目标 VM 位于 vSAN 数据存储中并且代理 VM 位于非 vSAN 数据存储中时，会发生这种情况，反之亦然。

解决方案

VMware 建议将目标 VM 和代理 VM 放在同一 vSAN 数据存储和同一主机中。有关更多信息，请参考 https://kb.vmware.com/s/article/75202。

无法在磁盘上收集分配的块

VMware 备份期间显示以下错误消息:

```
Could not gather allocated blocks on disk.
```

原因

Data Protector 使用编程方法获取属于已选定要备份的虚拟机的磁盘中已分配（已使用）块的列表。此方法需要连接到 ESXi 主机的“网络文件复制”(NFC) 服务，但在此实例中失败。

解决方案

检查备份主机是否能够连接到“网络文件复制”(NFC) 端口，默认情况下，该端口是 ESX/ESXi 主机上的 TCP 端口 902。

VMware ZDB 集成故障诊断

This page is still under development. No published version is available at this time.

无法将标签附加到虚拟机 - ZDB

This page is still under development. No published version is available at this time.

增量或差异 CBT 备份会话失败

This page is still under development. No published version is available at this time.

还原或移动到其他文件夹后，无法正确执行备份

将虚拟机还原或移动到其他文件夹后，未正确备份虚拟机。例如，执行完整备份，而不是增量备份。

原因

原因是数据中心配置文件已更新。因此，它包含两个具有相同 UUID 的虚拟机部分；这是出现不一致的地方。

解决方案

重新配置虚拟机:

1. 打开备份规范。
2. 在“源”页面中，右键单击 VMware 客户机，然后选择“配置虚拟机”。
3. 单击**确定**。

还原会话使用 LAN 传输模式进行还原

还原会话使用 LAN 传输模式而不是 SAN 进行还原。

原因

如果用于控制还原会话的备份主机是虚拟机，则 Data Protector 会自动切换到 LAN 传输模式。

解决方案

要使用 SAN 传输模式进行还原，请在物理系统上配置备份主机 (即，在物理系统上安装“虚拟环境集成”组件)，并选择此系统作为还原会话的备份主机。

vepa_util.exe 浏览命令在更高的 Red Hat Enterprise Linux (RHEL) 版本上性能下降

在更高的 RHEL 版本上执行 vepa_util.exe browse 命令时，其性能比在其他操作系统上明显下降。

原因

问题的根本原因是，在更高版本的 RHEL 系统上，默认情况下不启用名称服务缓存后台程序。

解决方案

通过调用以下命令启动名称服务缓存后台程序：/etc/init.d/nscd start .要在系统启动期间启用自动后台程序启动，请执行：chkconfig nscd on .

将虚拟机还原到由 vCenter Server 5.x 或更高版本管理的 ESX(i) 主机时，还原作业失败

将虚拟机还原到由 vCenter Server 5.x 或更高版本管理的 ESX(i) 主机时，还原作业将失败，并且虚拟机无法成功还原。

原因

从 ESX(i) 5.0 开始，VMware 已阻止将虚拟机还原到由 vCenter 管理的 ESX(i) 主机的能力。

解决方案

要解决此问题，请通过 vCenter Server 还原虚拟机，或者在从 vCenter Server 更改主机管理后通过 ESX/ESX(i) 还原虚拟机。

使用 ESX(i) Server 系统还原虚拟机以 VM 来宾操作系统损坏结束

在 vSphere 环境中，还原会话成功结束，但是虚拟机上的来宾操作系统已损坏。

原因

当您使用 ESX(i) 5.0 Server 系统或更高版本作为还原客户机将虚拟机还原到 /ha-datacenter 时，会发生此问题。

解决方案

选择要还原的对象时，在“目标”页面中的“还原客户机”下拉列表中，选择一个 vCenter Server，而不是 ESX(i) Server 系统。

栏备份会话已开始，但在 600 秒内无客户机连接。正在中止会话!

在某些情况下，启动备份且备份规范包含多个虚拟机时，将显示以下消息:

[重大] 来自: BSM@company.name.com "backup_spec_name" 时间: 4/10/2014 2:55:07 PM [61:2052] BAR 备份会话已启动，但在 600 秒内无客户机连接。正在中止会话!

原因

在启动备份过程之前，VEAgent 会收集所有虚拟机的元数据信息。当 VEAgent 忙于收集信息时，BSM 会等待 10 分钟 (默认超时) 以使 VEAgent 连接。在超过默认时间后，BSM 超时并显示上面显示的消息。

解决方案

提高以下 Data Protector 全局选项中可用的超时变量的值:

- SmWaitForFirstBackupClient=WaitForInMinutes
- SmWaitForFirstBackupClientSec=WaitForInSeconds

创建 VM 快照时发生异常。备份对象失败

虚拟环境的备份可能会失败，并显示以下错误消息:

- Exception occurred while creating VM snapshot
- Backup of object failed

原因

如果 vCenter 和 ESX 主机上的超时值较低，则可能会发生这些错误。

解决方案

提高 vCenter 配置文件 (vpxd.cfg) 和 ESX 主机配置文件 (vpxa.cfg) 中的超时值。

> **注意**您可以根据需求更改此处建议的值。

此外，请检查 vCenter 中的超时值和操作超时值:

提高 vCenter 中的操作超时值。

1. 使用管理员凭据登录 vCenter Server。
2. 转至以下位置:

   vCenter Server 设置 > 超时设置。

3. 在“客户机连接超时”下，设置以下值:
   - Normal Operations timeout：600
   - Long Operations timeout：2000

提高 vCenter 中的超时值

要增加 ESX 与 vCenter 主机之间的空闲连接数，请在 vpxd.cfg 文件中的 <config> 和 </config> 标记内添加以下值:

```
<vpxd>

<maxHostPooledConnections>20000</maxHostPooledConnections>

</vpxd>
```

> **注意**这将减少主机同步期间创建与代理的其他 TCP 连接。

未找到要备份的对象

升级后，VEAgent 备份失败，并显示以下错误:

[Critical] From: VEPALIB_VMWARE@<hostname> "<Datacenter>" Time: <Date Time>

No Objects found for backup

原因

如果使用 Data Protector 7.01 或更早版本创建备份规范，则会发生此错误。

解决方案

升级之后，请执行以下步骤:

1. 使用与之前相同的 VM 选择和选项重新创建备份规范。
2. 再次运行备份。

虚拟环境集成代理 (VEPA) 和会话管理器在等待超过超时值时停止

运行多个并行 VEPA 备份会话时，您可能会遇到一种情况，其中一小部分 (1 个或 2 个) 会话可能会停止，这样 VEPA 和 BSM 无法响应，直到达到超时期限。

这些会话的 VEPA 和 BSM 停止进程可能最终会超时，并显示以下消息：

[Major] From: BSM@machineName "barlist7" Time: 6/13/2014 2:05:41 AM

[61:1002] The OB2BAR Backup DA named "/Datacenter" on host machineName reached its inactivity timeout of xxxx seconds. The agent on host will be shutdown .

原因

这可能是由于 vCenter 是通过 VEPA 代理 (来自并行 VM 备份会话) 发出的多个并发连接请求加载的。

解决方案

在超时期限后：

1. 手动停止 vepa_bar 进程并等待与其关联的 BSM 进程也关闭。(BSM 在 vepa_bar 退出后关闭。)
2. 重新启动包含该失败 VM 对象的备份规范。

注意: 如果超时期限在备份启动之前 (正在解析对象时) 便已结束，则在“内部数据库”->“全局选项”中提高 SmWaitForFirstBackupClient 参数值。

并行备份会话失败

并行运行的备份会话失败。

原因

如果备份规范中的 VM 属于同一 LUN (已备份)，并且用于备份的装载代理主机相同，则对于并行备份，第二个备份会话将失败。

解决方案

为第二个备份会话使用另一个装载代理主机。

从 3PAR 副本进行的虚拟机零宕机时间备份失败

零宕机时间备份失败，并显示以下错误消息:

```
[重大] 来自: BSM@hostname.com "New2" 时间: MM/DD/YYYY HH:MM:SS AM
```

```
[61:2052] BAR 备份会话已启动，但
```

```
在 XX 秒内无客户机连接。
```

```
正在中止会话!
```

原因

如果备份规范包含大量虚拟机，或者虚拟中心或 ESX 服务器上的负载很高，则会发生此错误。

解决方案

通过重置 Data Protector SmWaitForFirstBackupClient 全局选项变量来扩展超时值。

配置的 IP 丢失

对 Linux 虚拟机执行还原操作后，配置的 IP 丢失。

原因

以下情况下可能会出现这种问题:

在执行还原操作之前，如果在还原工作流中单击“保留以用于取证”或“还原后删除”选项，则还原的 VM 会将新的 NIC 设置为 DHCP ，且其原始 NIC 隐藏。

解决方案

这是已知 VMware/Linux 限制。对于运行 Linux 客户机操作系统的虚拟机，在还原该虚拟机时，ESX 服务器可以为虚拟机分配新的 (虚拟) MAC 地址。重新启动虚拟机后，您可能必须配置其 MAC 地址。例如，虚拟机的原始 MAC 地址可能位于必须按以下知识库文章中所述进行更新的配置文件中。

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2002767

和

http://www.uptimemadeeasy.com/vmware/fixing-eth0-mac-address-vmware-clone-restore/

虚拟机还原: 在虚拟环境中的三个磁盘上找不到对象

在还原虚拟机时，在虚拟环境中的三个磁盘上找不到该对象。

解决方案

要启用数据存储上不再可用的虚拟机的部分还原，请继续执行以下步骤:

1. 使用与原始备份相同的 UUID 创建临时虚拟机。
2. 将部分数据从备份还原到临时虚拟机。

使用备份到磁盘 (B2D) 网关的 Data Protector 虚拟环境集成 (VEPA) 备份会话可能会失败

在使用 B2D 网关的虚拟环境备份中，当用于服务器端重复数据删除的 Cell Manager、VEPA 代理、介质代理网关位于同一台计算机上时，备份可能会失败。

原因

当虚拟环境备份使用 B2D 网关，以及当服务器端重复数据删除的 Cell Manager、VEPA 代理，介质代理网关在同一台计算机上时，会发生此错误。

解决方案

您可以执行以下任务来解决此问题:

- 将介质代理和 VEPA 代理移动到另一个主机。
- 减少介质代理中的并发流数。
- 将 omnirc 变量 OB2BMAUPDT 设置为 10000。
- 提高备份会话管理器的进程优先级。
- 切换到源端重复数据删除。
- 将 VEPA 备份从 SAN 模式切换到 NBD 模式。
- 避免在 Data Protector GUI 中监视会话。

VMware 虚拟机磁盘的备份可能会失败

VMware 虚拟机磁盘的备份可能会失败，并显示以下错误消息:

[20] [VddkUtil::diskLibWarning] VixDiskLib: Failed to load vixDiskLibVim.dll : ErrorCode = 0x7f.

原因

这是已知 VMware 问题。

解决方案

要解决此问题，请执行以下任务:

1. 在单独的服务器上安装 vCenter 和 VDDK。
2. 将 libldap_r.dll 和 liblber.dll 从 \Program Files\OmniBack\lib\vddk\AMD64 复制到 \Program Files\OmniBack\bin 。
3. 将 libcurl.dll 从 \Program Files\OmniBack\lib\x8664 复制到 \Program Files\OmniBack\bin 。

还原后，Windows 虚拟机的引导失败

当在还原操作后引导 Windows 虚拟机时，引导过程会失败，并显示以下错误：No operating system found.

原因

这是已知 VMware 问题。如果操作系统磁盘和数据磁盘来自不同的控制器类型 (如 SCSI 和 IDE)，则可能会出现此错误。有关更多详细信息，请参阅 http://kb.vmware.com/kb/1023592。

解决方案

您必须使用选项 bios.bootOrder 和 bios.hddOrder 更改虚拟机的引导顺序。有关详细过程，请参阅 http://kb.vmware.com/kb/2011654。

VMware ZDB 备份、启动和实时迁移可能会失败

有时，VMware ZDB 备份会话、启动和实时迁移会话可能会失败，并显示以下错误消息:

```
[严重] 来自: VEPALIB_VMWARE@<HostName> "<AppName>" 时间: <Timestamp>
```

```
装载数据存储时出错
```

原因

出现此错误可能是因为源 ESX 主机或装载 ESX 可能包含一些无法解析到数据存储的错误的未解析磁盘卷。

解决方案

您必须在源 ESX 服务器或装载代理 ESX 服务器主机上标识此类卷，并从主机中删除这些卷的呈现。

启动和实时迁移期间显示错误消息

启动和实时迁移会话期间显示以下错误消息:

Failed to install/start NFS service.

解决方案

在装载代理主机上打开 Windows PowerShell 窗口，然后运行以下命令:

```
PS C:\Program Files\OmniBack\bin> .\nfsServiceCheck.ps1
```

```
True
```

```
PS C:\Program Files\OmniBack\bin>
```

创建虚拟机快照和对象备份失败时出错

创建虚拟机的快照时发生错误:

[严重] 来自: VEPALIB_VMWARE@<HostName> "<AppName>" 时间: <Timestamp>

装载数据存储时出错

[正常] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/DATACENTERNAME"

虚拟机 'VMNAME': 正在创建快照...

[重大] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/DATACENTERNAME "

虚拟机 'VMNAME': 删除快照时出错

[严重] 来自: VEPALIB_VMWARE@BACKUPHOSTNAME "/CPD2" 时间: 19/03/2016 8:01:48

备份对象失败。

名称: VMNAME

路径: / DATACENTERNAME /DATASTORE/ VMNAME

InstanceUUID: IUUIDOFVM

原因

当虚拟机位于 Site Recovery Manager (SRM) 中时，会出现此问题。

解决方案

对 SRM 中的虚拟机禁用创建快照 API，因此不支持备份操作。

还原到数据中心后，虚拟硬件版本为 4 的虚拟机无法启动

当虚拟机从 Data Protector GUI 还原到数据中心时，虽然还原成功，但虚拟机无法启动。

解决方案

1. 从 Data Protector GUI，将虚拟机还原到备份主机上的某个文件夹。
2. 在 vCenter 中，创建一个没有附加任何磁盘的新虚拟机。
3. 转到 vCenter 数据存储浏览器，然后从步骤 1 中创建的文件夹上载 vmdk 文件。
4. 从 vCenter 编辑 VM 设置以附加上载的 vmdk 文件。
5. 重新启动虚拟机以进行引导。

GRE、启动和实时迁移操作失败

GRE、启动和实时迁移操作失败，并显示以下错误消息:

Object locked: The VM <*VM Name*> could be locked by another process for recovery/power on/live migrate.

Please retry after the process is either done or cancelled.

原因

如果正在进行的还原操作在 VM 上运行，则会发生此错误。

解决方案

确保满足以下条件:

- 虚拟机没有正在从 StoreOnce Catalyst 或数据域设备执行的还原操作 (对象复制、还原、启动、实时迁移或 GRE)。
- 检查是否在任何其他启动、实时迁移或 GRE 操作中使用相同的备份对象。如果使用，则清除请求并重试该操作。

如果找到的新磁盘附加到 Nova 实例，则无法执行还原

在还原过程中，会显示以下错误消息:

Virtual machine '9d28cd95-c158-45ec-b606-53f7c63a2a78': Cannot perform Restore. Found new disk attached to the Nova instance.

原因

如果找到的新磁盘附加到 Nova 实例，则会发生此错误。

解决方案

当需要进行时间点还原，且在备份中的该时间点之后添加了新磁盘时，不允许还原。必须从 OpenStack 中分离附加到实例的新卷，然后再次执行还原。

由于相关的影子 VM 已附加到另一个 Nov 实例，因此无法执行还原

还原时，会话日志中将显示以下错误消息:

Virtual machine '9d28cd95-c158-45ec-b606-53f7c63a2a78': Can not perform restore, as the related shadow VM is attached to another Nov Instance '8d28ad65-c158-45ec-b606-53f7c63a4578

原因

如果作为备份 Nova 实例一部分的卷影 VM 附加到另一个 Nova 实例，则会发生此错误。

解决方案

从新实例中分离卷影 VM 并开始还原。

OpenStack 仪表板中的已还原实例未反映正确状态并仍处于错误状态

解决方案

还原完成后，重新启动 Compute Nova 代理服务，并手动将错误状态重置为“活动”。有关详细信息，请参阅“还原使用 vStorage 映像 + Openstack 方法备份的 Nova 实例和卷影 VM”。

还原或对象操作可能失败

Data Protector 对象复制会话中将显示以下错误:

[Major] From: RMA@hostname <DataCenter> Time: <Timestamp>

Cannot open device (StoreOnce error: The object is already locked and multiple open sessions not supported, or the server is unable to lock any more objects due to resource constraints)

原因

如果正在对与 StoreOnce Catalyst 或数据域设备相同的 VEPA 备份会话执行 GRE、启动或实时迁移操作，则还原或对象操作可能会失败。

如果正在为在会话 “X” 中备份的同一对象执行 GRE，则对象操作 (对象复制) 将因备份会话 “X” 失败。

解决方案

请执行以下操作：

- 确保虚拟机没有正在从 StoreOnce Catalyst 或数据域设备执行的还原操作 (对象复制、还原、启动、实时迁移或 GRE)。
- 清理已启动的虚拟机。
- 完成活动的 GRE、启动或实时迁移操作后重试。

在任何详细信息编目目录中均没有更多可用空间。从这一点开始，此介质上的所有对象都将日志记录切换为“无日志”

如果出现以下情况，则 StoreOnce Catalyst 或数据域设备的备份会话无资格进行启动和实时迁移:

- 在备份规范中选择了“无日志”选项或
- 备份会话报告中显示以下错误消息:

  [Major] From: BSM@hostname.com <VMname> Time: <Timestamp>

  [61:4039] Following error occurred while storing detail catalog

  information for device <Catalyst_device>

  with loaded medium <Catalyst_medium> to Data Protector Internal Database:

  There is no more space available in any of the Detail Catalog directories.

  From this point on, all objects on this medium will have logging switched to "No Log".

原因

如果选择了 无日志选项，或者在详细编目目录中没有更多可用空间，则会发生此错误。

解决方案

可以采取以下操作:

- 删除“无日志”选项或
- 在 Cell Manager 的 IDB 驱动器上创建一个空间，并针对另一设备执行单一会话复制。确保针对另一 StoreOnce Catalyst 或数据域设备执行单一会话复制时未选择复制选项。

启动和实时迁移操作期间出现数据一致性问题

启动和实时迁移操作期间出现数据一致性问题。

原因

发生此问题的原因如下:

1. 您选择的会话是对象复制的结果。
2. 对象复制通过将许多备份会话聚合为单个对象复制会话来执行。

解决方案

执行对象复制时选择单个会话。

Linux 虚拟机的还原成功完成，但 ifconfig 显示缺少 NIC

启动和实时迁移操作期间出现数据一致性问题。

原因

发生此问题的原因如下:

1. 您选择的会话是对象复制的结果。
2. 对象复制通过将许多备份会话聚合为单个对象复制会话来执行。

解决方案

执行对象复制时选择单个会话。

磁盘描述符文件 (<disk_vmdk_file_name>) 下载失败

在虚拟机备份期间，将显示以下错误消息:

[Warning] From: VEPALIB_VMWARE@<backup_host> <datacenter> Time: <date> <time>

Virtual Machine <virtual_machine_name>: Download of disk descriptor file (<disk_vmdk_file_name>) failed.

原因

如果在 vCenter 配置文件中禁用了 **vpxd.enableHttpDatastoreAccess** 和 **vpxd.enableDebugBrowse**，则会发生此错误。

解决方案

检查 vCenter 配置文件中是否启用 **vpxd.enableHttpDatastoreAccess** 和 **vpxd.enableDebugBrowse**，

因为出于安全原因可能会禁用这些设置。

VCenter 中存在 MAC 地址冲突

为虚拟机分配 MAC 地址时，VCenter 有时可能会分配重复的 MAC 地址。

原因

有关此问题的原因的详细信息，请参阅 https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.troubleshooting.doc/GUID-8D7D0126-8E8A-470F-A61E-4197EE32D08F.html。

解决方案

使用非源 VCenter 启动虚拟机。

启动/实时迁移失败

启动/实时迁移失败，并显示以下错误:

NFS share creation failed

原因

在 Windows 备份代理上，如果 Data Protector INET 服务最近从“本地系统”更改为某个服务帐户以允许介质代理或磁盘代理访问网络资源 (例如 CIFS 共享或网络共享备份上的文件库)，则会发生此失败。

解决方案

停止 Data Protector 过滤侦听程序服务 (FilterListenerService)，将其重新配置为使用与 Data Protector INET (omniinet) 服务相同的帐户，而不是使用“本地系统”帐户。启动服务，重试操作。

VEPA 备份无响应

在从数据域或 StoreOnce 存储设备执行 VEPA 备份的还原操作期间，VEPA 备份无限挂起并显示以下警告消息。

Device "<*device_name*>" is occupied. Waiting for device to get free.

原因

如果最初使用的介质代理不再属于 Cell Manager 且最初使用的设备配置仍然存在于 MMD 数据库中，则会发生这种情况。

解决方案

要成功还原备份，请执行以下步骤:

1. 手动中止挂起的会话。
2. 导航到“设备和介质”上下文。
    1. 展开“设备”树。
    2. 右键单击“DD_boost”并选择“属性”。
    3. 选择“存储单元和网关”选项卡。
    4. 从“网关”下拉列表中添加新的介质代理主机用作新网关。单击**添加**。
    5. 将新介质代理主机的块大小设置为与旧介质代理主机的块大小设置相同。
       如果块大小未知，则从旧介质代理主机复制相应值。完成以下步骤:
        1. 从“网关”下拉列表中选择旧介质代理网关，然后单击“属性”。
        2. 在网关属性页中选择“设置”选项卡。
        3. 选择“高级”选项卡和“大小”选项卡。记下此选项卡中的值并将其添加到新介质代理网关。
    6. 单击**检查**。检查完毕后，“状态”显示为“正常”。
    7. 删除旧介质代理主机网关。选择该网关，然后单击“删除”。
    8. 单击**应用**保存更改。
3. 使用新添加的介质代理主机网关重试还原操作。

灾难恢复故障诊断（所有方法）

This feature is available in the Express and Premium Editions

执行灾难恢复时，可能会发生以下问题：

自动灾难恢复故障排除

AUTODR.log 文件

自动灾难恢复包括两种灾难恢复方法：EADR 和 OBDR。与这些方法相关的消息记录在 AUTODR.log 文件中，该文件位于默认的 Data Protector 临时文件目录中。如果发生错误，应该检查该文件。

AUTODR.log 记录了许多不同的消息，主要用于开发和支持。其中只有一部分与您相关并指示发生了错误。通常在日志文件的末尾记录这些错误消息，并在后面追加 traceback。

AUTODR.log 文件中有四个消息级别 (请注意，它们并非与 Data Protector GUI 中备份会话末尾报告的消息的相同报告级别相对应):

- Critical error ：错误很严重，以致于对象的备份无法继续并将中止。
- Error ：有错误，但是否为关键错误取决于不同因素。

  例如， AUTODR.log 报告一个错误: DR OS 中尚未包括某些驱动程序。缺少驱动程序可能是经过恢复的系统在恢复之后无法使用的原因。这种情况还可能会导致引导操作系统之后某些非关键服务不运行。错误的严重性取决于未备份哪个驱动程序。
- Warning 和 Info：这些不是错误消息，并且通常不表示有什么错误。

AUTODR.log 文件中所述的两个最常见的消息为:

- unsupported location：Data Protector 声明 %SystemRoot% 目录下没有 DR OS 中应包括的服务或驱动程序所需的某个文件。

  防病毒和远程控制软件 (例如 pcAnywhere) 通常使用此类驱动程序。此消息很重要，因为它可能表示服务/驱动程序需要缺少的文件，因此在引导之后无法正常运行。灾难恢复的成功取决于哪个服务或驱动程序受到了影响。对于此问题可能的解决方案是将缺少的文件复制到 %SystemRoot% 目录中，并在 Windows 注册表中更改其路径。请注意，错误地编辑 Windows 注册表可能对系统造成严重损坏。

调试灾难恢复会话

在灾难恢复会话期间，调试设置和调试日志位置取决于灾难恢复阶段：

- 在 DR OS 准备期间，调试日志会自动保存到 X:\DRM\log 或 /opt/omni/bin/drim/log/Phase1.log（Linux 系统）。
- 在数据还原步骤期间，必须在灾难恢复向导中手动选择调试选项以启用调试。

Windows

要创建调试日志：

1. 在灾难恢复向导中，按任意键在倒数期间停止向导。

   选中“调试”按钮左侧的复选框。

   在灾难恢复会话期间启用调试

2. 要指定调试选项（如保存调试的位置），请单击**调试...**。默认情况下，调试信息保存到 %SystemRoot%\system32\OB2DR\tmp 目录中。

   > **注意:**目录 %SystemRoot%\system32\OB2DR\tmp 驻留在 RAM 磁盘上。RAM 磁盘的大小通常限制为小于 64 MB。RAM 磁盘用量达到限制后，Data Protector 的行为可能会变得无法预测。因此，如果预计灾难恢复会话将产生大量调试，则必须更改调试将保存到的位置。

   此时将显示“调试选项”窗口。

   更改调试日志的位置

3. 输入保存调试日志的位置。驱动器的前面必须加上 \\? ，例如 \\?\Z:\debug.txt 。如果选择在网络共享上保存调试，则使用 net use 命令装载向其写入调试日志的共享。例如， net use X: "\\client\debug_output_folder /user:username password".

Linux 系统

要创建调试日志:

1. 在灾难恢复向导中，选择**使用调试**。
2. 在调试选项屏幕上，选择使用默认选项或选择对默认选项进行修改。

   Select one of following options:

   1) Use Default Debug Option "-debug 1-200 dr.txt"

   2) Specify Different Debug Option

   3) Disable Debug option

   Command [1-3]:

   > **注意**在 Linux 系统上，保存调试日志的目录位于 RAM 磁盘上。RAM 磁盘大小通常是有限的。RAM 磁盘用量达到限制后，Data Protector 的行为可能会变得无法预测。因此，如果预计灾难恢复会话将产生大量调试，则应当更改调试将保存到的位置。若要更改位置，请选择**指定其他调试选项**。

3. 将出现一个新屏幕，您可以在该屏幕上输入调试参数。

   Examples:

   -debug 1-200 debug.txt (local storage)

   -debug 1-200 //servername/sharename/debug.txt (windows share)

   -debug 1-200 servername:/sharename/debug.txt (nfs share)

   Specify the debug option string that you want to use:

   可以选择将调试文件保存到 Windows 共享磁盘或 NFS 共享文件夹。

在灾难恢复期间设置 omnirc 选项

如果需要在 Windows 或 Linux 系统中的灾难恢复期间设置 omnirc 选项，则执行以下步骤：

Windows 系统

1. 显示灾难恢复向导时，按任意键在倒数期间停止向导。
2. 单击 **Cmd** 启动命令提示符。
3. 运行以下命令：

   echo variable > %SystemRoot%\system32\OB2DR\omnirc

   其中，variable 是 omnirc 选项，与应在 omnirc 文件中写入的完全一样。

   例如：

   echo OB2RECONNECT_RETRY=1000 > %SystemRoot%\system32\OB2DR\omnirc

此命令在灾难恢复操作系统中创建一个将 OB2RECONNECT_RETRY 选项设置为 1000 秒的 omnirc 文件。

4. 关闭命令提示符，然后在灾难恢复向导中单击**下一步**以继续灾难恢复。

Linux 系统

1. 在灾难恢复向导中，通过按 **Alt F3**，切换到另一个控制台。
2. 在控制台中，运行以下命令：

   ```
   echo variable > /opt/omni/.omnirc
   ```

   其中， variable 是 omnirc 选项，与应在 .omnirc 文件中写入的完全一样。

   示例：

   ```
   echo OB2RECONNECT_RETRY=1000 > /opt/omni/.omnirc
   ```

   此命令在灾难恢复操作系统中创建一个将 OB2RECONNECT_RETRY 选项设置为 1000 秒的 .omnirc 文件。

3. 键入 **exit** 退出 shell，并在灾难恢复向导中继续进行灾难恢复。

Windows 上的 drm.cfg 文件

Data Protector 灾难恢复配置经过精心设置，以适用于大量系统配置。但是，在某些情况下，这些设置可能不是最合适的，或者可能要修改某些设置才能排除系统中的问题。

drm.cfg 文件包含可以修改并影响灾难恢复过程的几个参数，及其影响的说明。此文件对 EADR 和 OBDR 可用。

要更改参数：

1. 将模板文件 drm.cfg.tmpl 复制为 drm.cfg 。安装或升级期间将在 Data_Protector_home\bin\drim\config 中创建模板，并将所有参数设置为默认值。
2. 编辑 drm.cfg 文件。为参数设置所需的值。按照文件中的说明进行操作。

禁止自动收集 EADR 或 OBDR

运行客户机完整备份时，CONFIGURATION 备份可能会在收集某种备份方法所需的数据时失败，即使此方法不用于灾难恢复也是如此，因为 Data Protector 默认情况下收集所有自动灾难恢复方法的数据。例如，如果引导磁盘为 LDM 磁盘，则 Data Protector 收集 EADR 的数据时可能会发生这种情况。

禁用对灾难恢复方法数据已失败的自动收集。这样将允许 Data Protector 收集其他方法所需的数据。

将 OB2_TURNOFF_COLLECTING 选项设置为以下值之一：

值	描述
0	默认设置，打开对所有自动方法（EADR、OBDR）的数据收集。
1	关闭对 EADR/OBDR 数据的收集
2	仍收集 EADR/OBDR 数据。
3	关闭对所有方法的收集。

RHEL 8.x DR ISO image created for UEFI Secureboot ON or OFF does not boot

On RHEL 8.x with UEFI secure boot ON or OFF machines, the DR ISO image does not boot.

Cause

From RHEL 8.x onwards, the encryption keys used for system binaries (boot loaders) creation are different for different OS distribution versions. This causes the media host used for creating DR ISO imange to not boot on target UEFI+secureboot systems if the media OS distriburion version (8.x) host is different from DR client OS distribution version.

Solution

Ensure that both DA client OS distribution version and media creation host OS distribution version is the same.

Failed to create timezone change event source: Permission denied

RHEL 8.3 and above versions display the following error while the system is booting after a successful recovery of the system:

systemd[1]: Failed to create tomezone change event source: Permission denied

systemd[1]: Failed to allocate manager object: Permission denied

systemd[1]: Freezing execution.

[!!!!!!] Failed to allocate manager object, freezing.

Either this error message is displayed or the system hangs.

Cause

This error occurs because the re-labeling of file system objects is not happening during the recovered system boot in SELINUX enable mode (SELINUX=enforcing).

Solution

Boot the restored system in **SELINUX permissive mode.** Complete the following steps to make temporary changes to a kernel menu entry by changing the kernel parameters only during a single boot process:

1. Select the kernel that you want to start when the GRUB 2 boot menu appears and press the **e** key to edit the kernel parameters.
2. Find the kernel command line by moving the cursor down. The kernel command line starts with linux on 64-Bit IBM Power Series and x86-64 BIOS-based systems, or linuxefi on UEFI systems. Move the cursor to the end of the line.

> NOTE:
> Press **Ctrl+a** to jump to the start of the line and **Ctrl+e** to jump to the end of the line. On some systems, **Home** and **End** keys might also work.
> Edit the kernel parameters as required. For example, to run the system in SELINUX permissive mode, add the enforcing=0 parameter at the end of the linux16 line:
> linux16 /vmlinuz-3.10.0-0.rc4.59.el7.x86_64 root=/dev/mapper/rhel-root ro rd.md=0 rd.dm=0 rd.lvm.lv=rhel/swap crashkernel =auto rd.luks=0 vconsole.keymap=us rd.lvm.lv=rhel/root rhgb quiet enforcing=0

3. Press **Ctrl+x** to boot with the selected kernel and the modified command line parameters.

> IMPORTANT
> Press **Esc** key to leave command line editing and it will drop all the user made changes.

> NOTE
> This procedure applies only to single boot and does not persistently make changes.

By following these steps, the recovered system boots in **SELINUX permissive mode** and applies file objects labelling and then reboots itself to boot again in **SELINUX security enabled mode**.

Windows 主机灾难恢复因主机 Visual Studio 版本升级而失败

如果使用 Data Protector 2019.05 或更高版本对 DP 版本低于 2019.05 的 Windows 主机执行灾难恢复，则 ISO 映像创建失败。

原因

这是因为 Visual Studio 版本不一致。

解决方案

要成功创建 ISO，请使用与所考虑的 Windows 主机相同的 Data Protector 版本的介质创建主机。

Linux 主机灾难恢复因主机 GCC 版本升级而失败

如果使用 Data Protector 11.0 或更高版本对 DP 版本低于 11.0 的 Linux 主机执行灾难恢复，则恢复失败并显示以下错误:

GLIBCXX_3.4.*XX* not found
CXXABI_1.3.*X* not found

原因

这是因为 GCC 版本升级后出现 libstdc++.so.6 库依赖性问题。

解决方案

要执行 Linux 主机的灾难恢复，请执行以下操作:

1. 使用与所考虑的 Linux 主机相同的 Data Protector 版本的介质创建主机，创建用于灾难恢复的 ISO 映像。
2. 恢复灾难恢复主机
3. 将主机升级到 Data Protector 11.0 或更高版本。

由于签名验证问题，灾难恢复失败

Windows Server 2008 和 2008 R2 计算机的灾难恢复失败，并显示以下错误:

```
No valid DRIM P1S was found! Exiting
```

原因

这是由于 DLL 签名验证问题引起的。

解决方案

在执行 Windows Server 2008 或 Windows Server 2008 R2 计算机的灾难恢复之前，请在目标灾难恢复计算机上的 omnirc 文件中添加 ENV_SKIPSIGN_VERIFICATION omnirc 选项:

1. 将恢复 ISO 装载在目标计算机上以引导 Windows 计算机。
2. 选择恢复范围。
3. 单击“任务”，然后单击“运行命令提示符”。
4. 在计算机上的 omnirc 文件中添加以下变量。如果文件尚不存在，请在驱动器:\Windows\System32\OB2DR 的位置创建文件。
   ENV_SKIPSIGN_VERIFICATION=1 .
5. 从命令提示符退出。
6. 要修改恢复设置，请单击“设置”以打开“恢复设置”页面。
7. 单击“完成”启动恢复过程。

B2D 设备使用 EADR 脱机恢复对 Cell Manager 进行灾难恢复失败

当您选择从包含恢复数据的 DDBoost 设备或 StoreOnce Catalyst 执行脱机 Cell Manager 的灾难恢复并使用恢复 ISO 引导目标 VM 时，目标 VM 无法引导，并出现以下错误:

No supported local device found .

原因

由于无法连接到 Cell Manager 介质管理数据库和连接所需的访问凭据，因此目标 VM 无法连接到 B2D 设备。

解决方案

要执行灾难恢复，请通过在目标 VM 上使用以下 omnirc 变量创建 omnirc 文件，提供 B2D 系统的所需访问凭据。

- OB2_DR_B2D_CLIENTID = *<B2D 系统的用户名>*
- OB2_DR_B2D_PASSWORD = *<B2D 系统的密码>*

注意**:** 对于 StoreOnce Catalyst，如果在备份数据所驻留的 StoreOnce Catalyst 存储上启用了公共访问权限，则无需提供访问凭据。

要在 Windows VM 上使用变量创建 omnirc 文件并执行灾难恢复，请执行以下操作:

1. 将恢复 ISO 装载在目标 VM 上以引导 VM。
2. 选择恢复范围。
3. 单击“任务”，然后单击“运行命令提示符”。
4. 在 *drive*:\Windows\System32\OB2DR 位置中创建一个 omnirc 文件，并在文件中添加以下变量:
   - OB2_DR_B2D_CLIENTID = *<B2D 系统的用户名>*
   - OB2_DR_B2D_PASSWORD = *<B2D 系统的密码>*
5. 从命令提示符退出。
6. (可选) 要修改恢复设置，请单击“设置” 以打开“恢复设置”页面。
7. 单击“完成” 启动恢复过程。

要在 Linux VM 上使用变量创建 omnirc 文件并执行灾难恢复，请执行以下操作:

1. 在目标 VM 上装载恢复 ISO 以启动 VM
2. 选择“运行 Shell” 并按 Enter。
3. 在 opt/omni/ 目录中创建一个 omnirc 文件，并在该文件中添加以下变量:
   - OB2_DR_B2D_CLIENTID = *<B2D 系统的用户名>*
   - OB2_DR_B2D_PASSWORD = *<B2D 系统的密码>*
4. 选择恢复范围，然后按 Enter 键启动灾难恢复向导。
5. 按照系统提示完成灾难恢复。

无法从介质副本或对象副本执行灾难恢复

无法从介质副本或对象副本执行灾难恢复。

原因

默认情况下，Data Protector 使用原始介质集执行灾难恢复。因此，灾难恢复向导中不显示副本对象版本。

解决方案

- 对象副本：从 IDB 导出原始介质集中的所有介质，然后重新生成 SRD 文件。然后，Data Protector 在灾难恢复向导中向您提供原始介质集的第一个可用复本。
- 介质副本：在 SRD 文件中，使用介质副本的介质 ID 替换原始介质的介质 ID。Data Protector 之后将在灾难恢复向导中提供原始介质集的第一个可用复本。

无法在灾难恢复完成后登录

灾难恢复结束之后登录系统时出现问题。

可能会收到以下消息：

The system cannot log you on to this domain, because the system’s computer account in its primary domain is missing or the password on that account is incorrect.

原因

此类消息可能由以下某个原因导致：

- 收集灾难恢复的所有信息之后，重新安装了 Windows，并将其添加到问题域中。
- 收集灾难恢复的所有信息之后，从冲突域删除了系统，随后将其添加到同一域或其他某个域中。

在类似这种情况下，Windows 将生成新的系统安全信息，这些信息与灾难恢复期间还原的信息不兼容。

解决方案

1. 以管理员身份从本地登录系统。
2. 在控制面板中，单击**网络**，然后使用**标识**选项卡从系统的当前域将系统移至一个临时工作组。
3. 将系统重新插入以前从中移出该系统的域中。需要域管理员密码。单击**确定**。
4. 重新启动系统。

要更新此新状态，请重复灾难恢复的所有必要的准备步骤。

由于网络设置不当，灾难恢复失败

由于 Data Protector 恢复一个具有不当网络配置的客户机，导致灾难恢复会话失败。

原因

用于配置客户机网络的默认设置取决于客户机的操作系统：

Windows Server 2008 及更高版本:

由 DHCP 设置定义的网络配置。

解决方案

要切换到非默认的网络配置：

1. 启动灾难恢复会话。
2. 当 Data Protector 显示：

   Windows Server 2008 及更高版本:

   在下面的 10 秒钟内按 F8 切换到备份时的网络设置...

   按 **F8**。

对 BTRFS 型文件系统的支持有限

对 BTRFS 型文件系统的支持有限。

原因

如果装载的 btrfs 子卷具有子子卷，则备份期间将跳过子子卷中的数据。子子卷将作为空文件夹来备份。

解决方案

1. 将每个子卷装载为新的装载点。
2. 在备份规范中配置新的装载点。

灾难恢复期间显示错误消息

在灾难恢复期间，显示以下错误消息：
Failed to perform post-DR operations

解决方案

要完成灾难恢复进程，请手动运行 omnicc 命令。

- 对于联机恢复: 在 Cell Manager 上运行以下命令:

  omnicc -secure_comm –configure_peer <hostname_of_client_being_recovered> - overwrite

- 对于脱机恢复: 在介质代理上运行以下命令:

  omnicc -secure_comm -remove_peer <hostname_of_client_being_recovered>

无法复制文件

Drstart 报告： Can not copy filename

报告此错误是因为 *drstart* 实用程序无法复制指定的文件。

原因

其中一个原因可能是系统锁定了该文件。例如，如果 *drstart* 无法复制 *omniinet.exe*，则可能是因为已在运行 Inet 服务。这不是正常情况，并且不应在全新安装之后发生。

解决方案

此时将显示一个对话框，询问您是否要继续复制其余文件。如果单击“是”，则 drstart 将跳过锁定的文件，继续复制其他文件。如果系统锁定了文件，则这样做即可解决问题，由于灾难恢复所需的进程已在运行，因此不需要复制该文件。

还可以通过单击“中止”关闭 drstart 实用程序。

未能收集自动 DR 信息

使用 EADR 或 OBDR 时，可能会收到以下错误: “ Automatic DR information could not be collected. Aborting the collecting of system recovery data .”

原因

可能导致此错误的原因存储在位于默认 Data Protector 临时文件目录的 autodr.log 文件中。

解决方案

1. 检查是否正确配置了所有存储设备。如果设备管理器将设备报告为“未知设备”，则必须安装正确的设备驱动程序，然后才能执行 EADR/OBDR。如果有配置错误的存储设备连接到系统，则 autodr.log 中会显示类似条目:

   DRIM_WIN_ERROR 13 SetupDiGetDeviceRegistryProperty

2. 必须有足够的注册表空间可用。建议将最大注册表大小至少设置为当前注册表大小的两倍。如果没有足够的注册表空间可用，则 autodr.log 中会显示类似条目:

   ERROR registry 'Exception while saving registry' .... WindowsError: [Errno 1450] Insufficient system resources exist to complete the requested service.

3. 确保已启用自动装载功能。自动装载功能可确保所有卷（没有装载点）都处于联机状态。如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

   如果需要禁用自动装载功能，则确保已装载系统保留分区。

如果仍然存在问题，请卸载 Data Protector 自动灾难恢复组件 (以便至少可以进行手动灾难恢复)，然后与技术支持人员联系。

检测到某些非关键错误

使用 EADR 或 OBDR 时，可能会收到以下错误: “Some non-critical errors were detected during the collecting of Automatic DR data. Review the Automatic DR log file.

原因

执行自动灾难恢复模块期间检测到非关键错误意味着备份很可能仍用于灾难恢复目的。可能导致非严重错误的原因存储在位于默认 Data Protector 临时文件目录的 autodr.log 中。例如：

%SystemRoot% 文件夹以外的服务或驱动程序 (例如病毒扫描程序)。 Autodr.log 会包含类似的错误消息：

ERROR safeboot 'unsupported location' 'intercheck support 06' 2 u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.

解决方案

可以忽略此错误消息，因为它不影响灾难恢复的成功。

失去与主机上名为 “DeviceName” 的 B2D 网关的连接

从带有计划网关的 StoreOnce/DD Boost 设备配置设备，并且配置同一客户端用于灾难恢复时，还原会话将会结束，并在 Cell Manager 上显示以下警告消息：

[Major] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM

[61:3003] Lost connection to B2D gateway named "DeviceName" on host <hostname>

Ipc subsystem reports: "unknown"

[Warning] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM

Device <DeviceName> is disabled and will not be used.

原因

此错误是由于丢失与客户机 B2D 网关的连接而发生的。

解决方案

忽略还原会话结束时显示的警告消息。增强自动灾难恢复将会成功，您可以在客户机恢复控制台上查看结果。

还原期间网络不可用

还原期间网络不可用。

原因

有多种原因可以导致此问题，例如网络电缆或开关损坏。网络故障另一个可能的原因是 DNS 服务器（备份时配置）在还原期间脱机。由于 DR OS 的配置与备份同时进行，因此网络将不可用。

解决方案

请确保不是开关、电缆等问题。

如果 DNS 服务器（备份时配置）在还原期间脱机，则可以：

- 执行脱机恢复，并且在恢复之后更改 DNS 设置。
- 开始阶段 2 之前编辑注册表。在这种情况下，必须在阶段 2 之前重新启动系统，更改才能生效。阶段 2 结束之后，必须更正设置，然后才能开始阶段 3。

> 错误地编辑注册表可能会导致灾难恢复失败。

RMA 在 clientsystem.domain.org 上意外关闭

将 D2D 设备用于 EADR 联机还原时，RMA 失败并显示以下错误消息：

[61:1005] Got unexpected close from RMA on clientsystem.domain.org if the gateway is configured on the same EADR system

原因

网关是在同一 EADR 系统上配置的。

解决方案

删除分配给正在恢复的 DR 系统的网关并添加一个新网关。

在 G9 刀片服务器上启动 ISO 映像失败

启动 ISO 映像失败，特定 G9 刀片服务器上显示空白屏幕。

解决方案

执行以下步骤：

1. 从 http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056892 下载 Microsoft Windows 2016 知识库 (KB) 文章
   a. 选择 Microsoft Windows 2016 的“下载”选项。将文件保存到 C:\MiniOS 文件夹。如果该文件夹不可用，则创建新文件夹。
   b. 将下载的文件重命名为 WinUpdate.msu (.msu 为文件类型。不要将其包含到文件名中)。
2. 从以下链接下载工具以创建 ISO 映像:
   http://www.sevenforums.com/attachments/general-discussion/32382d1256189124-make-bootable-iso-student-d-l-oscdimg.zip
3. 提取文件并将其保存到 C:\ 下。
4. 在命令提示符下，运行以下命令:

   a. mkdir C:\MiniOS\offline b. dism /mount-wim /wimfile:C:\minios\sources\boot.wim /index:1/mountdir:C:\minios\offline c. dism /image:C:\minios\offline /add-package /packagepath:C:\winupdate.msu d. dism /unmount-image /mountdir:C:\minios\offline /commit e. C:\Oscdimg.exe -bootdata:2#p0,e,bC:\minios\Etfsboot.com#pEF,e,bC:\minios\Efisys.bin -u1 -udfver102 C:\minios C:\newMiniOs.iso

上述步骤为通用步骤，如果在其他服务器上启动 ISO 映像失败，也可以按以上步骤进行操作。

从 9.x 或更早版本升级到 10.x 失败

从 9.x 或更早发布升级到 10.x 失败。

原因

无法使用 9.x 或更早版本生成的备份创建 ISO 映像。

解决方案

升级并创建 ISO 映像后，对同一备份规范运行增量备份。

恢复后启动服务器失败

如果是不同的硬件，恢复后启动服务器失败。

解决方案

选择“手动初始化磁盘”，然后在“恢复设置”下选择“保存”以恢复到灾难恢复模块中的不同硬件。

网络不可用

在 Windows Server 2008 系统上，在灾难恢复期间网络不可用。

原因

这是因为 DR OS 不支持网卡。

解决方案

将缺少的驱动程序插入到 DR OS 映像中。

EADR 和 OBDR 联机恢复失败

当 Cell Manager 和客户机位于不同的域时，EADR 和 OBDR 联机恢复失败。

原因

这可能是由于错误的网络配置导致。

解决方案

1. 在 Cell Manager 和客户机系统上更新 host 文件。这些文件必须包含 Cell Manager 和客户机的主机名及其 IP 地址。
2. 检查 Cell Manager 和客户机之间的 ping 请求是否返回正确的值。如果发生问题，请联系您的网络管理员。
3. 使用 omnicheck -dns 命令检查 Cell Manager 和客户机之间的 DNS 解析是否正确。如果发生问题，请联系您的网络管理员。

自动登录不起作用

解决方案

使用密码为空的管理员帐户手动登录。

计算机停止响应

在 EADR 期间，计算机停止响应。

原因

灾难恢复 CD 有问题可能会导致这种情况。

解决方案

- 检查 CD 是否可读。
- 请勿重复使用 CD-RW 过多次数。

无法创建 CD ISO 映像

无法为 Microsoft 群集服务器的 EADR 创建 CD ISO 映像。

原因

必须备份仲裁磁盘，以便能够创建 CD ISO 映像。

解决方案

备份仲裁磁盘。

在 Microsoft 群集服务器客户机上创建 CD ISO 映像的操作失败

在 Microsoft 群集服务器环境中，不能在群集客户机上创建 ISO 映像。文件系统还原将按预期执行。

原因

出现问题的原因是 Data Protector 尝试使用群集 IP 地址（是虚拟地址）而不是域名（解析为物理客户机的 IP 地址）。

解决方案

更改网络服务的连接顺序，使得 Local Area Connection位于顶部。

ISO 映像创建失败

ISO 映像创建失败并显示以下错误消息:

在 GUI 中：

ISO 映像创建失败。请检查位于 Data Protector 临时目录中的 autodr 日志。

在 autodr.log 文件中:

“添加包 (Add-Package)”操作失败并显示“访问被拒绝 (Access Denied) (5)”错误。

原因

ISO 映像是使用 WAIK/ADK 创建的，且在介质创建主机上安装了防病毒软件。

解决方案

临时禁用介质创建主机上的防病毒代理，直至完成 ISO 映像创建过程。

阶段 1 期间不重新装载卷

在某些系统中（取决于磁盘控制器及其配置），灾难恢复的阶段 1 期间无法正确重新装载与不同卷上的装载点关联的卷（未分配驱动器号）。

原因

如果重新创建或重新格式化包含装载点的卷（例如含有 DR OS 的系统卷），导致操作系统以“安全模式”引导，以及检测不到原始装载点的目标卷上存在的文件系统。因此，灾难恢复模块无法识别此卷，并且在 drecovery.ini 文件中将其报告为 MISSING。此类卷的内容保留原样，即使无法识别该卷也是如此。

解决方案

- 装载含有驱动器号的卷，并用 chkdsk /v /f 命令验证该卷，或等待至系统完全还原为止，然后重新创建原始装载点。
- 手动将系统直接重新启动至 MiniOS（不从恢复 CD 启动）。以前卸载的卷将自动装载到驱动器号。

灾难恢复失败或中止后，引导描述符会留在 EFI 环境中

在 Intel Itanium 系统上，灾难恢复会话失败或中止后，在重新启动灾难恢复过程时会出现不需要的行为。

原因

引导描述符 (名为 DRM Temporary OS) 可能留在了 EFI 环境中。

解决方案

从范围选择菜单中使用**删除引导描述符**选项删除引导描述符。删除引导描述符之后，可以通过选择范围继续灾难恢复。

在 Intel Itanium 系统中选择了错误或非引导的磁盘

在 Intel Itanium 系统中，选择了错误的引导磁盘（或根本就是非引导磁盘）。

解决方案

1. 从范围选择菜单中选择**手动选择磁盘**。此时将显示一个新菜单，其中列出所有可用的磁盘。
2. 确定正确的引导磁盘。按 **o** 查看有关原始磁盘的信息，按 **d** 查看有关所选磁盘的详细信息。
3. 使用光标键从列表中选择磁盘，然后按 **b**。通过按 **c**，可以删除某个选择。

   如果引导磁盘与系统磁盘不同（默认情况下这两个磁盘相同），则还必须选择系统磁盘。

   选择**返回**。
4. 选择恢复的范围，然后将继续灾难恢复。

灾难恢复失败，并显示“空间不足”消息

对 Windows Server 2008 R2 域控制器执行的灾难恢复失败，并显示类似如下所示的错误消息：

[Major] From: VRDA@computer.company.com "Dev1" [/CONFIGURATION]" Time:

07.12.2012 15:33:58 X:\windows\System32\OB2DR\tmp\config\

ActiveDirectoryService\D$\ Windows\NTDS\ntds.dit Cannot write:

([112] There is not enough space on the disk.) => not restored.

原因

磁盘上没有足够的空间。

解决方案

1. 修改客户机备份的备份规范: 在源页面中，展开 CONFIGURATION 对象，并清除 ActiveDirectoryService 和 SYSVOL 项目的复选框。

   > 注意Active Directory 和 SYSVOL 将仍作为系统卷（C:/）备份的一部分进行备份。默认情况下，它们分别位于 C:/Windows/NTDS 和 C:/Windows/SYSVOL 中。

2. 重复灾难恢复过程。

恢复映像创建失败，报告 Windows 群集中缺少卷

在某些情况下，DR 恢复映像创建向导会失败。

原因

这是由于系统上不存在卷。磁盘见证仲裁配置可验证群集数据库没有损坏 (仲裁磁盘上存在群集文件夹)，并且事件日志与仲裁有关。

解决方案

要解决此问题，请重新创建仲裁并再次执行配置备份。

在客户机备份期间显示小错误或警告消息

在客户机备份期间，可能报告以下小错误：

Cannot perform stat(): ([2] No such file or directory)

File is shorter than it was when it was opened

原因

这类警告和错误消息可能由于临时 Data Protector 目录中被修改的文件而导致。例如，如果同时备份 /CONFIGURATION 装载点和 / (根) 装载点，就可能发生该情况。

解决方案

从备份规范中排除 /opt/omni/bin/drim/tmp 和 /opt/omni/bin/drim/log 目录。

在使用 8.10 或更高版本创建的备份规范中，系统将自动排除这些文件。

Cell Manager 和 RMA 主机不响应

在 RHEL 操作系统中对 Linux 虚拟机执行灾难恢复失败，并显示以下错误消息：

Cell Manager is not responding. Attempting offline restore.

RMA host is not responding.

原因

出现此类错误的原因可能是因为用于灾难恢复的虚拟机的 NIC 和 MAC 地址将与原始虚拟机的不同。该虚拟机将没有 IP 地址，并且联机恢复失败。

解决方案

执行以下步骤：

- 按 **Alt+F2** 打开另一个命令 shell。
- 导航到 /etc/sysconfig/network 。
- 修改接口文件以匹配当前接口和 MAC 地址。
- 重新启动网络服务。
- 如果需要，编辑用于网络连接的主机文件。
- 确保客户机可连接到 Cell Manager 和介质（备份）主机。
- 按 **Alt+F1** 返回到主命令 shell 窗口，然后选择恢复选项。

由于“未找到受支持的本地设备”错误，还原会话失败

还原会话失败后尝试执行 EADR 时，还原再次失败并显示错误“未找到受支持的本地设备”。

解决方案

要解决此问题，请配置介质主机异常并再次尝试还原。

EADR 脱机还原失败

使用 D2D 设备时，EADR 脱机还原失败。

原因

如果您正在使用已配置用户名和密码的磁盘到磁盘设备，则脱机 EADR 将会失败。

解决方案

临时删除用户名和密码以执行还原。

带有已分离 SAN-LVM 卷的 RHEL EADR 不起作用

在引导期间会显示以下错误消息:

尝试打开 <volume_name> 时，super-block 中的幻数不正确

原因

在 Linux 系统上，在 EADR 恢复之后，如果您使用的是**默认恢复**或**最小恢复**方法，则可能无法启动已恢复系统。

解决方案

EADR 恢复后，在启动恢复的系统之前，您应该输入 OS maintenance、root password、mount -o remount、rw / (在读/写模式下重新装载 "/" 装载点)，并编辑 /etc/fstab。

如果选择默认恢复选项，则您必须添加注释，或从 fstab 中删除所有装载点，/boot、/、/opt、/etc 和 /var 除外。

如果选择最小恢复选项，则必须添加注释，或从 fstab 中删除所有装载点，/boot、/ 除外。

对 DDBoost 执行 EADR 脱机还原失败

使用 DDBoost 设备进行灾难恢复 (EADR) 时，脱机还原失败。

解决方案

要解决此问题，用户必须执行联机还原。

依赖于 IIS 的服务不自动启动

恢复 IIS 之后任何依赖于 IIS 的服务（例如 SMTP、NNTP）都不自动启动。

解决方案

1. 手动启动这些服务。
2. 如果此操作失败，则停止 IIS 管理服务，并使用“覆盖”选项还原 %SystemRoot%\system32\inetsrv\MetaBase.bin 文件。

> **注意** %SystemRoot%\system32\inetsrv 目录是 IIS 服务的默认位置。如果已将服务安装到另一个位置，则使用此位置作为还原 MetaBase.bin 文件的目标。

3. 启动 IIS 管理服务和所有相关服务。

无法验证恢复集的完整性。将不会创建 ISO 映像

尝试创建恢复 ISO 映像时发生以下错误:

```
Failed to verify the recovery set integrity. ISO image will not be created
```

原因

如果使用 9.x 备份数据在 10.x 环境中创建 ISO 映像，则 ISO 映像创建将失败。

解决方案

如果您遵循以下任一升级路径:

- 从 Data Protector 9.x 到任何 Data Protector 10.x 版本
- 从 Data Protector 10.00 到 Data Protector 10.40 或更高版本

并且想要使用旧版 Data Protector 的备份来执行灾难恢复，那么您可以使用以下选项之一来计划 ISO 创建:

- 在灾难恢复备份之后立即创建 ISO 映像，然后执行升级
- 使用执行备份的旧 Data Protector 版本的介质创建主机，在升级版本中创建 ISO 映像。

如果要从 Data Protector 10.40 升级到任何更高版本，则不需要为进行灾难恢复的 ISO 创建进行特殊计划。

调度程序故障排除

This feature is available in the Express and Premium Editions

本节列出了调度程序 UI 和仪表板中的已知问题和变通方法。

图标和按钮不可见

在不同的“主页上下文”网页 (如仪表板、遥测和调度程序) 中，图标和网页按钮不可见。

原因

如果启用了 Internet Explorer 增强安全配置 (IE ESC)，则会发生此问题。

解决方案

如果启用了 Internet Explorer 增强安全配置 (IE ESC)，则会出现此问题。

要禁用 IE ESC 设置，请完成以下步骤:

1. 关闭所有 Microsoft Internet Explorer 实例。
2. 导航到 Windows“开始”菜单，指向“管理工具”，然后单击“服务器管理器”。
3. 在“安全信息”下，单击“配置 IE ECS”。
4. 在“管理员”下，单击“关闭”。
5. 在“用户”下，单击“关闭”。
6. 单击“确定”。

调度程序作业未被触发

调度程序作业停止响应。

原因

此问题的原因未知。

解决方案

要解决此问题，请使用以下步骤重新部署 jce-dispatcherwar 文件:

1. 启动 WildFly 管理控制台: 打开 Web 浏览器，并导航至 http://localhost:9990/console/App#home。
2. 使用 WildFly 管理用户凭据登录。
3. 单击“部署”选项卡。
4. 重新部署 jce-dispatcher.war 文件: 重新部署是一个两步过程，即先禁用再启用 war 文件。
    1. 禁用 war 文件: 在左侧窗格中，选择 jce-dispatcher.war 文件，然后选择“禁用”选项。
    2. 启用 war 文件: 在左侧窗格中，搜索 jce-dispatcher.war 文件并选择“启用”选项。**注意:** 重新部署 war 文件后，将清除先前的作业队列，并且仅运行下一批计划作业。

网络和通信

This feature is available in the Express and Premium Editions

TCP/IP 配置过程的一个重要方面是设置主机名解析机制。

要使通信成功，主机 A 需要通过完全限定域名 (FQDN) 解析主机 B。解析主机意味着主机 A 可以解释主机 B 的 FQDN，并确定其 IP 地址。

必须满足以下条件才能提供主机名解析：

- 每个客户机必须能够解析具有介质代理的 Cell Manager 和客户机的地址。
- Cell Manager 必须能够解析单元中所有客户机的名称。
- MoM 服务器（如果使用）还必须能够解析 MoM 环境中所有 Cell Manager 的名称。

检查 TCP/IP 设置

安装 TCP/IP 协议后，可以使用 ping 和 ipconfig (Windows 系统) 或 ifconfig (UNIX 系统) 实用程序验证 TCP/IP 配置。

请注意，在某些系统上，不能对 IPv6 地址使用 ping 命令，而应使用 ping6 命令。

测试 DNS 解析

通过运行以下命令可以测试主机之间的 DNS 解析：

```
omnicheck -dns
```

这将检查常规 Data Protector 操作所需的所有 DNS 连接。

有关命令的详细信息，请参阅 omnicheck 手册页或《Data Protector 命令行界面参考》。

网络和通信故障诊断包括以下情形:

- 连接的系统本身显示为客户机 X
- 客户机 A 未能连接到客户机 B
- 无法连接到客户机 X
- 单元中的时间设置
- 系统恢复后 IDB 不可访问
- Data Protector 会话实际上未运行，但仍标记为“进行中”
- hpdp-idb 服务无法启动
- TSA 登录被拒绝
- 客户机失败并显示“连接被对等端重置”
- 客户机失败并显示“客户机不是任何单元的成员”
- inet.log 文件包含过量日志记录

连接的系统本身显示为客户机 X

执行 omnicheck 命令后，显示以下消息:

client_1 connects to client_2, but connected system presents itself as client_3

原因

client_1 上的 hosts 文件配置不正确，或者 client_2 的主机名与其 DNS 名称不匹配。

解决方案

请咨询网络管理员。根据环境中配置的名称解析方式，必须在 DNS 配置中，或者在受影响客户机以下位置的 hosts 文件中解决该问题:

Windows 系统： %SystemRoot%\system32\drivers\etc

UNIX 系统： /etc

客户机 A 未能连接到客户机 B

执行 omnicheck 命令后，将显示以下消息:

client_1 failed to connect to client_2

原因

client_1 上的 hosts 文件配置不正确，或者 client_2 不可访问。

解决方案

要解决此问题，请确保满足以下条件:

- client_1 上的 hosts 文件已正确配置。
- client_2 已启动并运行。

无法连接到客户机 X

对 omnicheck 命令的响应是:

client_1 cannot connect to client_2

原因

这意味着已发送数据包，但由于超时而未收到。

解决方案

检查并解决远程主机上的网络问题。

由于单元中时间设置不同而导致的错误

通信错误，备份搜索失败或还原失败。

原因

Data Protector 将时间戳大量用于各个单元组件（Cell Manager、客户机）之间的通信。如果 Cell Manager 和客户机上的系统时钟显著不同，例如相差数周甚至数月（举例来说，如果您出于测试目的对设置进行了更改，但系统时钟未在还原虚拟机后更新等），可能会出现意外结果，包括通信错误、搜索或还原备份失败等等。

解决方案

检查系统时间设置并确保系统时钟不存在显著不同。

请记住，如果客户机上的时钟与 Cell Manager 上的时钟不同步，则证书可能变得无效，从而导致身份验证失败。例如，当 Cell Manager 上的时钟比客户机上的时钟快时，在安装期间创建的证书对尝试连接它的客户机无效。

系统恢复后 IDB 不可访问

在像断电、严重的操作系统故障或硬件故障等这样的意外事件过后，数据库能够恢复到一致状态。但是，在系统恢复后第一次访问数据库可能会失败并显示一个内部错误。这是一个仅会发生一次的临时性错误。

原因

此问题的原因未知。

解决方案

重新访问数据库。

Data Protector 会话未运行，但仍标记为“正在进行中”

在 Data Protector GUI 的“内部数据库” 上下文中，一个或多个 Data Protector 会话未运行，但会话状态仍标记为 “正在进行中”。

原因

此问题的原因未知。

解决方案

完成以下步骤：

1. 关闭 Data Protector GUI。
2. 执行 omnidbutil -clear 命令，将未运行但标记为“正在进行中” 的所有会话的状态设置为 “失败”。
3. 重新启动 Data Protector GUI。

hpdp-idb 服务无法启动

hpdp-idb-cp 服务不启动。

解决方案

完成以下步骤：

1. 停止 Data Protector 服务。
2. 删除以下文件：

   Windows 系统： Data_Protector_program_data\log\hpdp-idb-cp.pid

   UNIX 系统： /var/opt/omni/log/hpdp-idb-cp.pid
3. 重新启动 Data Protector 服务。

TSA 登录被拒绝

对 Novell Open Enterprise Server 运行还原操作时，DP UI 上将显示以下消息:

From: VRDA@computer.company.com

"/media/nss/NSS_VOLUME_5"

TSA: Cannot connect to Target Service (login denied).

原因

如果 HPLOGIN 实用程序包含不正确的用户凭据，则会发生此问题。

解决方案

使用正确的用户凭据运行 HPLOGIN 实用程序。 HPLOGIN 实用程序位于此处:
/usr/omni/bin/hplogin

客户机失败并显示“连接被对等端重置”

在 Windows 系统上，TCP/IP 协议的默认配置参数可能导致连接性问题。报告了以下错误：

[10054] Connection reset by peer.

原因

网络或计算机的高使用率、网络不可靠，尤其是连接到不同操作系统时可能会发生此问题。

解决方案

可以配置 TCP/IP 协议，以使用 8 个而不是默认的 5 个重新传输数。最好不要使用较高的值，因为每个增量都会使超时加倍。该设置适用于所有网络连接，而非仅适用于 Data Protector 所采用的连接。

如果 Cell Manager 正在 Windows 系统上运行，则首先在单元管理器系统上应用更改。如果问题仍然存在，或者 Cell Manager 正在 UNIX 系统上运行，则将更改应用到有问题的 Windows 客户机。

1. 在以下注册表项下添加 DWORD 参数 TcpMaxDataRetransmissions ，并将其值设置为 0x00000008(8)：

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\Tcpip\Parameters

2. 重新启动系统。

> ⚠ **警告**编辑注册表发生错误可能导致系统不稳定甚至不可用。

客户机操作失败并显示消息“客户机不是任何单元的成员”

在客户机上执行 Data Protector (DP) 操作时，该操作失败，并显示以下错误消息:

The Client is not a member of any cell.

原因

如果客户机系统未在 Data Protector 中配置为客户机，则会发生此问题。

解决方案

如果客户机在 Data Protector GUI 的“客户机”上下文中列出，请执行以下步骤，然后在客户机上重试 DP 操作:

1. 在“客户机”上下文中，展开“客户机”，右键单击该客户机，并单击“删除”。这时将出现一个对话框，询问您是否要从客户机卸载 Data Protector。
2. 单击**否**。
3. 右键单击**客户机**，并单击**导入客户机**。
4. 在“名称”字段中，指定客户机的主机名或 IP 地址，然后单击“完成”。

如果客户机未在“客户机” 上下文中列出，请按照以下步骤在客户机上重试 DP 操作:

1. 在“客户机”上下文中，右键单击“客户机”，并单击“导入客户机”。
2. 在“名称”字段中，指定客户机的主机名或 IP 地址，然后单击“完成”。

inet.log 文件包含过量日志记录

如果客户机不受保护且 Serviceguard 环境中配有 Cell Manager，或者 Cell Manager 有多个名称或 IP 地址，则 inet.log 文件可能包含许多以下类型的条目:

A request 3 (vbda.exe) came from host computer.company.com which is not a cell manager of this client.

原因

发生这种情况的原因是不受保护的客户机仅识别 Cell Manager 的主要主机名。允许来自任何其他客户机的请求，但这些请求将被记录到 inet.log 文件中。

解决方案

保护客户机。 allow_hosts 文件中所列客户机的请求不会被记录到 inet.log 中。来自其他客户机的请求将被拒绝。

如果出于某种原因，此方法在您的环境中不可能，则可以保护客户机并为要允许访问的系统指定 * 作为 IP 地址范围。这就意味着您的客户机将接受来自所有系统（任何 IP 地址）的请求而实际上没有受到保护，但是仍然解决了过量日志记录的问题。

重要说明Cell Manager 节点的所有可能主机名都应列在每个受保护的客户机上的 allow_hosts 文件中。这样即使在发生故障转移时也可访问客户机。如果意外锁定了某个客户机，则可以在该客户机上手动编辑 allow_hosts 文件。

服务和后台程序

This feature is available in the Express and Premium Editions

Data Protector 进程

简介

Data Protector 服务（Windows 系统）和后台程序（Linux 系统）在 Cell Manager 上运行。运行 omnisv -status 命令以检查服务/后台程序是否正在运行。

如果 Data Protector 服务/后台程序看似乎已停止或者尚未在目标 Data Protector 客户机上安装，请确保无名称解析问题。

Data Protector 进程列表

下表显示了 Data Protector 在空闲状态下或者执行一些基本操作（例如备份、还原或介质管理会话）时所运行的进程。

		始终	备份	还原	介质管理
Cell Manager	**Windows**	omniinet.exe mmd.exe crs.exe kms.exe hpdp-idb hpdp-idb-cp hpdp-as	bsm.exe	rsm.exe	msm.exe
	UNIX	mmd crs kms hpdp-idb (postgres) hpdp-idb-cp (pgbouncer) hpdp-as (standalone.sh)	bsm	rsm	msm
磁带客户机客户	**Windows**	omniinet.exe	vbda.exe	vrda.exe	
	UNIX		vbda	vrda	
介质代理客户机	**Windows**	omniinet.exe	bma.exe	rma.exe	mma.exe
	UNIX		bma	rma	mma

Data Protector 服务和后台程序的故障诊断包括以下部分：

- 在 Windows 上启动 Data Protector 服务时出现的问题
- 在 UNIX 上启动 Data Protector 后台程序时出现的问题

- Data Protector 进程的其他问题

在 Windows 上启动 Data Protector 服务时出现的问题

本节包含以下故障排除主题:

您没有启动服务的权限

当您尝试启动服务时，会显示以下错误消息:

Could not start the ServiceName on SystemName.

Access is denied.

原因

如果您的用户帐户没有所需的权限，则会发生此问题。

解决方案

请求系统管理员授予您在系统上启动、停止和修改服务的权限。

Inet 服务无法启动

当您尝试启动 Inet 服务时，显示以下错误:

The Data Protector Inet service failed to start due to the following error:

The service did not start due to a logon failure.

原因

如果服务帐户没有启动 Inet 服务的权限，或者服务帐户属性 (例如密码) 已更改，则会发生此问题。

解决方案

在 Windows“控制面板”>“管理工具”>“服务”中修改服务参数。

如果问题仍存在，请与系统管理员联系以设置具有适当权限的帐户。帐户应为 Admin 组的成员，且应具备 Log on as a service 用户权限。

系统找不到指定的文件

当您尝试启动服务时，会显示以下错误消息:

Could not start the ServiceName on SystemName. The system can not find the file specified!

原因

服务的位置在 ImagePath 注册表项中注册。如果此注册表项下指定的位置中不存在可执行文件，则会显示上面的消息。

解决方案

在 Cell Manager 上重新安装 Data Protector，保留 IDB。

MMD 无法启动 CRS 服务

当您尝试启动 Data Protector CRS 服务时，它无法启动。它还会导致 MMD 服务失败并调用 Dr Watson 诊断工具。

原因

如果数据库日志文件已损坏，则会发生此问题。

解决方案

1. 从默认的 mmd.ctx 内部数据库目录中删除 Data Protector 文件。
2. 使用 omnisv -stop 和 omnisv -start 命令重新启动服务。

在 Linux 上启动 Data Protector 后台程序时出现的问题

以下后台程序运行在 Linux Cell Manager 上：

- 在目录 /opt/omni/lbin 中:
  - Data Protector CRS 后台程序： crs
  - Data ProtectorIDB 后台程序： hpdp-idb (postgres)、 hpdp-idb-cp (pgbouncer)、 hpdp-as (standalone.sh)
  - Data Protector 介质管理后台程序： mmd

通常，在系统启动期间会自动启动这些后台程序。

应用程序尝试连接到 Data Protector 端口 (默认为 5565) 时，Data Protector Inet 进程 (/opt/omni/lbin/inet) 由系统 inet 后台程序启动。

要手动停止、启动或检查 Data Protector 后台程序的状态，请以 Cell Manager 用户身份登录到 root，并从 /opt/omni/sbin 目录运行:

- omnisv -stop
- omnisv -start
- omnisv -status

本节包含以下故障排除主题:

无法启动 Cell Manager 后台程序

执行 omnisv -start 命令后，将显示以下消息:

Could not start the Cell Manager daemon.

原因

此问题的原因未知。

解决方案

要解决此问题，请执行以下步骤:

- 有关详细信息，请查看 omni_start.log 文件。文件位于默认的 Data Protector 临时文件目录中。
- 确保存在以下配置文件：
  - /etc/opt/omni/server/options/global
  - /etc/opt/omni/server/options/users/UserList
  - /etc/opt/omni/server/options/ClassSpec

hpdp-idb 服务无法启动，报告共享内存不足

在 Linux 系统上，hpdp-idb 服务无法启动，且 PostgreSQL 日志文件（/var/opt/omni/server/db80/pg/pg_log）中记录以下错误：

FATAL: could not create shared memory segment: Not enough space

DETAIL: Failed system call was shmget(key=7112001, size=2473459712, 03600).

原因

如果由于系统上的内存碎片导致 hpdp-idb 服务无法获取所需的共享内存量，则会出现此问题。

解决方案

重新启动系统以整理内存碎片。

MMD 无法启动 CRS 服务

Data Protector CRS 服务启动失败并显示以下错误：

[Critical] From: CRS@computer.company.com "" Time: 03/04/13 11:47:24 Unable to start MMD: Unknown internal error..

数据库日志文件可能已损坏。

解决方案

1. 从默认的 mmd.ctx 内部数据库目录中删除 Data Protector 文件。
2. 使用 omnisv -stop 和 omnisv -start 命令重新启动服务。

Data Protector 进程的其他问题

本节包含以下故障排除主题:

在 Linux 上的 Data Protector 性能受到影响 (如果禁用名称服务器缓存)

Linux 系统上的 Data Protector 性能下降。

原因

如果禁用了名称服务器缓存后台程序 (nscd)，则可能会发生此问题。Linux 系统没有默认名称服务器缓存。Data Protector 操作会创建很多 DNS 请求，如果禁用 nscd 后台程序，则可能会影响这些请求。

解决方案

要解决此问题，请按照下列步骤操作：

1. 确保已配置并启用了 nscd。nscd 的配置因平台而异。有关详细信息，请参见您平台的文档。
2. 检查 DNS 设置并确保 DNS 搜索顺序在 etc/resolv.conf 文件中正确配置为本地域优先。
3. 使用 omnisv -stop 和 omnisv -start 命令重新启动服务。

备份会话停止并且 BSM 停止响应

执行备份时，备份会话在一段时间后停止，BSM 停止响应。

原因

此问题可能是由于防火墙关闭不活动的连接导致的。

解决方案

确保连接保持活动状态，以便防火墙不会将其关闭。设置以下 omnirc 选项:

```
OB2IPCKEEPALIVE=1 OB2IPCKEEPALIVETIME=number_of_seconds OB2IPCKEEPALIVEINTERVAL=number_of_seconds
```

OB2IPCKEEPALIVETIME 指定在发送第一个保持活动数据包之前连接可以在多长时间内保持不活动状态， OB2IPCKEEPALIVEINTERVAL 指定在未收到确认消息的情况下发送连续保持活动数据包的间隔。您必须在 Cell Manager 系统上设置这些选项。

用户界面问题的故障排除

This feature is available in the Express and Premium Editions

本节包含以下故障排除主题:

图形用户界面问题

本节包括以下图形用户界面问题：

主页上下文显示空白屏幕

从 GUI 访问“主页”上下文时，“主页”上下文显示空白屏幕。

原因

如果您使用代理服务器连接到 Cell Manager，则会发生此问题。

解决方案

Data Protector GUI 使用端口 7116 检索“主页”上下文的内容。默认情况下，Data Protector 将绕过所有系统代理设置。如果使用代理连接到 Cell Manager，则将系统变量 `OB2_USE_SYSTEM_PROXY` 设置为 1。示例：`OB2_USE_SYSTEM_PROXY=1`.

找不到受信任的根证书

当从 Data Protector GUI 访问“主页”上下文时，显示以下错误消息:

Trusted root certificate is not found. Would you like to proceed?

原因

如果未将 Cell Manager CA 证书添加到 Windows 客户机上的“受信任的根证书颁发机构”列表中，则会发生此问题。这会被用户帐户控制 (UAC) 阻止。

解决方案

要解决此问题，请将 Cell Manager CA 证书添加到“受信任的根证书颁发机构”。为此，请“以管理员身份”运行 Data Protector GUI。

连接性和可访问性问题

本节描述了以下连通性和可访问性问题的故障排除步骤：

无法列出设备

考虑具有一个 Data Protector Cell Manager 系统作为 MOM 服务器、另一个 Data Protector 系统作为 MOM 客户机的 MOM 环境。当您尝试在 Data Protector 用户界面中列出设备时，MOM 客户机系统上会发生以下错误。

Inter process communication error

原因

发生此问题的原因是来自 MOM 服务器的 CA 证书在连接到 MOM 服务器时未复制到 MOM 客户机。

解决方案

将 CA 证书从 MOM 服务器上的 \Users*<USERNAME>*\AppData\Roaming\Hewlett-Packard\Data Protector\ca*<CM_HOSTNAME>* 文件夹手动复制到 MOM 客户机上的 \Users*<USERNAME>*\AppData\Roaming\Hewlett-Packard\Data Protector\ca*<HOSTNAME>* 文件夹。

没有访问 **Cell Manager** 的权限

显示以下消息：

Your Data Protector administrator set your user rights so that you do not have access to any Data Protector functionality. Contact your Data Protect or administrator for details.

原因

如果您没有访问 Data Protector 所需的权限，则会显示此消息。

解决方案

与 Data Protector 管理员联系，将您添加为用户，并在单元中为您分配适当的用户权限。有关详细信息，请参阅“配置用户组”。

到远程系统的连接被拒绝

在 Windows 中， telnet hostname 5565 命令的响应是 Connection refused 。

原因

如果未安装 Data Protector 或 INET 服务未在远程系统上运行，则会发生此问题。

解决方案

- 如果 Data Protector Inet 服务没有在远程系统上运行，则运行 omnisv -start 命令启动该服务。
- 如果在远程系统上没有安装 Data Protector，应进行安装。

Inet 在 Cell Manager 上没有响应

显示以下消息：

Cannot access the system (inet is not responding). The Cell Manager host is not reachable, is not up and running, or has no Data Protector software installed and configured on it.

原因

如果无法访问、未运行 Cell Manager 或其上未安装和配置 Data Protector，则会发生此问题。

解决方案

执行以下检查以确定原因:

- 检查系统之间的通信。
- 使用 telnet 检查安装，确保正确安装了所有组件。检查“Data Protector 安装”一节中的安装步骤。
- 运行 omnisv -status 命令，以检查 Cell Manager 上的服务是否正确运行。

无法启动文件系统浏览代理

当具有足够特权的 Data Protector 用户尝试保存备份规范并启动备份时，会发生以下错误：

Unable to start filesystem browse agent

原因

如果未在 Inet 中正确配置 Data Protector 用户的模拟详细信息，则会出现此问题。

解决方案

确保在 Inet 中正确配置了 Data Protector 用户的模拟详细信息。有关详细信息，请参阅为 Data Protector Inet 服务用户模拟设置用户帐户。

无法访问 **AppServer**

启用通用条件后，将无法访问应用程序服务器。

原因

发生此问题的原因是在通用条件模式下使用了密码加密。

解决方案

通过运行以下命令来禁用密码加密：

```
omnidbutil -disable_common_criteria_mode
```

命令行界面问题

本节介绍以下命令行界面问题的疑难解答步骤：

无法调用 **Data Protector** 命令

在命令提示符或终端窗口中尝试调用 Data Protector 命令后，命令行解释器报告找不到此命令。

原因

如果您尝试从其他目录调用命令，则会出现此问题。默认情况下，只能从 omniintro 页面中列出的位置调用命令。

解决方案

要解决此问题，请在已配置命令位置路径的操作系统中扩展 PATH 环境变量的值。通过此操作，可以从任何目录中调用 Data Protector 命令。

Postgres 进程利用 CPU 比例较高

Postgres 进程利用 96％ 以上的 CPU。

解决方案

要解决此问题，请清除 JCE 过期记录:

1. 运行： omnidbutil -run_script dbsripts/CPE/QCCR2A65778_jce_purge_expired_records.sql –jce
2. 重新启动应用程序服务器。

omnicc -update_port 命令在被动节点上不起作用

当您尝试在群集环境中运行 omnicc -update_port 命令时，被动节点上的端口可能不会更新。

原因

此问题通常发生在被动节点上。

解决方案

要解决此问题，请按照下列步骤操作：

1. 在命令失败的节点上，将 omnirc 变量 OB2NOCLIENTREQCHECK 设置为 1。
2. 运行 omnicc -update_port 命令。

用户管理故障诊断

本节介绍与用户管理有关的问题:

- omniuser –list 不列出任何用户

omniusers –list 命令不列出任何用户

当您执行 omniusers –list 命令时，它不列出任何用户。

原因

出现此问题可能有各种原因。一些常见原因如下:

- LDAP 服务器不可访问。
- 运行单元请求服务器 (CRS) 的用户帐户在 UserList 文件中不可用。
- 应用程序服务器、CRS 或 IDB 服务已关闭。

解决方案

要解决此问题，请按照下列步骤操作:

1. 检查 LDAP 服务器是否可访问。如果不可访问:
   a. 从 Cell Manager 中删除 LDAP 服务器配置。
   b. 在 LDAP 服务器与 Cell Manager 之间建立连接。
   c. 在 Cell Manager 中重新配置 LDAP 服务器。
2. 验证 UserList 文件中是否存在 CRS 用户帐户。如果它不可用，请手动添加它。
3. 运行以下命令以检查应用程序服务器、CRS 和 IDB 服务是否正在运行:
   omnisv -status
   如果这些服务已关闭，请通过运行 omnisv -start 命令启动它们。
4. 运行 omniusers -list 命令以验证该问题是否已解决。

备份和还原会话故障排除

This feature is available in the Express and Premium Editions

备份和还原会话故障诊断包括以下部分:

执行完整备份而不是增量备份

执行完整备份而不是增量备份

原因 1

没有以前的完整备份。在执行对象的增量备份之前，Data Protector 需要一个完整备份作为比较的基础，以确定哪些文件已经更改，因此需要在增量备份中包括完整备份。如果受保护的完整备份不可用，将执行完整备份

解决方案 1

在执行增量备份之前，确保存在对象的受保护的完整备份。

原因 2

备份对象由客户机、装载点和说明定义。如果这三个值中的任何一个发生改变，Data Protector 会将其视为一个新的备份对象，并执行完整备份而非增量备份。

解决方案 2

对完整备份和增量备份使用相同说明。

原因 3

受保护的完整备份已经存在，但与增量备份使用不同的树。此情况有两个可能的原因：

- 已经在受保护的完整备份的备份规范中更改了树。
- 已经创建了多个具有相同备份对象的备份规范，但为备份对象指定了不同的树。

解决方案 3

如果有多个具有相同备份对象的备份规范，请更改（自动生成的）备份对象统一说明。Data Protector 会将它们视为新对象并将运行完整备份。在执行完整备份之后，才可能进行增量备份。

原因 4

备份所有者不同。如果将备份配置为专用运行，则启动备份的用户就是数据的所有者。例如，如果用户 A 执行完整备份，用户 B 尝试启动增量备份，则增量备份将作为完整备份执行。这是因为用户 A 的数据是专用的，无法用作用户 B 的增量备份的基础。

解决方案

在高级备份规范选项中指定备份所有权。备份所有者应位于 Admin 用户组中。此用户将基于此备份规范成为所有备份的所有者，不管谁实际启动备份会话。

原因 5

升级后不执行增强型增量备份。

此问题可能出现在 Windows 和 Linux 系统上。如果将 Data Protector 从版本 A.06.11 进行升级，则原有的增强型增量备份存储库将再也无法与新产品版本配合使用。因此，将执行完整备份。在完整备份期间，会在以下位置创建一个新的增强型增量备份存储库：

Windows 系统： Data_Protector_home\enhincrdb

UNIX 系统： /var/opt/omni/enhincrdb

解决方案

运行完整备份。将创建新的增强型增量备份存储库，并能够执行增强型增量备份。

原因 6

如果 ZDB 配置为将会话 ID 目录添加到装载路径，则已启用增强型增量备份选项的 ZDB 文件系统备份将导致完整备份。

解决方案

在备份系统选项部分下，针对要添加到装载路径的目录，使用主机名选项。通过使用在目标装载点自动卸除文件系统 选项或确保未选中让备份系统处于启用状态，确保在下次会话之前装载路径处于空闲状态。

Data Protector 未能启动会话

由于下列原因之一，Data Protector 无法启动会话:

- 交互会话未能启动
- 计划的会话不再运行
- 计划的备份不启动（特定于 UNIX 系统）
- 会话失败，状态为“无可用许可证”

本节介绍所有上述原因的解决方案。

原因 1

每次启动备份时，都需要具有启动备份会话的权限并对当前运行 Data Protector 的用户检查该权限。如果用户没有此权限，则会话将无法启动。

解决方案 1

确保用户位于具有适当用户权限的用户组中。有关如何配置用户组的详细信息，请参阅

原因 2

由于 Data Protector 系统帐户 (假定该帐户启动计划会话) 不在 Cell Manager 上的 Admin 用户组中，因此计划会话不再运行。

此帐户在安装时被添加到 Cell Manager 上的 Data Protector Admin 组中。如果对其进行了修改，将删除此帐户的权限，如果服务帐户更改，则计划的会话不再运行。

解决方案 2

将 Data Protector 帐户添加到 Cell Manager 上的Admin 用户组中。

原因 3

在 UNIX 系统上无法启动计划的备份。

解决方案 3

通过运行 omnisv -stop 和 omnisv -start ，停止然后启动 Data Protector 后台程序。

原因 4

仅在 Data Protector 已经检查可用许可证之后才会启动备份会话。如果没有可用许可证，会话将失败，且 Data Protector 会发出会话状态No licenses available 。

解决方案 4

通过运行以下命令获取可用许可证的信息：

```
omnicc -check_licenses -detail
```

请求新许可证，并应用它们。有关许可的详细信息，请参阅“Data Protector 安装”一节。

交互会话未能启动

每次启动备份时，都需要具有启动备份会话的权限并对当前运行 Data Protector 的用户检查该权限。如果用户没有此权限，则会话将无法启动。

解决方案

确保用户位于具有适当用户权限的用户组中。

有关如何配置用户组的信息，请参阅《Data Protector 帮助》索引：“用户组”。

计划的会话不再运行

由于 Data Protector 系统帐户 (假定该帐户启动计划会话) 不在 Cell Manager 上的 Admin 用户组中，因此计划会话不再运行。

此帐户在安装时被添加到 Cell Manager 上的 Data Protector Admin 组中。如果对其进行了修改，将删除此帐户的权限，如果服务帐户更改，则计划的会话不再运行。

解决方案

将 Data Protector 帐户添加到 Cell Manager 上的Admin 用户组中。

计划的备份不启动（特定于 UNIX 系统）

在 UNIX 系统上无法启动计划的备份。

解决方案

通过运行 omnisv -stop 和 omnisv -start ，停止然后启动 Data Protector 后台程序。

会话失败，状态为“无可用许可证”

仅在 Data Protector 已经检查可用许可证之后才会启动备份会话。如果没有可用许可证，会话将失败，且 Data Protector 会发出会话状态 No licenses available 。

解决方案

通过运行以下命令获取可用许可证的信息：

```
omnicc -check_licenses -detail
```

请求新许可证，并应用它们。有关许可的详细信息，请参阅“Data Protector 安装”一节。

不必要的装载其他介质的请求

当您在交互的对象复制会话中从介质起点选择特定介质时，虽然介质已在设备中可用，但系统仍发出装载其他介质的请求。

原因

如果在介质上驻留的对象跨另一个介质，则会发生此情况。

解决方案

将所需介质插入设备中，并确认装载请求。

设备中的介质未用于备份

无论介质中是否有可用空间，介质都未用于备份。

原因

介质池策略配置为不可追加。

解决方案

编辑介质池策略，将“分配策略”配置为“可追加”。

设备中的介质未格式化

设备中的介质未格式化。

原因

默认情况下，不自动格式化介质。如果没有可用的格式化介质，就会发出装载请求。

解决方案

格式化介质。

设备中的介质与预分配列表中的不同

设备中的介质已格式化，但与备份规范的预分配列表中的不同，且指定的介质池采用 Strict 策略。

原因

如果将介质的预分配列表与 Strict 介质策略结合使用，则在启动备份时，预分配列表中指定的精确介质需要在设备中可用。

解决方案

- 要将设备中的可用介质与预分配列表结合使用，请将介质池策略修改为 Loose 。
- 要使用设备中的任何可用介质，请从备份规范中删除预分配列表。通过在备份规范中更改备份设备选项可以做到这一点。

发出文件库装载请求

在使用文件库设备时，可能收到以下装载请求消息：

There is no disk space available for file library File Library Device. Add some new disk space to this library.

原因

如果文件库所在的磁盘上没有足够的空间，则可能会出现此问题。

解决方案

在文件库所在的磁盘上创建更多空间：

- 在要备份文件的磁盘上释放一些空间。
- 向文件库设备所在的系统添加更多磁盘。

Data Protector GUI 中未正确显示文件名或会话消息

包含非 ASCII 字符的一些文件名或会话消息不能正确显示。

原因

在 Data Protector GUI 中使用不适当的字符编码显示文件名和会话消息时，就会发生这种情况。

解决方案

指定合适的编码。从“视图”菜单中选择编码，并选择适当编码的字符集。

群集问题

本节包含以下故障排除主题:

- IDB 服务不同步
- 在群集故障转移之后，使用 Windows NTFS 更改日志提供程序的群集共享卷增量文件系统备份将退回到完整备份
- 如果在群集中配置了 Cell Manager，则产生还原问题
- 备份 Microsoft 群集服务器节点的 CONFIGURATION 对象失败

IDB 服务不同步

在 UNIX 系统上将 IDB 还原到 Serviceguard 环境中的不同位置时，会话完成后所有节点的 IDB 服务将不同步。

原因

如果一个或多个群集节点处于脱机状态，则会发生此问题。

解决方案

要同步所有节点的 IDB 数据文件在群集环境中的位置，请在活动的群集节点上执行 omnidbutil -sync_srv 命令。

在群集故障转移之后，使用 Windows NTFS 更改日志提供程序的群集共享卷增量文件系统备份将退回到完整备份

在对备份规范中选中如果可用，使用本机文件系统更改日志提供程序选项的群集共享卷执行增量文件系统备份时，将执行完整备份，并显示以下错误消息：

[Major] From: VBDA@Host Name "F:" Time: Date Time

The Change Log Provider could not use the Directory Database. This session will use the normal file system traversal.

原因

如果在备份规范中针对群集共享卷选择了“使用本机文件系统更改日志提供程序 (如果有)”选项，则会出现此问题

解决方案

要确保正确执行增量备份，请为更改日志提供程序数据库创建一个符号链接以指向独立的群集共享卷，如下所示：

1. 选择一个共享磁盘，并将共享卷的更改日志提供程序指向该磁盘。如果是 Data Protector 群集 Cell Manager，则可以选择 Data Protector 共享磁盘。
2. 在共享磁盘上创建目录，例如： E:\Omniback\clp .
3. 转至目录 Data_Protector_home\clp 并创建指向所创建目录的符号链接。例如，要备份共享磁盘 J ，则执行 mklink /D J E:\Omniback\clp\J ，其中 E:\Omniback\clp\J 是为共享磁盘 J 创建的符号链接， E 是可以从其他群集节点访问的群集共享卷。

在所有群集节点上为共享卷创建更改日志提供程序数据库链接，并在群集故障转移之后在这些群集节点上执行增量备份。

如果在群集中配置了 Cell Manager，则产生还原问题

在已启用“重新启动所有对象的备份” 备份选项的情况下使用群集感知 Data Protector Cell Manager 进行了备份。在备份期间发生了故障转移，备份会话在另一个群集节点上重新启动并成功完成。在尝试从最后一个备份中还原时，尽管成功完成了会话，但仍显示以下错误:

You have selected a version that was not successfully completed. If you restore from such a backup, some or all the files may not be restored correctly.

原因

如果 Cell Manager 群集节点上的系统时间不同步，则失败的备份比重新启动的备份可能有更新的时间戳。选择用于还原的数据时，默认情况下会选择最后一个备份版本，从而导致从失败的备份还原。

解决方案

要从最后一个成功备份还原，请选择用于还原的正确备份版本。

要防止此类错误，建议在网络上配置时间服务器。这可以确保在 Cell Manager 群集节点上自动同步系统时间。

备份 Microsoft 群集服务器节点的 CONFIGURATION 对象失败

在 Windows Server 2012 系统上，备份群集节点上的 CONFIGURATION 对象失败，并显示以下错误:

[Minor] From: VBDA@computer.company.com "CONFIGURATION:" Time: Date Time

[81:141] \Registry\0.Cluster

Cannot export configuration object: (Details unknown.) = backup incomplete

原因

此问题的原因未知。

解决方案

使用运行群集服务的用户帐户重新启动 Data Protector Inet 服务，并重新启动备份。

IDB 还原问题

本节包含以下故障排除主题:

其他 Linux Cell Manager 上的 IDB 还原可能会失败

在其他 Linux Cell Manager 上执行 IDB 还原可能会失败，并显示以下消息：

Recovery of the Internal Database failed.

原因

此问题的原因未知。

解决方案

在还原时无法匹配原先进行 IDB 备份的 Cell Manager 上的操作系统用户的用户 ID 和组 ID 的 Cell Manager 上，更改操作系统用户的用户 ID 和组 ID。

完成还原操作后，从 GUI 连接到 Linux Cell Manager 失败

在完成还原操作并应用为“其他 Cell Manager 上的 IDB 还原可能会失败”问题提供的解决方法后，从 GUI 连接到 Linux Cell Manager 失败，并显示以下错误：

A server error has occurred. Reported error message: couldn't connect to host.

原因

此问题的原因未知。

解决方案

1. 获取 /etc/opt/omni/server/AppServer/standalone.xml 文件的备份
2. 将 /etc/opt/omni/server/AppServer/standalone.xml 中的所有密钥库和信任库密码替换为在此位置存储的密码 /etc/opt/omni/client/components/webservice.properties

其他 Windows Cell Manager 上的 IDB 还原可能会失败

不同 Windows Cell Manager 上的 IDB 还原将在还原过程结束时失败，并显示以下错误消息:

```
出现内部错误
```

```
R6025
```

```
- 纯虚函数调用
```

原因

如果选择了将 DCBF 还原到其他位置，则会发生此问题。

解决方案

用户必须选择将 DCBF 还原到原始位置，或者根本不还原它们。

基于块的备份、还原和恢复故障排除

本节包含以下故障排除主题:

卷的并行增量备份失败

并行触发同一卷的增量备份失败，并显示以下错误:

Failed to get changed blocks, hence backup cannot proceed

原因

当您触发同一卷的并行增量备份时，两个备份代理都会尝试创建快照。但是，其中一个备份代理的快照创建成功，而另一个备份代理则失败。

解决方案

不要并行运行同一卷的增量备份。但是，不同卷的并行增量备份是成功的。

无法锁定卷时，卷还原失败

卷还原失败，并显示以下错误:

Section <volumename:>cannot be locked!

原因

卷还原操作尝试锁定选定的目标卷以使其可以将备份数据还原到该卷时，会发生此错误。但是，无法锁定该卷，因为某些其他应用程序已经锁定了该卷。

在以下情况下，卷可能被锁定:

- 防病毒软件在系统上运行
- 其他应用程序使用该卷
- 卷已在 Windows 资源管理器应用程序中打开
- 在其他应用程序中打开一个或多个卷文件或文件夹

解决方案

确保在卷还原操作期间该卷没有被任何其他应用程序锁定，然后再运行还原操作。如果该卷被任何应用程序锁定，则可以停止该应用程序或按照特定于应用程序的说明来解锁该卷。

与源卷的实际数据大小相比，完整备份数据大小较大

日志文件中报告的完整备份数据大小远远大于源卷的实际数据大小。

原因

基于块的完整备份确定快照卷上 NTFS 文件系统中的已使用 (已分配) 块，并仅执行此类已使用块的备份。但是，据观察，作为快照一部分分配的其他块也可能进行备份，因为这些块也用于文件系统中。因此，日志文件中报告的完整备份数据大小远远大于源卷的实际数据大小，这可能是由于以下原因引起的:

- 原因 **1:** 应用程序、工具或基于块的备份 (完整或增量) 期间创建的快照 (卷影副本) 会占用卷空间。由于备份代理崩溃等问题，可能在基于块的备份期间创建了孤立 VSS 快照。在下次备份运行时，这些孤立的 VSS 快照会自动删除。但是，必须手动删除其他应用程序或工具创建的快照以及在下次备份过程中不会自动删除的快照。
- 原因 **2:** 将快照存储配置为无限制 有以下影响
  - Microsoft VSS 子系统使用大量的磁盘空间。
  - 即使删除快照后，创建的快照空间也不会自动释放。
  - 磁盘空间使用量增加，从而限制了可用于存储实际数据的空间。
  - 在“系统卷信息”目录上占用大量空间。
  - VSS 子系统可根据要求自由调整快照位置和最大大小。

解决方案

- 原因 **1** 的解决方案**:** 使用 ‘vssadmin.exe’ 或 ‘diskShadow.exe’ 之类的工具删除不再需要的现有孤立快照。有关在系统中删除特定快照或所有快照的选项的信息，请参阅相应工具的文档。
- 原因 **2** 的解决方案**:** 理想情况是有一个专用于卷影副本的单独驱动器，既不进行备份也不包含分页文件。如果这不可能，请指定一个包含分页文件的单独驱动器，而不是将卷影副本存储在要备份的驱动器上。建议您在执行完整备份之前，将快照存储配置为“使用限制” 并分配 10％ 卷大小的空间。

  要将快照存储限制的配置从“无限制” 更改为“使用限制” ，请执行以下操作:

  使用 **GUI:**

  1. 在 Windows 资源管理器中，右键单击存储缓存文件的卷，然后单击“属性” 。
  2. 在“卷影副本” 选项卡上，单击“设置” 。
  3. 在“存储区域”部分中，选择“使用限制” 并输入卷影副本缓存文件可使用的空间量。
  4. 单击“确定” 。

  > **重要说明:** 据观察，即使在 GUI 中进行了上述更改之后，VSS 子系统也不接受这些更改，因为它在快照创建过程中将设置更改为“无限制” 。建议您使用 vssadmin 命令设置卷影副本限制。允许的最小卷影副本存储空间设置为 320 MB。但是，可以将其配置为源卷的 10％。

  使用 **CLI:**

  1. 打开已升级的命令提示符窗口。
  2. 使用以下命令更改卷影副本存储区域:
     - vssadmin resize shadowstorage /on=x: /for=x: /maxsize=10%
     - vssadmin resize shadowstorage /on=x: /for=x: /maxsize=320MB
       " /on ": 指定卷影存储的位置。
       " /for ": 指定存储的源卷。
       " /maxsize ": 设置卷影存储区域的最大大小。

  有关 vssadmin.exe 实用程序的信息，请参阅 Microsoft 文档。

群集共享卷的基于块的还原失败

如果无法获得独占锁，则将使用基于块的备份进行备份的卷还原到其原始位置可能会失败。

原因

在以下情况下可能会发生这种问题:

- 要还原的卷已安装操作系统。
- 群集卷是预期的目标。
- 另一个应用程序正在主动使用目标卷。

解决方案

如果使用备用卷或在手动干预下，还原可以成功。手动干预涉及:

- 手动解锁锁定的卷，并采取必要的措施将这些卷置于维护模式。
- 重新触发还原操作。
- 恢复在还原操作之前停止的服务/操作。

尝试在还原上下文中选择对象时发生未知的内部错误

无法浏览以选择要在还原上下文中还原的对象。显示以下错误:

Unknown internal error

原因

此问题的原因未知。

解决方案

1. 从 C:\ProgramData\OmniBack\tmp\ 文件夹中删除 **BBB 文件夹**。
2. 从 *services.msc* 中，重新启动 **FilterListener** 服务。

从备份执行数据还原时发生错误

基于块的文件恢复失败并显示以下错误:

```
[重大] 来自: RRDA@host.hpeswlab.net "E:" 时间: 11/28/2019 3:24:47 PM 从备份执行数据还原时发生错误!
```

原因

如果正在执行还原、浏览和恢复的 DA 客户机系统无权通过 FC 连接路径访问目标存储，则可能会发生此错误。

解决方案

解决方案 **1:**

1. 从 C:\ProgramData\OmniBack\tmp\ 文件夹中删除 **BBB 文件夹**。
2. 从 *services.msc* 中，重新启动 **FilterListener** 服务。

解决方案 **2:**
如果正在通过 FC 路径执行基于块的文件系统备份，请确保 DA 客户机系统有权通过 FC 连接路径访问目标存储。

未还原某些文件或文件夹

基于块的恢复失败并显示以下错误:

```
[重大] 来自: <客户机名称> "E:" 时间: <日期> <时间> 未还原某些文件或文件夹。
```

位于 C:\Program Files\OmniBack\bin 文件中的 *discutilswrapperDll.txt* 显示以下错误消息:

The process cannot access the folder '<foldername>' because it is being used by another process.

原因

当运行恢复过程时，如果某些文件或文件夹被打开或被另一个进程使用，会发生此错误。

解决方案

1. 关闭错误消息中提到的文件夹。
2. 重新启动恢复过程。

浏览卷时发生错误

在基于块的恢复期间，浏览卷时可能会发生以下错误:

Error occurred while browsing the volume

可能原因

原因 1 : 从基于块的备份会话浏览和恢复文件和文件夹所需的 Imdisk 驱动程序未成功安装为 DA 组件的一部分。

原因 2 : 无法正确卸载 Imdisk 装载点，从而导致句柄打开。这可能导致浏览操作失败。

原因 3: imdskvsc 服务未启动并运行，在 **services.msc** 向导中找不到它。

原因 4: 执行还原、浏览和恢复操作的 DA 客户机系统无权通过 FC 连接路径访问目标存储。

原因 **5:** 当浏览容量超过 16 TB 的大卷时，基于块的浏览和恢复所需的16 TB 存根文件的创建失败。这是因为默认情况下，存根文件是在 C 驱动器中创建的，该驱动器不支持创建大于 16 TB 的文件。

原因 **6:** Data Protector 过滤侦听程序服务不能使用 Data Protector Inet 服务所用的用户帐户来运行。

原因 **7:** 您浏览的是绝对路径名超过 1024 字节的深层文件或文件夹。

解决方案

原因 1 的解决方案: 重新安装 IMDisk 驱动程序。完成以下步骤：

1. 重新引导系统。
2. 按照列出顺序执行 *drive*:>\Program Files\Omniback\bin 文件夹中的以下文件:
   a. **dp_uninstall_imdisk.bat**
   b. **dp_install_imdisk.bat**
3. 重试浏览操作。

原因 2 的解决方案: 正确卸载驱动程序。完成以下步骤：

1. 在服务窗口 (services.msc) 中停止 Data Protector 过滤侦听程序。
2. 转到 Data Protector 基于块的文件系统备份临时文件夹 (programData\omniback\tmp\BBB)。可找到两个文件夹:
   1. 具有用于浏览的备份会话名称的文件夹
   2. 装载点以 "_<driver letter>" 为后缀的文件夹。记下装载点文件夹。
3. 打开 Windows 命令提示符窗口，键入下面的命令以卸载装载点:
   Imdisk.exe -d -m <path of mount point noted in the step 2>
4. 在 BBB 文件夹中，删除步骤 2 中提到的两个文件夹。
5. 在服务窗口中启动 Data Protector 过滤侦听程序。
6. 重试浏览操作。

原因 3 的解决方案**:** 重新安装 IMDisk 驱动程序。完成以下步骤：

1. 重新引导系统。
2. 按照列出顺序执行 *drive*:>\Program Files\Omniback\bin 文件夹中的以下文件:
   a. **dp_uninstall_imdisk.bat**
   b. **dp_install_imdisk.bat**
3. 重试浏览操作。

原因 4 的 解决方案**:** 当基于块的文件系统备份通过 FC 路径进行时，请确保 DA 客户机系统有权通过 FC 连接路径访问目标存储。

原因 5 的 解决方案**:** 要处理此 NTFS 大小限制，请使用 'OB2_BBB_PATH_FOR_TEMP_FILES ' omnirc 变量来配置用于生成基于块的临时文件的替代位置。替代位置可以是驱动器装载点 (例如 E:\ ) 或驱动器装载点内的目录 (例如 E:\temp\ )。此外，驱动器的群集大小/分配单位大小必须与您浏览的已备份驱动器卷的分配大小相匹配。

示例：对于 16 TB 到 32 TB 的卷大小，建议的分配单位为 8 KB。有关详细信息，请参阅 NTFS 的默认群集大小。

原因 6 的 解决方案**:** 为了成功浏览和恢复文件和文件夹，必须确保 Data Protector INET 服务和 Data Protector 过滤侦听程序服务都在同一用户帐户下运行。

原因 7 的 解决方案**:** 为了成功浏览和恢复文件和文件夹，必须确保要浏览的文件或文件夹的绝对路径名不超过 1024 字节。

基于块的恢复：安装失败

在安装或卸载 IMDisk 驱动程序期间发生以下错误:

Installation failed

原因

由于重复安装或卸载 IMDisk 驱动程序而发生此错误。尽管出现此错误消息，但安装或卸载成功完成。

解决方案

可以忽略此错误。

增量备份期间更改后的块不可用

在安装更改后的块驱动程序之后，对大小已更改的备份卷执行增量备份时，显示以下错误消息：Detected volume size changes but changed block driver is not reconfigured, hence changed blocks are not available.

原因

当备份卷的大小与上次备份相比已更改时，会发生此问题。卷大小的更改可能是由卷的缩小和扩大所致。

解决方案

每当备份卷的大小更改时，您都必须重新配置已安装的更改后的块驱动程序。要重新配置更改后的块驱动程序，必须卸载已安装的驱动程序并重新安装它。卸载并重新安装驱动程序后，必须重新引导系统才能使驱动程序正常工作。请参阅重新配置更改后的块驱动程序。

未通过更改后的块驱动程序配置卷

在客户机系统上执行卷的增量备份之前，必须确保已在 DA 客户机系统上安装了更改后的块驱动程序。如果更改后的块驱动程序未配置所选的卷，则会显示以下错误消息。

The volume <volumename> is not configured for monitoring by changed block driver. Please configure the volume for monitoring by uninstalling and re-installing changed block driver

原因

发生此问题的原因可能为:

- 主机 DA 系统上未安装更改后的块驱动程序。
- 安装更改后的块驱动程序后，已添加选定的卷。因此，新添加的卷不受更改后的块驱动程序监视。

解决方案

- 在运行增量备份之前，必须在 DA 客户机系统上安装更改后的块驱动程序。请参阅安装更改后的块驱动程序。
- 如果在安装更改后的块驱动程序后对卷进行了更改，则必须重新配置更改后的块驱动程序。请参阅重新配置更改后的块驱动程序。

装载还原到同一主机上的其他卷的卷时出错

考虑一下，您使用“还原为” 选项将备份还原到装有 **XFS** 文件系统的同一主机上的其他卷。装载此还原的卷失败，并显示如下错误:
mount: <*mount_path*> wrong fs type, bad option, bad superblock on <device_*name*>, missing codepage or helper program, or other error.

原因

这是因为在 **XFS** 文件系统的情况下，同一 UUID 同时应用于原始备份设备和还原的设备。

解决方案

使用以下带有 nouuid 选项的 mount 命令装载还原的卷。

```
mount -o nouuid <device_name> /mnt
```

某些文件和文件夹的还原失败

在恢复文件和文件夹期间出现以下错误消息:

Restore of some files and folders failed.

原因

如果所选目标路径或设备上没有剩余存储空间，则会显示此消息。

解决方案

检查用于恢复操作的所选目标路径或设备是否已满。

其他问题

本节包含以下故障排除主题:

Unable to establish local proxy connection for backup

Failure to establish local proxy connection for any cloud targets causes backup to fail.

Cause

This occurs due to internal errors on the deduplication engine.

Solution

Try to create a device with a different container/bucket.

Device creation and backup failure

Channel creation error occurs during device creation or backup, causing a failure.

Cause

This error occurs if a stale sdfs-proxy port forwarder process is running. This happens when all the volumes under port forwarder are shutdown.

Solution

If a dedicated port is not used, complete the following:

- Shut down port unifier on deduplication store system using the DPDUtils -shutdown_portUnifier command and try again.
- Kill any sdfs-proxy processes still running and try again.

Device creation fails due to channel creation error

Device creation fails due to channel creation error.

Cause

This occurs when the deduplication store port or port-range is under firewall.

Solution

Check for firewall status, make sure the specific port range (using OB2PORTRANGE omnirc variable) is opened on the deduplication store system. By default the port number starts from 6442 for a store created using a dedicated port and 16442 when store is created without a dedicated port, unless the port range is specified.

无法解密数据

会话无法解密已加密的驱动器，失败并出现以下错误:

Drive unable to decrypt data: Invalid decryption key retrieved from key management server.

原因

这是因为用于加密驱动器的算法较旧，与用于解密的逻辑不兼容。

解决方案

要强制解密使用旧算法加密的驱动器，请将介质代理服务器上的 OB2_FORCE_OLD_DECR_MODE omnirc 变量的值更改为 1。 OB2_FORCE_OLD_DECR_MODE 的默认值为 0。

> **重要说明:** 建议您在对此 omnirc 变量进行更改时，在介质代理主机上重新启动 Data Protector INET 服务。

备份保护过期

备份保护过期。

原因

在计划备份时，为完整备份和增量备份设置了相同的保护期间，这意味着增量备份的保护期间与相关的完整备份的相同。因此，数据实际上仅在完整备份过期前才受到保护。无法还原基于过期的完整备份的增量备份。

解决方案

配置完整备份的保护时间，使完整备份的保护时间超过增量备份的时间。

完整备份与增量备份保护之间的时间差应是完整备份与下一个完整备份之前最后一个增量备份之间的时间量。

例如，如果在周一至周五运行增量备份，周六运行完整备份，则设置的完整备份的保护时间至少应比增量备份多 6 天。这样可使完整备份得到保护，并在最后一个增量备份过期之前一直可用。

间歇性连接被拒绝错误

备份会话中止，并显示以下重大错误：

Cannot connect to Media Agent on system computer.company.com, port 40005 (IPC Cannot Connect System error: [10061] Connection refused)

原因

如果介质代理在非服务器版的 Windows 上运行且磁盘代理并发设为大于 5 的值，可能会发生此问题。由于在非服务器版的 Windows 操作系统上实施 TCP/IP，操作系统只能同时接受 5 个传入连接。

解决方案

将磁盘代理并发数设置为 5 或更少。

建议对涉及密集备份操作的系统使用 Windows 的服务器版本，例如 Cell Manager、介质代理、应用程序代理客户机、文件服务器等。

增强型增量备份因文件数量过多而失败

在 HP-UX 系统上，备份大量文件时增强型增量备份失败。

原因

当备份大量文件时，会发生此问题。

解决方案

要允许磁盘代理在执行增强型增量备份时访问更多内存，请设置可调内核参数 maxdsiz ，如下所示：

HP-UX 11.11 系统：

kmtune set maxdsiz=2147483648

kmtune set maxdsiz_64bit=2147483648

HP-UX 11.23/11.31 系统：

kctune set maxdsiz=2147483648

kctune set maxdsiz_64bit=2147483648

还原磁盘映像时检测到意外装载的文件系统

还原磁盘映像时，收到正在还原的磁盘映像是已装载的文件系统并且未被还原的消息：

```
Object is a mounted filesystem = not restored.
```

原因

磁盘映像上的应用程序在磁盘映像上留下某些模式时，会发生这种情况。这些模式混淆了系统调用，使其无法验证是否装载了磁盘映像上的文件系统，因此系统调用会报告磁盘映像上有装载的文件系统。

解决方案

在启动还原之前，擦除 Data Protector 客户机上要还原的磁盘映像：

```
prealloc null_file 65536
```

```
dd if=null_file of=device_file
```

其中 device_file 是要还原的磁盘映像的设备文件。

应用程序数据库还原问题

在尝试还原数据库时，还原操作会失败并显示以下消息：

- Cannot connect to target database
- Cannot create restore set

原因

配置低劣的 DNS 环境可能导致数据库应用程序问题。问题如下：

备份数据库时，在驻留数据库的客户机上启动的代理在数据库上将客户机名称记录为 computer.company.com 。

在还原时，还原会话管理器会尝试还原到 computer.company.com ，但它无法还原，因为它只知道此客户机是 computer 。因为 DNS 未正确配置，无法将客户机名称展开为完整名称。

如果在 Cell Manager 上配置了 DNS，但没有在应用程序客户机配置，也会发生这种情况。

解决方案

正确设置 TCP/IP 协议和配置 DNS。有关信息，请参阅“Data Protector 安装”一节中的附录 B。

异步读取未改进备份性能

在备份规范中选择了异步读取（特定于 Windows）选项后，没有改进备份性能，甚至可能造成性能降低。

原因

发生此问题的原因如下:

- omnirc 选项 OB2DAASYNC 设置为 0。
- 异步读取不适合您的备份环境。

解决方案

1. 检查 omnirc 选项 OB2DAASYNC 是否设置为 0。将该选项设置为 1 始终使用异步读取，或者在备份规范中注释掉该选项并使用异步读取选项。
2. 考虑异步读取是否适合您的备份环境。通常，异步读取适合于大于 1 MB 的文件。另外，可以尝试微调 omnirc 选项 OB2DAASYNC_SECTORS 。作为一种规则，文件的大小（以字节为单位）应当比选项的值大 2-3 倍。

在 Windows 系统上备份 IIS 配置对象失败

在 Windows 系统上，当备份 IIS 配置对象时，Data Protector 报告以下错误:

[Minor]

From: VBDA@computer.company.com "CONFIGURATION:" Time: Date & Time [81:141]

\IISDatabase Cannot export configuration object: (Details unknown.) = backup incomplete.

原因

如果 Windows 系统上未安装 IIS 6 元数据库兼容性组件，则会发生此问题。

解决方案

在 IIS 6 Management Compatibility 之下安装 IIS 6 Metabase Compatibility 组件，并重新启动备份。

从具有硬链接的卷还原子树失败

从具有硬链接的卷还原子树失败，并显示以下错误消息：

Lost connection to Filesystem restore DA named ""

incomplete.

原因

如果将全局选项 RepositionWithinRestoredObject 设置为以下值，则发生此问题：1.

解决方案

如果正在还原具有硬链接的树，则将全局选项 RepositionWithinRestoredObject 设置为 0 。

尽管将此选项设置为 0 可能使还原速度稍微减慢，但在还原硬链接时需要这样做。默认情况下，此选项设置为 1。

备份为系统保留的镜像分区时可能失败

尝试备份系统保留分区和多个完整卷对象时，备份可能失败，并显示以下错误消息之一：

Fallback to legacy filesystem backup was not allowed. Aborting the backup.

Not a valid mount point => aborting.

原因

仅当 VSS 选项已启用，并且系统保留的分区已镜像时才会出现该问题。

解决方案

将 omnirc 变量 OB2_DISABLE_REGLIST_FOR_FULL_VOLUME 设置为 1 ，并重新启动备份。

找不到中断的文件备份或文件

尝试备份系统保留分区和多个完整卷对象时，备份失败，并显示以下错误消息之一：

- Cannot read <number> bytes at offset <number>(:1): ([21] The device is not ready.).

- Cannot open: ([2] The system cannot find the file specified.) => not backed up.

原因

仅当已启用 VSS 选项且系统保留分区空间不足、无法容纳多个快照时，才会发生此问题。

解决方案

将 omnirc 变量 OB2_DISABLE_REGLIST_FOR_FULL_VOLUME 设置为 1 ，并重新启动备份。如果错误仍然存在，请参见以下 Microsoft 网页，了解有关如何解决此问题的信息：

http://support.microsoft.com/kb/2930294

计划程序在尝试计划备份时失败

计划程序在尝试使用不同的定时计划备份时失败。

原因

Java 服务导致出现此问题。

解决方案

执行以下步骤：

1. 关闭 Data Protector GUI。
2. 执行 omnisv stop 。
3. 通过任务管理器结束 Java 服务。
4. 执行 omnisv start 。
5. 启动 Data Protector GUI。

Windows 重复数据删除卷的 ZDB 文件系统备份失败

在未安装重复数据删除功能的情况下，对 Windows 备份主机上已删除重复数据的 Windows 卷执行 ZDB 文件系统备份失败，并显示以下错误消息：

[Warning] From: VBDA@computer.company.com "<volume label>" Time: <Date Time>

[81:77] <Path name>

Cannot open: ([1920] The file cannot be accessed by the system.) => not backed up.

原因

如果备份主机上未安装 Windows 重复数据删除功能，则会发生此问题。

解决方案

1. 在备份主机上安装 Windows 重复数据删除功能。
2. 通过以下操作，确保在 ZDB 备份期间没有任何重复数据删除作业：
   - 将重复数据删除作业排定在 ZDB 备份过程之前或之后。
   - 实施 pre-exec 脚本，在备份前停止重复数据删除作业；并实施 post-exec，在备份后启动重复数据删除作业。

Pre-exec 和 post-exec 脚本失败并出现错误消息

pre- 和 post-exec 脚本失败，并显示以下错误消息：

```
[重要] 来自：OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>
```

```
..\script.bat
```

```
非法命令格式。命令未执行。
```

```
[重大] 来自: OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间: <DATE><TIME>
```

```
[131:104] Script returned error.(返回值: -1）。
```

原因

如果未在正确的位置提供 pre- 和 post-exec 脚本，则会发生此问题。

解决方案

确保 pre- 和 post-exec 脚本位于以下目录：

- Windows 系统： Data_Protector_home\bin 目录或其子目录。
- Unix 系统: /opt/omni/lbin 目录或其子目录。

此处的问题陈述列出了 SQL 代理的错误消息。在 pre- 和 post-exec 脚本故障期间，所有集成和 ZDB 模块都会显示相似的错误消息。

Pre-exec 和 Post-exec 脚本在设置 OB2OEXECOFF 后失败

pre- 和 post-exec 脚本的执行失败，并显示以下错误消息：

[重要] 来自：OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>

OB2OEXECOFF 变量值导致无法在此主机上执行 pre/post-exec 脚本。

原因

如果已针对此客户机启用 omnirc 文件中的 OB2OEXECOFF 变量，则会发生此问题。设置此变量将会禁止执行 pre- 和 post-exec 脚本。

解决方案

要禁用 OB2OEXECOFF 变量，请将该值设为 0 。

Post-exec 脚本在 pre-exec 失败时不运行

如果某个客户机的 pre-exec 脚本失败，post-exec 脚本将被跳过并显示以下错误消息:

```
[重大] 来自: OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>

..\script.bat

非法命令格式。命令未执行。

[重大] 来自: OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>

[131:104] 脚本返回了错误。(返回值: -1）。

[警告] 来自：OB2BAR_SQLBAR@hostname.com "1" 时间:<DATE><TIME>

Pre-exec script failed.正在跳过 Post-exec！
```

原因

此问题的原因未知。

解决方案

将 omnirc 文件中的 OB2FORCEPOSTEXEC 变量设置为 1 ，以确保始终运行 post-exec 脚本，即使当某个客户机的 pre-exec 脚本失败时亦如此。

在启用 OB2FORCEPOSTEXEC 变量并运行备份规范后，将会出现以下消息：

```
[正常] 来自: OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>

Starting post-exec script 'script.bat'...

[正常] 来自: OB2BAR_SQLBAR@hostname.com "(<Instance>)" 时间:<DATE><TIME>

已成功执行脚本。
```

该消息表明，尽管 pre-exec 脚本失败，但客户机的 post-exec 脚本仍旧成功运行。

随机备份到 B2D (COFC) Catalyst 失败

随机备份到 B2D (COFC) Catalyst 失败，并显示以下错误:

会话报告错误：

```
[严重] 来自: OB2BAR_SAPBACK@<hostname> "<specname>" 时间: <timestamp> 读取 NET 消息时意外关闭 => 正在中止。 [重要] 来自：
BSM@<hostname> "<specname>" 时间: <timestamp> [61:3003] 在主机 <hostname> 上与 OB2BAR Backup DA 失去连接， 这种问题叫做 "
<specname>"。 Ipc 子系统报告：IPC 读取错误 系统错误: [10053] 软件导致连接中止 [重大] 来自: BMA@<hostname> "<specname>" 时间:
<timestamp> [90:51] \\<path> 无法写入到设备 (StoreOnce 错误: 发生了未指定的 (内部) 错误)
```

xMA-D2D 调试错误：

```
Unable to create thread, error : 11
```

原因

此问题的原因未知。

解决方案

如果 DP 是在 xinetd 上配置的，则通过在 /etc/xinetd.d/omni 文件中设置 TasksMax=infinity 提高 SUSE Linux Enterprise Server 12 (SP2 和 SP3) 的 xinetd 限制。

如果 DP 是在 systemd 上配置的，请执行以下这些步骤:

1. 通过在 /usr/lib/systemd/system/omni@.service 文件中设置 TasksMax=infinity 提高 SUSE Linux Enterprise Server 12 (SP2 和 SP3) 的 xinetd 限制。
2. 运行以下命令：
   /usr/bin/systemctl daemon-reload
   /usr/bin/systemctl restart omni.socket

Novell OES 上的增量备份失败

在 Novell Open Enterprise Server (OES) 上执行的增量备份失败。

原因

如果 Novell OES 客户端上正在运行文件系统目标服务代理 (TSAFS) 缓存，则会出现此问题。

解决方案

通过运行以下命令，在 Novell OES 客户机上禁用 Target Service Agent for File Systems (TSAFS) 缓存:

```
/opt/novell/sms/bin/smsconfig -u tsafs
/opt/novell/sms/bin/smsconfig -l tsafs --tsaMode=Dual --noCachingMode
```

有关详细信息，请参阅 Novell 文档:
https://www.novell.com/documentation/open-enterprise-server-2018/bkup_sms_lx/data/hhc3nq5m.html

创建备份规范时无法查看深层文件和文件夹

创建备份规范时浏览深层文件夹时，不显示子文件和文件夹。

原因

当您浏览深度文件和文件夹的绝对路径名超过 1024 个字符时，会发生此问题。这是因为浏览所允许的最大文件或文件夹绝对路径名为 1024 个字符。

解决方案

确保要浏览的文件或文件夹的绝对路径名不超过 1024 个字符。

无法模拟用户

用户模拟失败，并显示以下错误消息:

```
[警告] 来自：<主机名> "" <时间> 无法模拟用户 <用户>
```

原因

出现此问题是因为域用户不属于 Data Protector 用户列表。在重新安装 Data Protector 的主机上对 IDB 进行脱机还原后，会发生这种情况。

解决方案

确保您有管理员权限，可在使用 Data Protector 用户列表配置备份规范之前将域用户添加到该列表中。为要模拟的每个域用户手动运行以下命令:
omniinetpasswd –add <domain_user><domain_password>

如果在同一主机上重新安装 DP 时 IDB 脱机还原

1. 要模拟管理员 (安装所有者) 用户，请执行以下步骤:
    - omniinetpasswd -list
      Administrator@IWF1113064
    - omniinetpasswd -delete Administrator@iwf1113064
      已成功从 inet 配置中删除用户 'Administrator@iwf1113064'。
    - omniinetpasswd -add Administrator@iwf1113064 Data*pr0
      已成功添加用户 'Administrator@iwf1113064'。

磁盘代理

This feature is available in the Express and Premium Editions

本节包含以下故障排除主题:

在并行还原期间，磁带客户机失败并显示错误消息

尝试进行所用的磁带客户机数目多于当前介质代理并发数目的并行还原时，部分磁带客户机会失败并显示以下错误：

Cannot handshake with Media Agent (Details unknown.) => aborting.

原因

当您尝试使用比当前介质代理并发设置更多的磁盘代理进行并行还原时，会出现此问题。

解决方案

重新启动失败的磁带客户机的还原对象。

在恢复期间，未显示实际恢复目标装载点

在还原过程中，卷恢复磁带客户机 (VRDA) 会在监视器中显示应用程序系统的装载点。例如，它实际显示的不是还原目标装载点 /var/opt/omni/tmp/<主机名>/BC/fs/LVM/VXFS，而是对应的应用程序源装载点 /BC/fs/LVM/VXFS。

原因

此问题的原因未知。

解决方案

无。

恢复失败并在会话日志中显示消息

将文件通过 UNC 共享还原到其他系统时，还原将失败，并在会话日志中显示以下消息：

Can not open: ([112] There is not enough space on the disk.) => not restored. [Warning] From: VRDA@hostname "host2.test.com [/H]" Time: < Date > < Time > Nothing restored

原因

发生此问题的原因如下:

- Data Protector Inet 登录用户帐户应具有登录到远程系统的访问权限，这是在 UNC 路径中指定的。
- 对于要通过 UNC 共享还原的文件，您没有这些文件的写权限。

解决方案

确保 Data Protector Inet 登录用户帐户必须具有登录到远程系统的访问权限，这是在 UNC 路径中指定的。对于要通过 UNC 共享还原的文件，您还应该是其所有者，或具有这些文件的写权限。

在目录结构备份期间，同一消息显示了两次

尝试备份具有 100 个以上目录的目录结构时，以下消息将显示两次，而不是一次：

[Major] From: VBDA@hostname "C:" Time: < Date > < Time >

[81:74] File system too deep: (100) levels.

原因

此问题的原因未知。

解决方案

无。

备份装载点

在 Windows 系统上备份装载点时，即使通过取消选择子目录将其从备份中排除，但是仍将备份整个装载点。

原因

此问题的原因未知。

解决方案

无。

展开空的装载点失败并显示一条错误消息

尝试在树形结构视图中展开空的 Windows 装载点时，将报告以下错误：

Cannot read directory contents.

原因

此问题的原因未知。

解决方案

无。

只有帐户用户才能删除加密的属性

在 Windows 上，将还原已加密文件夹的加密属性。但是，只有用帐户在客户机上运行 Inet 服务的用户或管理员，才能删除该属性。

原因

此问题的原因未知。

解决方案

无。

在 Macintosh 文件备份期间，文件名中的某些字符可能导致问题

在 Macintosh 文件备份期间，不会备份单个文件，或者磁盘代理异常终止。

原因

在 Windows 系统上备份 Macintosh 文件时，文件名中的某些字符可能会出问题。如果文件名包含 Windows 文件系统认为无效的字符（通常是“*”和“?”），或者包含映射到此类无效字符的字符（例如 Macintosh 项目符号字符），则可能出现个别文件未备份或磁带客户机异常终止的情况。

解决方案

重命名有问题的文件。

备份数据无法还原到其原始位置

用安装在受支持 Windows 系统上的 Data Protector 磁盘代理从共享网络文件夹备份的数据，即使备份会话中所用的用户帐户被授予该文件夹的写权限，也无法将数据还原到其原始位置。

原因

发生该问题是由于 Data Protector 不具有文件系统还原会话的模拟能力。

解决方案

使用 runas.exe 命令，以备份会话中所用帐户的用户身份启动 Data Protector GUI，此时才能启动还原会话。

在磁盘映像备份期间显示了一条警告消息

当执行磁盘映像备份时，尽管备份会话成功，但仍会显示一条警告消息：

Object is a mounted filesystem.

原因

此问题的原因未知。

解决方案

无。检查是否磁盘或卷已安装。如果未安装，可忽略该警告消息。

在复制会话期间，会话失败并显示一条错误消息

如果您安排并行运行多个复制会话，且复制源也为复制会话，那么这些会话可能会失败，并显示与以下类似的错误：

[Major] From: CSM@hostname "QCTP2A53730" Time: < Date > < Time > [65:99] Import failed with possible cause: this media already has valid copy in DB.

原因

该问题由出现在多个备份规范中的带有相同标签的对象引起，例如，如果您在相同客户机上为相同文件系统的不同目录创建了多个备份规范。

解决方案

使用 Data Protector GUI 为备份规范中作为替换规范初始源的冲突对象提供不同描述，或确保包含这些对象的替换会话不会并行启动。

Data Protector GUI 无法区分活动的源设备

当复制的源和目标是相同的 B2D 设备时，可以启动替换，这是因为 Data Protector GUI 不能区分活动的源设备。

如果用户尝试使用“能够替换”选项创建对象复制规范，则可在 Data Protector GUI 中选择源和目标相同的 B2D 设备。

原因

如果源和目标 B2D 设备相同，则可能会出现此问题。

解决方案

请确保复制源和目标为不同的 B2D 设备。

在继续备份期间，无法分析已经备份哪些文件

在文件系统上继续备份时，Data Protector 无法分析已经备份哪些文件。在这种情况下，文件系统扫描将忽略所有与继续操作时相关的信息。备份会话将显示为继续执行，但是所有文件将重新备份，这可能导致继续执行的备份文件的大小比预期的更大。

原因

当在文件系统 (从会话中止以来发生很多更改) 上恢复备份时，Data Protector 可能无法使用 Windows 本地更改日记分析已经备份了哪些文件。

解决方案

无。

备份失败并显示一条错误消息

尝试备份系统保留分区和多个完整卷对象时，备份失败，并显示以下错误消息之一：

- 无法读取偏移量 <number>(:1) 处的 <number> 个字节：([21] 设备未就绪。)。
- 无法打开: ([2] 系统找不到指定的文件。) => 不备份。

原因

仅当已启用 VSS 选项且系统保留分区空间不足、无法容纳多个快照时，才会发生此问题。

解决方案

将 omnirc 变量 OB2_DISABLE_REGLIST_FOR_FULL_VOLUME 设置为 1，并重新启动备份。如果错误仍然存在，请参见以下 Microsoft 网页，了解有关如何解决此问题的信息：

http://support.microsoft.com/kb/2930294

增强型增量备份选项将导致完整备份

在启用了增强型增量备份选项时进行 ZDB 文件系统备份会导致完整备份。

原因

如果 ZDB 配置为将会话 ID 目录添加到装载路径，则会发生此问题。

解决方案

在备份系统选项部分下，针对要添加到装载路径的目录，使用主机名选项。通过使用在目标装载点自动卸除文件系统 选项或确保未选中让备份系统处于启用状态，确保在下次会话之前装载路径处于空闲状态。

磁盘代理无法备份子卷的文件

磁盘代理无法备份子卷的文件。

原因

如果使用父子卷访问磁带客户机，则该磁带客户机不会直接备份其所有子卷。因此，必须单独装载和备份子卷。BTRFS（一种适用于 Linux 的新文件系统）作为一项功能，可实现从一个文件夹树创建子卷。因此，您可以在一个文件系统上拥有许多子卷。在创建此类子卷之后，磁带客户机将不能从该子卷备份文件。

解决方案

将该卷装载为新的装载点，并在备份规范中进行配置以备份装载点。

“增强型增量备份”选项备份已备份的文件

对于驻留在启用了 Windows 卷重复数据删除的卷上的文件，已启用“增强型增量备份”或“如有可能，请使用本机文件系统更改日志提供程序”选项的备份导致备份已备份的文件。

在文件重复数据删除期间，属性 FILE_ATTRIBUTE_REPARSE_POINT 和 FILE_ATTRIBUTE_SPARSE_FILE 将添加到文件中。“增强型增量备份”选项检测更改的属性，文件系统更改日志提供程序则记录修改，从而导致重新备份文件。

原因

此问题的原因未知。

解决方案

无。

设备和介质故障排除

This feature is available in the Express and Premium Editions

备份设备受特定 Data Protector 许可证的约束。有关详细信息，请参阅《Data Protector 产品声明、软件说明和参考》。

本节包含以下故障排除主题:

- 常规设备和介质问题
- ADIC/GRAU DAS 和 STK ACS 库问题
- 云设备问题

常规设备和介质问题

本节包含以下故障排除主题：

介质代理客户机上的 StoreOnce 光纤通道设备不足

备份大量对象或运行多个并发会话时，出现以下错误消息：

|Major| From: BMA@abc.com "DEV_FC_gw2 [GW 23117:0:6931224894398172655]" Time: <DATE> <TIME>

|90:54| \\abcd\FC/75232e10_5322f96a_445f_01b1

Cannot open device (StoreOnce error: StoreOnce device offline, network error occurred or secure communication failed while contacting the StoreOnce device)

原因

介质代理缺少足够数量的 StoreOnce 光纤通道 (FC) 设备。

解决方案

增加介质代理客户机上的可用 FC 设备数量。例如，如果连接 FC 的介质代理只有 16 个 StoreOnce FC 设备可用，当您需要并发备份 200 个对象时，您应将可用 FC 设备的数量增加至 200 或更多，因为 Data Protector 需使用 200 个连接。

要增加介质代理客户机上的可用 FC 设备数量，请执行以下操作：

1. 打开 B6200 StoreOnce 备份系统应用程序。
2. 展开 StoreOnce，然后展开 StoreOnce Catalyst。
3. 在“光纤通道设置”选项卡中，向下滚动至“设备”部分，然后单击编辑。
4. 将每个启动器端口的设备数字段设为所需值（每个端口都需要设置）。

在 Windows 中，您可以在“设备管理器”窗口验证可用的 StoreOnce FC 设备数。请注意，介质代理客户机上的可见设备数等于所有 FC 端口的“每个启动器端口的设备数”值之和。

无法清理分布式文件库

无法从已备份的分布式文件库中导出或删除介质池。

原因

这是因为您无法从使用分布式文件介质格式的文件库导入或导出介质。分布式文件库具有无法导出的磁带和无法删除的池。

解决方案

要清理和删除分布式文件库仓库和池，请按照以下步骤操作。

1. 确保磁盘上存在使用分布式文件介质格式的物理文件仓库。
2. 选择所有使用分布式文件介质格式的文件仓库。
3. 右键单击并单击“回收” 以回收选定的仓库。
4. 右键单击包含分布式文件库仓库的文件库设备，然后单击“属性” 。
5. 在“设置” 选项卡下，取消选择“使用分布式文件介质格式” 选项。
6. 使用此库执行测试备份。
   备份作业会自动清理所有过期的仓库，并以非分布式文件库格式创建新的文件仓库。
7. 回收并导出仓库。
8. 删除文件库，然后删除池。

无法访问 Windows 上的交换器控制设备

当启动诸如介质格式化或扫描这样的设备操作时，将显示以下错误:

Cannot access exchanger control device

原因

Data Protector 使用 SCSI 微型端口驱动程序控制备份驱动器和库。如果在相同系统上加载了其他设备驱动程序，则 Data Protector 可能无法管理设备。

解决方案

在设备驻留的系统上，运行以下命令以列出在系统上配置的所有物理设备:

<Data_Protector_home>\bin\devbra -dev

如果任何 SCSI 地址的状态值为 CLAIMED ，则将由另一个设备驱动程序使用。

禁用 Windows 机械手驱动程序。

SCSI 设备保持锁定，并且会话失败

SCSI 驱动器或机械手控制保持锁定状态。将显示以下消息：

```
Cannot open device
```

如果介质代理失败，则保留的设备将无法释放。Data Protector 可能未能解除 SCSI 驱动器或机械手控件的锁定，因此后续会话无法使用它。

原因

由于 SCSI 保留或释放操作不完整，可能会出现此问题。

解决方案

确保其他应用程序没有使用此设备。要解除 SCSI 驱动器或 SCSI 机械手控件的锁定，设备必须使用循环电源，即需要先关闭设备然后再打开。

设备打开问题

在尝试使用 DDS 设备时，显示以下错误:

Cannot open device (not owner)

原因

如果正在使用与介质识别系统不兼容的介质，则会发生此问题。与 DDS 驱动器一起使用的介质必须符合介质识别系统的要求。

解决方案

确保与 DDS 驱动器一起使用的介质必须符合介质识别系统的要求。

在 Windows 上使用不受支持的 SCSI HBA/FC HBA

由于备份设备使用不受支持的 SCSI HBA/FC HBA，系统失败。

原因

通常情况下，若 SCSI 设备同时被多个介质代理访问，或者设备块大小定义的传输数据的长度大于 SCSI HBA/FC HBA 支持的长度，就会发生此问题。

解决方案

要解决此问题，请修改设备的块大小。

有关修改块大小的更多信息，请参阅设置设备和介质的高级选项。

有关支持的 SCSI HBA/FC HBA 的信息，请参阅支持矩阵。

带库重新配置失败

更改设备列表文件之后，在使用 sanconf 命令修改现有库配置期间报告配置错误。仅创建了部分带库配置。

原因

如果设备列表文件已更改，则会在修改现有库配置的过程中发生此问题。

解决方案

如果在 SAN 环境中重新使用主机列表文件，并再次使用 sanconf 扫描主机，则可以恢复先前的库配置。

1. 扫描单元中的主机：
   sanconf -list_devices mySAN.txt -hostsfile hosts.txt
2. 使用保存的配置文件配带库：
   sanconf -configure mySAN.txt -library LibrarySerialNumberLibraryName [RoboticControlHostName] [DeviceTypeNumber] -hostsfile hosts.txt
   这会自动恢复以前成功的库配置。

如果在之后添加、删除或修改库，且使用 sanconf 命令扫描配置失败，则可以重复上面的过程还原成功配置。

加密介质在读取或写入操作之后标记为低劣

在对使用基于驱动器的加密的介质进行读取或写入操作期间，会话失败，并且介质自动标记为低劣。

显示以下错误：

```
Cannot read from device ([5] I/O error)
```

原因

如果在不支持基于驱动器加密的平台上执行读取或写入操作，则会发生此问题。有关受支持平台的最新列表，请参阅最新支持矩阵。

解决方案

要更正介质状态，请使用以下命令重置介质条件:

```
omnimm -reset_poor_medium
```

有关详细信息，请参阅 omnimm。

使用 Data Protector GUI 和 CLI 创建 null 设备

在诸如 UNIX 的操作系统中，null 设备是丢弃所有写入其中的数据的特殊文件。因此，数据对任何从此文件中读取和立即导致文件结束的处理不可用。但是，有关此写入操作的报告显示为成功。

为了故障诊断，如果不需要实际数据输出，可以根据支持的要求创建 null 设备。本节提供有关使用 Data Protector GUI 和 CLI 创建 null 设备的信息。

解决方案

警告：Null 设备应作为临时解决方案而创建和使用，并在成功完成故障排除操作后删除。否则，如果被生产备份意外使用，该流程将导致立即的数据丢失。

使用 **Data Protector GUI** 创建 **null** 设备
请遵循以下步骤：

1. 在“上下文”列表中，单击“设备和介质”。
2. 在“范围”窗格中，右键单击“设备”，然后单击“添加设备”以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明（可选）。
5. 在“设备类型”列表中，选择“独立”设备类型。
6. 单击“下一步”。
7. 对于 Windows 客户机，为 UNIX 客户机指定 *nul* 或 */dev/null* 作为 SCSI 地址，然后单击“添加”。
8. 单击“下一步”。
9. 在“介质类型”列表中，保留默认值。
10. 对于“默认介质池”，保留默认值。
11. 单击“完成”退出向导。此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。

使用 **CLI** 创建 **null** 设备

使用 Data Protector GUI 创建的 null 设备可以在使用 CLI 的其他系统上进行复制。

omnidownload 命令让您可以显示有关备份设备的信息或将指定备份设备的配置下载到 ASCII 文件。此命令可从 Data Protector 内部数据库 (IDB) 下载有关备份设备和库的信息。该命令在安装 Data Protector 用户界面组件的系统上可用。

通过将 omnidownload 命令和 omniupload 实用程序配合使用，可以使用命令行界面创建和维护备份设备。

omniupload 实用程序将备份设备文件上传到 Data Protector 内部数据库 (IDB)。关于 Data Protector 备份设备的信息存储在 IDB 中。要配置备份设备，您必须通过运行 omnidownload 命令将该设备上的信息下载到文件中。然后您可以修改并将文件上载回 IDB。

有关详细信息，请参阅 Data Protector 命令行界面参考。

请遵循以下步骤：

1. 在使用 Data Protector GUI 创建文件设备之后，使用以下命令列出可用设备:
   omnidownload -list_devices
   该命令可显示有关 Data Protector 备份设备的信息。报告包括每个设备的以下信息：设备名称、客户机、设备类型和介质池。
2. 使用以下 CLI 命令将创建的备份设备的配置下载或导出到 ASCII 文件：
   omnidownload -device BackupDevice [-file FileName]
   例如： omnidownload -device ThisIsNULLDevice -file NULL.dev
   该命令可更新带有所有备份设备配置详细信息的 ASCII 文件或文本文件。例如：

```
NAME "ThisIsNULLDevice"
DESCRIPTION ""
HOST dppvt5140.company.com
POLICY Standalone
TYPE File
POOL "Default File"
ENCRCAPABLE
DRIVES "/dev/null"
DEVSERIAL ""
RESTOREDEVICEPOOL NO
COPYDEVICEPOOL NO
```

> 注意: 确保为 HOST 指定的值是 Cell Manager 中的常规客户机。如果您导出一个 Cell Manager 上的设备并将其导入到一个新的或不同的 Cell Manager，则您必须将 HOST 名称更改为新的介质代理主机，它将是新的 Cell Manager 的一部分。

3. 如果正在使用新的或不同的 Cell Manager，则在 ASCII 或文本文件中修改主机名称，然后使用以下命令将 ASCII 文件上载到系统:
   omniupload -create_device FileName
   例如： omniupload -create_device NULL.dev

各种介质问题

本主题介绍如何解决在使用介质时可能遇到的各种问题。

原因

介质问题可能是由于诸如介质损坏和通信故障之类的问题而发生的。

解决方案

使用介质质量统计功能可以检测介质的早期问题。

在驱动器弹出每个介质之前，Data Protector 使用 SCSI log sense 命令查询介质读取和写入统计信息。将这些信息写到 media.log 文件中。

默认情况下禁用介质质量统计功能。要启用这一功能，请将全局选项 Ob2TapeStatistics 设置为 1。

如果在读取或写入操作期间收到与介质相关的错误，或者介质被标记为较差，可检查 media.log 文件中是否含有介质错误统计信息。

Media.log 包含以下错误统计信息，其中 n 表示错误的数量：

错误统计信息	描述
errsubdel=n	使用重要延迟更正的错误
errposdel=n	使用可能延迟更正的错误
total=n	重新写入的总数
toterrcorr=n	写入时更正和恢复的错误总数
totcorralgproc=n	处理的更正算法总次数
totb=n	处理的总字节数（写入）
totuncorrerr=n	未纠正错误的总数（写入）

如果参数的值为 -1，则设备不支持此统计信息参数。如果所有参数的值均为 -1，则表示在磁带质量统计信息处理期间发生错误，或者设备不支持介质质量统计信息。

对于处理的总字节数，将报告大多数设备的统计结果（以字节为单位）。但是，LTO 和 DDS 设备分别报告数据集和组，而不报告字节。

示例

下面是几个不同设备类型的 media.log 文件的示例。

- DLT/SDLT 设备
- LTO 设备
- DDS 设备

DLT/SDLT 设备

DLT/SDLT 设备的 Log Sense 写入报告 - 处理的总字节数。

```
Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium Label= DLT10; Logical drive= dlt1; Errors corrected no delay= 0; Errors corrected delay= 0; Total= 13639; Total errors corrected= 13639; Total correction algorithm processed= 0; Total bytes processed= 46774780560; Total uncorrected errors= 0
```

处理的压缩后本机数据是 46774780560 字节（一个完整 DLT8000 磁带）。

LTO 设备

LTO 设备的 Log Sense 写入报告 - 处理的总数据集。

```
Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium Label= ULT2; Logical drive=ultrium1; Errors corrected no delay= 0; Errors corrected delay= 0; Total= 0;Total errors corrected= 0; Total correction algorithm processed= 0; Total bytes processed= 47246; Total uncorrected errors= 0
```

一个数据集有 404352 字节。要计算处理的总字节数，请使用以下公式：

```
47246 data sets * 404352 bytes = 19104014592 bytes after compression (a full tape)
```

DDS 设备

DDS 设备的 Log Sense 写入报告 - 处理的总组数。

```
Media ID from tape= 0fa0049f:3df881e9:41f3:0001; Medium Label= Default DDS_5; Logical drive= DDS; Errors corrected no delay= -1; Errors corrected delay= -1; Total= -1; Total errors corrected= 0; Total correction algorithm processed= 154; Total bytes processed= 2244; Total uncorrected errors= 0
```

DDS1/2：一个组是 126632 字节。

DDS3/4: 一个组是 384296 字节。

要计算处理的总字节数，请使用以下公式：

```
2244 groups * 126632 bytes = 284162208 bytes after compression (a 359 MB backup on DDS2)
```

备份了 359 MB 的数据，导致在磁带上有本机数据 271 MB。

介质标头健全检查错误

默认情况下，在从驱动器弹出介质之前，Data Protector 会执行介质标头健全检查。

如果介质标头健全检查检测到介质上存在任何标头一致性错误，则会显示一条错误消息。此介质上的所有对象都将被标记为失败，并且包含此介质中对象的会话的状态也会发生变化。

如果介质标头损坏，则会将受影响介质上的所有对象标记为失败，并将介质标记为低劣。

原因

发生此问题的原因是介质上的标头一致性错误。

解决方案

从 IDB 导出介质，并使用其他介质重新启动失败的会话。

设备序列号问题

执行涉及有问题的备份设备或机械手的任何操作 (例如备份、还原、格式化、扫描等) 时，显示以下错误:

Device DeviceName could not be opened (Serial number has changed).

原因

设备路径指向的设备的序列号与 IDB 中存储的号码不同时，会报告此错误。在以下情况下可能发生此问题：

- 错误地配置了设备 (例如，使用 omniupload 命令，或者配置了错误的设备文件)。
- 替换了物理设备但没有更新相应的逻辑设备（重新加载新序列号）。
- 物理替换了位于 SCSI 带库中的 SCSI 磁带驱动器。没有启用“自动发现更改的 SCSI 地址”选项，或者将 omnirc 选项 OB2MADETECTDRIVESWAP 设置为 0。
- 多路径设备中的路径配置错误。

解决方案

1. 在 Data Protector GUI 中，切换到“设备和介质”上下文。
2. 在范围窗格中，展开“设备”，右键单击有问题的设备，并单击“属性”。
3. 单击“控制”选项卡，并选中“自动发现已更改的 SCSI 地址”。
4. 单击“重新加载”以更新 IDB 中的设备序列号。如果物理替换位于 SCSI 带库中的 SCSI 磁带驱动器，请确保将 omnirc 选项 OB2MADETECTDRIVESWAP 设置为 1 (默认)。不需要重新加载设备序列号。

无法还原或复制损坏的数据

默认情况下，始终在磁带驱动器上检查循环冗余校验 (CRC) 值，并且从不还原或复制发现的由于 CRC 不匹配而损坏的数据。但是，在某些情况下，可能仍要还原或复制此类数据。

原因

这是避免复制损坏的数据的预期行为。

解决方案

如果要还原或复制损坏的数据，请将介质代理主机上的 omnirc 选项 OB2CRCCHECK 临时设置为 0。恢复损坏的对象 (数据) 后，将设置恢复为默认值 1。

与硬件相关的常见问题

解决方案

检查系统和设备之间的 SCSI 通信，例如适配器或 SCSI 线缆及其长度。尝试运行操作系统提供的命令（例如 tar），验证系统和设备是否正在通信。

与 StoreOnce 软件的连接失败

在使用包含多个对象的 StoreOnce 软件的会话中，某些对象会失败并显示以下错误消息:

[Major] From: RMA@hostname.com "soda_gw1 [GW 18437:17:5373994507538143831]" Time: 09/18/2017 01:15:12 PM

[90:54] \\hostname.com\store/0d09310a_59bfa4e3_666d_0012

Cannot open the device.

StoreOnce error: StoreOnce device offline, network error occurred or secure communication failed while contacting the StoreOnce device.

原因

如错误消息中所示，发生此问题是由于以下原因导致:

- StoreOnce 设备脱机
- 网络错误
- 安全通信失败

解决方案

要解决此问题，请在运行 StoreOnce 软件的主机上设置 omnirc 变量 OB2UNSECURE_STOREONCESOFTWARE=1 ，然后重新启动 StoreOnceSoftware 服务。

在数据格式不兼容时不会自动重新格式化自由池介质

备份或还原会话中止，并显示以下警告：

[Warning] From: BSM@cell_manager.com "xtest" Time: 4.4.2014 11:45:41

[60:1023] Medium "200011ac:533e6a06:0134:0001" labeled "[MTV341L4] MTV341L4"

of data format NDMP - Hitachi is not compatible with device "EML-Tape1" of dataformat OB2 - Generic.

原因

如果用户具有用于标准文件系统备份和 NDMP 备份的单独介质池，并且两个介质池共享一个公共的自由池，则会发生此问题。

解决方案

要解决此问题，请将全局参数 CheckNDMPDataFormatType 设置为 1 并再次运行备份或还原会话。

ADIC/GRAU DAS 和 STK ACS 库问题

本节包含以下故障排除方案：

ADIC/GRAU DAS 带库安装失败

ADIC/GRAU DAS 库安装失败。

解决方案

1. 在控制 GRAU 机械手 (PC/robot) 的客户机上安装介质代理。
2. 在连接驱动器 (PC/drive) 的客户机上安装介质代理。
3. 将 aci.dll + winrpc.dll + ezrpcw32.dll 复制到 %SystemRoot%\system32 和 Data_Protector_home\bin 目录。
4. 在 PC/robot 上创建 aci 目录。
5. 将 dasadmin.exe 、 portmapper 和 portinst 复制到 aci 目录。
6. 启动 portinst 以安装 portmapper （仅在 PC/robot 上）。
7. 在 Cell Manager 上安装 mmd 修补程序。
8. 重新启动系统。
9. 在 Windows 的控制面板 > 管理工具 > 服务中，检查 portmapper 和 rpc 服务是否正在运行。
10. 在 OS/2 系统的 GRAU 库中，编辑文件 /das/etc/config 。添加包含 PC/robot 的 IP 地址且名为 OMNIBACK 的客户机。

看不到任何驱动器

解决方案

从 PC/robot 运行以下命令：

1. dasadmin listd
2. dasadmin all DLT7000 UP AMUCLIENT
3. dasadmin mount VOLSER （然后按驱动器上的 UNLOAD 按钮）
4. dasadmin dismount VOLSER 或 dasadmin dismount -d DRIVENAME)

其中：

- AMUCLIENT = OMNIBACK
- VOLSER ，例如 001565
- DRIVENAME ，例如 DLT7001
- all ，代表分配

如果这些命令（与 DAS 服务器 (OS/2) 的通信）不成功，请尝试从 OS/2 系统上的 /das/bin/ directory 运行这些命令。

从 OS/2 系统运行这些命令时，请使用 AMUCLIENT = AMUCLIENT 。

1. 登录到 AMU 客户机。常用的登录是： user: Administrator pwd: administrator user: Supervisor pwd: supervisor
2. 可能需要设置介质类型：设置 ACI_MEDIA_TYPE 设置 ACI_MEDIA_TYPE=DECDLT
3. 重新启动带库：
    1. 关闭 OS/2，然后关闭机械手。
    2. 重新启动 OS/2，在 OS/2 准备好时，AMU 日志将显示机械手尚未准备好。打开机械手。

GRAU CAP 未正确配置

解决方案

只能将介质从 CAP 移动到插槽，然后使用设备机械手移动到驱动器。使用 import 和 export 命令，例如：

import CAP: I01

import CAP range: I01-I03

export CAP: E01

export CAP range: E01-E03

GRAU 和 STK 库上的库操作失败

原因

由于使用 Data Protector uma 实用程序时语法不正确，可能会出现此问题。

解决方案

在使用 uma 实用程序管理 GRAU 和 STK 库驱动器时，请使用以下语法:

uma -pol POLNUMBER -ioctl LIBRARYNAME -type MEDIATYPE

其中 POLNUMBER 对于 GRAU 是 8 ，对于 STK 是 9 。

例如： uma -pol 8 -ioctl grauamu

默认介质类型是 DLT。

云设备问题

本节包含以下故障排除主题:

- 云 (Helion)、云 (Azure) 和云 (Amazon S3 兼容 API) 设备出现通信错误
- 无法启动工作请求
- Amazon S3 Glacier 对象的还原失败

云 (Azure) 和云 (Amazon S3 兼容 API) 设备出现通信错误

云 (Azure) 和 云 (Amazon S3 兼容 API) 设备在与云对象存储通信时遇到错误。如果遇到此类错误，设备将重试操作。

在发生通信错误时，会显示以下消息:

```
与云发生通信错误 [ERROR]，正在重试
```

原因

如果存在网络连接问题，可能会发生此问题。但是，您可以增加云的重试次数，以确保有更多的通信尝试次数。

解决方案

云的默认重试次数是 5 次。

将介质代理主机上的 omnirc 选项 OB2_CLOUDDEV_MAXRETRIES 设置为大于 5 的值。

无法启动工作请求

从 Amazon S3 Glacier 设备还原失败，并显示以下错误:

```
Failed to initiate job request. Failure reason: "UNKNOWN"
```

原因

失败可能是由于以下原因之一:

- 如果使用了加速层策略，则即使多次重试后服务也不可用，这可能是失败的原因。
- 如果使用标准层策略，则检索策略可能是失败的原因。

解决方案

- 如果使用了加速层策略，则通过更改 OB2_CLOUDDEV_MAXRETRIES omnirc 标志来增加重试次数。
- 如果使用了标准层策略，则通过在“设备”选项卡中右键单击选定的设备，从默认的“无检索限制”更改检索策略。

Amazon S3 Glacier 对象的还原失败

还原 14MB 以上的 Amazon S3 Glacier 对象失败。

原因

发生此问题是因为“标准检索策略”设置为“仅自由层”。“仅自由层”每小时提供的数据检索限制为 14MB。

解决方案

将您的数据检索策略设置为“最大检索率”。有关检索允许值计算的更多信息，请参阅 AWS S3 Glacier 文档。

对象复制会话故障诊断

This feature is available in the Express and Premium Editions

本节包含以下故障排除主题:

复制的对象比预期的少

使用备份后或计划的对象副本，匹配所选过滤器的对象数比实际复制的对象数多。

将显示以下消息：

Too many objects match specified filters.

原因

与指定过滤器匹配的对象太多。

解决方案

- 减少对象版本选择的条件。
- 通过设置全局选项 CopyAutomatedMaxObjects ，增加在会话中复制的最大对象数量。

未复制所选库中的全部对象

使用备份后或计划的对象副本，不复制在所选库中的介质上驻留的某些对象。

原因

如果对象在所选库中没有完整的介质集，则会发生此情况。

解决方案

将缺少的介质插入所选库中，或者选择有这些对象的完整介质集的库。

不必要的装载其他介质的请求

当您在交互的对象复制会话中从介质起点选择特定介质时，虽然介质已在设备中可用，但系统仍发出装载其他介质的请求。

原因

如果在介质上驻留的对象跨另一个介质，则会发生此情况。

解决方案

将所需介质插入设备中，并确认装载请求。

当创建对象副本时，保护结束时间会延长

当创建对象副本时，不从原始对象继承保护结束时间。而是复制保护时间长度，但将开始时间设置为对象副本创建时间而不是对象创建时间。这导致保护时间比原始保护时间长。原始备份和对象复制会话之间经过的时间越长，保护结束时间之间的差别就越大。

例如，如果对象在 9 月 5 日创建，保护设置为 14 天，则保护将在 9 月 19 日过期。如果在 9 月 10 日启动对象复制会话，则对象副本保护将在 9 月 24 日过期。

在某些情况下，不希望出现这种行为，必须保留保护结束时间。

解决方案

将全局选项 CopyDataProtectionEndtimeEqualToBackup 设置为 1，可确保对象副本保护结束时间等于备份对象保护结束时间。默认情况下，该选项设置为 0。增加允许文件的最大数。

对象复制/复制会话失败

对象复制/复制会话失败，并显示以下错误:

connection reset by peer

原因

当 Cell Manager 和介质服务器位于两个单独的主机上，并且复制会话管理器 (CSM) 通过传输控制协议 (TCP) 与备份介质代理 (BMA) 交互时，通常会发生此问题。

CSM 将 MSG_STOP 发送到 BMA 以指示会话结束，BMA 响应 MSG_STOP 作为确认。如果存在网络拥塞，则 CSM 无法从 BMA 接收 MSG_STOP，并且 BMA 一旦向 CSM 发送 MSG_STOP，BMA 就会关闭 TCP 套接字端。当 CSM 尝试从 BMA 检索 MSG_STOP 时，BMA 端的 TCP 套接字已经关闭，导致 CSM 端出现 connection reset by peer 错误。

解决方案

设置以下 omnirc 变量:

- OB2SHUTDOWNFLAGS=9
- OB2SHUTDOWNTIMEOUT=X

其中 X 是 BMA 关闭 TCP 套接字端之前等待的时间 (以秒为单位)，从而允许 CSM 从 BMA 读取 MSG_STOP。您可以根据网络运行状况和流量，修改变量 OB2SHUTDOWNTIMEOUT，以增加或减少 BMA 端关闭 TCP 套接字的延迟。

复制包含多个对象的会话时会话停止响应

将会话复制到另一个设备上时，会话停止响应。会话输出提供以下信息：

[正常] 来自: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]" 时间：2013/3/21 9:13:06

已完成介质代理 "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"

原因

已知此问题会在包含介质代理的双 IP 堆栈网络配置中发生。

解决方案

配置 IP 堆栈网络时，在介质代理客户机上的 /etc/hosts 文件中为 IPv6 localhost 地址添加一个单独的条目。

例如，在 hosts 文件中有如下条目：

::1 localhost loopback

要解决此问题，请为 IPv6 地址添加以下行：

::1 ipv6-localhost ipv6-loopback

数据域提升设备上的复制会话无法在重试期间响应中止操作

将会话从一个数据域提升备份设备复制到另一个备份设备时或者当设备的可用流不足时，复制会话将无法在重试期间响应中止操作。

原因

已知当 omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT 设置为 0 时（不受支持）时，此问题将会发生。

此变量定义当数据域提升设备没有足够的流时，复制会话在开始另一重试操作前要等待的时间。如果间隔太长或设置为 0，则会话无法响应中止操作。

DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT 的默认值为 60 秒。

解决方案

确保 omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT 未设置为 0。有关 DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT 的完整说明，请参见 omnirc 文件。

许多时间点的对象整合打开太多的文件

当 Data Protector 打开的文件超过操作系统允许的文件数时，会显示与以下类似的消息：

[重大] 来自：RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time /omni/temp/Cons_Media/AFL1/

0a1109ab54417fab351d15500c6.fd

无法打开设备（[24] 打开的文件太多）

原因

如果启动具有许多时间点的对象合并操作，则 Data Protector 要读取所需的全部介质才能完成操作。这将同时打开所有文件。

解决方案

增加允许文件的最大数。

Linux 系统：

使用系统管理管理器 (SAM) 设置打开文件的最大数：

选择“核心配置”>“可配置参数”，然后选择“操作”>“修改可配置参数”。

在公式/值字段中输入新的 maxfiles_lim 和 maxfiles 值。

在应用新值之后，重新启动计算机。

Solaris 系统：

通过编辑 /etc/system 文件设置打开文件的最大数量。添加以下行：

set rlim_fd_cur=value

set rlim_fd_max=value

在应用新值之后，重新启动计算机。

第二次尝试对象合并至 B2D 设备失败

如果第一次对象合并后执行增量备份，并随后执行第二次对象合并，则操作将会失败。

原因

该操作失败的原因是您在第一个对象合并之后执行了增量备份。

解决方案

要确保第二次合并成功，请在第一次对象合并后执行完整备份。然后再执行增量备份，稍后可能会合并。

内部数据库

This feature is available in the Express and Premium Editions

本节包含以下故障排除主题:

由于丢失目录而出现的问题

无法打开数据库/文件或数据库网络通信错误

当 Data Protector 尝试访问 IDB 时显示以下错误:

- Cannot open database/file
- Database network communication error

原因

如果一个或多个 IDB 数据文件或目录缺失，则会发生此错误。

解决方案

重新安装 IDB 数据文件和目录：

1. 重新安装 Data Protector。
2. 重新启动 Cell Manager。

无法访问 **Cell Manager**

Data Protector GUI 在尝试连接到 Cell Manager 时，显示以下错误消息:

Cannot access the Cell Manager system. (inet is not responding) The Cell Manager host is not reachable or is not up and running or has no Data Protector software installed and configured on it.

原因

如果 Data Protector 临时目录缺失，则会发生此错误。

解决方案

1. 在 Cell Manager 上，关闭 Data Protector GUI。
2. 启动“维护模式”： omnisv -maintenance
3. 在以下位置手动创建 tmp 目录: Windows 系统： Data_Protector_program_data UNIX 系统： /var/opt/omni
4. 退出“维护模式”： omnisv -maintenance -stop
5. 重新启动 Data Protector GUI。

在备份或导入期间出现问题

备份期间文件名未记录到 IDB

在使用 Data Protector 执行备份时，如果存在以下情况，则不会将文件名记录到 IDB。

原因

在以下情况下会发生此问题:

- 已经为备份选择了 No Log 选项。
- IDB 的 DCBF 部分空间用尽，或者 IDB 所在的磁盘空间用尽。将在会话输出中显示一个错误来通知您此情况。

解决方案

- 检查是否已经为备份选定 No Log 选项。
- 检查备份会话的会话消息，了解相关警告和错误。

在 IDB 备份或导入期间 BSM 或 RSM 终止

如果在 IDB 备份或导入会话期间 BSM 或 RSM 终止，则显示以下错误：

IPC Read Error System Error: [10054] Connection reset by peer

原因

在 Data Protector GUI 的“内部数据库”上下文中，会话状态仍标记为 In Progress ，但会话实际未运行。

解决方案

1. 关闭 Data Protector GUI。
2. 执行 omnidbutil -clear 命令，将实际未运行但标记为“正在进行中”的所有会话的状态设置为“失败”。
3. 执行 omnidbutil -show_locked_devs 命令，了解是否有任何设备和介质被 Data Protector 锁定。
4. 如果有，则执行 omnidbutil -free_locked_devs 解除锁定。
5. 重新启动 Data Protector GUI。

在 IDB 备份或导入期间 MMD 终止

如果在 IDB 备份或导入会话期间介质管理后台程序 (MMD) 终止，则显示以下错误：

- Lost connection to MMD
- IPC Read Error System Error: [10054] Connection reset by peer

原因

如果 MMD 服务/进程未运行：

- omnisv -status 命令的输出指示 MMD 服务/进程已关闭。
- 将看到以下内容：Windows 系统：在 Windows 任务管理器中，不显示 Data Protector MMD 进程（mmd.exe）。UNIX 系统：使用 ps -ef | grep omni 命令列出 Data Protector 进程时，不会显示 Data Protector MMD 进程（/opt/omni/lbin/mmd）。

解决方案

1. 关闭 Data Protector GUI。
2. 执行 omnisv -stop 命令以停止 Data Protector 服务/进程。
3. 执行 omnisv -start 命令以启动 Data Protector 服务/进程。
4. 执行 omnisv -status 命令以检查是否正在运行所有服务/进程。

DC 二进制文件损坏或丢失

在 Data Protector GUI 的还原上下文中浏览备份的对象时，显示以下错误：

Open of Detail Catalog Binary File failed

原因

- omnidbcheck -bf 命令报告一个或多个 DC 二进制文件丢失或大小不正确，或者 omnidbcheck -dc 命令报告一个或多个 DC 二进制文件损坏。
- debug.log 上的 Cell Manager 文件包含有关 Data Protector 无法打开 DC 二进制文件的一个或多个条目。

解决方案

通过从介质导入编目重新创建 DC 二进制文件。

有关说明，请参阅《Data Protector 帮助》索引:“DCBF 中的细微 IDB 损坏”。

内部数据库备份失败

用于备份 Data Protector 内部数据库的会话失败，并显示以下错误：

[Critical] From: OB2BAR_POSTGRES_BAR@computer.company.com "DPIDB" Time: 4/2/2013 4:05:20 PM

Error while running the PSQL script

[Normal] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM

OB2BAR application on "computer.company.com" disconnected.

[Critical] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM

None of the Disk Agents completed successfully. Session has failed.

原因

如果 Data Protector Inet 服务正在使用域用户帐户运行，那么问题很可能是由于该帐户的安全策略特权不足导致的。

解决方案

必须对用于 Data Protector Inet 服务的 Windows 域用户帐户授予以下 Windows 操作系统安全策略特权，然后重新启动会话：

- 身份验证后模拟客户机
- 替换进程级别令牌

有关详细信息，请参阅《Data Protector 帮助》索引: “Inet 用户模拟”。

DCBF 段的 DC 二进制文件报告错误

使用恢复的数据库作为新内部数据库执行 IDB 恢复后， omnidbcheck -dc 报告错误。

解决方案

执行放置 IDB 备份对象的介质的导出和重新导入。

IDB 增长问题

IDB 空间用尽

发出了“IDB 空间不足”通知。

原因

IDB 的一部分空间用尽。

解决方案

增加 IDB 的大小。

IDB 的 DCBF 部分增长太快

在 Client Statistics 报告中，写入的数据 [GB] 或文件数的数字对某些系统而言 considerably 过大。

原因

IDB 的 DCBF 部分的大小过大。

解决方案

要减少 IDB 的 DCBF 部分的大小，可在 omnidbutil -purge -dcbf 上运行 Cell Manager 命令，以清除 IDB 中编目保护过期的所有介质的 DCBF。确保在清除会话期间没有运行 Data Protector 会话。

要减少 IDB 的 DCBF 部分的增长，请将日志记录级别更改为日志目录。

pg_log 目录中的日志文件不断增长

减少了用于添加 IDB 数据的磁盘空间。

原因

如果在 <dp_data>/server/db80/pg/pg_log 下创建的日志文件显著增长，则 IDB 备份大小会增加，且用于添加 IDB 数据的磁盘空间减少。

解决方案

删除超过 30 天的文件。有两种方法可以删除这些文件。如下所示:

- 如果日志文件显著增长，则手动删除超过 30 天的文件。
- 通过在 <dp_data>/server/db80/pg/postgresql.conf 中配置以下参数，实现流程自动化:

查看全屏

参数	描述
log_filename = 'postgresql-%d.log'	可以包含 strftime() 转义符。
log_truncate_on_rotation = on	如果打开，与新日志文件同名的现有日志文件将被截断，而不是附加到其中。但是这种截断只发生在时间驱动的循环中，而不发生在重新启动时或大小驱动的循环中。默认值为关闭，意味着在所有情况下都附加到现有文件。
log_rotation_size = 0	在输出大量日志后，日志文件将自动循环。 0 表示禁用。

还原浏览缓慢

当浏览要在 Data Protector GUI 中还原的对象版本和单个文件时，从 IDB 读取和显示信息需要很长时间。

原因

IDB 中的所选对象的对象版本数太大。

解决方案

设置用于浏览还原对象版本的时间间隔：

- 对于特定还原，在“源”页中设置“搜索间隔”选项。
- 全局，对于所有后续还原：
  1. 在“文件”菜单中，单击“首选项”。
  2. 单击“还原”选项卡。
  3. 设置“搜索间隔”选项，并单击“确定”。

IDB 备份失败报告存档日志文件名格式不正确

升级到 Data Protector 9.00 补丁后，IDB 备份失败，并出现以下消息： "The archive log filename format is incorrect."

原因

即使升级后，注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\hpdp-idb\ImagePath 中的 IDB 位置路径仍指向旧 IDB 位置。

解决方案

执行以下步骤：

1. 运行 omnisv stop 。
2. 在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\hpdp-idb\ImagePath 中手动更改 IDB 位置的路径，以指向新恢复的 IDB 位置，因为升级后，注册表中的路径指向原来的 IDB 位置。
3. 运行 omnisv start 。
4. 运行 omnidbutil -set_schema_crc 。

注意: 每个 IDB 体系结构都具有相关的 CRC 文件。更改 IDB 位置（如第 2 步所述）后，您必须修改 CRC 文件，以匹配新 IDB 位置的架构。最后一步创建了与新 IDB 架构匹配的 CRC 文件。

其他问题

进程间通信错误

Data Protector GUI 访问 IDB 时，显示以下错误:

Interprocess communication problem

在 Cell Manager 上，将看到：

Windows 系统：在 Windows 任务管理器中，不显示 Data Protector 进程 dbsm.exe 。

UNIX 系统：使用 ps -ef | grep omni 命令列出 Data Protector 进程时，不显示 /opt/omni/lbin/dbsm 。

原因

发生此错误的原因是 Cell Manager 的数据库会话管理器进程非正常关闭或终止。

解决方案

重新启动 Data Protector GUI。

MMDB 和 CDB 不同步

在 MoM 环境中，由于进行 CMMDB 还原，MMDB 和 CDB 可能不同步。

解决方案

在已安装 CMMDB 的系统上执行以下命令：

```
omnidbutil -cdbsync CellManagerHostname
```

如果 CMMDB 发生更改，可对此 MoM 单元中的每个 Cell Manager 执行此命令，方法是将此单元中的每个 Cell Manager 指定为 *CellManagerHostname* 参数。

IDB 损坏

将显示以下任何消息：

- Database is corrupted.
- Interprocess communication problem.
- Cannot open Database/File.
- Error - Details Unknown.

解决方案

恢复 IDB。

将 MMDB 合并到 CMMDB 失败

在执行 omnidbutil -mergemmdb 命令后，MMDB 到 CMMDB 的合并失败，并显示以下错误消息：

Could not establish connection.

原因

在使用 omnidbutil -mergemmdb 之前，需要启用远程数据库连接。

解决方案

要允许建立连接，请修改配置文件并重新启动服务：

1. 在 MoM 客户机上，导航到默认 Data Protector 内部数据库目录的 pg 子目录。
2. 在文本编辑器中打开 pg_hba.conf 文件，并添加以下行：host hpdpidb hpdpidb_app MoM_Server_IP_Address/32 trust
3. 在 MoM 客户机上重新启动服务： omnisv -stop omnisv -start

在 IDB 恢复期间，会话完成并出现错误

将 IDB 备份到独立设备。执行 IDB 还原时，会话完成但有错误。

升级完成后，修补程序文件被添加到以下位置：

C:\ProgramData\OmniBack\Config\Server\install

例如 patch_CC

此文件由 IDB 备份进行备份。然而，当尝试还原该文件 (覆盖) 时，会收到“Access denied” 错误。

解决方案

如果要将 Data Protector 配置文件还原到原始位置，请执行以下操作：

1. 转至 <dp_data>\Config\Server\install\ 并找到以下文件： patch_CC，patch_CORE，patch_CS，patch_DA，patch_DOC，patch_MA，patch_NETAPP，patch_SMISA，patch_VEPA
2. 对于这些文件，取消选择隐藏的标记选项。
3. 执行 IDB 还原。
4. 重新为上述文件设置隐藏标记。

注意: 该问题仅存在于 Windows CM，因此解决方法仅适用于 Windows。如果将文件还原到其他位置时这些文件已经存在于该位置，可采用相同的解决办法。

PDB Oracle 的时间点恢复失败，并出现错误

在执行 PDB Oracle 的时间点恢复时，显示以下错误：

PLS-00306: wrong number or types of arguments in call to 'GETCNCTSTR'

当执行 PDB 的时间点恢复时，Oracle Bundle 补丁中存在问题。

解决方案

要解决该问题，寻找较新的 Oracle 补丁包或联系/Oracle 支持。

手动中止恢复后，3PAR Oracle ASM IR 恢复失败

如果手动中止 IR ASM Oracle 数据库还原和恢复，重新启动会话失败并出现错误。

解决方案

失败后，装载 ASM 磁盘群并从 RMAN 执行手动恢复。

备份可插拔的数据库失败，并显示错误：可插拔的数据库不存在

显示以下错误：

ORA-65011：可插拔的数据库不存在。

原因

如果从 CDB 删除了 PDB，则会发生此错误。

解决方案

该错误特定于 Oracle。

登录 Oracle 支持页面并搜索错误 ID 18967466。

Bug 18967466 : ALTER DATABASE BEGIN BACKUP" COMMAND FAILS DUE TO ORA-65011 IF PDB HAS BEEN DROPED

Error restoring IDB backup

When you restore an IDB backed up after backing up PostgreSQL, the restore session might fail with the following error message:

```
The OS reported error while accessing C:\ProgramData\OmniBack\config\server\Integ\Config\PostgreSQL\postgresqlmkey.in
```

Cause

This issue occurs because the **postgresqlmkey.in** file created during the PostgreSQL backup specification creation has *readonly* property set.

Solution

Depending on the status of the PostgreSQL backup after restore, do one of the following

- If the PostgreSQL backup works fine after the restore, ignore the error.
- If the PostgreSQL backup fails after the restore, delete the PostgreSQL configruation files and configure the instance again.

使用 GUI 进行 IDB 还原会话失败

使用 GUI 进行 Data Protector IDB 还原会话失败，并显示以下错误消息:

|Critical| From: OB2BAR_POSTGRES_BAR@<hostname> "DPIDB" Time: *<Date><Time>* Copying the file: "" to "" failed

解决方案

使用 Data Protector GUI 进行还原:

1. 删除以下目录中的文件，防止复制旧预写日志 (WAL) 文件: <DP_data>\Config\Server\Integ\Config\idb\ 。
2. 通过 Data Protector GUI 还原内部数据库 (IDB)。

使用 Data Protector CLI 进行还原:

运行以下命令并使用 "-force" 选项:

```
omniofflr -idb -autorecover -force
```

> 注意**:** 对于加密的 IDB 脱机还原，使用 -keyfile 选项。有关此问题的详细信息，请参阅 omniofflr。

由于 NLS 设置不正确而导致报告重复

在执行 Oracle 还原到特定日期时报告错误，然后检查 Oracle 用户的 NLS_LANG 变量的值，以及以下 SQL 命令的输出：

SELECT * FROM NLS_SESSION_PARAMETERS;

SELECT * FROM NLS_INSTANCE_PARAMETERS;

SELECT * FROM NLS_DATABASE_PARAMETERS;

原因

问题可能是由于 NLS_LANG 、 NLS_LANGUAGE 、 NLS_DATE_FORMAT 或 NLS_DATE_LANGUAGE 设置冲突造成的。

解决方案

NLS 设置必须一致。将 NLS_LANG 变量导出为适合数据库中语言或字符集的值。

日志文件中报告了 **PostgreSQL** 错误

由于共享内存问题，日志文件中报告 PostgreSQL 错误。

原因

这些问题是由防病毒程序引起的。

解决方案

禁用防病毒应用程序一段时间，然后查看问题是否已解决。如果禁用防病毒应用程序可以解决该问题，则防病毒供应商可能需要发布补丁，或者可能需要使用其他防病毒软件。

在还原 IDB 时，Data Protector 10.0 之前的客户机无法连接到已恢复的 Cell Manager

在使用混合客户机 (既有版本低于 10.x 的 Data Protector 客户机，也有版本高于 10.x 的 Data Protector 客户机) 备份和卸载 Cell Manager 之后还原 IDB 时，版本低于 10.x 的客户机无法与新 Cell Manager 连接 (重新安装后)。

将 Cell Manager 从 Data Protector 版本 9.x 升级到 10.x 后，混合客户机 (既有版本低于 10.0 的 Data Protector 客户机，也有版本高于 10.0 的 Data Protector 客户机) 继续与 Cell Manager 连接。但在执行 IDB 备份、重新安装 Cell Manager 和还原 IDB 时，Data Protector 10.0 之前的客户机无法连接到新安装的 Cell Manager。

原因

之所以出现这种情况，是因为 Cell Manager 中存在的客户机和所有客户机证书的例外列表不属于备份。

解决方案

要重新建立客户机与 Cell Manager 之间的连接，请执行以下步骤:

1. 确保 Cell Manager 和所有客户机在同一 INET 端口上运行。
2. 运行以下命令：
   - 对于 Data Protector 版本 10.x 的客户机，请运行 omnicc –secure_comm –configure_peer <*client*>
   - 对于 Data Protector 版本 10.x 之前的客户机，请运行 omnicc -secure_comm -configure_for_legacy_client Hostname [-overwrite]

报告和通知

This feature is available in the Express and Premium Editions

本节提供有关对 Data Protector 报告和通知进行故障诊断的信息。

- 发送方法为 Windows 上的电子邮件时，Data Protector GUI 停止响应
- SNMP 发送方法失败

发送方法为 Windows 上的电子邮件时，Data Protector GUI 停止响应

如果您使用安装了最新安全补丁的 Microsoft Outlook XP，则会出现以下问题：将报告添加到将电子邮件指定为发送方法的报告组，然后尝试启动该报告组时，GUI 会停止响应。如果您配置通知并选择电子邮件为发送方法，也会出现相同情况。

原因

发生该问题的原因是 Outlook 发送电子邮件通知前需要用户交互。由于此功能是 Outlook 安全策略的一部分，因此无法禁用此功能。

解决方案

- 如果网络上有可用的 SMTP 服务器，则指定 E-mail (SMTP) 作为发送方法。此方法是建议的电子邮件发送方法。
- 使用 Data Protector CLI 启动报告： omnirpt -report licensing -email email_address 当显示警告询问您是否允许代您发送电子邮件时，单击是以接收报告。有关详细信息，请参阅 Data Protector 产品公告、软件说明和参考。

SNMP 发送方法失败

当作为 SNMP 陷阱发送报告时，该报告未到达目标。

原因

发生这种情况的原因是，使用 SNMP 陷阱发送方法发送的报告超过了已配置的 SNMP 陷阱的最大大小。

解决方案

仅对没有超过配置的 SNMP 陷阱最大大小的报告使用 SNMP 陷阱发送方法。

联机帮助故障排除

This feature is available in the Express and Premium Editions

Data Protector 联机帮助现在是当前发布的整个文档的脱机捆绑包。保留上下文敏感性。除了查看帮助主题之外，您现在还可以浏览整个文档。
Data Protector 帮助由两个部分组成:

- 帮助主题提供概念信息、分步过程和示例。
- 上下文相关帮助是一种动态的且属于帮助的上下文相关部分，讲解了 Data Protector GUI 中的各种屏幕和选项。

帮助采用网页格式 (.html 格式)。

- 单击本地化帮助包目录中的“主页”链接可能无法打开主页
- Internet Explorer: 内容已阻止错误

访问帮助时脚本出错

从 Data Protector GUI 访问上下文相关帮助时，将显示以下递归消息:

An error has occured on the script of this page. Do you want to continue running scripts on this page?

原因

在只有 Internet Explorer 浏览器的系统上发现此问题。Internet Explorer 阻止脚本执行，从而无法显示帮助页面。

解决方案

按照以下步骤解决此问题:

1. 导航到 <Data_Protector_Home>\help\enu\mediawiki\skinjs 并使用文本编辑器打开 VRTemplate.js 。
2. 找到第 290 行，将 myTree 替换为空的单引号，也就是将 data: myTree 更改为 data: ''
3. 保存并关闭文件。

实施此解决方法后，您在访问帮助时仍会看到一条错误消息，但不会发生递归错误。

或者，您可以通过使用启用了脚本的 Internet Explorer 或任何其他浏览器打开 <Data_Protector_Home>\help\enu\dpHelp_CSH.htm 来访问帮助。

单击本地化帮助包目录中的“主页”链接可能无法打开主页

从已本地化的帮助包的目录 (左侧导航栏) 中单击“主页”链接可能不会打开主页。

解决方案

在浏览器的地址栏中手动输入“主页”路径，如下所示:

- 对于法语区域设置: 输入“主页”路径: **file:///<安装文件夹>/OmniBack/Help/FRA/itom/Data_Protector_2020.08/Home/fr.html**
- 对于日文区域设置: 输入“主页”路径: **file:///<安装文件夹>/OmniBack/Help/jpn/itom/Data_Protector_2020.08/Home/ja.html**
- 对于简体中文区域设置: 输入“主页”路径: **file:///<安装文件夹>/OmniBack/Help/chs/itom/Data_Protector_2020.08/Home/zh-cn.html**

Internet Explorer: 内容已阻止错误

This page is still under development. No published version is available at this time.

日志文件

This page is still under development. No published version is available at this time.

联系支持人员

您可以通过支持和服务与 Micro Focus 支持联系。在与客户支持服务联系之前，请确保：

- 已经执行常规检查。请参见常规检查。
- 并已检查适用的用户部分中的故障诊断部分是否已对您的问题进行了描述。
- 您已收集了将发送给客户支持服务的问题的相关数据:问题描述 (包括会话输出，或等效输出，取决于问题类型) 和环境描述。

客户支持服务然后将提供详细说明。可能会要求您：

1. 在调试模式下运行 Data Protector。
2. 准备发送到客户支持服务的生成数据。

以下各节中描述了这些步骤。注意，仅在客户支持服务请求时才需要执行这些过程。

在与支持人员联系之前，请按照以下步骤收集支持人员所需的信息。

调试

仅当支持组织需要调试信息来解决技术问题时才收集这些调试信息。当 Data Protector 在调试模式下运行时，它将创建消耗大量磁盘空间的调试信息。有关执行调试所需的详细级别和环境条件，请咨询支持组织。

启用调试

可以用不同方式在调试模式下启动 Data Protector。有关调试选项，请参阅调试语法。

> **重要说明**当 Data Protector 在调试模式下运行时，将为每个操作生成调试信息。例如，如果在调试模式下启动备份会话，磁带客户机会对在此备份规范中备份的每个客户机提供输出。

> **注意**要在 Windows Server 2012 系统上启用对网络共享备份和还原会话的调试，必须将运行此类会话的操作系统帐户的写入权限分配给文件夹 Data_Protector_program_data\tmp 。

使用 Data Protector GUI

在“文件”菜单中，单击**首选参数**，然后单击**调试**选项卡。指定调试选项，并重新启动 GUI。GUI 将在调试模式下重新启动。

使用 OB2DBG 变量

单元服务器 omnirc 文件

在单元服务器上或特定的客户机上运行调试。

```
OB2DBG=1-200 MA.txt "BMA@computer1.company.com,UMA@computer2.company.com"
```

客户机 omnirc 文件

程序启动时，总是会验证是否在本地设置了一个 omnirc 变量。仅在客户机上以本地方式运行调试。

OB2DBG=1-200 bma.txt "BMA,UMA"

使用 OB2OPTS 变量

可以使用 OB2OPTS 环境变量设置 Data Protector 集成的调试参数。支持代表将指导您如何设置此变量。

要按每个系统更改调试文件的默认位置，请使用 omnirc 选项 OB2DBGDIR 。

调试语法

几乎所有 Data Protector 命令都可以从具有以下语法的其他 -debug 参数开始：

-debug 1-200[,C:n][,T:s][,U] XYZ Progname[@hostname]

其中：

- 1-200 是调试范围。除非有其他说明，否则请指定范围 1-200。将可选参数指定为范围参数的一部分，并用逗号分隔：
  - C:n 将调试文件的大小限制在 n KB。最小值是 4 (4 KB)，默认值是 1024 (1 MB)。有关详细信息，请参阅限制调试的最大大小。
  - T:s 是时间戳分辨率，其中默认值为 1000。

    在某些平台上，毫米分辨率可能不可用。
  - U 是 Unicode 标志。如果指定该标志，则以 Unicode 格式写入 Windows 上的调试文件。
- XYZ 是调试后缀，例如 DBG_01.txt 。
- host 是已打开调试功能的客户机列表。

使用此选项仅在指定的客户机上运行调试。由空格分隔多个客户机。并由引号括住列表，例如： "computer1.company.com computer2.company.com" 。

压缩日志文件

您可以通过在范围后面指定 gz 选项 (1-200,gz)，选择压缩调试日志文件。这样将创建压缩格式而不是纯文本格式的日志。创建的日志将带有 **.gz** 扩展名，您可以使用任何商业工具提取日志文件。

以下限制适用：

- 此功能仅在 CM 平台上受支持。
- 在 Windows VEPA 会话中，CDpSessionLogerSingelton 和 Lotus 组件会忽略 gz 标志，并且不会创建压缩的日志。
- 此功能将不会与循环调试组合搭配使用。
- 调试日志归档在异常终止期间不能使用。

调试选项

- **范围**：1-200 是调试范围。系统指示时，指定扩展范围。将可选参数指定为范围参数的一部分，并用逗号分隔。设置的范围越大，调试文件也越大。确保调试文件存储库中有足够的空间。范围可以拆分。分隔符可以是双引号字符串内的“,”或“空格”。例如，可以使用 -debug "1-99 104-140" debug.txt 。
- **循环调试**：C:n 将调试文件的大小限制在 *n* KB。最小值是 4 (4 KB)，默认值是 1024 (1 MB)。
- **以秒和毫秒为单位的时间戳**：T:s 是时间戳分辨率，接受的值为 0、1 和 1000，其中默认值是 1，1000 表示分辨率为一毫秒，0 表示关闭时间戳。
- **Unicode 格式的调试文件**：U 是 Unicode 标志。如果指定该标志，则以 Unicode 格式写入 Windows 上的调试文件。
- **后缀**：XYZ 是调试后缀，例如 *My_debug.txt*。

> **注意:** 可使用后缀将调试文件重定向到其他目录。目标目录必须存在，并且写入调试的进程的完整路径权限必须正确无误。例如， <DirPath>/My_debug.txt 。

- **程序和主机名**：*select* 是已打开调试功能的客户机列表。使用此选项仅在指定的客户机上运行调试。由空格分隔多个客户机。将列表括在引号内。例如， progname[@hostname] [;progname@[@hostname]] 。

必要的调试文件

常规调试

在大多数情况下，常规调试的范围为 1-200。完整的调试可能较大，具体取决于 DA 和 MA 调试文件。

Veagent 调试日志文件

如果问题与 VEAgent 备份主机相关，则建议采用以下常规设置。在 GUI 的“首选项”->“调试”选项卡中，执行 -debug 1-199 。

如果问题在 VEAgent 内，多余的 BMA 调试信息量可能很大。为了限制调试信息量，建议执行以下操作。

创建一个 VEAgent 备份主机 omnirc 文件或添加以下行：

```
OB2DBG=1-199,240 VM.txt "VEPA_BAR,VEPALIB_VMWARE_EXECUTION_THREAD,VEPALIB_VMWARE,VEPALIB_VMWARE_THREAD"
```

范围 1-199 不够；范围 240 在 vepa_bar 调试文件中添加 omni_cell 内容。如果需要网络详细信息，请使用以下范围：0-199,240-270。

VMware VDDK 日志文件

对于 6.21、7.01 和 8.0 版，如果 vmware 集成失败，vddk 日志文件可揭示关于根本原因的更多信息。要在 VEagent 备份主机上启用，请转到

C:\ProgramData\OmniBack\Config\client 。或在 linux 上，转到 /etc/opt/omni/client 。编辑文件 *vepa_vddk.config* ，并将 LogLevel 更改为最高值 6。

VMware 详尽传输日志

要启用详尽调试，必须更新 **vepa_vddk.config** 文件。此文件位于 Vepa 备份主机的 /etc/opt/omni/client 或 C:\ProgramData\OmniBack\Config\client 下面。编辑文件，使用日志级别 6。要从 VMware 收集详尽输出，应该为 VEAgent 启用调试。传输日志使用 VEPALIB_VMWARE_EXECUTION_THREAD 文件中的已执行命令进行隔行处理。

VMware 日志文件

管理代理 (hostd)、VirtualCenter 代理服务 (vpxa) 和 VirtualCenter (vpxd) 日志会自动轮换和维护，以管理其增长。如果日志的轮换速度过快，日志中的信息可能会丢失。有关详细信息，请参阅 http://kb.vmware.com/kb/1001457。

VMware ESX(i) 日志文件

Esx(i) 主机具有所有已执行活动（例如快照创建、删除等等）的日志文件。这些日志文件是以 hostd 开头的文本文件，并且在写满后压缩为 zip 包。hostd.log 是活动日志文件。这些文件位于数据存储上（例如 /var/log ->/scratch/log->/vmfs/volumes/4e265cdb-6b91f4b2-bc38-e4115b13545a/log ）。

vCenter Server 详尽日志文件

通常通过导航到“管理”>“vCenter Server 设置”>“日志记录选项”>“详尽”来启用详尽级别日志记录。

Windows 崩溃时的 Vepa_bar localdump

请参阅 http://msdn.microsoft.com/en-us/library/windows/desktop/bb787181%28v=vs.85%29.aspx。编辑注册表，并在 LocalDumps 下面添加 *vepa_bar.exe*。

介质代理调试

有关介质代理特定的问题，可应用以下一般准则：

- 1-200 用于最常见的情形
- 19
- 1-300 用于 SHMIPC
- 1-350 用于合并
- 1-505 用于内存跟踪

限制调试的最大大小

Data Protector 可以在名为循环调试的特殊调试模式中运行。在此模式中，可以添加调试消息，直到调试文件的大小达到预设大小 (*n*) 为止。然后重置计数器，并覆盖最早的调试消息。这可以限制调试文件的大小，但不会影响最新的记录。

仅在以下情况下才建议使用此模式：在会话接近结束时发生问题，或者 Data Protector 在发生问题之后不久终止或完成。

打开循环调试后，估计需要的最大磁盘空间如下：

系统	需要的最大磁盘空间
介质代理客户机	在备份或还原会话中，每个运行的介质代理都需要 2**n* [kB]
磁带客户机客户	在备份或还原会话中，每个装载点需要 2**n* [KB]
Cell Manager	2**n* [kB]
集成客户机	2**n* [kB] * *并行*

对于 Inet 和 CRS 调试，由于为各种操作生成单独的调试文件，因此无法可靠地确定上限。

调试文件的名称和位置

调试后缀选项用于在默认的 Data Protector 临时文件目录中创建调试文件：

在 Windows 系统上: Data_Protector_program_data\tmp

UNIX 系统： /tmp

文件名为

```
OB2DBG_DID__Program_Host_PID_XYZ
```

其中：

- DID （调试 ID）是接受调试参数的第一个进程的进程 ID。这是调试会话的 ID，并由所有后续进程使用。
- Program 是写入调试文件的 Data Protector 程序的代码名称。
- Host 是在其中创建调试文件的客户机。
- PID 是进程 ID。
- XYZ 是在 -debug 参数中指定的后缀。

一旦确定备份或还原会话 ID SID ，会将其添加到文件名：

OB2DBG_DID_SID_Program_Host_PID_XYZ

添加 SID 的进程是由会话启动的 BMA/RMA、xBDA/xRDA 和其他进程，但不是由 BSM/RSM 本身启动。

> **注意**会话 ID 帮助标识调试文件集。其他调试文件可能属于同一会话，可能同样需要提供它们。

ctrace.log 文件在 Cell Manager 上生成，其中包含调试文件在何处（在哪些客户机）生成和使用哪些调试前缀的信息。注意，此文件不包含所有生成文件的完整列表。

要按每个系统更改调试文件的默认位置，请使用 omnirc 选项 OB2DBGDIR 。

调试 Inet

> **注意** Inet 是 Windows 平台上的一项服务，要使 omnirc 条目生效，必须重新启动该服务：(sc stop OmniInet && sc start OmniInet)。

要仅启用 inet 调试，请修改 inet 客户机上的 .omnirc 文件:

a) 要仅启用 inet 调试: OB2DBG=1-200 inet.txt INET,INET-THREAD

b) 要启用所有调试： OB2DBG=1-200 all.txt

调试 CRS

Windows 系统：

<Data Protector bin>\crs -redebug <range><postfix><select>

UNIX 系统：

<Data Protector lbin>/crs -redebug <range><postfix><select>

> **警告**不要从 Windows 服务控制管理器停止 CRS，因为这会导致 Data Protector 群集组故障转移。

Serviceguard/Symantec Veritas 群集服务器环境:

1. 要开始调试： crs -debug <ranges><postfix> [<select>]，或在启动 CRS 之前将 OB2DBG 置于 omnirc 文件中。
2. 要停止调试： /opt/omni/lbin/crs -redebug
3. 要重新启动调试： crs -redebug <ranges><postfix> [<select>]

调试 AppServer

查看详细的 AppServer 日志

默认情况下，AppServer 日志会显示 warn 级别的消息。要查看详细的 AppServer 日志，请按以下代码所示，修改 standalone.xml 文件中的 level name 参数：

```
<size-rotating-file-handler name="DP_LOGGER" autoflush="true">
```

```
<level name="ALL"/>
    <formatter>
    <pattern-formatter pattern="%d{HH:mm:ss,SSS} %-5p [%C{1}:%L:%t] %s%E%n"/>
    </formatter>
    <file relative-to="jboss.server.log.dir" path="DPServer.log"/>
    <rotate-size value="10M"/>
    <max-backup-index value="5"/>
    <append value="true"/>
    </size-rotating-file-handler>
```

在 standalone.xml 文件中进行任何更改后，重新启动 AppServer。

查看详细的 WildFly 日志

要查看详细的 WildFly 日志，请将 <level name> 参数添加到 standalone.xml 文件的 <root logger> 标记之前。添加该参数后，standalone.xml 中的代码必须显示如下：

```
<logger category="org.jboss.as">
    <level name="ALL" />
</logger>
<root-logger>
    <handlers>
    <handler name="CONSOLE"/>
    <handler name="FILE"/>
    </handlers>
</root-logger>
```

在 standalone.xml 文件中进行任何更改后，重新启动 AppServer。

启用 WildFly 数据源的统计信息

打开 standalone.xml 文件，并将属性 statistics-enabled="true" 添加到数据源定义中，如下所示:

```
<datasource jta="true" jndi-name="java:jboss/datasources/HPJobControlEngineDS" pool-name="HPJobControlEngineDS" use-ccm="true" statistics-enabled="true">
<datasource jta="true" jndi-name="java:jboss/IDBPostgreSQLDS" pool-name="IDBPostgreSQLDS_Pool" use-java-context="true" use-ccm="true" statistics-enabled="true">
<datasource jta="false" jndi-name="java:jboss/datasources/HPJobControlEngineQuartzDS" pool-name="HPJobControlEngineQuartzDS" use-ccm="true" statistics-enabled="true">
```

在 standalone.xml 文件中进行任何更改后，重新启动 AppServer。

可以在 Microsoft 管理控制台 (MMC) 中查看统计信息。选择服务器: “独立服务器”>“监视器”: “子系统”>“子系统”: 要查看数据的数据源。

调试调度程序和缺失的作业执行

要调试调度程序和缺失作业执行，请查看应用程序服务器日志。

打开 server.log ，然后查看输出以了解更多信息、错误代码和错误消息。

有关详细信息，请参见日志文件的位置。

准备发送到客户支持的生成数据

客户支持服务可能要求您收集并向他们发送解决技术问题所需的数据。由于 Data Protector 在大型网络环境中操作，收集数据有时可能比较困难。Data Protector omnidlc 命令是用于收集和打包日志、调试和 getinfo 文件的工具。如果客户支持服务要求使用，则使用此命令。

可以从 Data Protector CLI 或 Data Protector GUI 中运行 omnidlc 命令。本节对这两种方法均将进行了说明。

> **注意**不可将 omnidlc 命令用于收集 Data Protector 安装执行跟踪。有关如何创建和收集这些跟踪的详细信息，请参阅“Data Protector 安装”一节。

- omnidlc 命令
- 使用 omnidlc 命令处理调试文件
- 使用 Data Protector GUI 处理调试文件

omnidlc 命令

在生成 Data Protector 调试数据之后，可以使用 omnidlc 命令从 Data Protector 单元 (默认情况下从每个客户机) 收集 Data Protector 调试、日志和 getinfo 文件。此命令将数据从选择的客户机传输到 Cell Manager，然后将其打包。

该命令还可以有选择地收集数据，例如，仅收集来自某个客户机的日志文件，或仅收集在特定 Data Protector 会话期间创建的调试文件。

> **注意**在作为备份后会话的一部分计划对象整合时，备份和整合会话会获得不同会话 ID。但是，调试 ID 对于备份和整合是相同的。在这种情况下，如果运行 omnidlc 命令并使用 -session 参数指定整合会话 ID，则同时为备份和整合收集调试信息。

限制

- 此命令只能在 Cell Manager 上运行。
- 在 MoM 环境中，通过从各自 Cell Manager 运行该命令，只能单独收集每个 Data Protector 单元的数据。
- 如果从默认目录移动了调试文件，请使用 -debug_loc Directory1 选项指定新位置。否则，不会收集调试文件。
- 在 HP OpenVMS 上使用调试和日志文件收集器时，会有以下限制：
- ** OpenVMS ODS-2 磁盘结构文件名最多可以包含 39 个字符。
  - OpenVMS 系统没有 get_info 实用程序，因此 get_info.out 文件为空白文件，不会进行收集。
  - 运行 omnidlc 命令（通过 -session 选项）时，不会收集在指定会话期间产生的调试文件，因为会话名称不是 OpenVMS 调试文件名的一部分。而会收集所有可用日志。

使用 omnidlc 命令处理调试文件

包括以下部分:

- omnidlc 命令语法
- 限制收集的数据的作用域
- 数据的分段
- 对收集的数据禁用压缩
- 保存打包的数据
- 保存解包的数据
- 估计所需空间
- 删除客户机上的调试文件
- 对 Cell Manager 上的遥测文件进行打包
- 删除有关调试文件的信息
- 问题和解决办法

- 其他操作

限制收集的数据的作用域

要限制收集的数据的作用域，请使用以下 omnidlc 命令选项：

{-session SessionID | -did DebugID | -postfix String | -no_filter} [-hosts List] [-no_getinfo] [-no_config] [-no_logs] [-no_debugs] [-debug_loc Directory1 [Directory2]...]

可以组合以下功能：

- 要仅从所选客户机收集数据，请使用 -hosts List 选项。指定客户机的名称（由空格分隔）。

  在群集环境中，使用 -hosts 选项指定群集节点。如果不使用此选项，则仅从活动节点收集数据。
- 要从收集的数据中排除 getinfo、配置信息、日志或调试日志文件，请分别使用 -no_getinfo 、 -no_config, -no_logs 或 -no_debugs 选项。请注意， -no_getinfo 不适用于 HP OpenVMS 系统。
- 要仅从特定会话收集调试文件，请使用 -session SessionID 选项。注意，在 OpenVMS 上，将收集所有可用日志。
- 要收集匹配特定调试 ID 的调试文件，请使用 -did DebugID 选项。
- 要收集与特定后缀匹配的调试文件，请使用 -postfix String 选项。
- 要收集所有调试文件，请使用 -no_filter 选项。
- 要同时从默认调试文件目录和其他目录收集调试文件，请使用 -debug_loc Directory1[Directory2]... 选项。注意，在搜索中不包括子目录。如果特定客户机上不存在指定的目录，则忽略该目录。

数据的分段

如果要发送到 Cell Manager 的文件大于 2 GB，该文件会被拆分为 2 GB 的区块。为每个区块附加一个 s001 到 s999 之间的扩展名。如果压缩文件，则添加第二个扩展名 (.gz)。

在 Cell Manager 侧，如果收集的所有压缩或未压缩文件的大小超过 2 GB，则将收集的文件打包到 2 GB 的包内，并添加一个 s001 到 s999 。

对收集的数据禁用压缩

默认情况下，收集的数据在发送到 Cell Manager 之前会被压缩。要禁用压缩，请使用 -no_compress 选项。

保存打包的数据

默认情况下，通过网络将数据发送到 Cell Manager，并在当前目录中将其打包并另存为 dlc.pck 。

打包的文件包括一个生成的目录结构，其中包括所涉及客户机的主机名、路径以及收集的文件。

限制

- 产生的打包文件的大小不能超过 2 GB。否则，不要打包数据。

使用 -pack Filename 选项可以打包和保存数据：

- 使用不同的文件名。将 Filename 指定为文件名。
- 在不同目录中和使用不同的文件名。将 Filename 指定为完整路径名。

保存解包的数据

要将数据保持解包状态并保存，请使用 -depot [Directory] 选项。文件将收集到 dlc 子目录中。如果未指定 Directory ，则文件保存在 Cell Manager 上的默认 Data Protector 临时文件目录的 dlc 目录中。

打包或解包文件的目录按如下方式生成：

./dlc/client_1/tmp/debug_files

./dlc/client_1/log/log_files

./dlc/client_1/getinfo/get_info.txt

./dlc/client_2/tmp/debug_files

./dlc/client_2/log/log_files

./dlc/client_2/getinfo/get_info.txt

...

估计所需空间

要显示 Cell Manager 上收集数据所需的磁盘空间容量，请使用 -space 选项。

删除客户机上的调试文件

要在客户机上删除收集的数据，请使用 -delete_dbg 选项。注意，仅删除调试文件；不会删除 getinfo 和日志文件。在 HP OpenVMS 上，如果运行时带 -session 选项， omnidlc 命令则不会从调试文件目录中删除任何调试信息。

删除有关调试文件的信息

要删除 ctrace.log 文件，其中包含生成调试日志的位置（在哪些客户机上）以及所用的调试前缀的相关信息，请使用 -del_ctracelog 选项。请注意，如果与 -hosts List 选项一起使用，则该命令仅删除指定客户机上的 ctrace.log 文件。否则，将删除一个单元中所有客户机上的 ctrace.log 文件。

> **注意**使用此选项可进行 ctrace.log 文件清理。注意，如果删除了此文件，则调试日志收集器将仅从默认 Data Protector 临时文件目录中的默认 dlc 目录而非其他指定的调试目录获取调试信息。

问题和解决办法

调试日志收集失败

问题
在调试日志收集操作期间， omnidlc 无法连接到客户机。显示以下错误： Collection from client1.company.com started. Error: Data retrieval from client1.company.com failed. Warning: Collection from client1.company.com incomplete. 当客户机上的配置文件中指定的 Cell Manager 名称与请求调试记录收集的单元管理器的名称不匹配时，会发生此问题。
操作
将 Cell Manager 主机名添加到位于默认的 Data Protector 客户机配置目录下的 omnidlc_hosts 文件中。

其他操作

- 要打包使用 -depot 选项发送到 Cell Manager 的未打包数据（压缩或未压缩），请使用 -localpack [Filename] 选项。

  此选项打包当前目录的目录结构（目录中必须包含 dlc 目录（由 -depot 选项生成））。如果不指定 Filename 参数，则在当前目录中创建文件 dlc.pck。

  此选项等同于 -pack 选项，但仅应在使用 -depot 选项收集数据时使用。
- 要从客户机上的指定目录获取其他信息（例如屏幕截图、图片及类似内容），请使用 -add_info [-any | Host] Path 选项。

  当所有客户机的目录路径都相同时，请使用 -any 选项。
- 要对数据进行解包，请使用 -unpack [Filename] 选项。

  如果不指定 Filename 参数，则对当前目录中的 dlc.pck 文件进行解包。数据始终被解包到当前目录中的 dlc 目录。

  当使用 -pack 或 -localpack 选项在 Cell Manager 上打包收集的数据时，请使用此选项。
- 要解压缩单个压缩文件，请使用 -uncompress Filename 选项。必须首先解包打包的数据。

- 要启用详细输出，请使用 -verbose 选项。

使用 Data Protector GUI 处理调试文件

在调试会话期间，可以生成以下类型的文件：调试、日志和 getinfo

可以在 Data Protector GUI 中执行以下调试文件操作：

- 调用调试文件操作

  可以从 Data Protector GUI 中的不同位置开始调试文件操作。

- 收集调试文件

  从客户机系统收集调试文件，并存储在 Cell Manager 中。

- 计算调试文件空间

  计算 Cell Manager 中存储收集的文件所需的空间。

- 删除调试文件

  从客户机系统中删除调试文件。

这些文件可以从**内部数据库**上下文或**客户机**上下文中进行调用。

GUI 操作使用 omnidlc 命令的各种选项。在命令行界面中可直接使用 omnidlc 命令对所收集的文件执行其他操作。有关详细信息，请参阅使用 omnidlc 命令处理调试文件或《Data Protector 命令行界面参考》。

执行以下章节中的任意操作时，可以在**结果**窗口中看到所使用的 omnidlc 语法。

调用调试文件操作

要从**客户机**上下文中访问调试文件操作：

1. 在“范围窗格”中，展开**客户机**文件夹，选择需要执行调试文件操作的客户机。
2. 选择要执行的操作：
   - 右键单击选择项，并选择所需的操作：**收集调试文件**、**计算调试文件空间**或**删除调试文件**。

     或

   - 在菜单栏中依次选择**操作 -> 调试文件**、**收集**、**检查空间**或**删除**

要从**内部数据库**上下文中访问调试文件操作，请执行以下操作：

1. 在“范围窗格”中，展开**会话**文件夹，选择需要执行调试文件操作的会话。
2. 选择要执行的操作：
   - 右键单击选择项，并选择所需的操作：**收集调试文件**、**计算调试文件空间**或**删除调试文件**。

     或

   - 在菜单栏中依次选择**操作 -> 调试文件**、**收集**、**检查空间**或**删除**。

在每个示例中，选择一个操作可启动一个向导，引导您完成所有所需的步骤。

启动/停止 MMD 调试，不重新启动服务

1. 若要启动 MMD 调试，请在 MMD 运行时运行以下命令：

   mmd.exe -redebug [ranges] [postfix] [select]

2. 如要停止 MMD 调试，请在 MMD 运行时运行以下命令：

   mmd.exe -stopdebug

收集调试文件

要收集调试文件，请执行以下操作：

1. 根据调用调试文件操作中的说明启动“调试文件收集器”向导。

   如果通过选择会话从“内部数据库”上下文中启动，则将在该向导客户机页面的筛选器部分预选择会话，并选择会话中涉及的客户机。

如果从“客户机”上下文启动，则将在该向导客户机页面中预选择在此处所选的客户机。

2. 在“客户机”页中，限制所涉及的客户机：
   a. 仅选择要在其上收集文件的客户机。如果预选了客户机，则可以取消选择其中的任意客户机。
   b. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要检查调试文件的任何其他目录，然后单击**添加**。
   b. 在目录树中，选择任何其他要收集其内容的目录（不收集子目录的内容）。
   c. 单击“下一步”。
4. 在“选项”和“操作”页中：
   a. 取消选择任何不想使用的调试收集选项。有关 omnidlc 选项的信息，请参阅《Data Protector 命令行界面参考》。
   b. 可以指定多个用来收集调试日志的过滤器选项。可用的过滤器选项如下：
      - 会话 ID：生成调试文件所用于的备份会话。
      - 调试 ID：已为其生成调试文件的备份会话。
      - 后缀：调试文件名。
      - 模块：需要使用其调试日志的模块。可以输入多个模块，模块之间用逗号分隔。示例：BSM、BDSM、VBDA。
   c. 选择将调试文件存储在 Cell Manager 上所用的操作：
      - **创建仓库**将文件（未打包）存储在默认 Data Protector 临时文件目录的 dlc 子目录中。

        要指定备用位置，请在**目标路径**中输入现有目录。如果要使用默认位置，请确保文本框清晰。

        您可以使用此选项查看收集的文件，还可以在发送信息之前删除其中的任意文件。之后，可以使用 CLI 命令 omnidlc -localpack [Filename] 创建打包文件 (有关详细信息，请参阅《Data Protector 命令行界面参考》)。
      - **创建打包文件**创建包含已收集文件的打包文件。

        在**目标路径**中指定该文件的全路径。
   d. 单击**完成**。

计算调试文件空间

在实际执行收集操作之前，可以先计算 Cell Manager 上用于存储调试文件收集所需的总空间大小，方法是在“调试文件空间计算”向导中输入所有所需的收集信息。在执行计算之后，可以选择使用指定条件启动收集。

要计算 Cell Manager 上用于存储调试文件集所需的总空间大小，请执行以下操作：

1. 根据调用调试文件操作中的说明启动“调试文件空间计算”向导。
2. 在“客户机”页中，限制所涉及的客户机：
   a. 仅选择要在其上收集文件的客户机。如果预选了客户机，则可以取消选择其中的任意客户机。
   b. 在**过滤器**中，选择过滤器标准：**会话 ID**、**调试 ID**、**后缀**或**无过滤器**，并输入所需的标识符。如果选择**无过滤器**，则将收集所选客户机上的所有调试文件。如果为您预选了会话，则无法对其进行更改。
   c. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要检查调试文件的任何其他目录，然后单击**添加**。
   b. 在目录树中，选择任何其他要收集其内容的目录（不收集子目录的内容）。
   c. 单击“下一步”。
4. 在“选项”页中：
   a. 取消选择任何不想使用的调试收集选项。有关 omnidlc 选项的信息，请参阅《Data Protector 命令行界面参考》。
   b. 单击“下一步”。

检查的结果即显示在**结果**选项卡中。

计算完成后，将显示一个对话框，询问您是否要启动调试文件收集。

要使用选择用于空间计算的选项启动调试文件收集，请执行以下操作：

- 单击**是**。

  将在 Cell Manager 上使用默认操作行为（创建打包文件）。请参见收集调试文件(C)。

删除调试文件

要从客户机中删除调试文件：

1. 根据调用调试文件操作中的说明启动“删除调试文件”向导。
2. 在“客户机”页中，限制要删除的文件：
   a. 仅选择要从中删除文件的客户机。
   b. 在**过滤器**中，选择过滤器标准：**会话 ID**、**调试 ID**、**后缀**或**无过滤器**，并输入所需的标识符。
      如果选择**无过滤器**，则将删除所选客户机上的所有调试文件。
   c. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要从中删除调试文件的其他目录，然后单击**添加**。
   b. 单击**完成**。

使用 omnidlc 命令的示例

1. 要使用详细输出收集并压缩单元中的所有调试、日志和 getinfo 文件，并将它们打包到 dlc.pck 上当前目录下的 Cell Manager 文件中，请运行:

   omnidlc -no_filter -verbose

2. 要只收集客户机 client1.company.com 和 client2.company.com 中的日志和调试文件，并将其存储到 Cell Manager 上的目录 c:\depot 下而不压缩和打包文件，请运行:

   omnidlc -no_filter -hosts client1.company.com client2.company.com -depot c:\depot -no_getinfo -no_compress

3. 要从客户机 client1.company.com 中收集日志、调试和 getinfo 文件，并将其压缩和打包到 c:\pack\pack.pck 上的文件 Cell Manager 中，请运行:

   omnidlc -hosts client1.company.com -pack c:\pack\pack.pck

4. 要从客户机 client1.company.com 和 client2.company.com 的默认位置收集日志、调试和 getinfo 文件并从其他目录 (C:\tmp 和 /temp/debugs) 调试文件，且在 Cell Manager 上压缩和打包文件，请运行:

   omnidlc -hosts client1.company.com client2.company.com -debug_loc C:\tmp /tmp/debugs

5. 要删除 ID 为 2012/02/16-11 的会话的所有调试文件，请运行：

   omnidlc -session 2012/02/16-11 -delete_dbg

6. 对于来自客户机 client.company.com 且调试 ID 为 2351 的解压缩调试文件，要在 Cell Manager 上显示所需的磁盘空间，请运行:

   omnidlc -did 2351 -hosts client.company.com -space -no_getinfo -no_logs -no_compress

7. 要将位于客户机 client1.company.com 的 C:\debug 目录中的其他文件与 ID 为 2012/02/12-24 的会话的调试日志文件打包在一起，请运行:

   omnidlc -session 2012/02/12-24 -add_info -host client1.company.com C:\debug

8. 要将当前目录 (必须为包含由 -depot 选项生成的 dlc 目录的目录) 中的目录结构打包到同一目录下的 dlc.pck 文件中，请运行:

   omnidlc -localpack

9. 要将 dlc.pck 文件解压到当前目录的 dlc 目录下，请运行：

   omnidlc -unpack

收集主页上下文的调试信息

如果遇到主页上下文问题，请完成以下步骤以收集信息以获取支持：

1. 在“主页”上下文中，右键单击结果区域中的任意位置，然后选择“检查”。此时将显示“开发人员工具”对话框。
2. 从菜单栏中选择“网络”标签。
3. 最小化“开发人员工具”对话框，并在“主页”上下文中重现该问题。
4. 最大化“开发人员工具”，然后单击红色的“停止录制网络日志”按钮。
5. 右键单击记录的任何 HTTP 请求，然后选择“复制”>>“全部复制为 HAR”。
6. 打开任何文本编辑器（例如记事本），然后将复制的信息粘贴到新文档中。
7. 将信息另存为“network-trace.har”并将其发送给支持部门。

使用 Data Protector GUI 进行调试

在调试会话期间，可以生成以下类型的文件：调试、日志和 getinfo。

可以在 Data Protector GUI 中执行以下调试文件操作：

- 调用调试文件操作

  可以从 Data Protector GUI 中的不同位置开始调试文件操作。

- 收集调试文件

  从客户机系统收集调试文件，并存储在 Cell Manager 中。

- 计算调试文件空间

  计算 Cell Manager 中存储收集的文件所需的空间。

- 删除调试文件

  从客户机系统中删除调试文件。

这些文件可以从**内部数据库**上下文或**客户机**上下文中进行调用。

GUI 操作使用 omnidlc 命令的各种选项。在命令行界面中可直接使用 omnidlc 命令对所收集的文件执行其他操作。有关详细信息，请参阅在 CLI 中使用 omnidlc 命令处理调试文件或《Data Protector 命令行界面参考》。

执行以下章节中的任意操作时，可以在**结果**窗口中看到所使用的 omnidlc 语法。

调用调试文件操作

要从**内部数据库**上下文中访问调试文件操作，请执行以下操作：

1. 在“范围窗格”中，展开**会话**文件夹，选择需要执行调试文件操作的会话。
2. 选择要执行的操作：
   - 右键单击选择项，并选择所需的操作：**收集调试文件**、**计算调试文件空间**或**删除调试文件**。

     或
   - 在菜单栏中依次选择**操作 - 调试文件**、**收集**、**检查空间**或**删除**。

要从客户机上下文中访问调试文件操作：

1. 在“范围窗格”中，展开**客户机**文件夹，选择需要执行调试文件操作的客户机。
2. 选择要执行的操作：
   - 右键单击选择项，并选择所需的操作：**收集调试文件**、**计算调试文件空间**或**删除调试文件**。

     或
   - 在菜单栏中依次选择**操作 - 调试文件**、**收集**、**检查空间**或**删除**。

在每个示例中，选择一个操作可启动一个向导，引导您完成所有所需的步骤。

收集调试文件

1. 根据调用调试文件操作中的说明启动“调试文件收集器”向导。

   如果通过选择会话从“内部数据库”上下文中启动，则将在该向导客户机页面的筛选器部分预选择会话，并选择会话中涉及的客户机。

   如果从“客户机”上下文启动，则将在该向导的“客户机”面板中预选择此处所选的客户机。
2. 在“客户机”页中，限制所涉及的客户机：
   a. 仅选择要在其上收集文件的客户机。如果预选了客户机，则可以取消选择其中的任意客户机。
   b. 在**过滤器**中，选择过滤器标准：**会话 ID**、**调试 ID**、**后缀**或**无过滤器**，并输入所需的标识符。如果选择**无过滤器**，则将收集所选客户机上的所有调试文件。如果为您预选了会话 ID，则无法对其进行更改。
   c. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要检查调试文件的任何其他目录，然后单击**添加**。
   b. 在目录树中，选择任何其他要收集其内容的目录（不收集子目录的内容）。
   c. 单击“下一步”。
4. 在“选项”和“操作”页中：
   a. 取消选择任何不想使用的调试收集选项。首次打开时，所选内容与 omnidlc 命令所用的标准默认设置匹配。有关它们的信息，请参阅《Data Protector 命令行界面参考》。

b. 选择将调试文件存储在 Cell Manager 上所用的操作：

- **创建仓库**可将文件未打包）存储在默认 Data Protector 临时文件目录的 dlc 子目录中。

  要指定备用位置，请在**目标路径**中输入现有目录。如果要使用默认位置，请确保文本框清晰。

  您可以使用此选项查看收集的文件，还可以在发送信息之前删除其中的任意文件。随后可以使用 CLI 命令 omnidlc -localpack [file name] 创建打包文件 (有关详细信息，请参阅《Data Protector 命令行界面参考》)。

- **创建打包文件**创建包含已收集文件的打包文件。

  在**目标路径**中指定该文件的全路径。

c. 单击**完成**。

计算调试文件空间

在实际执行收集操作之前，可以先计算 Cell Manager 上用于存储调试文件收集所需的总空间大小，方法是在“调试文件空间计算”向导中输入所有所需的收集信息。在执行计算之后，可以选择使用指定条件启动收集。

要计算 Cell Manager 上用于存储调试文件集所需的总空间大小，请执行以下操作：

1. 根据调用调试文件操作中的说明启动“调试文件空间计算”向导。
2. 在“客户机”页中，限制所涉及的客户机：
   a. 仅选择要在其上收集文件的客户机。如果预选了客户机，则可以取消选择其中的任意客户机。
   b. 在**过滤器**中，选择过滤器标准：**会话 ID**、**调试 ID**、**后缀**或**无过滤器**，并输入所需的标识符。如果选择**无过滤器**，则将收集所选客户机上的所有调试文件。如果为您预选了会话，则无法对其进行更改。
   c. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要检查调试文件的任何其他目录，然后单击**添加**。
   b. 在目录树中，选择任何其他要收集其内容的目录（不收集子目录的内容）。
   c. 单击“下一步”。
4. 在“选项”页中：
   a. 取消选择任何不想使用的调试收集选项。首次打开时，所选内容与 omnidlc 命令所用的标准默认设置匹配。有关它们的信息，请参阅《Data Protector 命令行界面参考》。
   b. 单击“下一步”。

检查的结果即显示在**结果**选项卡中。

计算完成后，将显示一个对话框，询问您是否要启动调试文件收集。

要使用选择用于空间计算的选项启动调试文件收集，请执行以下操作：

- 单击**是**。

  将在 Cell Manager 上使用默认操作行为（创建打包文件）。请参见收集调试文件(C)。

删除调试文件

要从客户机中删除调试文件：

1. 根据调用调试文件操作中的说明启动“删除调试文件”向导。
2. 在“客户机”页中，限制要删除的文件：
   a. 仅选择要从中删除文件的客户机。
   b. 在**过滤器**中，选择过滤器标准：**会话 ID**、**调试 ID**、**后缀**或**无过滤器**，并输入所需的标识符。

      如果选择**无过滤器**，则将删除所选客户机上的所有调试文件。
   c. 单击“下一步”。
3. 在“目录”页中：
   a. 除了默认调试文件目录之外，还应输入要从中删除调试文件的其他目录，然后单击**添加**。
   b. 单击**完成**。

收集要发送到客户支持的数据的示例

要收集调试、日志和 getinfo 文件，以了解在涉及一个客户机和 Cell Manager 的备份会话期间出现的问题，请循环以下要求：

1. 尽可能减少错误环境：
   - 创建只包含一个或多个文件或目录的备份规范。
   - 在调试运行中仅包括一个失败客户机。
2. 创建包含以下内容的 info 文本文件：
   - Cell Manager、介质代理和磁带客户机的硬件标识。例如， -9000 T-600 Series ； Vectra XA。
   - SCSI 控制器的名称，例如，Windows 介质代理客户机的 onboard_type/Adaptec xxx/... 。
   - 从 omnicellinfo -cell 命令输出获取的拓扑信息。
   - devbra -dev命令的输出（如果备份设备有问题）。
3. 与支持组织讨论技术问题，并请求以下信息：
   - 调试级别 (例如， 1-200 。这是随后需要的命令选项。)。
   - 调试作用域（例如，仅客户机、仅 Cell Manager、每个系统）。
4. 退出所有用户界面，并停止单元中所有其他备份活动。
5. 如果还要收集 Inet 或 CRS 调试信息，则在 Cell Manager 上，在调试模式下重新启动 Inet 或 CRS 服务。
6. 在 Cell Manager 上，在调试模式下启动 GUI：

   ```
   manager -debug 1-200 error_run.txt
   ```

   使用首选项代替 error_run 文本，可以定义所创建调试文件名的后缀。
7. 使用 Data Protector 复制问题。
8. 退出所有用户界面以退出调试模式。

   如果还收集了 Inet 和 CRS 调试信息，则在 Cell Manager 上重新启动 Data Protector 服务，而不使用调试选项。
9. 在 Cell Manager 上，运行：

   ```
   omnidlc -postfix error_run.txt
   ```

   此命令将日志、getinfo 和调试文件与客户机上的 error_run.txt 后缀压缩在一起，通过网络将其发送到 Cell Manager，并将其打包和保存到当前目录下的 dlc.pck 文件中。
10. 通过电子邮件将打包的文件 (dlc.pck) 发送到支持的组织内。
11. 通过在 Cell Manager 上运行以下命令，删除在客户机上创建的调试文件 (带 error_run.txt 后缀):

    ```
    omnidlc -postfix error_run.txt -delete_dbg
    ```

Develop

This section introduces you to REST Application Programming Interfaces (APIs) available with Data Protector.

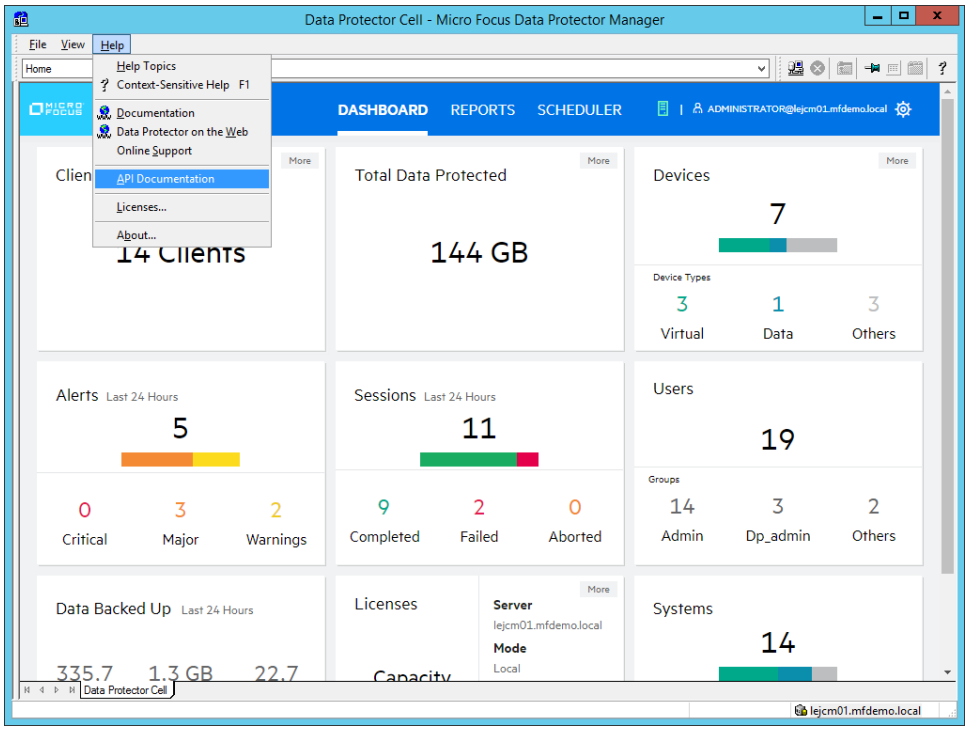
Related topics

REST API reference

CLI - REST API bridge

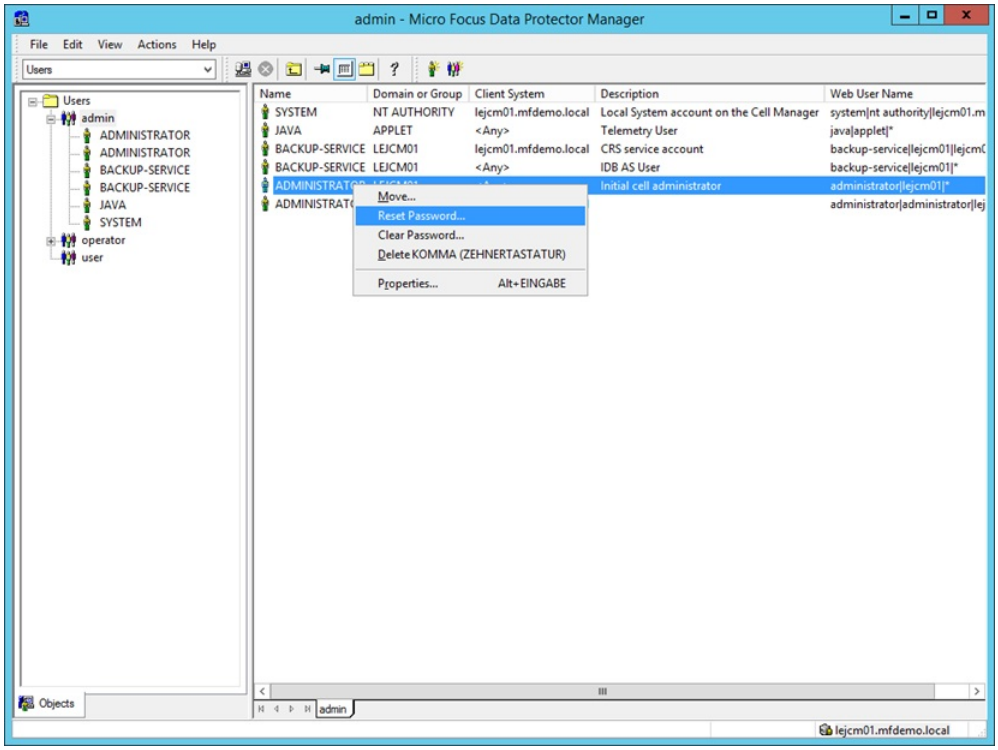
REST API Reference

Data Protector uses Swagger to document the framework for the RESTful APIs. You can access it from the API Documentation in the **Help** menu option on the Data Protector GUI. Alternatively, you can find the complete list of APIs in an interactive format here. In addition to the well-defined REST endpoints in the reference you can use theCLI-API Bridge to execute CLI commands on the Cell Manager in a RESTful manner.



Prepare a user for REST API access

To access the Data Protector REST API you need to authenticate with the Application Server to receive an OpenAPI Bearer token for all other operations. The Web user name required to log in is in the Username|Group|Client format. You can create a new user for this purpose or reset the password of a an existing user from the **Users** context.



Getting Started with REST API

This section contains examples on how to interact with the Data Protector REST API. In these examples, the sample REST call is done using cURL and PowerShell, but you can use any other client application such as Postman.

Authenticate with the Application Server

To receive a Bearer access_token you have to authenticate with the Application Server. Make sure to use the Web User name and password defined for this purpose. In this example, the username is administrator|lejcm01|* and the password is MyP4ssw*rd . You must use the same access_token in all subsequent calls so the Application Server is aware that the request is coming from an authenticated client.

cURL command

```
curl --insecure  -X POST "https:// <Cell Manager>:7116/auth/realms/DataProtector/protocol/openid-connect/token" -H "accept: application/json" -
d "username= administrator|lejcm01|*&password= MyP4ssw*rd&refresh_token=string&client_id=dp-gui&grant_type=password"
```

PowerShell command

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Url = "https:// <Cell Manager>:7116/auth/realms/DataProtector/protocol/openid-connect/token"
$Body = @{
   username = " administrator|lejcm01|*"
   password = " MyP4ssw*rd"
   refresh_token = "string"
   client_id = "dp-gui"
   grant_type = "password"
}
Invoke-RestMethod  -Method 'Post' -Uri $url -Body $body | ConvertTo-Json
```

The result is as follows in both cases, while the access_token and fresh_token have been truncated for better readability.

```
{
   "access_token":  " eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJVMGljTmZBTmhMMnRiWHUwZUlF...",
   "expires_in":  1800,
   "refresh_expires_in":  2592000,
   "refresh_token":  "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJmYWFhNDk3Ny03MjA5LTQwYTUtY...",
   "token_type":  "bearer",
   "not-before-policy":  0,
   "session_state":  "54f4501c-3a27-44ac-b84f-f219a0cc841c",
   "scope":  "email profile"
}
```

Get Total Protected Data

With the access_token from the authentication request, you can issue a REST API call to get the Total Protected Data.

cURL command

```
curl --insecure -X GET "https:// <Cell Manager>:7116/idb/v2/dashboard/backup/dataprotected" -H "accept: application/json" -H "Authorization: B
earer  <access_token>"
```

PowerShell command

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Url = "https:// <Cell Manager>:7116/idb/v2/dashboard/backup/dataprotected"
$headers = @{
  Authorization = "Bearer  <access_token>"
  accept = "application/json"
}
Invoke-RestMethod  -Method 'GET' -Uri $url -Headers $headers | ConvertTo-Json
```

The result is as follows in both cases:

```
{
   "size":  "15144 GB"
}
```

Fetch backup objects for a client system

By using the access_token from the authentication request, you can issue a REST API call to get all backup objects for a specific client system. You can use this information for more advanced operations.

cURL command

```
curl --insecure -X GET "https:// <Cell Manager>:7116/idb/restoretree/fs?host= <Client>" -H "accept: application/json" -H "Authorization: Bearer
 <access_token>"
```

PowerShell command

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Url = "https:// <Cell Manager>:7116/idb/restoretree/fs?host= <Client>"
$headers = @{
```

```
 Authorization = "Bearer  <access_token>"
 accept = "application/json"
}
Invoke-RestMethod  -Method 'GET' -Uri $url -Headers $headers | ConvertTo-Json
```

The result is as follows in both cases:

```
{
 "type": "filesystem",
 "hosts": [
  {
   "hostname": "lejcm01.mfdemo.local",
   "sessions": [
    {
     "session_name": "2020/11/12-6",
     "mountpoints": [
      {
       "copy_id": "de3bd081-8a10-4682-80df-33f363e2ae80/19808",
       "device": "SOS_lejcm01",
       "label": "C: [SYSTEM]",
       "mountpoint": "/C",
       "object_type": "winfs",
       "tree": [
        "/Folder1",
        "/Folder2"
       ],
       "diskagent_id": 1605184203
      }
     ],
     "session_type": 0
    }
   ]
  }
 ]
}
```

Fetch backed up folders of a backup object on a client

By using the access_token from the authentication request and the information from the previous call, you can issue a REST API call to get all containers (folders) backed up in a particular timeframe.

cURL command

```
curl --insecure -X POST "https:// <Cell Manager>:7116/idb/v1/catalog/backedupobjects/children" -H  "accept: application/json" -H  "Authorization: Bearer  <access_token>" -H  "Content-Type: application/json" -d '{"hostName":" lejcm01.mfdemo.local","mountPoint":" /C","label":" C: [SYSTEM]","parentPath":" /","intervalStartTime":" 2020-11-01T10:00:00Z","intervalEndTime":" 2020-11-30T10:00:00Z","selectableOnly": true}'
```

PowerShell command

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Url = "https:// <Cell Manager>:7116/idb/v1/catalog/backedupobjects/children"
$headers = @{
 Authorization = "Bearer  <access_token>"
 accept = "application/json"
}
$Body = @{
   hostName = " lejcm01.mfdemo.local"
   mountPoint = " /C"
   label = " C: [SYSTEM]"
   parentPath = " /"
   intervalStartTime = " 2020-10-12T10:00:00Z"
   intervalEndTime = " 2020-12-12T10:00:00Z"
   selectableOnly = [bool]  1
}
$Body = $Body | ConvertTo-Json
Invoke-RestMethod  -Method 'POST' -Uri $url -Headers $headers -Body $body -ContentType "application/json" | ConvertTo-Json
```

The result is as follows in both cases.

```
{
 "entries": [
  {
   "container": true,
   "pathName": "/Folder1",
   "mountPoint": "/C",
   "selectable": true,
   "objectName": "Folder1",
   "label": "C: [SYSTEM]"
  },
  {
   "container": true,
```

```
    "pathName": "/Folder2",
    "mountPoint": "/C",
    "selectable": true,
    "objectName": "Folder2",
    "label": "C: [SYSTEM]"
   }
  ],
  "count": 2
}
```

CLI - API bridge

Application Programming Interface (API) is a set of developer tools and protocols that help you build customized software applications by providing building blocks. APIs govern how multiple software components and applications interact with each other.

Data Protector REST APIs are a new REST endpoint that offers Data Protector CLI in a RESTful manner. Operations that can be performed through CLIs are exposed through a single REST endpoint. You can configure devices, run backups, monitor sessions, etc in a RESTful manner.

Outputs are in the standard JSON format. There are additional supporting API operations, to execute API in sync and async mode.

You can get, as well as set various counters and parameters.

Data Protector provides the following RESTful APIs:

API	Description
command API	Executes the CLI command.
output API	Gets the output of the execution of a command.
settings API	Sets the REST API bridge settings.
settings API (GET method)	Gets the current settings of the REST API bridge.
outputcatalog API	Lists the output catalog entries.
clean API	Cleans the user work space.
abortrun API	Aborts a running CLI session.

Limitations

The following limitations apply:

- APIs work only for CLI commands that are installed on the Cell Manager. The following commands can be executed:
  1. omnib
  2. omnistat
  3. omnidb
  4. omniabort
  5. omnir
  6. omnicheck
  7. omnimm
  8. omnimnt
  9. omniminit
  10. omnimver
  11. omniobjcopy
  12. omniobjverify
  13. omniobjconsolidate
  14. omnirpt
  15. omnib2dinfo
  16. omniusers
  17. omnicellinfo
  18. omnicreatedl
  19. omnimlist
  20. omniupload
  21. omnidownload
  22. omnimcopy
  23. omnicjutil
  24. omniamo
  25. omnihealthcheck
- Commands that require user interaction are not supported.

For example, `omnidbinit -force` requires the user to enter an option, yes or no.

command API

Use this API to execute the CLI command.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/command

Method

POST

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

```
{ "name": "omnidb", "options": "-session 2018/11/08-1 -detail", "wait": 3000 }
```

name : Specify the command to run.

options : Specify the parameter required to get the desired information.

wait : Specify the runtime waiting period. This field is specified in milliseconds.

Response codes

Code	Status	Description
200	SUCCESS	Returns the output as a a jsonarray named cli_output if the CLI is complete. If the CLI is waiting for the completion even after the given waiting time, then the reunId is returned. The output can be retrieved at a later stage using the runId .
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/command

Successful output:

{ "result": { "cli_output": ["", "Object name : iwf1119076.hostname.net:/C 'C:'", "\tObject type : WinFS", "\tObject status : Completed", "\tStarted : Thursday, November 8, 2018, 11:48:34 AM", "\tFinished : Thursday, November 8, 2018, 11:49:23 AM", "\tObject size : 2480352 KB", "\tBackup type : Full", "\tProtection : Protected permanently", "\tCatalog retention : Same as data protection.", "\tVersion type : Normal", "\tAccess : Private", "\tNumber of warnings : 0", "\tNumber of errors : 0", "\tDevice name : FLDevice1_Writer0", "\tBackup ID : n/a", "\tCopy ID : F064D90A-9E46-4E35-B9BD-470E1C9B8F06/1030 (Orig)", "\tEncrypted : No", "\tDiskAgent ID : 1541657913", "\tPoint in time : Thursday, November 8, 2018, 11:48:34 AM"], "runid": "2018-11-08-2", "command": "omnidb -session 2018/11/08-1 -detail", "status": "complete" } }

output API

Use this API to get the output of a run. Use the runId of a previous run. The runId can be obtained from the output catalog.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/output?runId=<run-id>

Method

GET

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

None

Response codes

Code	Status	Description
200	SUCCESS	Returns the list of Cell Manager(s).
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/output?runId=2018-10-16-01
```

Successful output:

```
{ "output": { "output": [ "WARNING Calculation of total protected data size may take some time." ] "command": "omnicc -check_lic" } }
```

settings API

Use this API to set the REST Bridge settings.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/settings

Method

POST

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

```
{ "max_concurrent_sessions": "100" }
```

max_concurrent_sessions : Specifies the maximum number of concurrent sessions that can be triggered.

Response codes

Code	Status	Description
200	SUCCESS	On success, it returns to the Bridge settings after the update.
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/settings
```

Successful output:

```
{ "status_check_interval": "100", "defaultwait": "1000", "max_concurrent_sessions": "10", "maxoutputs": "1000" }
```

status_check_interval : Checks the status internally.

defaultwait : Specifies the default waiting time, which is **1000** milliseconds. This can be changed according to your requirement.

max_concurrent_sessions : Specifies the maximum number of concurrent sessions that can be triggered.

maxoutputs : Specifies the maximum number of outputs that can be stored.

settings API - GET

Use this API to get the current settings of the REST Bridge.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/settings

Method

GET

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

None

Response codes

Code	Status	Description
200	SUCCESS	Gets the current settings of the REST Bridge.
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/settings
```

Successful output:

```
{ "appconfig":{ "cliworkspace": "cliws", "status_check_interval": "100", "defaultwait": "1000", "max_concurrent_sessions": "100", "maxoutputs": "10" } }
```

cliworkspace : Specifies where the output catalog information is stored. The storage location cannot be changed.

The information is stored in the following locations:

- For Windows:

```
C:\ProgramData\OmniBack\CliBridgeWorkspaces\administrator-<hostname>-<hostname>
```

- For Linux:

```
/var/opt/omni/log/CliBridgeWorkspaces/root-any-<hostname>
```

maxoutputs : Specifies the maximum number of outputs that can be stored.

status_check_interval : Checks the status internally.

defaultwait : Specifies the default waiting time, which is **1000** milliseconds. This can be changed according to your requirement.

max_concurrent_sessions : Specifies the maximum number of concurrent sessions that can be triggered.

outputcatalog API

Use this API to get the output catalog. The output catalog keeps catalog of the CLI runs that are executed through the bridge.

URL

```
https://<hostname>:<port>/dp-rest-cli-bridge/restws/workspace/outputcatalog
```

Method

GET

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

None

Response codes

Code	Status	Description
200	SUCCESS	Lists the catalog entries in the output catalog.
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/workspace/outputcatalog
```

Successful output:

```
{ "outputcatalog":{ "entries": [ { "runId": "2018-09-13-1", "command": "omnicc -check_lic", "status": "complete" } ] } }
```

clean API

Use this API to clean the workspace.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/workspace/clean

Method

POST

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

```
{ }
```

Response codes

Code	Status	Description
200	SUCCESS	Cleans the user work space.
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/workspace/clean
```

abortrun API

Use this API to abort a running CLI session.

URL

https://<hostname>:<port>/dp-rest-cli-bridge/restws/abortrun/{runId}

Method

PUT

Parameters

None

Header

Name	Description
X-Auth-Token	(*Required*) Authenticates the request call to the API server and provides secure access to the resources while protecting your user credentials. **Type:** string **Attribute:** <valid_token>

JSON body

```
{ }
```

Response codes

Code	Status	Description
200	SUCCESS	Returns the list of Cell Manager(s)
400	BAD REQUEST	Returns an error message describing the specific problem. This could be caused by an invalid URL or header sent in request.
401	NOT AUTHORIZED	The X-Auth-token used for authentication is incorrect.
500	INTERNAL SERVER ERROR	Issues with the website's server.

Example

```
https://iwf1114030.hostname.net:7116/dp-rest-cli-bridge/restws/abortrun/{runId}
```

Successful output:

```
{ "status": "success" }
```

Practitioner notes

The Practitioner notes section contains technical information as an addition to the product's official documentation. The practitioner notes are provided by Micro Focus product practitioners including Micro Focus employees, partners, and customers. Information includes, but is not limited to:

- Technical blogs
- Knowledge articles
- Whitepapers
- Best practices

Please note that the user-contributed content in the Practitioner notes has not been tested by the developers of the product. Information here has not gone through an official review process but will be reviewed from time to time and assimilated into product documentation.

Deployment of a Linux Cell Manager

The following document will assist with the deployment of Micro Focus Data Protector on Linux, connecting the Data Protector GUI and installation of a Windows Installation Server. While all of this information is available in the general documentation, it serves as a step-by-step guide to assist new users.

General Preparation

- Check the Data Protector Platform and Integration Support Matrix for operating system support for Linux Cell Manager and other components
- Ensure the network ports between Cell Manager, GUI and clients are open. This includes external firewalls and the firewall on the client or server itself.

Prepare Linux for the Cell Manager

The following section describes general assumptions for the Linux operating system for a successful Data Protector Cell Manager deployment. While most of the requirements are identical, there are small differences for RHEL-based distributions and SLES. Please follow the steps in the appropriate section.

Since Data Protector is using a distributed and modular architecture, networking and name resolution are important. The system should be configured with a FQDN whenever possible. The short hostname and the FQDN must be resolved using `/etc/hosts` and/or DNS. Using NTP is highly recommended to allow proper scheduling and being in sync with other systems on the network.

This guide was created with Micro Focus Data Protector A.10.91 on SLES15 SP2 and RHEL8 U1. It is expected that the steps shared will be also valid for more recent versions of Data Protector and the Linux distribution.

> **Note:** Using different installation options as described here is supported but might require additional steps not covered in this guide.

A Data Protector Cell Manager should have at least 4 CPU cores and 16 GB of system memory. The requirements for disk space depend on number of files protected. Additional compute ressources are neccesary if the Cell Manager system is also used as Media Agent with deduplication or VEPA backup host for example.

Red Hat Linux Server

The following assumes a `Minimal Installation` of Red Hat Linux Server (RHEL) 8.x was performed to a physical or virtual system.

At least the following software components have been selected as part of the installation:

- Standard
- Headless Management
- Guest Agents (If the server is a Virtual Machine)

Packages required by Data Protector that should be installed using `yum install` after the installation has been completed:

- libnsl
- nscd

> **Note:** Cell Manager deployments on Oracle Enterprise Linux and CentOS have the same requirements.

SUSE Linux Enterprise Server

The following assumes a `Minimal Installation` of SUSE Linux Enterprise Server (SLES) 15.x with the `Basesystem Module` and `Server Applications Module` enabled was performed to a physical or virtual system.

At least the following software components have been selected as part of the installation:

- Minimal Base System
- Enhanced Base System
- 32-Bit Runtime Environment
- YaST System Administration
- Software Management

Packages required by Data Protector that should be installed using `YaST` after the installation has been completed:

- bc

Deploy the Cell Manager on Linux

This first section is about fulfilling Data Protector-specific installation requirements.

Fulfill the Installation Requirements

Software Downloads

Download the media kit for Windows and Linux from Software Licenses and Downloads the Evaluation Portal.

Operating System	Filename Media Kit
Linux	Micro_Focus_DP_10.91_Linux_DP_A1091_GPLx86_64.tar.gz
	Micro_Focus_DP_10.91_Linux_Signature_File_DP_A1091_GPLx86_64.tar.gz.sig
Windows	Micro_Focus_DP_10.91_Windows_DP_A1091_Windows_OVMS.zip
	Micro_Focus_DP_10.91_Windows_Signature_File_DP_A1091_Windows_OVMS.zip.sig

Note: Using the latest version of Data Protector for evaluation purposes is highly recommended.

Name Resolution on the Cell Manager

Data Protector requires a properly configured name resolution. The preferred choice for name resolution is DNS with nameserver, domain and search options configured in /etc/resolv.conf. To ensure the Cell Manager is also fully operational in case DNS becomes unavailable, there should be also an appropriate entry in /etc/hosts for the Cell Manager system.

Let's assume the the primary IP of the Cell Manager lejcm08.mfdemo.local is 172.25.1.42. Then the /etc/hosts should contain the following entry.

```
172.25.1.42  lejcm08.mfdemo.local lejcm08
```

Verify the output of the hostname and dnsdomainname commands. Both should return expected results, even if DNS is not responding. Please also verify if DNS records for forward and reverse name resolution are properly configured. This can be done with the host command.

```
[root@lejcm08 ~]# hostname lejcm08 [root@lejcm08 ~]# dnsdomainname mfdemo.local [root@lejcm08 ~]# host lejcm08.mfdemo.local lejcm08.mfdemo.local has address 172.25.1.42 [root@lejcm08 ~]# host 172.25.1.42 42.1.25.172.in-addr.arpa domain name pointer lejcm08.mfdemo.local.
```

Check and enable nscd to cache DNS requests on the new Cell Manager if the service is not enabled.

```
[root@lejcm08 ~]# systemctl status nscd [root@lejcm08 ~]# systemctl enable nscd [root@lejcm08 ~]# systemctl start nscd
```

Create the User Running Data Protector Services

The AppServer is executed as an unprivileged user hpdp on the Cell Manager. This user must be created and have a existing home directory. It does not need to have a password.

```
[root@lejcm08 ~]# useradd -m hpdp
```

Adjust the Open File Limit

Edit the /etc/security/limits.conf and add the following lines to the end of the file. There are two entries for root and the hpdp user each.

```
# Open file limit for Micro Focus Data Protector Cell Manager root soft nofile 8192 root hard nofile 16384 hpdp soft nofile 8192 hpdp hard nofile 16384
```

Note: After changing this file the user must logout and login to activate the changes.

Perform the Cell Manager Installation

Copy the Linux installation package Micro_Focus_DP_10.91_Linux_DP_A1091_GPLx86_64.tar.gz to the server system. Use SCP/SFTP or mount a CIFS/NFS network share from the Linux Server and copy it to a local file system. It is recommended to copy the entire file and extract it locally to ensure no files are missing or damaged.

On the Cell Manager login as the root user. If root is unable to login use su - root or sudo bash to gain root level access to the system. It is recommended to run unset LANG before starting the installation or upgrade to ensure there are localization-related issues.

The omnisetup.sh script used for the installation and upgrade of Data Protector comes with a wide range of built-in pre-flight checks. So running the script will inform the user about missing dependencies and possible configuration issues. If a problem is found the installation is aborted and the user can fix the issues and retry. When asked, if the previously failed installation should be resumed, always answer with NO.

The setup process will ask the user to confirm general Obsolescence Information of the current version. This is mandatory to proceed with the installation or upgrade. The options Secure Data Communication and Audit Log as well as Telemetry License Agreement are considered optional.

```
[root@lejcm08 ~]# id uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 [root@lejcm08 ~]# unset LANG [root@lejcm08 ~]# mkdir /tmp/1091 [root@lejcm08 ~]# tar zxf Micro_Focus_DP_10.91_Linux_DP_A1091_GPLx86_64.tar.gz -C /tmp/1091 [root@lejcm08 ~]# cd /tmp/1091/LOCAL_INSTALL/ [root@lejcm08 LOCAL_INSTALL]# ./omnisetup.sh -CM -IS -inetport 5565 [...] No Data Protector software detected on the target system. Validating System requirements... Passed: Reporting Server instance not found. Cell Manager can be Installed. Passed: The user account "hpdp" will be used for the IDB service. Passed: Port number "7112" will be used for the "hpdp-idb" service. Passed: Port number "7113" will be used for the "hpdp-idb-cp" service. Passed: Port number "7116" will be used for the "hpdp-as" service. Passed: Port number "9999" will be used for the "hpdp-as" service. Passed: The kernel parameter value: SHMMAX = 18446744073692774399 (17179869183.98 GB). The minimum required parameter value is "2.5 GB". Passed: There are "16814817280" bytes (15.66 GB) (approx. 16 GB) of available system memory. 16 GB of system memory is required. Passed: Requires 3079168 kilobytes (2.93 GB) of free storage space on the "/" filesystem. The filesystem "/" has 23941912 kilobytes (22.83 GB) of free space. Passed: Package glibc-2.28-72.el8.x86_64 is installed on the system. Passed: Package libnsl-2.28-72.el8.x86_64 is installed on the system. Passed: Hostname restrictions verified. Passed: Open file limit restriction verified. Validating system requirements completed successfully. [...] Installing OB2-CS packet Verifying... ################################## [100%] Preparing... ################################## [100%] Updating / installing... 1:OB2-CS-A.10.91-1 ################################## [100%] NOTE: No Data Protector A.10.91 Internal Database found. Initializing... Configuring and starting up Internal Database... Done! Configuring and starting up Internal Database Connection Pool... Done! Initializing Internal Database version A.10.91... Done! Configuring and starting up Application Server... Done! Starting up Data Protector Services... Done! Deploying Application Server Web Services... Done! NOTE: Data Protector A.10.91 Internal Database initialized. [...] DONE! Telemetry details updated successfully. Migrating Ldap Configuration to Keycloak .. Migrating Users .. Log file: /var/opt/omni/server/log/dp_user_migrate.log User Migration completed successfully. pausing quartz scheduler...ok [...] Migration of Template(s) completed successfully. Installation/upgrade session finished. [root@lejcm08 LOCAL_INSTALL]#
```

Post-Installation Steps

Proceed with the Post-Installation steps if not error have been found in the setup process.

Add Data Protector to Search PATH

Create a file `/etc/profile.d/omni.sh` and add the following content.

```
# Search path extension for Micro Focus Data Protector PATH=$PATH:/opt/omni/bin:/opt/omni/lbin:/opt/omni/sbin export PATH
```

> **Note:** Logout and login to make the changes active or execute the command `source /etc/profile.d/omni.sh` .

Check the Cell Manager Services

If Data Protector was not added to the search `PATH` , specify the full path to `omnisv` command which is `/opt/omni/sbin/omnisv` .

```
[root@lejcm08 LOCAL_INSTALL]# omnisv status ProcName Status [PID] ================================ crs : Active [17332] mmd : Active [17331] kms : Active [17330] hpdp-idb : Active [17366] hpdp-idb-cp : Active [17393] hpdp-as : Active [17417] omnitrig : Active Sending of traps disabled. ================================ Status: All Cell Server processes/services up and running.
```

Open the Firewall on the Cell Manager

If the Linux firewall is enabled, open the ports used by Data Protector accordingly. Or disable the firewall entirely, if it is not required in the environment.

```
[root@lejcm08 ~]# systemctl status firewalld [root@lejcm08 ~]# systemctl stop firewalld [root@lejcm08 ~]# systemctl disable firewalld
```

Deploy the Data Protector GUI on Windows

While parts of Data Protector can be managed from a modern web interface, most of the initial configuration is still done with a Windows-based GUI. After the Cell Manager deployment on Linux, follow this procedure to install and configure a Windows-based management station using the Data Protector GUI.

> **Note:** It is highly recommended that the Data Protector GUI version matches the version of the Cell Manager.

Test Client Communication with Cell Manager

Ensure the network ports for the Data Protector GUI are open between the client system and the Cell Manager and both systems are able to resolve each other using DNS. The `nslookup` or `ping` command may be used.

Since `telnet` is no longer part of a Windows installation by default, it is recommended to use Power Shell `Test-NetConnection <Cell Manager> -Port <InetPort>` for testing basic client communication. Specify the Data Protector INET port configured during the Cell Manager installation. The default port number is 5565.

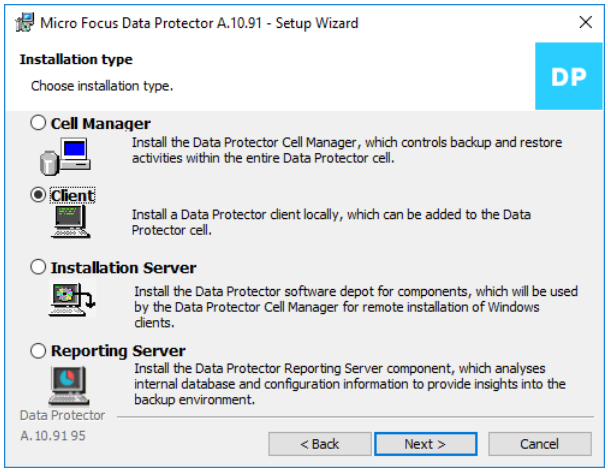
```
PS C:\> tnc lejcm08.mfdemo.local -Port 5565 ComputerName : lejcm08.mfdemo.local RemoteAddress : 172.25.1.42 RemotePort : 5565 InterfaceAlias : Ethernet0 SourceAddress : 172.25.100.201 TcpTestSucceeded : True
```

If the port is unreachable, check if the firewall is properly configured on the Cell Manager **before** proceeding with the next step.

Perform the GUI Installation

Copy the Windows installation package `Micro_Focus_DP_10.91_Windows_DP_A1091_Windows_OVMS.zip` to the client system. It is recommended to copy the entire file and extract it locally to ensure no files are missing or damaged.

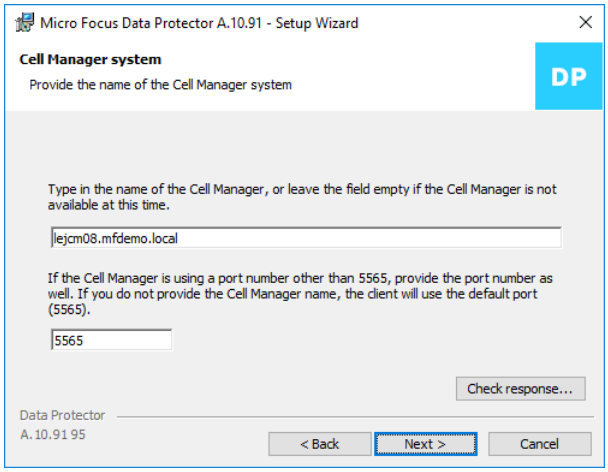
Extract the content from the archive to a temporary location. Run setup.exe from the folder Windows\x8664 as Administrator and choose a Client installation.



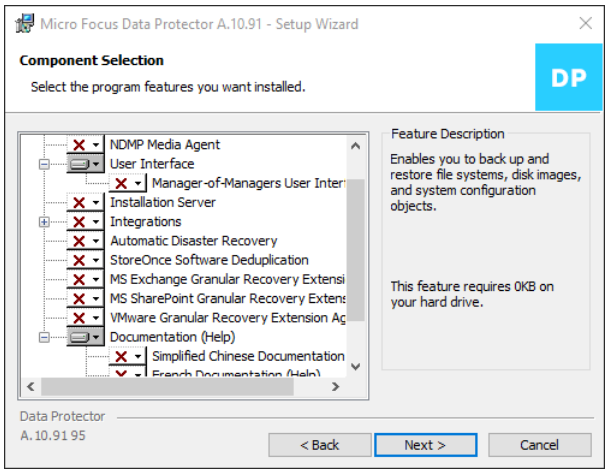
On one of the next screens specify the FQDN of the Cell Manager and the Data Protector INET port configured during the Cell Manager installation. The default port number is 5565.

Important: If the Windows client is not able to to resolve the Cell Manager name using DNS, edit C:\Windows\system32\drivers\etc\hosts on the client system and include the Cell Manager system and primary IP. Also make sure that the client system exists in /etc/hosts of the Cell Manager. This is usually only required for test environments or special isolated management stations.

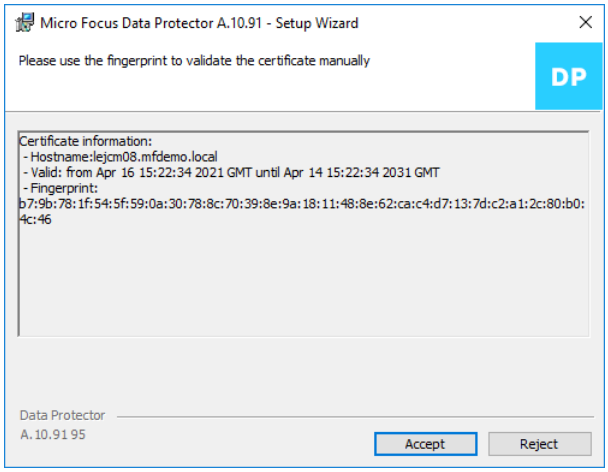
Note: Clicking next or using Check response may take a while to complete. If it times out, navigate back and retry, probably a few times. This will each time increase the timeout waiting for the Cell Manager to respond. This is expected behavior. Or proceed after removing the checkbox on Check Cell Manager name.



On one of the next screens select User Interface and Documentation only. This is sufficient for a pure management station. Proceed with the client installation.



If the Cell Manager is responding properly, the setup will request to confirm the Cell Manager certificate, which is used to secure the client-server communication.



Note: To get the fingerprint of the client certificate on the Cell Manager, run `omnicc -secure_comm -get_fingerprint` on the Cell Manager system.

Import the Client to the Cell Manager

This step is optional, but recommended for environments where only a single Cell Manager is used. Import the client running the Data Protector GUI to the Cell Manager. Importing the client makes it easy to keep track of the installed versions of the GUI on various client systems managing the environment.

Note: If the client should not be part of the Data Protector cell, or the client certificate was not accepted as part of the client installation, follow the steps shared in Configure the GUI for Additional Cell Managers.

To import the client from the Cell Manager, run the command `omnicc -update_host <Client FQDN>` on the Cell Manager system.

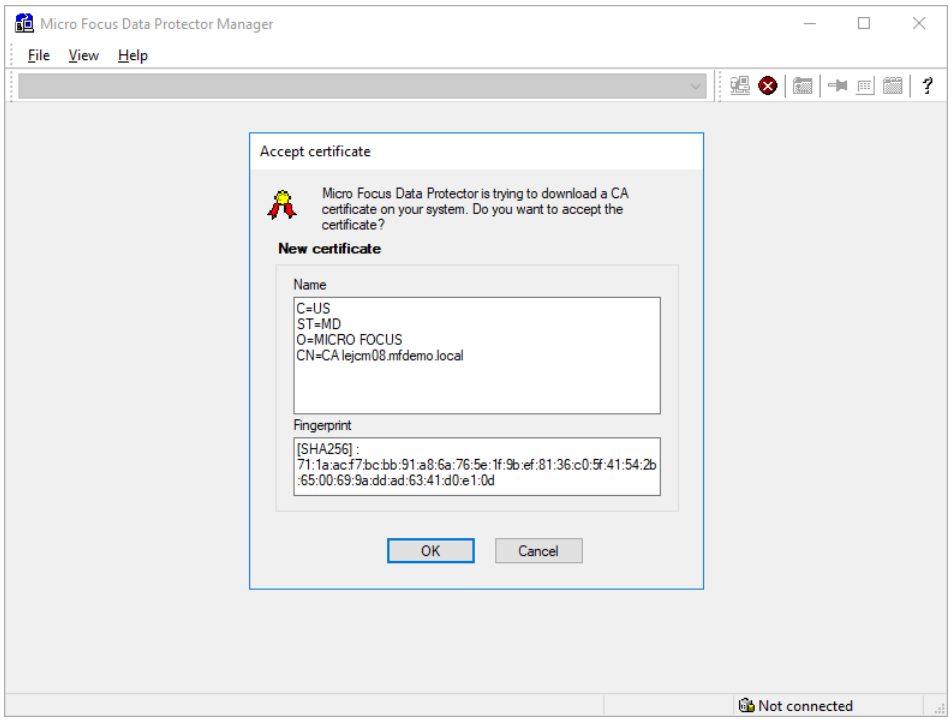
```
[root@lejcm08 ~]# omnicc -update_host lejwn10.mfdemo.local  - Please use the fingerprint to validate the certificate manually! Certificate information:  - Hostname:lejwn10.mfdemo.local  - Valid: from Feb 15 07:44:05 2021 GMT until Feb 13 07:44:05 2031 GMT  - Fingerprint: ca:c2:65:80:d9:ee:58:63:bb:a9:de:bf:43:0d:33:ea:ed:b4:d8:6c:a6:64:f5:ba:68:a2:d6:ba:4e:ab:95:ba Do you want to continue (y/n)?y Import host successful.
```

Note: The import process will request to confirm the client certificate, which is used to secure the client-server communication. To get the fingerprint of the certificate on the client, run `omnicc -secure_comm -get_fingerprint` on the GUI client system.

Configure the Cell Manager User Management

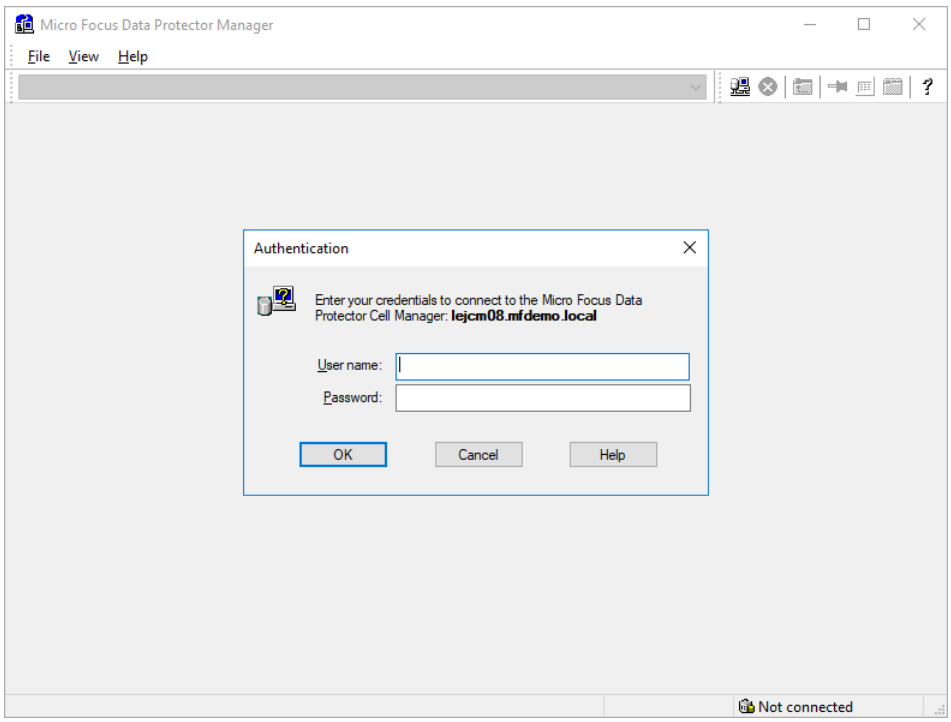
With the client-server certificate being trusted on the Cell Manager and client the Data Protector GUI will be able to connect the Cell Manager. During the first connection attempt, confirm the `AppServer` certificate. The certificate is is different to the

certificate used to secure the client-server communication.



Since there has is no Data Protector user for the client system, a login prompt will be displayed. This is expected at this point. Please close the GUI and continue with the next step.

Note: The login prompt is only actively used when the Cell Manager has been configured forLDAP authentication.



On the Cell Manager run the omniusers command to add the Windows user logged in to the client system accordingly to the Data Protector user management. This step depends on the environment setup. After this step, the GUI will be able to connect without the login prompt.

Important: The password specified in omniusers -setpass is only used internally by the AppServer. Only a user with a password defined will be granted access to the Data Protector GUI. No login prompt will be displayed. The password may be different to the password used by the user used to run the Data Protector GUI.

Note: Users without a password are commonly used as part of application integration backups in Data Protector.

Local User on the Client System Example

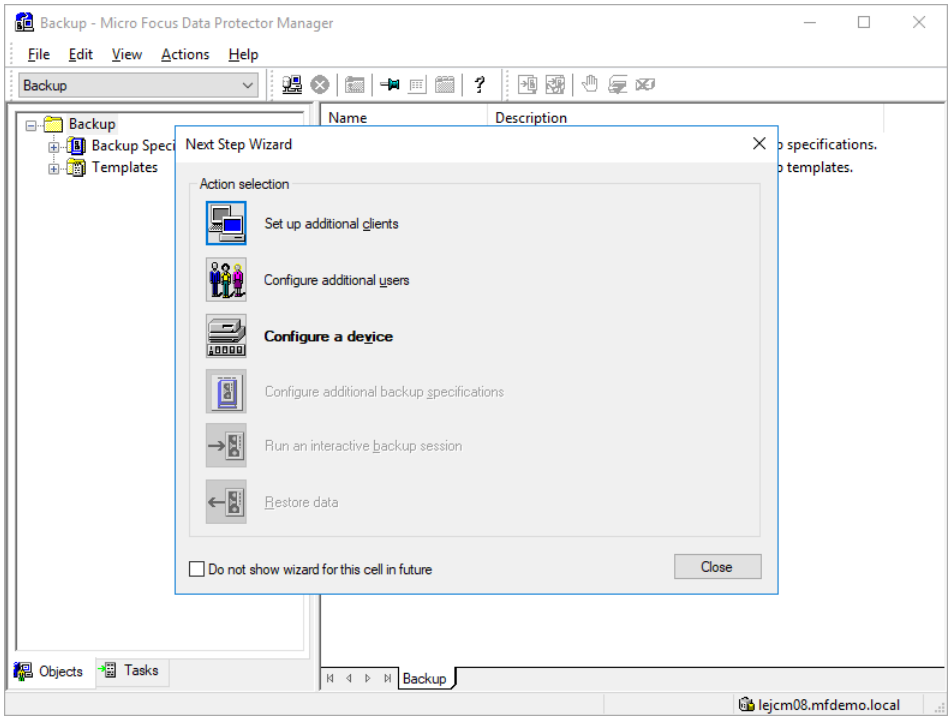
The local Administrator on the client system LEJWN10, which is identified on the network as lejwn10.mfdemo.local, is added. This is a Windows user account.

```
[root@lejcm08 ~]# omniusers -add -type W -usergroup admin -name Administrator -group LEJWN10 -client lejwn10.mfdemo.local -setpass Enter Password : Re-Enter Password : User 'ADMINISTRATOR' successfully added to 'admin' group.
```

Domain User on the Client System Example

The domain user MFDEMO\Jane on the client system lejwn10.mfdemo.local is added. This is a Windows user account.

```
[root@lejcm08 ~]# omniusers -add -type W -usergroup admin -name Jane -group MFDEMO -client lejwn10.mfdemo.local -setpass Enter Password : Re-Enter Password : User 'JANE' successfully added to 'admin' group.
```



Configure the GUI for Additional Cell Managers

If a Data Protector GUI should manageme more than just one Cell Manager, use the following procedure. To establish a connection to a Cell Manager the client system must be authorized accordingly.

Note: The client must not be imported to the Cell Manager to enable management.

A client can only be part of one Data Protector cell at a time. Run the command `omnicc -secure_comm -configure_oeer <Cell Manager FQDN>` on the client system before running the command `omnicc -secure_comm -configure_peer <Client FQDN>` on the Cell Manager system. This is required to properly configure the client-server certificate trust.

Try connecting to the Cell Manager using the Data Protector GUI. If a login prompt is displayed and LDAP authentication has not been configured, add the Windows user running the Data Protector GUI according to Configure the Cell Manager User Management with the `omniusers` command and try again.

Deploy and Configure a Windows Installation Server

This step is optional. A Windows Installation Server should be part of the Data Protector cell to allow remote installation and upgrades of Windows clients. Manual local installations and upgrade are also an option, if the number of clients is small. The Installation sources are made available via SMB on the `OmniBack` share on the installation server.

Note: A Windows Installation server can be used as management station with the Data Protector GUI.

Test Client Communication with Cell Manager

Ensure the network ports for the Installation Server are open between the client system and the Cell Manager and both systems are able to resolve each other using DNS. The nslookup or ping command may be used.

Since telnet is no longer part of a Windows installation by default, it is recommended to use Power Shell Test-NetConnection <Cell Manager> -Port <InetPort> for testing basic client communication. Specify the Data Protector INET port configured during the Cell Manager installation. The default port number is 5565.

```
PS C:\> tnc lejcm08.mfdemo.local -Port 5565 ComputerName     : lejcm08.mfdemo.local RemoteAddress    : 172.25.1.42 RemotePort      : 5565
InterfaceAlias   : Ethernet0 SourceAddress    : 172.25.100.201 TcpTestSucceeded : True
```

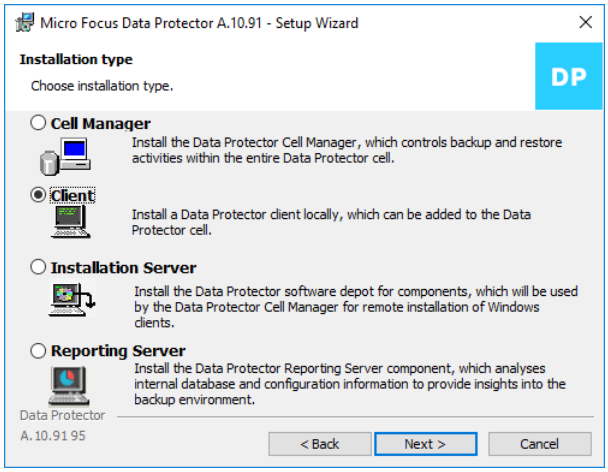
If the port is unreachable, check if the firewall is properly configured on the Cell Manager before proceeding with the next step.

Perform the Installation Server Installation

Copy the Windows installation package Micro_Focus_DP_10.91_Windows_DP_A1091_Windows_OVMS.zip to the client system. Extract the content from the archive to a temporary location. It is recommended to copy the entire file and extract it locally to ensure no files are missing or damaged.

Run setup.exe from the folder Windows\x8664 as Administrator and choose a Client or Installation Server installation. Using Client allows the installation of the Installation Server and other components such as the Data Protector GUI.

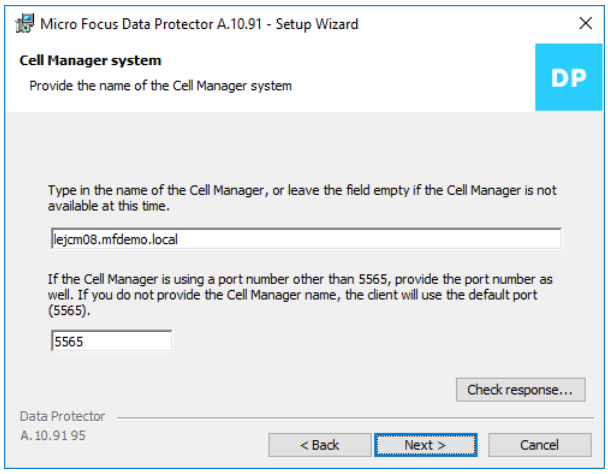
Note: Installing and using the Data Protector GUI directly from the Windows Installation server is recommended especially for initial client deployments.



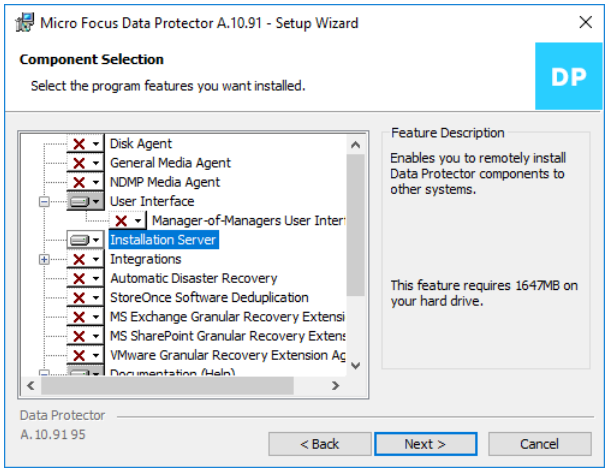
On one of the next screens specify the FQDN of the Cell Manager and the Data Protector INET port configured during the Cell Manager installation. The default port number is 5565.

Important: If the Windows client is not able to to resolve the Cell Manager name using DNS, edit C:\Windows\system32\drivers\etc\hosts on the client system and include the Cell Manager system and primary IP. Also make sure that the client system exists in /etc/hosts of the Cell Manager. This is usually only required for test environments or special isolated management stations.

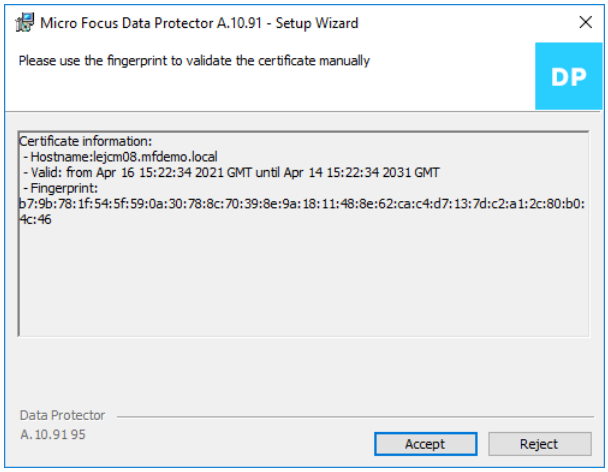
Note: Clicking next or using Check response may take a while to complete. If it times out, navigate back and retry, probably a few times. This will each time increase the timeout waiting for the Cell Manager to respond. This is expected behavior. Or proceed after removing the checkbox on Check Cell Manager name.



On one of the next screens select Installation Server , User Interface and Documentation only. This is sufficient for most Windows Installation servers. Proceed with the client installation.



If the Cell Manager is responding properly, the setup will request to confirm the Cell Manager certificate, which is used to secure the client-server communication.



Import the Installation Server to the Cell Manager

Import the client running the Windows Installation server to the Cell Manager. This is necessary to remotely deploy new Windows clients or upgrade existing clients.

To import the Windows installation server from the Cell Manager, run the command omnicc -import_is <Client FQDN> on the Cell Manager system.

```
[root@lejcm08 ~]# omnicc -import_is lejis19.mfdemo.local  - Please use the fingerprint to validate the certificate manually! Certificate information:  - Hostname:lejis19.mfdemo.local  - Valid: from Feb 15 07:44:05 2021 GMT until Feb 13 07:44:05 2031 GMT  - Fingerprint: ca:c2:65:80:d9:ee:58:63:bb:a9:de:bf:43:0d:33:ea:ed:b4:d8:6c:a6:64:f5:ba:68:a2:d6:ba:4e:ab:95:ba Do you want to continue (y/n)?y Import host successful.
```

Note: The import process will request to confirm the client certificate, which is used to secure the client-server communication. To get the fingerprint of the certificate on the client, run `omnicc -secure_comm -get_fingerprint` on the Installation Server client system.

An Installation Server can be part of multiple Data Protector cells. To import an Installation Server to another Cell Manager, run the command `omnicc -secure_comm -configure_oeer <Cell Manager FQDN>` on the Installation Server system before running the command `omnicc -import_is <Client FQDN>` on the Cell Manager system. This is required to properly configure the client-server certificate trust.

Installation Server Configuration

On the Cell Manager execute the `omnicc -update_omnirc` command to configure the Installation Server to smoothly work with the Windows client firewall for newly deployed clients.

```
[root@lejcm08 ~]# omnicc -update_omnirc OB2FWPASSTHRU -value 1 -host lejis19.mfdemo.local lejis19.mfdemo.local          Success
```

On the Windows Installation server, run the `omniinetpasswd` command from an **elevated** command prompt. Add a Windows user account to the Data Protector INET impersonation database, which is able to remotely connect to the `OmniBack` share on the Installation server. This is necessary for initial remote client deployments of new Windows clients. If not configured you will see `[110:1022] Cannot connect to the SCM (Service Control Manager)` errors during remote client deployment.

```
C:\>omniinetpasswd -add LEJIS19\Administrator Please enter password:******** Please retype password:******** User 'LEJIS19\Administrator' was successfully added. C:\>omniinetpasswd -inst_srv_user LEJIS19\Administrator User 'LEJIS19\Administrator' is configured to be used by Installation Server. C:\>omniinetpasswd -list  * Administrator@LEJIS19 (*)  Installation Server is using this user's credentials during push installation.
```

Note: Avoid adding an user account with expiring passwords. Using a service account is highly recommended.

Maintenance on a busy Cell Manager

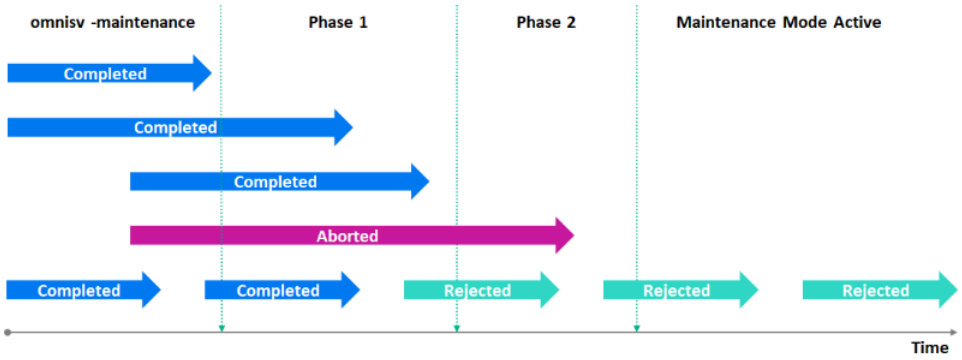
To allow system patching and other routine maintenance activities on the Cell Manager or a central Media Agent it may be required to stop and prevent new sessions from being started.

There are several options for this. You may stop the trigger on the Cell Manager using `omnitrig -stop` or change schedules of backups to prevent scheduled sessions from being executed. This will work in most of the cases, but does not prevent sessions from being executed started on client systems. This is quite often seen in environments with SAP HANA, where backups are triggered by the database itself or the SAP HANA Cockpit, or Oracle where RMAN is used to perform backups, restores or verifications.

Enter the Maintenance Mode

Use the command `omnisv -maintenance` to transition from Production to Maintenance Mode on the Cell Manager.

- **Production to Phase 1:** Sessions in progress will continue to run and new sessions are rejected by the Cell Manager. The trigger will be stopped.
- **Phase 1 to Phase 2:** All sessions still in progress will be actively terminated including GUI connections
- **Phase 2 to Maintenance Mode:** No sessions are running and new sessions are rejected by the Cell Manager. The trigger remains stopped.



> Restore sessions have priority in most environments. `omnisv -maintenance` will never abort a restore session. As a result you can't enter maintenance mode if a restore session in progress. Wait for them to complete or abort them manually.

Leave the Maintenance Mode

Once the Cell Manager is in Maintenance Mode you can stop the services using `omnisv -stop` if needed or reboot the system. Maintenance Mode is persistent until you leave it using `omnisv -maintenance -stop`.

> Upgrading the Cell Manager system to a more recent version of Data Protector will also use the Maintenance Mode as part of the process. Once the upgrade is complete the system will leave the Maintenance Mode automatically.

Related global Configuration Options

There are two global options related to Maintenance Mode. `MaintenanceModeGracefulTime` (time to wait from entering `omnisv -maintenance` to Phase 1) and `MaintenanceModeShutdownTime` (time to wait from Phase 1 to Phase 2) can be used to adjust the wait times to match your environment.

Abort Entering Maintenance Mode

If you notice that important sessions will not complete in time, you can abort entering the Maintenance Mode by using `STRG+C` combination on your keyboard. Sessions will not abort, the Cell Manager will accept new backups and the trigger will be re-enabled.

```
C:\>omnisv -maintenance Cell Server is entering maintenance mode 295  seconds left to abortion of all running sessions ...
```

Force Maintenance Mode

If you need for quickly enter Maintenance Mode you can use the command `omnisv -maintenance 1`. It will not wait for the session to complete and immediately try to abort them.

Monthly Schedules with Legacy Scheduler

The Legacy Scheduler was so popular that it was made available (again) in Data Protector A.10.20. With all its benefits there are some limitations such as scheduling beginning- and end of month backups, copies and reports is not directly possible. But it can be done if you know how to modify the schedule file for the corresponding specification.

Background Information on Legacy Scheduler

If you're new to this, we need to start with some basics. If the Legacy Scheduler is available in your Data Protector (not the case for releases A.10.00 up to A.10.10), a schedule for a specification (backup, copy, replication, consolidation, report groups) is stored in an ASCII file on the Cell Manager. If you create a new specification a corresponding file with the same name will be created in the directory. If there is no schedule defined, the file will be empty. You can find the files in the corresponding folders on the Cell Manager. The files are read by a process called omnitrig every 1 or 15 minutes depending on your configuration (SchedulerGranularity in global configuration file).

> It is not required to restart the services when changing those files. Just be careful when using tools like `vi` or `vim` as they will create a swap file in the same directory and this may produce warnings.

Location of the Legacy Scheduler Files

File system Backup Specs, including NDMP

> %DP_DATA_DIR%\Config\Server\Schedules or
> /etc/opt/omni/server/schedules

Integration Backup Specs, such as MSSQL, Exchange, VEAgent (VMware) and others in seperate folders

> %DP_DATA_DIR%\Config\Server \Barschedules or
> /etc/opt/omni/server/barschedules

Object Copy and Replication

> %DP_DATA_DIR%\Config\Server\copylists\scheduled\schedules or
> /etc/opt/omni/server/copylists/scheduled/schedules

Object Consolidation

> %DP_DATA_DIR%\Config\Server\consolidationlists\scheduled\schedules or
> /etc/opt/omni/server/consolidationlists/scheduled/schedules

Object Verification

> %DP_DATA_DIR%\Config\Server\verificationlists\scheduled\schedules or
> /etc/opt/omni/server/verificationlists/scheduled/schedules

Report Groups

> %DP_DATA_DIR%\Config\Server\rptschedules or
> /etc/opt/omni/server/rptschedules

Monthly Schedule Samples

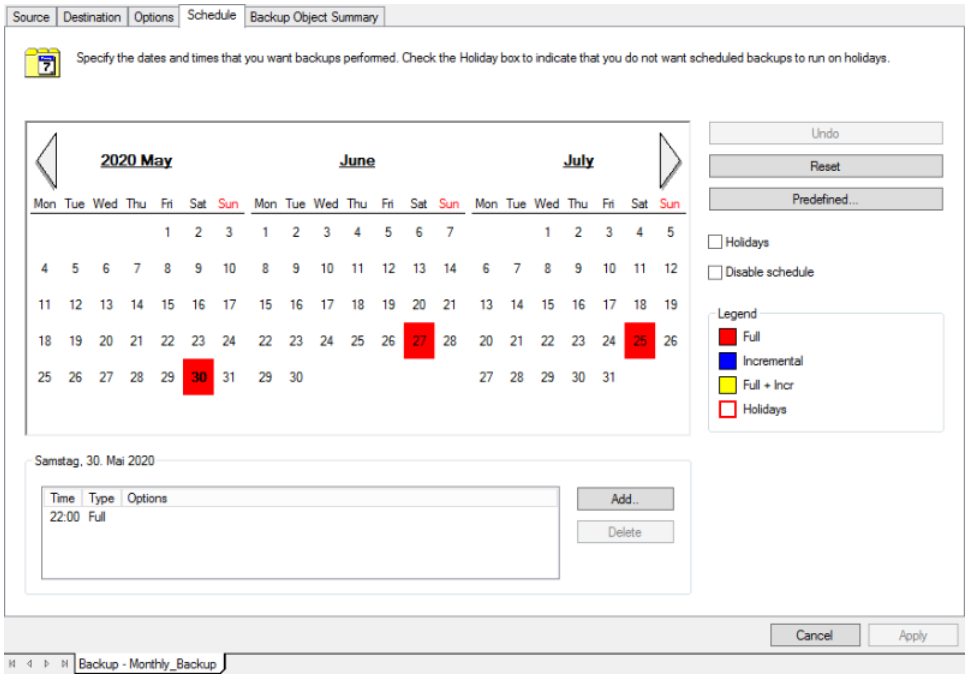
There are small differences in the syntax of the schedule files so we need to cover three cases here: Backup, Object Operation and Reporting.

Monthly Backup Sample

This may be used for all kind of Backup Specs. It will execute a Full Backup on the last Saturday in the month at 22:00.

```
-full -every -day 25 26 27 28 29 30 31 -month Oct Dec Jan Mar May Jul Aug -at 22:00 -full -every -day 24 25 26 27 28 29 30 -month Sep Nov Apr Jun -at 22:00 -full -every -day 22 23 24 25 26 27 28 29 -month Feb -at 22:00 -full -exclude -day Mon Tue Wed Thu Fri Sun -at 22:00
```

This is how it looks like in the Data Protector GUI.

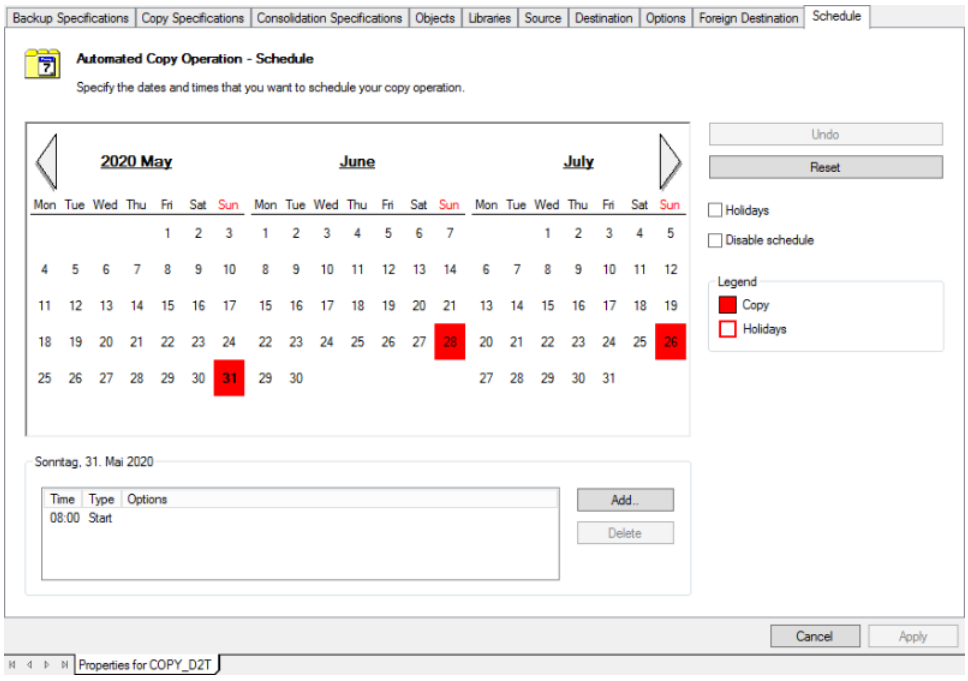


Monthly Object Operation Sample

This may be used for Object Copy (including Replication), Object Consolidation and Object Verification. It will execute the Object Copy on the last Sunday in the month at 08:00.

```
-start -every -day 25 26 27 28 29 30 31 -month Oct Dec Jan Mar May Jul Aug -at 08:00 -start -every -day 24 25 26 27 28 29 30 -month Sep Nov Apr Jun -at 08:00 -start -every -day 22 23 24 25 26 27 28 29 -month Feb -at 08:00 -start -exclude -day Mon Tue Wed Thu Fri Sat -at 08:00
```

This is how it looks like in the Data Protector GUI.

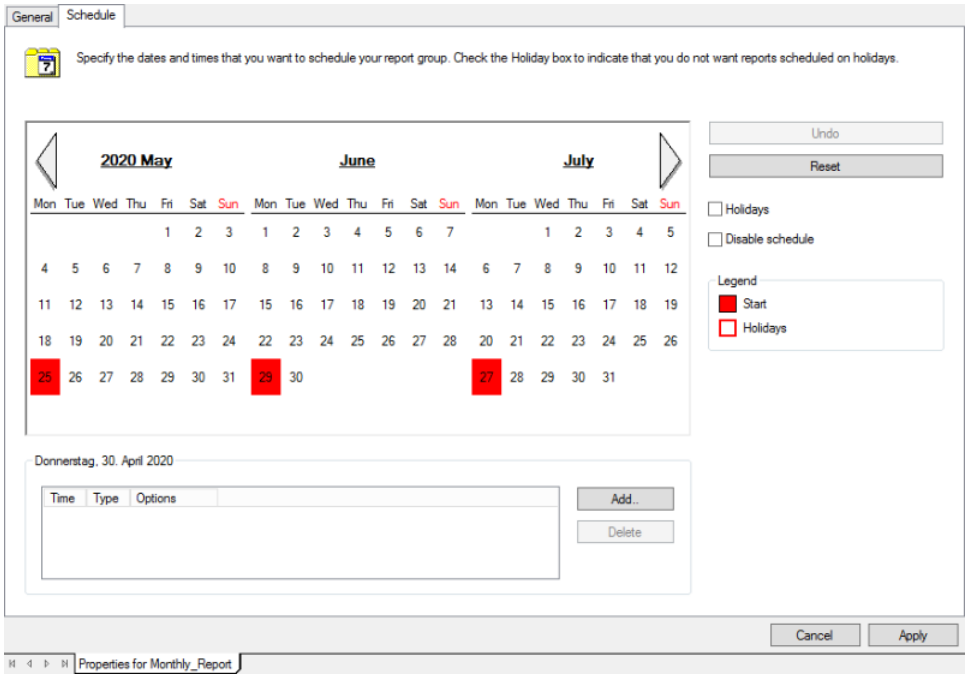


Monthly Reporting Sample

This may be used for Report Groups. It will execute the Report Group on the last Monday in the month at 10:00.

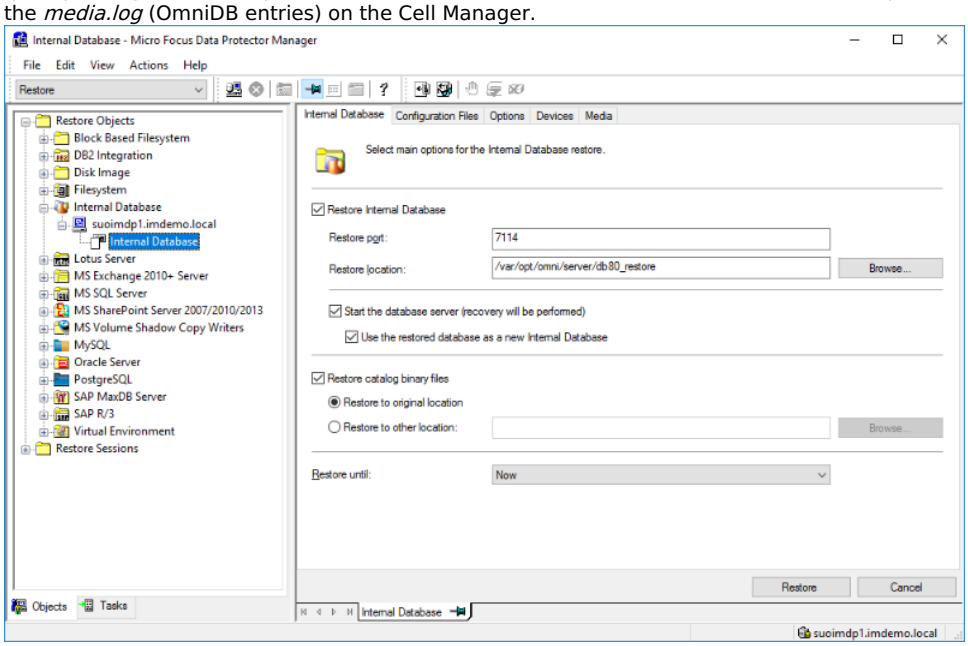
```
-start -every -day 25 26 27 28 29 30 31 -month Oct Dec Jan Mar May Jul Aug -at 10:00 -start -every -day 24 25 26 27 28 29 30 -month Sep Nov Apr Jun -at 10:00 -start -every -day 22 23 24 25 26 27 28 29 -month Feb -at 10:00 -start -exclude -day Tue Wed Thu Fri Sat Sun -at 10:00
```

This is how it looks like in the Data Protector GUI.



Clean up after Internal Database Restore

Data Protector allows online backups of its Internal Database (IDB). The IDB consists of database files, archive logs, Detail Catalog Binary Files (DCBF) and configuration files. The Internal Database can be protected by full and/or incremental backups virtually at any given time. An easy to use GUI-driven restore of the PostgreSQL-based database (with point-in-time recovery using archive logs), DCBFs and configuration files can be done in a one-step process or individually depending on the level of corruption. Missing or damaged configuration files or damaged DCBFs can be restored or repaired without bringing the Cell Manager down.
Regular IDB backups should be created on a daily or even more frequently basis to an reliable backup device that can be quickly configured and imported in case of disaster. Information on the lastet IDB backups can be found in the *media.log* (OmniDB entries) on the Cell Manager.



As soon as the IDB restore is complete, the Cell Manager is operational. Reconnect the GUI, since the IDB was switched to the restored instance. Verify Devices & Media and Internal Database context in the GUI. While the restore and recovery is simple a Clean up at a later time might be requested so that standard directories are used again.

Linux Cell Manager Clean Up

On a Linux Cell Manager the Internal Database is located in */var/opt/omni/server/db80*. In this example we will restore the database to */var/opt/omni/server/db80_restore*. If you need to adjust the restore path also adjust the commands and configuration file changes accordingly.

Note: The Clean up is disruptive to Data Protector since the services must be stopped and should be scheduled in a maintenance window. It is not a required operation after an IDB restore. The only purpose is to remove stale files and directories from file system and return the directory structure to normal. It can be done immediately or weeks after the restore. Creating an offline backup, filesystem snapshot or similar as a fallback.

Stop the services and check restored directory structure

[root@linux ~]# **omnisv stop** Cell Server services successfully stopped. [root@linux ~]# **ls -l /var/opt/omni/server** drwxr-xr-x 5 hpdp hpdp 4096 May 9 12:44 AppServer **drwxr-xr-x 19 root sys 4096 May 10 10:52 db80 drwxrwxrwx 5 root root 4096 May 10 10:49 db80_restore** drwxr-xr-x 4 root sys 4096 Mar 17 18:21 export drwxr-xr-x 4 root sys 4096 Mar 17 18:21 import drwxr-xr-x 4 root sys 4096 May 10 10:48 log drwxr-xr-x 2 root sys 4096 Mar 17 18:21 sessions [root@linux ~]# **ls -l /var/opt/omni/server/db80_restore** drwx------ 3 hpdp hpdp 4096 May 10 10:49 idb drwx------ 3 hpdp hpdp 4096 May 10 10:49 jce drwx------ 15 hpdp hpdp 4096 May 10 10:56 pg

Move the restored database to the target directory and adjust symlinks

The name of the symlinks might be different on your Cell Manager.

[root@linux ~]# **rm -rf /var/opt/omni/server/db80/idb** [root@linux ~]# **rm -rf /var/opt/omni/server/db80/jce** [root@linux ~]# **rm -rf /var/opt/omni/server/db80/pg** [root@linux ~]# **mv /var/opt/omni/server/db80_restore/* /var/opt/omni/server/db80/** [root@linux ~]# **ls -l /var/opt/omni/server/db80/pg/pg_tblspc** lrwxrwxrwx 1 hpdp hpdp 37 May 10 10:49**16387 -> /var/opt/omni/server/db80_restore/idb** lrwxrwxrwx 1 hpdp hpdp 37 May 10 10:49 **16445 -> /var/opt/omni/server/db80_restore/jce** [root@linux ~]# **ln -sf /var/opt/omni/server/db80/idb /var/opt/omni/server/db80/pg/pg_tblspc/16387** [root@linux ~]# **ln -sf /var/opt/omni/server/db80/jce /var/opt/omni/server/db80/pg/pg_tblspc/16445**

Update Configuration Files

More complex changes should be done using a text editor such as vi.

[root@linux ~]# **perl -p -i -e 's/db80_restore/db80/g' /var/opt/omni/server/db80/pg/postgresql.conf** [root@linux ~]# **perl -p -i -e 's/db80_restore/db80/g' /var/opt/omni/server/db80/pg/postmaster.opts** [root@linux ~]# **perl -p -i -e 's/db80_restore/db80/g' /etc/opt/omni/server/idb/idb.config** [root@linux ~]# **perl -p -i -e 's/db80_restore/db80/g' /etc/init.d/hpdp-idb**

Additional Clean up

This may or may not apply to your configuration.

[root@linux ~]# **rm -rf /var/opt/omni/server/db80_restore** [root@linux ~]# **rm -rf /var/opt/omni/server/db80/msg_*** [root@linux ~]# **rm -rf /var/opt/omni/server/db80/meta_*** [root@linux ~]# **rm -rf /var/opt/omni/server/log/auditing_***

Start the services and do basic verification

This also updates the references to the table spaces before starting the remaining services.

[root@linux ~]# omnisv start -idb_only The Internal database services successfully started. [root@linux ~]# omnisv status ProcName Status [PID] ================================ crs : Down mmd : Down kms : Down hpdp-idb : Active [31686] hpdp-idb-cp : Active [31707] hpdp-as : Down omnitrig : Down Sending of traps disabled. ================================ Status: At least one of the Cell Server processes/services is not running. [root@linux ~]# **grep PGSUPERUSER /etc/opt/omni/server/idb/idb.config** PGSUPERUSER='**hpdp**'; [root@linux ~]# **grep PGPORT /etc/opt/omni/server/idb/idb.config** PGPORT='**7112**'; [root@linux ~]# su - hpdp [hpdp@linux ~]$ /opt/omni/idb/bin/psql -U hpdp -h /var/opt/omni/tmp -p 7112 postgres postgres=# SELECT spcname, spclocation FROM pg_tablespace; spcname | spclocation ------------+---------- pg_default | pg_global | hpdpidb | /var/opt/omni/server/db80_restore/idb hpjce | /var/opt/omni/server/db80_restore/jce (4 rows) postgres=# **UPDATE pg_tablespace SET spclocation = '/var/opt/omni/server/db80/idb' where spcname='hpdpidb';** UPDATE 1 postgres=# **UPDATE pg_tablespace SET spclocation = '/var/opt/omni/server/db80/jce' where spcname='hpjce';** UPDATE 1 postgres=# **\q** [hpdp@linux ~]$ **exit** [root@linux ~]# **omnisv start** Cell Server services successfully started. [root@linux ~]# omnidbcheck -extended Check Level Mode Status == Database connection -connection OK Schema consistency -schema_consistency OK Datafiles consistency -verify_db_files OK Database consistency -database_consistency OK Media consistency -media_consistency OK SIBF(readability) -sibf OK DCBF(presence and size) -bf OK OMNIDC(consistency) -dc OK DONE! [root@linux ~]# omnib -idb_list LINUX_IDB - barmode full [Normal] From: BSM@linux.domain.tld "LINUX_IDB" Time: 05/10/2014 12:44:16 PM OB2BAR application on "linux.domain.tld" successfully started. [Normal] From: OB2BAR_POSTGRES_BAR@linux.domain.tld "DPIDB" Time: 05/10/2014 12:44:16 PM Checking the Internal Database consistency [Normal] From: OB2BAR_POSTGRES_BAR@linux.domain.tld "DPIDB" Time: 05/10/2014 12:44:17 PM Check of the Internal Database consistency succeeded [Normal] From: OB2BAR_POSTGRES_BAR@linux.domain.tld "DPIDB" Time: 05/10/2014 12:44:17 PM Putting the Internal database into the backup mode finished

Windows Cell Manager Clean Up

On a Windows Cell Manager the default installation paths are *C:|Program Files|OmniBack* and *C:|ProgramData|OmniBack*. In this example Data Protector is installed completely to *O:|OmniBack*. The IDB was stored in *O:|OmniBack|server|db80* and the restore was done to *O:|OmniBack|server|db80_restore*. Please adjust the original path and the restore path, commands and configuration file changes accordingly.

Stop the services and check restored directory structure

O:\>omnisv stop Cell Server services successfully stopped. O:\>**dir O:\OmniBack\server** Volume in drive O is OmniBack Volume Serial Number is 261B-48D4 Directory of O:\OmniBack\server 07/02/2015 10:36 AM <DIR> . 07/02/2015 10:36 AM <DIR> .. 06/15/2015 04:46 PM <DIR> AppServer **07/02/2015 10:40 AM <DIR> db80 07/02/2015 10:37 AM <DIR> db80_restore** 0 File(s) 0 bytes 5 Dir(s) 86,840,508,416 bytes free O:\>**dir O:\OmniBack\server\db80** Volume in drive O is OmniBack Volume Serial Number is 261B-48D4 Directory of O:\OmniBack\server\db80 07/02/2015 10:40 AM <DIR> . 07/02/2015 10:40 AM <DIR> .. 06/15/2015 04:47 PM <DIR> dcbf 07/01/2015 08:46 PM <DIR> idb 07/01/2015 08:46 PM <DIR> jce 06/15/2015 09:38 PM <DIR> keystore 06/15/2015 04:46 PM <DIR> logfiles **06/15/2015 04:46 PM <DIR> meta 07/02/2015 10:36 AM <DIR> meta_2015_07_02-4_1435826212** 07/02/2015 10:40 AM 13,276 mmd.ctx 06/15/2015 05:08 PM 16 mmd.id **06/15/2015 08:18 PM <DIR> msg 07/02/2015 10:36 AM <DIR> msg_2015_07_02-4_1435826212** 07/02/2015 10:39 AM <DIR> pg 06/15/2015 04:46 PM <DIR> reportdb 06/15/2015 04:46 PM <DIR> smisdb 06/15/2015 04:46 PM <DIR> sqldb 06/15/2015 04:46 PM <DIR> sysdb 06/15/2015 04:46 PM <DIR> vssdb 06/15/2015 04:46 PM <DIR> xpdb 2 File(s) 13,292 bytes 18 Dir(s) 86,840,508,416 bytes free O:\>**dir O:\OmniBack\server\db80_restore** Volume in drive O is OmniBack Volume Serial Number is 261B-48D4 Directory of O:\OmniBack\server\db80_restore 07/02/2015 10:37 AM <DIR> . 07/02/2015 10:37 AM <DIR> .. 07/02/2015 10:37 AM <DIR> idb 07/02/2015 10:37 AM <DIR> jce 07/02/2015 10:43 AM <DIR> pg 0 File(s) 0 bytes 5 Dir(s) 86,840,508,416 bytes free

Move the restored database to the target directory and adjust directory junctions

The name of the directory junctions might be different on your Cell Manager.

O:\>**rmdir /S /Q O:\OmniBack\server\db80\idb** O:\>**rmdir /S /Q O:\OmniBack\server\db80\jce** O:\>**rmdir /S /Q O:\OmniBack\server\db80\pg** O:\>**move /Y O:\OmniBack\server\db80_restore\idb O:\OmniBack\server\db80** O:\>**move /Y O:\OmniBack\server\db80_restore\jce O:\OmniBack\server\db80** O:\>**move /Y O:\OmniBack\server\db80_restore\pg O:\OmniBack\server\db80** O:\>**dir O:\OmniBack\server\db80\pg\pg_tblspc** Volume in drive O is OmniBack Volume Serial Number is 261B-48D4 Directory of O:\OmniBack\server\db80\pg\pg_tblspc 07/02/2015 10:37 AM <DIR> . 07/02/2015 10:37 AM <DIR> .. 07/02/2015 10:37 AM **<JUNCTION> 16387 [O:\OmniBack\server\db80_restore\idb]** 07/02/2015 10:37 AM **<JUNCTION> 16445 [O:\OmniBack\server\db80_restore\jce]** 0 File(s) 0 bytes 4 Dir(s) 87,235,559,424 bytes free O:\>**rmdir /Q O:\OmniBack\server\db80\pg\pg_tblspc\16387** O:\>**rmdir /Q O:\OmniBack\server\db80\pg\pg_tblspc\16445** O:\>**mklink /J O:\OmniBack\server\db80\pg\pg_tblspc\16387 O:\OmniBack\server\db80\idb** Junction created for O:\OmniBack\server\db80\pg\pg_tblspc\16387 <<===>> O:\OmniBack\server\db80\idb O:\>**mklink /J O:\OmniBack\server\db80\pg\pg_tblspc\16445 O:\OmniBack\server\db80\jce** Junction created for O:\OmniBack\server\db80\pg\pg_tblspc\16445 <<===>> O:\OmniBack\server\db80\jce

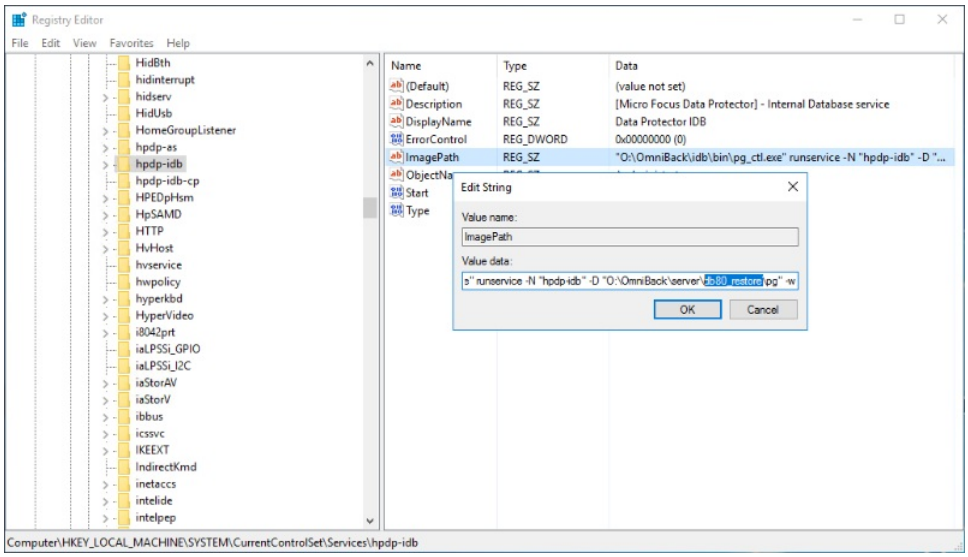
Update Configuration Files

For example replace all occurrences of *db80_restore* with *db80*. While looking at the *idb.config* file take a note of the values *PGSUPERUSER* and *PGPORT* as we need them when using the *psql* command.

O:\>**notepad O:\OmniBack\server\db80\pg\postgresql.conf** O:\>**notepad O:\OmniBack\server\db80\pg\postmaster.opts** O:\>**notepad O:\OmniBack\Config\Server\idb\idb.config**

Changes to the Windows Registry

Adjust the *ImagePath* registry value for the *hpdp-idb* service in *HKEY_LOCAL_MACHINE|SYSTEM|CurrentControlSet|Services|hpdp-idb* to reflect the previous changes



Additional Clean up

This may or may not apply to your configuration.

O:\>**rmdir /Q /S O:\OmniBack\server\db80_restore** O:\>**rmdir /Q /S O:\OmniBack\server\db80\meta_*** O:\>**rmdir /Q /S O:\OmniBack\server\db80\msg_*** O:\>**rmdir /Q /S O:\OmniBack\log\server\auditing_***

Start the services and do basic verification

This also updates the references to the table spaces before starting the remaining services.

O:\>**omnisv start -idb_only** The Internal database services successfully started. O:\>**omnisv status** ProcName Status [PID] ================================ crs : Down mmd : Down kms : Down hpdp-idb : Active [4136] hpdp-idb-cp : Active [5528] hpdp-as : Down omnitrig : Down omniinet : Down Sending of traps disabled ================================ Status: At least one of the Cell Server processes/services is not running. O:\>**O:\OmniBack\idb\bin\psql.exe -U hpdp -h localhost -p 7112 postgres** postgres=# **SELECT spcname, spclocation FROM pg_tablespace;** spcname | spclocation ------------+---------------------------- pg_default | pg_global | **hpdpidb | O:/OmniBack/server/db80_restore/idb hpjce | O:/OmniBack/server/db80_restore/jce** (4 rows) postgres=# **UPDATE pg_tablespace SET spclocation = 'O:/OmniBack/server/db80/idb' WHERE spcname = 'hpdpidb';** UPDATE 1 postgres=# **UPDATE pg_tablespace SET spclocation = 'O:/OmniBack/server/db80/jce' WHERE spcname = 'hpjce';** UPDATE 1 postgres=# **\q** O:\>**omnisv start** Cell Server services successfully started. O:\>**omnidbcheck -extended** Check Level Mode Status ========== Database connection -connection OK Schema consistency -schema_consistency OK Datafiles consistency -verify_db_files OK Database consistency -database_consistency OK Media consistency -media_consistency OK SIBF(readability) -sibf OK DCBF(presence and size) -bf OK OMNIDC(consistency) -dc OK DONE! O:\>**omnib -idb_list WINDOWS_IDB** [Normal] From: BSM@windows.domain.tld "WINDOWS_IDB" Time: 7/2/2015 11:15:17 AM OB2BAR application on "windows.domain.tld" successfully started. [Normal] From: OB2BAR_POSTGRES_BAR@windows.domain.tld "DPIDB" Time: 7/2/2015 11:15:18 AM Checking the Internal Database consistency [Normal] From: OB2BAR_POSTGRES_BAR@windows.domain.tld "DPIDB" Time: 7/2/2015 11:15:19 AM Check of the Internal Database consistency succeeded [Normal] From: OB2BAR_POSTGRES_BAR@windows.domain.tld "DPIDB" Time: 7/2/2015 11:15:19 AM Putting the Internal database into the backup mode finished

VMware Integration with Pre-Freeze and Post-Thaw Scripts

Prerequisites

The VMware Tools (or open-vm-tools) must be installed and running on the Virtual Machine. You must create the *backupScripts.d* directory where the scripts need to be executed.

- */etc/vmware-tools/backupScripts.d* on Linux VMs
- *C:\Program Files\VMware\VMware Tools\backupScripts.d* on Windows VMs

The *backupScripts.d* directory may contain one or multiple scripts that will be executed in sequence. The file names of the scripts affect the execution order (e.g. *10-application.sh*, then *20-database.sh*). Each script must be able to handle *freeze, freezeFail* and *thaw* arguments passed by the VMware Tools during the different phases. Make sure the scripts are executable (permissions, correct type for the VM operating system).

Sample Scripts

The following sample scripts may be used to start custom integrations with VMware Tools and the application running on the VM.

Sample Script for Linux

```
#!/bin/bash if [[ $1 == "freeze" ]] then     echo "This section is executed before the Snapshot is created" elif [[ $1 == "freezeFail" ]] then     echo "This section is executed when a problem occurs during snapshot creation and cleanup is needed since thaw is not executed" elif [[ $1 == "thaw" ]] then     echo "This section is executed when the Snapshot is removed" else     echo "Usage: `/bin/basename $0` [ freeze | freezeFail | thaw ]"     exit 1 fi
```

Sample Script for Windows

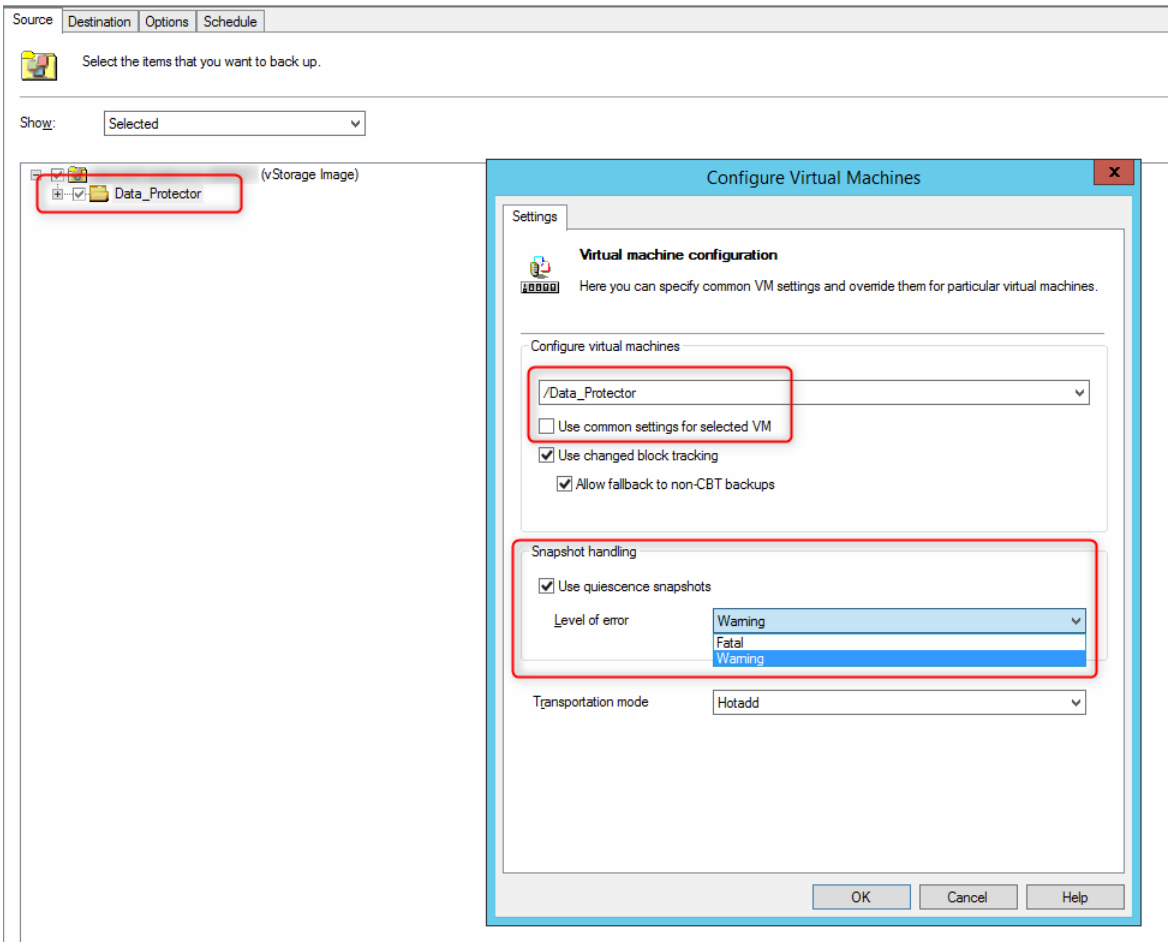
```
@echo off if "%~1" == ""       goto USAGE if %1    == freeze     goto FREEZE if %1    == freezeFail goto FREEZEFAIL if %1    == thaw      goto THAW :USAGE echo "Usage: %~nx0 [ freeze | freezeFail | thaw ]" goto END :FREEZE echo "This section is executed before the Snapshot is created" goto END :FREEZEFAIL echo "This section is executed when a problem occurs during snapshot creation and cleanup is needed since thaw is not executed" goto END :THAW echo "This section is executed when the Snapshot is removed" goto END :END
```

Manually Testing the Scripts

While developing your pre-freeze/post-thaw script solution it might be handy to have a quick solution to test it without running a backup. In that case use the VMware vCenter client to create a VM snapshot with the *Quiesce guest file system* option defined.

Using the Scripts in a Data Protector VMware backup

To allow the VMware Tools to execute the scripts during the VMware Snapshot backup the option *Use quiescence snapshots* must be used. This can be enabled on the top of the VMware Datacenter, a folder or on an individual VM. To configure it use Configure Virtual Machine from the context menu on the VM, folder or Datacenter in the Source tree. You may need to un-tick the *Use common settings for selected VM* are selected. Adjust the *Level of Error* to your needs. If the backup of the VM should be performed even if the quiescence operation failed select *Warning*. Select *Fatal* only if the backup of the VM should not be performed unless prepared by VSS and the scripts.


Source
Destination
Options
Schedule
Select the items that you want to back up.
Show:
Selected
(vStorage Image)
Data_Protector
Configure Virtual Machines
Settings
Virtual machine configuration
Here you can specify common VM settings and override them for particular virtual machines.
Configure virtual machines
/Data_Protector
Use common settings for selected VM
Use changed block tracking
Allow fallback to non-CBT backups
Snapshot handling
Use quiescence snapshots
Level of error
Warning
Fatal
Warning
Transportation mode
Hotadd
OK
Cancel
Help

Use Oracle RMAN with Data Protector

While Data Protector is usually using Recovery Manager (RMAN) to perform efficient backups and restores of Oracle Databases the process can be reversed to match the needs of more advanced Oracle DBAs. This means RMAN can be used to control Data Protector to perform backups, restores or validate backups. Data Protector will act as the media manager software leveraging the Media Management Layer (MML).

Prerequsites

The Oracle integration needs to be configured for the database in Data Protector and at least one backup spec must be configured to use an available backup device. It is recommended to test the backup spec. Please see the available documentation for configuration details.

If you don't want to allocate the Data Protector SBT library with each script, you can configure the RMAN defaults. This is especially useful for RMAN restore and maintenance operations.

```
CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE'; CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS
'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll';
```

The path to the SBT library for Oracle is different on Linux and UNIX. Oracle on a 64 bit Linux, HP-UX and Solaris needs `/opt/omni/lib/libob2oracle8_64bit.so` and AIX `/usr/omni/lib/libob2oracle8_64bit.a` . Please refer to the Data Protector session report after running a backup. For RMAN backup operations it is mandatory to allocate the Data Protector SBT library with the appropriate parameters.

RMAN Sample Scripts

The following scripts use **sample values** that must be changed according to the customer environment.

> Oracle Database Server: ORASRV
> Oracle SID: SID
> Oracle User: sys
> Oracle Password: password
> Oracle Backup Spec: ORASRV_SID_Full
> Oracle SBT library: C:/PROGRA~1/OmniBack/bin/orasbt.dll

Backup the Oracle Control File

Must be embedded in a run-block.

```
connect target sys/password@SID run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=SID,OB2BARLIST=ORASRV_SID_Full)'; backup format 'ORASRV_SID_Full<SID_%s:%t:%p>.dbf'
current controlfile; }
```

Validate the Backup of the Oracle Control File

Must be embedded in a run-block.

```
connect target sys/password@SID run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=SID,OB2BARLIST=ORASRV_SID_Full)'; restore controlfile validate; }
```

Restore the Oracle Control File

Must be embedded in a run-block.

```
connect target sys/password@SID run { allocate channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=SID,OB2BARLIST=ORASRV_SID_Full)'; restore controlfile to 'C:\Temp\control_file'; }
```

Sync RMAN Metadata with Data Protector MMDB

A run-block is not required for this command. Use `connect target sys/password@SID catalog rman/password@RCAT` instead of `connect target sys/password@SID` if a Recovery Catalog is used.

```
connect target sys/password@SID allocate channel for maintenance type 'sbt_tape' parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll
ENV=(OB2MAINTENANCE=1)'; crosscheck backup; delete noprompt expired backup;
```

Execute Scripts from RMAN

There are several ways to execute RMAN scripts. While you could simply paste the script into a RMAN session you could also save the script (e.g. validate.txt) to a file and run it using `@validate.txt` .

C:\>rman Recovery Manager: Release 12.2.0.1.0 - Production on Mon Dec 16 18:08:31 2019 Copyright (c) 1982, 2017, Oracle and/or its affiliates. All rights reserved. RMAN> @C:\RMAN\validate.txt RMAN> connect target * connected to target database: DCM (DBID=1582047051) RMAN> run { 2> allocate channel 'dev_0' type 'sbt_tape' 3> parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll [...]

Backup a single file system with multiple streams

File systems continue to grow and the underlaying disk subsystems become faster. Backing up a single file system with just one Disk Agent limits the backup and restore throughput. This document will guide you on how to quickly setup a file system backup spec that can start a large amount of Data Protector Disk Agents in parallel. It may be used to backup very large file systems on Windows File servers or NAS systems using CIFS.

Create the Datalist for a Windows Client

Create a new ASCII file in `%DP_HOME_DIR%\Config\Server\Datalists` (Windows) or `/etc/opt/omni/server/datalists` (Linux, HP-UX). The file (e.g. FS_FILESERVER) should not have an extension with the following content.

```
DATALIST "FS_FILESYSTEM" DESCRIPTION "Multi-Streaming Backup Spec" DYNAMIC 1 27 DEFAULTS { FILESYSTEM { -opt_dedupe_vol_bkp -vss no_fallback -no_async } -protect weeks 1 RAWDISK { } } DEVICE "REPLACE_BACKUP_DEVICE" { } WINFS "H:\Home" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/$Recycle.Bin" } WINFS "H:\Home\A*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\B*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\C*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\D*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\E*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\F*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\G*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\H*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\I*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\J*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\K*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\L*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\M*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\N*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\O*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\P*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\Q*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\R*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\S*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\T*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\U*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\V*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\W*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P
```

" "/Home/Q" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\X*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\Y*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Z*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" } WINFS "H:\Home\Z*" client.domain.com:"/H" { -trees "/Home" -exclude "/Home/A*" "/Home/B*" "/Home/C*" "/Home/D*" "/Home/E*" "/Home/F*" "/Home/G*" "/Home/H*" "/Home/I*" "/Home/J*" "/Home/K*" "/Home/L*" "/Home/M*" "/Home/N*" "/Home/O*" "/Home/P*" "/Home/Q*" "/Home/R*" "/Home/S*" "/Home/T*" "/Home/U*" "/Home/V*" "/Home/W*" "/Home/X*" "/Home/Y*" "/Home/0*" "/Home/1*" "/Home/2*" "/Home/3*" "/Home/4*" "/Home/5*" "/Home/6*" "/Home/7*" "/Home/8*" "/Home/9*" "/Home/.*" "/Home/_*" "/Home/$*" }

Modify the Backup Spec for a Windows Client

Replace the following strings using search and replace of your favorite text editor. You need to be exact and should follow the sequence to ensure consistent results. In the following example we will change the backup spec from *H:|Home* to *X:|*.

1. **FS_FILESYSTEM** with the file name of the datalist that is used (e.g. FS_FILESERVER if the datalist is saved as FS_FILESERVER)
2. **client.domain.com** with the client where the backup needs to be executed (e.g. fileserver.company.local)
3. **:"/H"** with the corresponding drive letter where the folder and/or drive resides (e.g. :"/X")
4. **H:\Home** with the folder and/or drive that you want to backup (e.g X:\)
5. **H:\Home** with the folder and/or drive that you want to backup (e.g X:\)
6. **"/Home/** with the tree where to start the backup (e.g. "/)
7. **"/Home** with the tree where to start the backup (e.g. "/)
8. **REPLACE_BACKUP_DEVICE** with the backup device you want to use. This can be done in the GUI. You should also consider adjusting the load balancing to match source performance and target device capabilities.

Setup the Datalist for a Linux or UNIX Client

Create a new ASCII file in %DP_HOME_DIR%\Config\Server\Datalists (Windows) or /etc/opt/omni/server/datalists (Linux, HP-UX). The file (e.g. FS_FILESERVER) should not have an extension with the following content.

DATALIST "FS_FILESYSTEM" DESCRIPTION "Multi-Streaming Backup Spec" DYNAMIC 1 27 DEFAULTS { FILESYSTEM { } -protect weeks 1 RAWDISK { } } DEVICE "REPLACE_BACKUP_DEVICE" { } FILESYSTEM "/tmp" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" } FILESYSTEM "/tmp/A*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/B*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/C*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/D*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/E*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/F*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/G*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/H*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/I*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/J*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/K*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/L*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/t

mp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/M*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/N*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/O*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/P*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/Q*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/R*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/S*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/T*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/U*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/V*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/W*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/X*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/X*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/Y*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/z*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/Y*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Z*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" } FILESYSTEM "/tmp/Z*" client.domain.com:"/tmp" { -trees "/tmp" -exclude "/tmp/A*" "/tmp/B*" "/tmp/C*" "/tmp/D*" "/tmp/E*" "/tmp/F*" "/tmp/G*" "/tmp/H*" "/tmp/I*" "/tmp/J*" "/tmp/K*" "/tmp/L*" "/tmp/M*" "/tmp/N*" "/tmp/O*" "/tmp/P*" "/tmp/Q*" "/tmp/R*" "/tmp/S*" "/tmp/T*" "/tmp/U*" "/tmp/V*" "/tmp/W*" "/tmp/X*" "/tmp/Y*" "/tmp/a*" "/tmp/b*" "/tmp/c*" "/tmp/d*" "/tmp/e*" "/tmp/f*" "/tmp/g*" "/tmp/h*" "/tmp/i*" "/tmp/j*" "/tmp/k*" "/tmp/l*" "/tmp/m*" "/tmp/n*" "/tmp/o*" "/tmp/p*" "/tmp/q*" "/tmp/r*" "/tmp/s*" "/tmp/t*" "/tmp/u*" "/tmp/v*" "/tmp/w*" "/tmp/x*" "/tmp/y*" "/tmp/1*" "/tmp/2*" "/tmp/3*" "/tmp/4*" "/tmp/5*" "/tmp/6*" "/tmp/7*" "/tmp/8*" "/tmp/9*" "/tmp/0*" "/tmp/.*" "/tmp/-*" "/tmp/_*" "/tmp/$*" "/tmp/~*" }

Modify the Backup Spec for a Linux/UNIX Client

Replace the following strings using search and replace of your favorite text editor. You need to be exact and should follow the sequence to ensure consistent results. In the following example we will change the backup spec from *H:|Home* to *X:|*.

1. **FS_FILESYSTEM** with the file name of the datalist that is used (e.g. FS_FILESERVER if the datalist is saved as FS_FILESERVER)
2. **client.domain.com** with the client where the backup needs to be executed (e.g. fileserver.company.local)
3. **"/tmp** with the corresponding mount point or folder where the data resides (e.g. "/home)
4. **REPLACE_BACKUP_DEVICE** with the backup device you want to use. This can be done in the GUI. You should also consider adjusting the load balancing to match source performance and target device capabilities.

Validation

After saving the datalist, verify the results in the Data Protector GUI. Also review the other important options such as data and catalog protection and adjust them accordingly. Consider the number of CPU cores available on the backup client. Especially when using Server-side or Source-side Deduplication this kind of backup adds additional load to the system.

Execute the backup and also verify the results in the *Restore* context of the Data Protector GUI. Select *Flesystem* and browse the objects backed up on the client. You will see a large number of objects for the client. Each of them should only contain a subset of the files backed up. All files and folders starting with A will be in the *X:|A** object and so on. All other files will be backed up in the *X:|* object.

For more info, visit docs.microfocus.com