MICRO FOCUS

Data Protector

软件版本：10.00

安装指南

文档发行日期：2017 年 6 月
软件发行日期：2017 年 6 月

法律声明

担保

Micro Focus or one of its affiliates 产品和服务随附的明示担保声明中说明了对此类产品和服务的全部担保。 本文所述的任何内容均不构成额外担保。Micro Focus 对本文中的技术或编辑错误或遗漏概不负责。

本文所含信息如有更改，恕不另行通知。

受限权利说明

机密计算机软件。 占有、使用或复制本文档需要 Micro Focus 提供有效许可证。根据 FAR 12.211 和 12.212 的规定，商业计算机软件、计算机软件文档和商业项目的技术数据依据供应商的标准商业许可授权给美国政府使用。

版权通知

商标通知

Adobe™ 是 Adobe Systems Incorporated 的商标。

Microsoft® 和 Windows® 是 Microsoft Corporation 在美国的注册商标。

UNIX® 是 The Open Group 的注册商标。

本产品包含版权归 © 1995-2002 Jean-loup Gailly and Mark Adler 所有的“zlib”通用压缩库界面。

文档更新

该文档的标题页面包含如下标识信息：

- 软件版本号，表示软件版本。
- 文档发行日期，会在文档每次更新时进行更改。
- 软件发行日期，表示该软件版本的发行日期。

要查看最近的软件更新，请转到 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=。

要验证是否在使用最新版本的文档，请转到 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

该站点要求注册 Passport 并登录。要注册 Passport ID，请转到 https://cf.passport.softwaregrp.com/hppcf/login.do。

如果您订阅了相应的产品支持服务，您还将收到该产品的更新或新版本。 请联系您的销售代表了解详细信息。

支持

请访问软件在线支持网站，网址为 https://softwaresupport.softwaregrp.com/。

该网站提供有关软件所提供的产品、服务和支持的联系信息和详细信息。

软件在线支持为客户提供自助解决的能力。 通过它，可以快捷高效地访问管理业务所必需的交互式技术支持工具。 作为一名重要的支持客户，您可通过使用支持网站获得以下益处：

- 搜索您所感兴趣的知识文档
- 提交并追踪支持案例和增强请求
- 下载软件修补程序
- 访问产品文档
- 管理支持合同
- 查找客户支持合同

- 查看关于可用服务的信息
- 与其他软件客户一起探讨
- 研究软件培训并注册

大多数支持区域要求注册为 Passport 用户并登录。许多地方还要求阅读支持合同。

要注册 Passport ID，请转到 https://cf.passport.softwaregrp.com/hppcf/login.do。

有关访问级别的详细信息，请转到 https://softwaresupport.softwaregrp.com/。

内容

第 1 章： 安装过程概述

本章提供 Data Protector 安装过程的概述，并介绍适用于安装的概念。 本章还将介绍 Data Protector Cell Manager 和 Data Protector 用户界面。

安装过程概述

Data Protector 备份环境是一组系统，具有位于相同时区的通用备份策略，并存在于同一个 LAN/SAN 上。此网络环境称为 Data Protector **单元**。典型单元由 Cell Manager、安装服务器、客户机和备份设备组成。

Cell Manager 是从一个中心点管理单元的主系统。它包含 Data Protector 内部数据库 (IDB)，并运行核心 Data Protector 软件和会话管理器。

IDB 跟踪备份的文件和单元配置。

安装服务器是一个单独的系统或 Cell Manager 组件，它包含用于远程客户机安装的 Data Protector 软件存储库。这项 Data Protector 功能极大地简化了软件安装过程，尤其是对于远程客户机。

一个单元通常有一个 Cell Manager 和多个客户机组成。只要计算机系统上安装了某个 Data Protector 软件组件，该系统就将成为 Data Protector **客户机**。系统上安装的客户机组件取决于该系统在备份环境中的角色。Data Protector 组件既可以本地安装到单个系统，也可以通过 安装服务器 安装到多个系统。

用户界面组件需要用来访问 Data Protector 功能，并执行所有配置和管理任务。它必须安装在用于备份管理的系统上。Data Protector 提供图形用户界面 (GUI) 和命令行界面 (CLI)。

具有需备份的磁盘的客户机系统中必须已安装适当的 Data Protector **磁盘代理**组件。磁盘代理可用于备份客户机磁盘中的数据，或者还原这些数据。

具有需备份的应用程序和虚拟环境的客户机系统中必须已安装适当的 Data Protector 集成代理组件。集成代理可用于从应用程序或虚拟环境备份数据，或者还原数据。

连接了备份设备的客户机系统必须装有**介质代理**组件。此软件将管理备份设备和介质。Data Protector 具有两个介质代理：**常规介质代理**和**NDMP 介质代理**。只有在控制 NDMP 服务器备份的客户机系统上才需要 NDMP 介质代理(在控制 NDMP 专用驱动器的客户机系统上)。在所有其他情况下，两个介质代理可互换。

在网络上安装 Data Protector 之前，定义：

- 将要安装 Cell Manager 的系统。如需了解受支持的操作系统和版本，请参见 https://softwaresupport.softwaregrp.com/ 上的最新支持矩阵。

  每个单元仅可拥有一个 Cell Manager。如果不安装 Cell Manager，则无法运行 Data Protector。
- 用于通过用户界面访问 Data Protector 功能的系统。这些系统必须安装了用户界面组件。
- 将要备份的系统。这些系统必须安装了磁盘代理组件(用于文件系统备份)以及相关的应用程序代理组件(用于联机数据库集成)。
- 连接备份设备的系统。这些系统必须安装介质代理组件。
- 要在其上安装 Data Protector 安装服务器 的一个或多个系统。有两种 安装服务器 可用于远程软件安装：一种用于 UNIX 客户机，另一种用于 Windows 客户机。

针对 安装服务器 选择系统独立于 Cell Manager 和要在其上安装“用户界面”的系统。Cell Manager 和 安装服务器 可以安装在相同系统上，也可以安装在不同系统上。

安装服务器 可在多个 Data Protector 单元之间共享。

重要：
在 Solaris 系统上安装 Data Protector 客户机时，请确保将 /usr/omni 目录中的所有文件保存到其他目录。Data Protector 安装将删除 /usr/omni 目录中的所有文件。

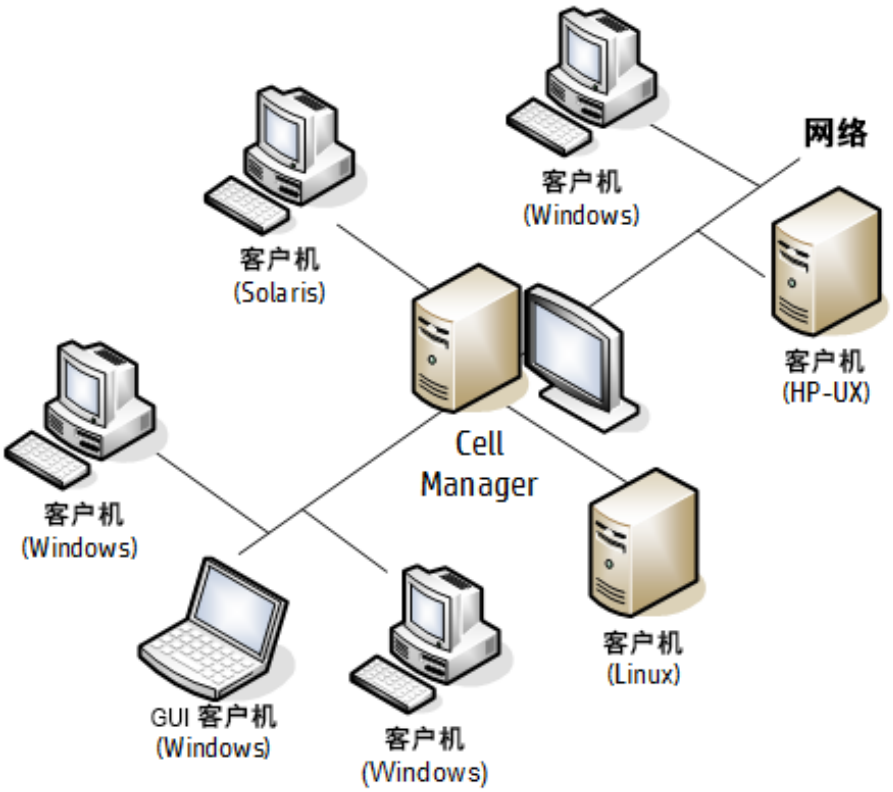
定义好系统在未来 Data Protector 单元中的角色之后，安装过程将由以下常规步骤组成：

1. 检查安装的必备条件。
2. 安装 Data Protector Cell Manager。
3. 安装 安装服务器 和用户界面。
4. 远程安装客户机系统(推荐选项，适用情况下)，或者从安装程序包 (zip/tar) 本地安装。

注意：
如果 Windows 系统上已经安装了 安装服务器，那么不可在该系统上远程安装 Data Protector 客户机。若要在同一系统上安装 安装服务器 和客户机组件，必须从 Data Protector Windows 安装程序包 (zip) 执行本地客户机安装。在“自定义安装 (Custom Setup)”窗口中，选中所有需要的客户机组件和 安装服务器 组件。

Windows XP Home Edition 和 HP OpenVMS 客户机也无法进行远程安装。在这些客户机上必须进行本地安装。

Data Protector 单元



远程安装概念

每次执行远程安装时，都需要通过 GUI 访问 安装服务器。用户界面组件可安装在 Cell Manager 上(虽然这不是必需的)。明智的做法是在多台系统上安装用户界面，这样就可以从不同的位置访问 Cell Manager。

可以从 Windows 版的 安装服务器 将客户机软件分发到任何 Windows 系统。

Windows 系统必须通过 Data Protector Windows 安装程序包 (zip) 进行本地安装。

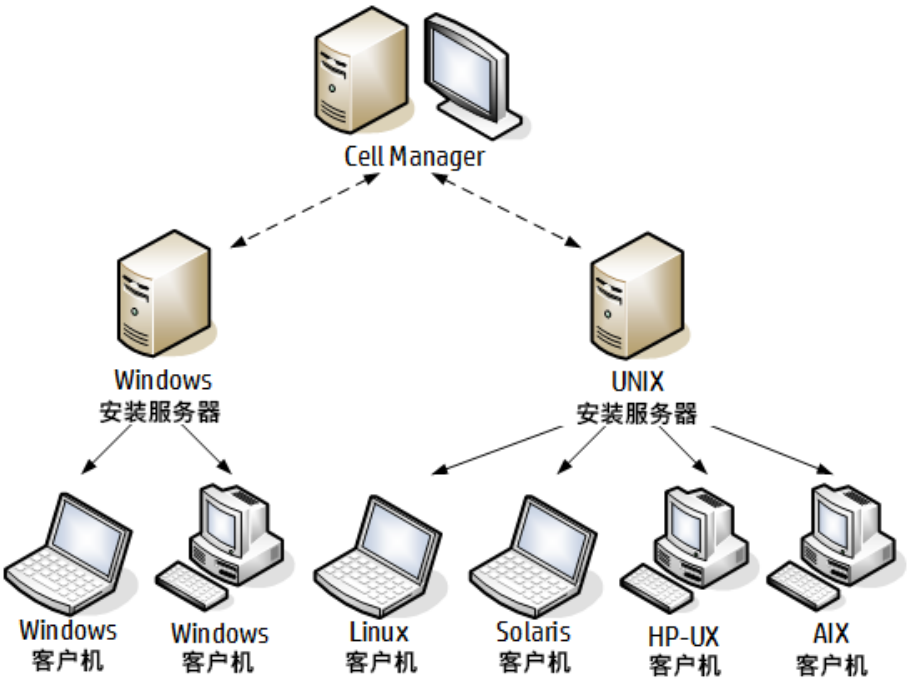
可以适用于 UNIX 系统的 安装服务器 在 HP-UX、Solaris、Linux、AIX 以及其他受支持的 UNIX 操作系统上，远程安装客户机软件。有关受支持平台的列表，请参见《》。 *Data Protector 支持矩阵*。尽管在本地安装客户机不需要 安装服务器，但保持客户机补丁更新需要它。

对于不支持远程安装的 UNIX 操作系统，或者，如果未安装 UNIX 版的 安装服务器，则可以从 Data Protector UNIX 安装程序包 (tar) 本地安装 UNIX 客户机。

有关不同 Data Protector 客户机的可用安装方法的更多信息，请参见安装 Data Protector 客户机 (第 49 页)。

有关在本地卸载 UNIX 客户机的过程，请参见在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)。

Data Protector 安装概念



Data Protector 安装介质

Data Protector支持各种操作系统和多种处理器架构。该软件以 zip/tar 形式提供。

> **注意：**
> Data Protector 适用于 Windows Server 2008 和 Windows Server 2012 系统的安装文件由 Micro Focus 进行数字签名。

下表列出了可从 https://softwaresupport.softwaregrp.com/ 下载的不同程序包。

程序包名称	内容
Data Protector 软件 10.00，Windows DP_A1000_Windows_OVMS.zip	• 针对 64 位 (AMD64/Intel EM64T) Windows 系统的 Cell Manager 和 安装服务器 • 电子 PDF 格式的全套英语和本地化指南。 • Windows 32/64 位客户机 • HP OpenVMS 客户机 (Alpha 和 Itanium 系统) • 产品信息 • 软件集成包
Data Protector 软件 10.00 HP-UX DP_A1000_UX11x.tar.gz	• 针对 HP-UX 系统的 Cell Manager、安装服务器 和客户机 • 针对其他 UNIX 系统的客户机 • 适用于 Mac OS X 系统的客户机 • 电子 PDF 格式的全套英语和本地化指南。 • 软件集成包
Data Protector 软件 10.00 Linux DP_A1000_GPLx86_64.tar.gz	• 适用于 Linux 系统的 Cell Manager、安装服务器和客户机 • 针对其他 UNIX 系统的客户机 • 适用于 Mac OS X 系统的客户机 • 电子 PDF 格式的全套英语和本地化指南。 • 软件集成包

选择 Cell Manager 系统

Cell Manager 是 Data Protector 单元中的主系统。它从中心点管理单元。Cell Manager 执行以下功能：

- 运行核心 Data Protector 软件。
- 主机 Data Protector 内部数据库 (IDB) 服务器。
- 收集和维护包含有关 Data Protector 会话信息的数据。
- 运行启动的会话管理器，停止不同类型的 Data Protector 会话，并将相关信息存储到 IDB 中。

在决定要在环境中的哪个系统上安装 Cell Manager 之前，请注意以下几点：

- 支持的平台

  Cell Manager 可以安装在 Windows、HP-UX 或 Linux 平台上。

  有关这些平台受支持的版本或发行版的详细信息，请参见 https://softwaresupport.softwaregrp.com/ 上的最新支持矩阵。

- Cell Manager 系统的可靠性

  由于 Cell Manager 包含 IDB，并且一旦 Cell Manager 不正常工作，备份和还原将无法执行，因此选择环境中极其可靠的系统进行安装就显得非常重要。

- 数据库增长和和所需磁盘空间

  Cell Manager 包含 Data Protector 内部数据库 (IDB)。IDB 包含有关已备份数据及其介质、会话消息和设备的信息。IDB 的规模可能会增长到非常大，具体取决于您的环境。例如，如果大部分备份始于文件系统备份，那么通常 IDB 大小为备份数据所使用的磁盘空间的 2%。

  有关规划和管理数据库大小和增长的相关信息，请参见 *Data Protector 帮助*索引：“IDB 的增长和性能”。

  有关 IDB 的最低磁盘空间要求，请参见Data Protector产品声明、软件说明和参考。

> **注意：**
> 不必将 Cell Manager 用作用户界面系统。例如，可以将 UNIX Cell Manager 系统和 Data Protector 用户界面组件安装在带 Windows 平台的其他系统上。

下面的步骤

要确定未来的 Cell Manager 系统的最低要求，请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。

选择 Data Protector 用户界面系统

Data Protector 提供两种用户界面：图形用户界面 (GUI) 和命令行界面 (CLI)。GUI 适用于 Windows 平台，CLI 适用于 Windows、HP-UX、Solaris 和 Linux 平台。两种用户界面都由单个 Data Protector 软件组件提供，也作为该组件安装。

选择用于控制单元的系统将由网络管理员或备份操作员使用。但是，在大型计算机环境中，理想的做法可能是在多个系统上运行用户界面，而对于混合环境，则在不同的平台上运行。

有关用户界面支持的操作系统(发行版、版本、版次)的详细信息，请参见 https://softwaresupport.softwaregrp.com/ 上的最新支持矩阵。有关本地语言支持，以及文件名中非 ASCII 字符用法的更多信息，请参见 *Data Protector 帮助*索引：“语言设置, 自定义”。

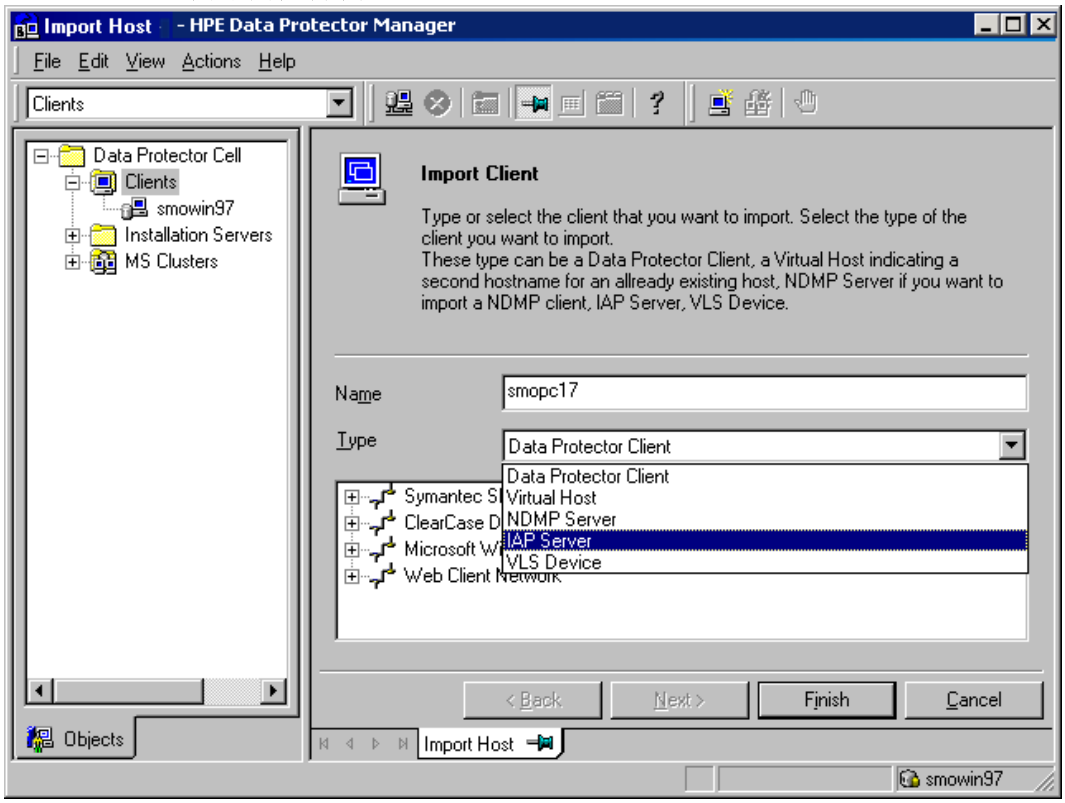
在单元中的某台系统上安装用户界面后，就可以从该系统远程访问 Cell Manager。不必在 Cell Manager 上使用图形用户界面系统。

Data Protector 图形用户界面

Data Protector GUI 是便于访问 Data Protector 功能的强大用户界面。主窗口包含多个视图，如**客户机**、**用户**、**设备和介质**、**备份**、**还原**、**对象操作**、**报告**、**监视器**、**即时恢复**和**内部数据库**，可用于执行所有相关任务。

例如，在**客户机 (Clients)**视图中，可通过指定所有目标系统，并定义发送给指定安装服务器的安装路径和选项来远程安装(添加)客户机。在客户机上运行安装时，监视窗口中将只显示与安装有关的消息。

Data Protector 图形用户界面



另请参见Data Protector 图形用户界面 (第 350 页)，其中定义了 Data Protector GUI 中最重要的区域。

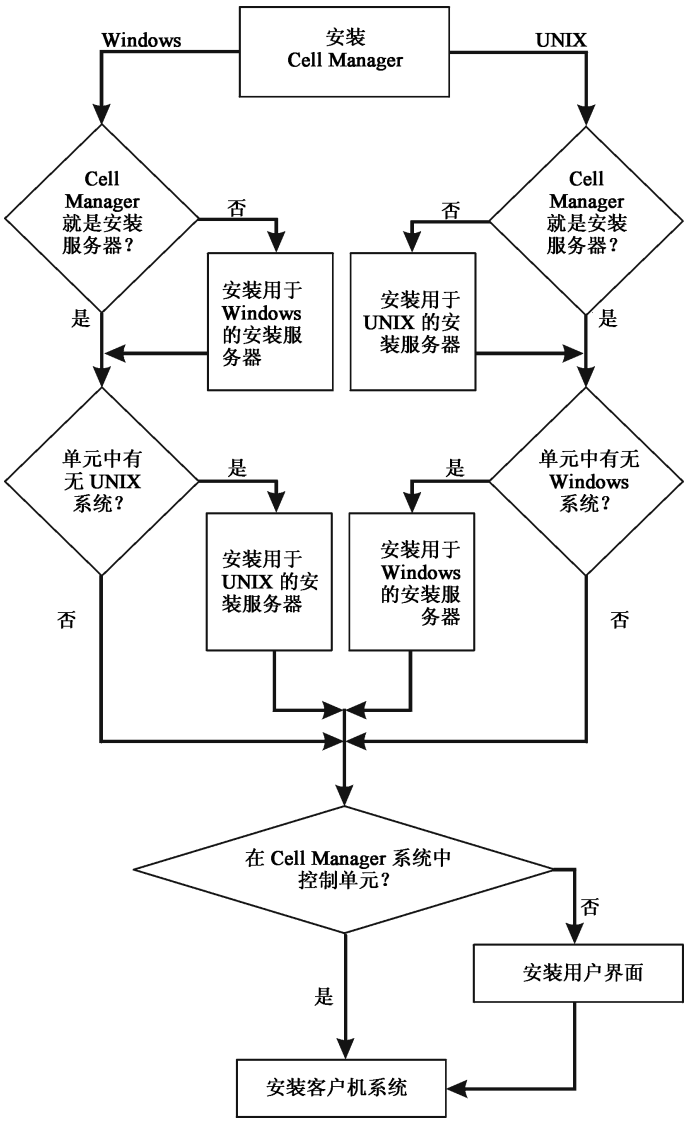
第 2 章： 正在安装 Data Protector

本章包含有关以下方面的详细说明信息：

- 安装 Data Protector Cell Manager 和 安装服务器
- 安装 Data Protector单服务器版

安装 Data Protector Cell Manager 和 安装服务器

安装过程



如果在同一系统上安装 Cell Manager 和 安装服务器，可以在一步中执行该任务。

重要：
Data Protector 单元中的所有配置和会话信息文件都存储在 Cell Manager 上。要将该信息传输到另一个系统是很困难的。因此，请确保 Cell Manager 是处于稳定受控环境中的可靠系统。

注意：
Data Protector 10.00 GUI 的先前版本与 Data Protector 10.00 Cell Manager 不兼容。

安装 UNIX Cell Manager

本节提供有关如何安装 UNIX Cell Manager的逐步指示信息。 要仅安装 Windows Cell Manager，请参见安装 Windows Cell Manager (第 32 页)。

先决条件

- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 默认用户 `unmask` 必须设置为 `022`，否则一些 Data Protector 服务可能无法启动。
- 用于安装的用户帐户必须对选定的目标系统具有管理 (`root`) 特权。
- 成为 Cell Manager 的系统必须：
  - 安装了受支持的 UNIX 操作系统。 有关 Cell Manager 支持的操作系统的列表，请参见 https://softwaresupport.softwaregrp.com/。
  - 有足够的磁盘空间可用于 Data Protector Cell Manager 软件。 Cell Manager 必须满足以下最低要求：
    - Cell Manager 上每个进程的软文件限制至少应为 1024。
    - ***HP-UX 系统：*** 8 GB 的总 RAM；***Linux 系统：*** 4 GB 的总 RAM。

    对于每个并行备份会话，需要 40 MB RAM，每个数据段大小 5–8 MB。 例如，如果您要运行 60 个并行备份会话，就需要 3 GB RAM + 512 MB 的数据段。

    您可以通过安装 Data Protector 到链接目录中来克服可用磁盘空间不足。 在创建链接之前，请参见在 HP-UX 和 Linux 系统上安装的目录结构 (第 29 页)。
  - 有足够的磁盘空间可用于 Data Protector 内部数据库 (IDB)。 要恢复内部数据库，需要两倍的总 RAM。 1.5 GB 可用磁盘空间 + /var 目录(其中已存储 IDB)中每个备份文件大约 100 字节(供 IDB 使用)。 请注意，当前的 IDB 设计允许重新放置数据库二进制文件(如果由于数据库规模增长而需要这么做)。

    如果磁盘卷的可用存储空间不足，则可以使用链接目录，但必须在安装之前先创建这些链接，并确保目标目录存在。
  - TCP/IP 协议已安装，并且正在运行。 协议必须能够解析主机名。
  - 可识别 Cell Manager 系统(如果使用 NIS 服务器)。 请参见准备 NIS 服务器 (第 311 页)。
  - 有以下空闲端口：

- 5565 — 在 Data Protector 中执行新安装所需的端口。
- 5555 — Data Protector 安装升级期间所需的端口。
- 7112 — 内部数据库服务端口
- 7113 — 内部数据库连接池程序 (IDB CP) 端口
- 7116 — 应用程序服务器 (HTTPS AS) 端口
- 9999 — 应用程序服务器管理端口

要更改默认通信端口号，请参见更改默认的 Data Protector Inet 端口 (第 306 页)。
要更改默认 IDB 和应用程序服务器端口，请参见在 UNIX 系统中更改默认的 Data Protector IDB 端口和用户帐户 (第 308 页)。

- 支持长文件名。 要检查文件系统是否支持长文件名，请执行 `getconf NAME_MAX DirectoryPath` 命令。
- 已安装基本的命令行计算器 (bc)。
- 已将用户组 hpdp 和该用户组中的专用用户帐户 hpdp 配置为由 Data Protector 使用。 要更改默认用户帐户，请参见在 UNIX 系统中更改默认的 Data Protector IDB 端口和用户帐户 (第 308 页)。
- 已经为 hpdp 用户配置现有主文件夹，否则部分 Data Protector 服务将无法启动。
- hpdp 用户必须能够从系统中已经存在的以下路径访问任何目录：
  - `/opt/omni/*`
  - `/etc/opt/omni/*`
  - `/var/opt/omni/*`

Linux 系统：

- 已在 64 位 Linux 系统 (x86_64) 上安装 32 位 GNU C 库 (glibc)。
- 已安装 net 工具(安装期间需要一些 net 工具实用程序)。

群集感知Cell Manager

对于安装群集感知 Cell Manager，还有另外一些先决条件和步骤。 请参见安装群集感知 Cell Manager (第 144 页)。

> **注意：**
> 在多单元环境 (MoM) 中，所有 Cell Manager 必须安装相同的 Data Protector 版本。

建议

- Micro Focus 建议在储存 Data Protector 内部数据库和预计可增长到大于 2GB 的 DC 二进制文件的文件系统上使用大文件支持 (LFS)。

设置内核参数

HP-UX 系统：

- 将内核参数 shmmax(最大共享内存段大小)至少设置为 2.5 GB。 要检查此配置，请执行以下命令：

  ```
  kcusage shmmax
  ```

- Micro Focus 建议将内核参数 maxdsiz(最大数据段大小)或 maxdsiz_64 至少设置为 134217728 个字节 (128 MB)，将内核参数 semmnu(信号量撤消结构数量)至少设置为 4000。 semmnu 参数必须允许最大数量的并行备份或还原或复制会话 (1000) 和相同数量的数据库查询会话 (1000)。 如果您不计划执行最大数量的并行会话，则不需要更改 semmnu 参数的值。

  提交这些更改后，重新启动系统。

Linux 系统：

- 将内核参数 shmmax(最大共享内存段大小)至少设置为 2.5 GB。 要检查此配置，请执行以下命令：

  ```
  cat /proc/sys/kernel/shmmax
  ```

  要恢复内部数据库，内核参数值应设为以上值的两倍。

安装过程

如果在同一系统上安装 Cell Manager 和 安装服务器，可以通过执行 omnisetup.sh -CM -IS 在一步中执行安装。

有关 omnisetup.sh 命令的说明，请参见 tar 程序包 中的 README 文件或 tar 程序包的 /DOCS/C/MAN 目录中的 *Data Protector 命令行界面参考*。

要在 **HP-UX** 或 **Linux** 系统上安装 **Cell Manager**，请执行以下操作：

1. 复制 HP-UX 或 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。

   ```
   LOCAL_INSTALL
    platform_dir /DP_DEPOT
   ```

   其中，*platform_dir* 为：

hpux	对于 HP-UX 系统
linux_x86_64	对于 Linux 系统

2. 转到 LOCAL_INSTALL 目录并执行：

   ```
   ./omnisetup.sh -CM
   ```

   有关 omnisetup.sh 命令的详细信息，请参见 *Data Protector 命令行界面参考*。

如果要在 Cell Manager 上安装 UNIX 的 安装服务器，则可以在此时进行。 有关所需步骤，请参见在 UNIX 系统上安装 安装服务器 (第 39 页)。

在 HP-UX 和 Linux 系统上安装的目录结构

安装完成时，核心 Data Protector 软件位于 /opt/omni/bin 目录中， 适用于 UNIX 的 安装服务器 位于 /opt/omni/databases/vendor 目录中。 以下列表显示了 Data Protector 子目录及其内容：

重要：
要将 Data Protector 安装到链接目录中，例如：

/opt/omni/ -> /*prefix*/opt/omni/

/var/opt/omni/ -> /*prefix*/var/opt/omni/

/etc/opt/omni/ -> /*prefix*/etc/opt/omni/

应该在安装前创建链接并确保目标目录存在。

/opt/omni/bin	用户命令
/opt/omni/help/C	帮助
/opt/omni/lbin	管理命令、命令行实用程序
/opt/omni/sbin	管理命令、命令行实用程序
/opt/omni/sbin/install	安装脚本
/etc/opt/omni	配置数据
/opt/omni/lib	用于压缩、数据编码和设备处理的共享库
/opt/omni/doc/C	指南采用电子 PDF 格式
/var/opt/omni/log /var/opt/omni/server/log	日志文件
/opt/omni/lib/nls/C	消息编目文件
/opt/omni/lib/man	手册页面
/var/opt/omni/tmp	临时文件
/var/opt/omni/server/db80	IDB 文件 有关详细信息，请参见 *Data Protector 帮助* 索引：“IDB, 目录位置”。
/opt/omni/AppServer	Data Protector 应用程序服务器。
/opt/omni/idb	Data Protector 内部数据库。
/opt/omni/jre	与 Data Protector 一起使用的 Java 运行时环境。

配置自动启动和关闭

Data Protector 安装程序会配置每次系统重新启动时所有 Data Protector 进程的自动启动和关闭。 该配置的有些部分与操作系统有关。

它会自动配置以下文件：

HP-UX 系统：

/sbin/init.d/omni	带有启动和关闭程序的脚本。
/sbin/rc1.d/K162omni	指向用来关闭 /sbin/init.d/omni 的 Data Protector 脚本的链接。
/sbin/rc2.d/S838omni	指向用来启动 /sbin/init.d/omni 的 Data Protector 脚本的链接。
/etc/rc.config.d/omni	包含 omni 参数，它定义： omni=1 Data Protector 在系统重新启动时自动停止和启动。这是默认选项。 omni=0 在系统重新启动时不自动停止和启动 Data Protector。

Linux 系统：

/etc/init.d/omni	带有启动和关闭程序的脚本。
/etc/rc*init_level*.d/K10omni	指向用来关闭 /etc/init.d/omni 的 Data Protector 脚本的链接。 其中，*init_level* 为 1 和 6。
/etc/rc*init_level*.d/S90omni	指向用来启动 /etc/init.d/omni 的 Data Protector 脚本的链接。 其中，*init_level* 为 2、3、4 和 5。

在安装期间，会修改 Cell Manager 系统上的以下系统文件：

HP-UX 系统：

/etc/services	向文件中添加服务的 Data Protector 端口号。
/opt/omni/lbin/crs	添加 Data Protector CRS 服务。

安装完成时，在 Cell Manager 上会有以下进程在运行：

/opt/omni/lbin/crs	Data Protector Cell Request Server (CRS) 服务在 Cell Manager 系统上运行，并且会在将 Cell Manager 软件安装到系统上时启动。 CRS 负责启动和控制单元中的备份和还原会话。
/opt/omni/lbin/mmd	Data Protector Media Management Daemon (MMD) 服务在 Cell Manager 上运行，并且会在将 Cell

	Manager 软件安装到系统上时启动。 MMD 管理设备和介质管理操作。
/opt/omni/lbin/kms	Data Protector Key Management Server (KMS) 服务在 Cell Manager 上运行，并且会在将 Cell Manager 软件安装到系统上时启动。 KMS 为 Data Protector 加密功能提供密钥管理。
/opt/omni/idb/bin/postgres	Data Protector Internal Database Service (hpdp-idb) 是 IDB 在其中运行的服务。 需要内部服务器上信息的进程可从 Cell Manager 本地访问该服务。 远程访问此服务，仅获取有关从 Cell Manager 上的 IDB 传输到 Manager-of-Manager (MoM) 上 IDB 的介质管理信息。
/opt/omni/idb/bin/pgbouncer	Data Protector Internal Database Connection Pooler (hpdp-idb-cp) 服务提供了一系列到 hpdb-idb 的开放连接，可以根据需要使用这些连接，无需为每个请求打开一个新连接，从而确保 hpdp-idb 连接的可扩展性。 此服务在 Cell Manager 上运行，并且仅由本地进程访问。
/opt/omni/AppServer/bin/standalone.sh	Data Protector Application Server (hpdp-as) 服务用于通过 HTTPS 连接(Web 服务)将 GUI 连接到 IDB。 它在 Cell Manager 上运行，并且具有到 hpdp-idb-cp 服务的本地连接。

设置环境变量

使用 Data Protector 之前， Micro Focus 建议您在操作系统配置中扩展特定环境变量的值：

- 要使 Data Protector 手册页可从任何位置进行查看，请添加 /opt/omni/lib/man 到 MANPATH 变量。
- 要使 Data Protector 命令可从任何目录调用，请添加命令位置到 PATH 变量。 Data Protector 文档中的步骤假设变量值已经扩展。 omniintro 参考页(*Data Protector 命令行界面参考*中)和 omniintro 手册页中列出了命令位置。

下面的步骤

在此阶段，将安装 Cell Manager 和适用于 UNIX 系统的 安装服务器(如果已选择)。 下一步的任务是：

1. 如果未在同一系统上安装适用于 UNIX 的 安装服务器，请参见安装 UNIX Cell Manager (第 26 页)。
2. 如果希望向 Windows 客户机远程安装软件，则安装 安装服务器 for Windows。 请参见在 Windows 系统上安装 安装服务器 (第 41 页)。
3. 将软件分发到客户机上。 请参见安装 Data Protector 客户机 (第 49 页)。

安装 Windows Cell Manager

先决条件

- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 用于安装的用户帐户必须：
  - 对选定的目标系统具有管理 (Administrator) 特权。
  - 在 Windows 本地安全策略中设置了网络访问用户权限。
- 默认情况下，Data Protector Inet 服务必须在 Windows 本地用户帐户 SYSTEM 下运行。 然而，如果因各种原因导致 Inet 服务使用 Windows 域用户帐户运行，则必须额外地对其授予以下 Windows 操作系统安全策略权限：
  - 身份验证后模拟客户机
  - 替换进程级别令牌

  有关详细信息，请参见《*Data Protector 帮助*》的索引："Inet 用户模拟"。
- 成为 Cell Manager 的系统必须：
  - 安装了受支持的 Windows 操作系统。 有关 Cell Manager 支持的操作系统的列表，请参见 https://softwaresupport.softwaregrp.com/。
  - 有足够的磁盘空间可用于 Data Protector Cell Manager 软件。 Cell Manager 需要 4 GB 的总 RAM。

    要恢复内部数据库，需要两倍的总 RAM。

    对于每个并发备份会话，需要 40 MB RAM。 例如，如果要运行 60 个并行备份会话，就需要 3 GB RAM。
  - 有足够的磁盘空间可用于 Data Protector 内部数据库 (IDB)。 1.5 GB 可用磁盘空间 + 每个备份文件大约 100 字节 (供 IDB 使用)。

    如果所选磁盘卷上的可用存储空间不足，可以将其他卷装载到此磁盘卷中的目录，但应在安装之前执行此操作。
  - 系统驱动器具有 2 × *size_of_the_biggest_package_to_be_installed* + 10 MB 的磁盘空间。
  - 已配置防火墙，以额外接受"远程服务管理"(NP) 连接 (端口 445)。
  - 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。 协议必须能够解析主机名。 计算机名和主机名必须相同。
  - 分配有静态 IP 地址。 如果系统配置为 DHCP 客户机，则它的 IP 地址会改变；因此，需要或者为该系统分配一个永久的 DNS 条目 (并重新配置它)，或者配置 DHCP 服务

器，使之为该系统保留一个静态 IP 地址(IP 地址与系统的 MAC 地址绑定)。

- 有以下空闲端口：
  - 5565 — 在 Data Protector 中执行新安装所需的端口。
  - 5555 — Data Protector 安装升级期间所需的端口。
  - 7112 — 内部数据库服务端口
  - 7113 — 内部数据库连接池程序 (IDB CP) 端口
  - 7116 — 应用程序服务器 (HTTPS AS) 端口
  - 9999 — 应用程序服务器管理端口

  在安装期间可以更改上述服务端口。 要更改默认通信端口号，请参见更改默认的 Data Protector Inet 端口 (第 306 页)。

- 要在 Windows Cell Manager 上运行大量会话，您必须更改桌面堆限制。 每个桌面堆分配的大小由以下注册表值控制：

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows
  ```

  该注册表值的默认数据看起来与以下内容相似：

  ```
  %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
  ```

  "SharedSection=" 后的数字值控制桌面堆的分配方式。 这些 SharedSection 值以 KB 为单位指定。

  - 1024 — 所有桌面常用的共享堆大小。
  - 20480 — 与交互式窗口站关联的每个桌面的桌面堆大小
  - 768 — 与非交互式窗口站关联的每个桌面的桌面堆大小

  您必须将与非交互式窗口站关联的 SharedSection 值更改为 20480。 此更改需要重新启动才能生效。

Microsoft 终端服务客户端

- 要通过 Microsoft 终端服务客户端在 Windows 上安装 Data Protector，请确保要在其上安装 Data Protector 的系统已针对**终端服务器模式**选择**远程管理**：
  1. 在 Windows 控制面板中，单击**管理工具**，然后单击**终端服务配置**。
  2. 在“终端服务配置”对话框中，单击**服务器设置**。 确保“终端服务”服务器以“远程管理”模式运行。

建议

- 如果预计 DC 二进制文件会增长到大于 2 GB(其大小仅受文件系统设置限制)，建议使用 NTFS 文件系统进行存储。

群集感知Cell Manager

对于安装群集感知 Cell Manager，还有另外一些先决条件和步骤。 请参见安装群集感知 Cell Manager (第 157 页)。

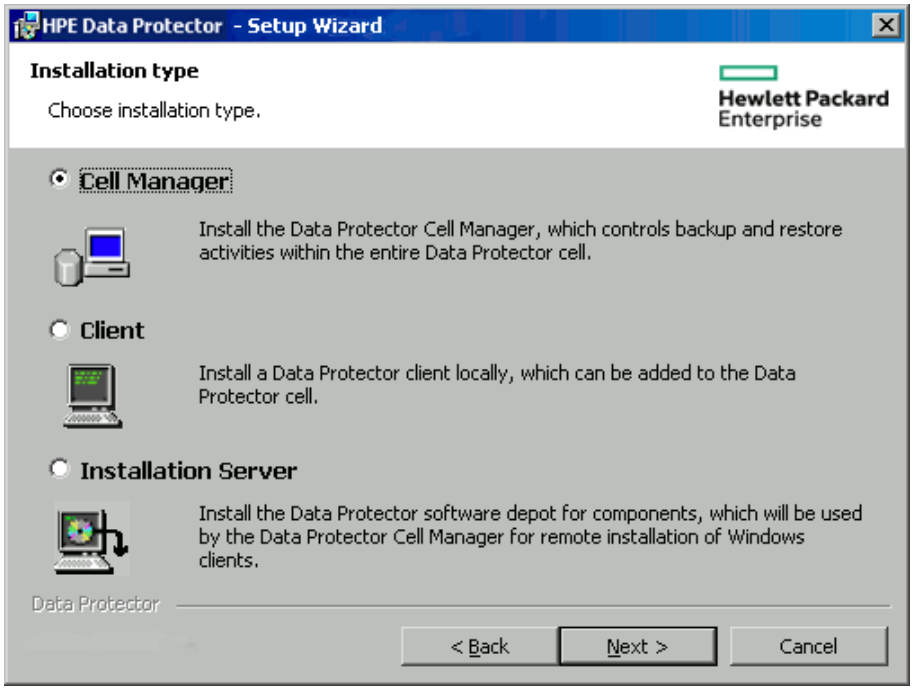
> **注意：**
> 在多单元环境 (MoM) 中，所有 Cell Manager 必须安装相同的 Data Protector 版本。

安装过程

在 Windows 系统上执行新的安装

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。 运行适用于平台的文件夹中的 `setup.exe` 文件。
2. 按照安装向导操作，并仔细阅读许可协议。 如果接受协议的条款，则单击**下一步 (Next)** 继续。
3. 查看“过时信息”页面中的详细信息，然后单击**我了解对所支持平台的更改**，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在“安装类型”页面中，选择 **Cell Manager**，然后单击**下一步**安装 Data ProtectorCell Manager 软件。

   选择安装类型



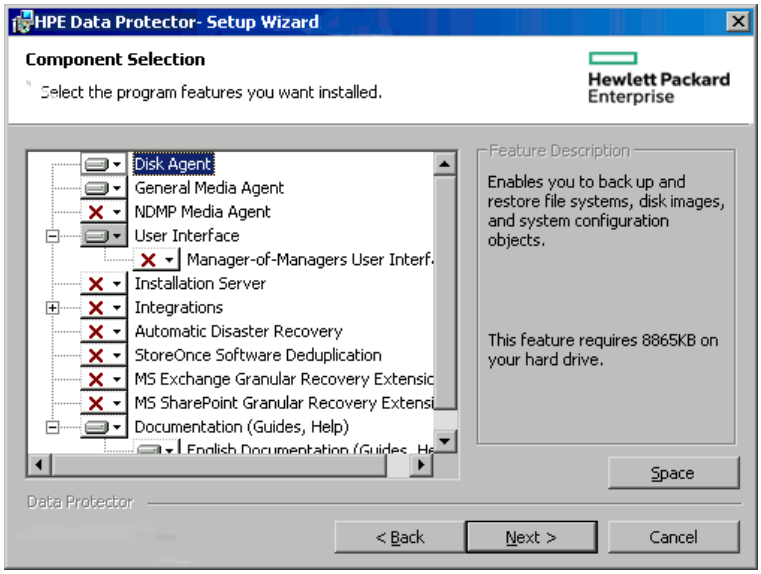
5. 提供 Data Protector 服务运行所使用的帐户的用户名和密码。

   单击**下一步 (Next)** 继续。
6. 单击**下一步 (Next)** 将 Data Protector 安装到默认安装文件夹中。

或者单击**更改 (Change)** 打开“更改当前目标文件夹 (Change Current Destination Folder)”或“更改当前程序数据目标文件夹 (Change Current Program Data Destination Folder)”对话框，然后根据需要更改安装文件夹。 程序数据安装文件夹的路径不应超过 80 个字符。

7. 在“组件选择”页中，选择要安装的组件。 有关 Data Protector 组件的列表和说明信息，请参见Data Protector 组件 (第 52 页)。

选择软件组件

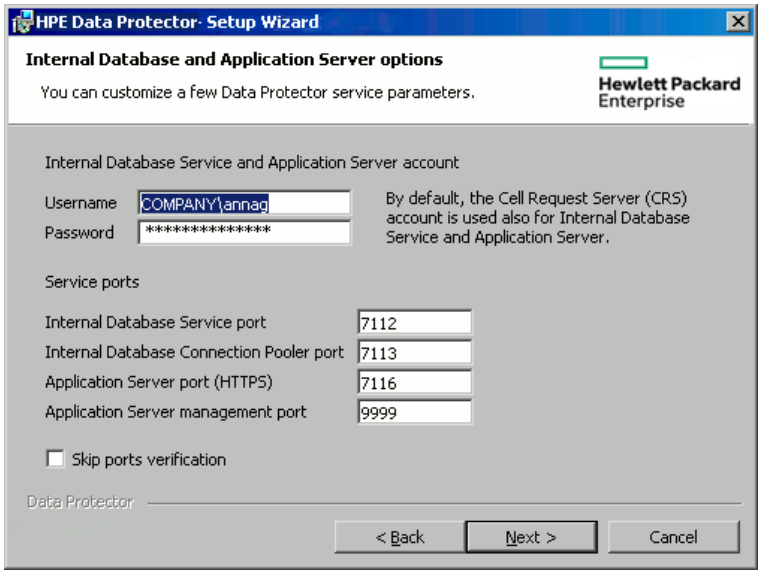


默认情况下选择了**磁盘代理**、**常规介质代理**、**用户界面**和**安装服务器**。 单击**下一步 (Next)**。

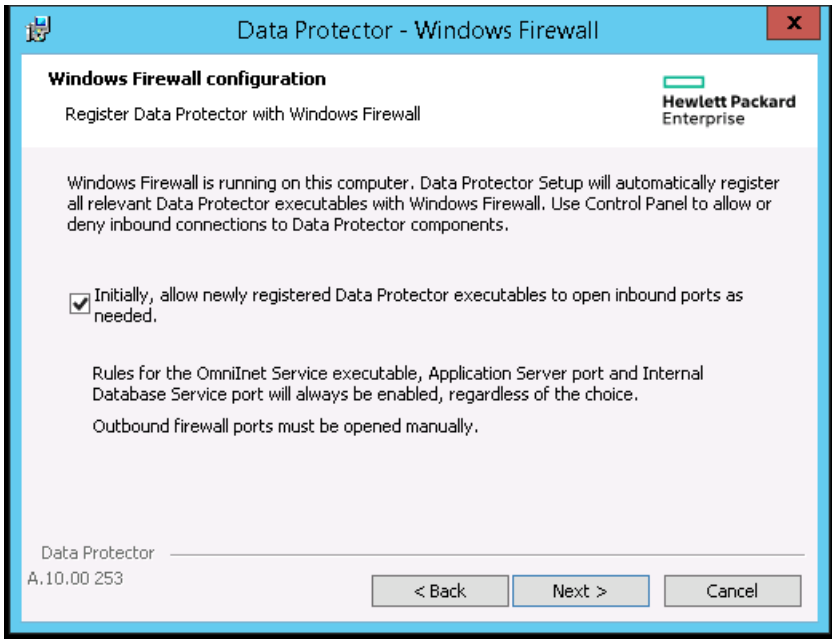
8. 此外，还可以更改 Data Protector IDB 和应用程序服务器所使用的用户帐户，以及这些服务所使用的端口。

单击**下一步 (Next)**。

更改 IDB 和应用程序服务器选项



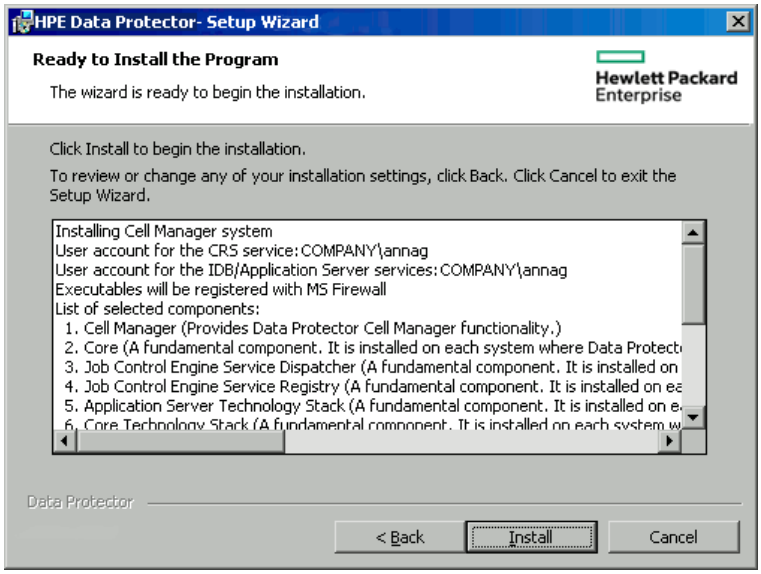
9. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。 Data Protector 设置会注册所有必要的 Data Protector 可执行文件。 默认情况下，**最初，允许新注册的 Data Protector 可执行文件按需打开入站端口**选项已选中。 如果此时不想让 Data Protector 能打开端口，请取消选中此选项。 为了正常运行具有先前版本的 10.00 客户机的 Data Protector，必须启用 Windows 防火墙中的 Data Protector 规则。 无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。



单击**下一步 (Next)**。

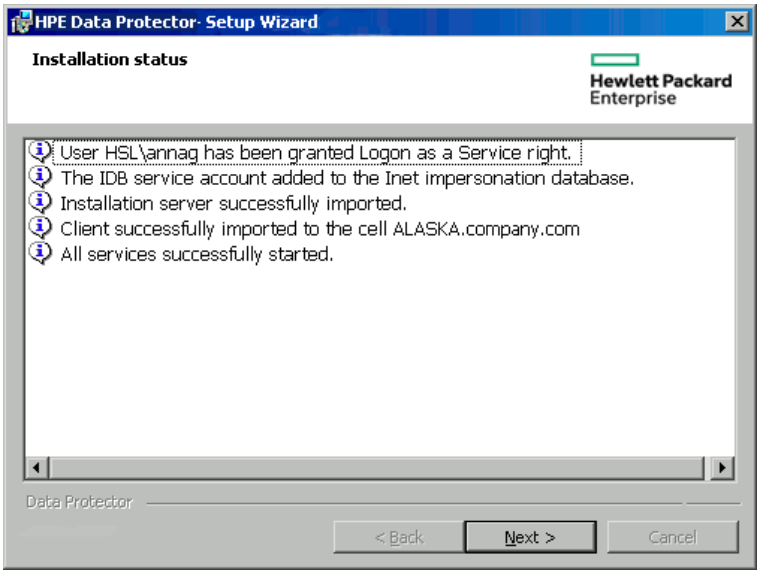
10. 组件摘要列表随即显示。 单击**安装**开始安装选定组件。 这可能需要几分钟时间。

组件摘要列表



11. **安装状态**页随即显示。 单击**下一步**。

安装状态页面



12. 如果已安装 User Interface 组件，要在设置后立即开始使用 Data Protector GUI，请选择**启动 Data Protector GUI**。

    如果已安装 English Documentation (Guides, Help) 组件，要在设置后立即查看《Data Protector 产品声明、软件说明和参考》，请选择**打开产品声明、软件说明和参考**。

    单击**完成**。

安装之后

Cell Manager 文件位于 *Data_Protector_home* 目录和 *Data_Protector_program_data* 中。

软件仓库位于 *Data_Protector_program_data*\Depot 目录中。

Data Protector 命令位于目录中，列在 omniintro 参考页里(在 *Data Protector 命令行界面参考* 中)和 omniintro 手册页中。

> **重要：**
> 建议通过命令位置在操作系统配置中扩展相应环境变量值来从任何目录中调用 Data Protector 命令。 Data Protector 文档中的步骤假设值已经扩展。

以下进程在 Cell Manager 系统上运行：

crs.exe	Data Protector Cell Request Server (CRS) 服务在 Cell Manager 系统上运行，并且在系统上安装 Cell Manager 软件时启动该服务。 CRS 负责启动和控制单元中的备份和还原会话。 它在 *Data_Protector_home*\bin 目录中运行。
mmd.exe	Data Protector 介质管理后台程序 (MMD) 服务在 Cell Manager 系统上运行，并且在软件安装到 Cell Manager 系统上时启动。 MMD 管理设备和介质管理操作。 它在 *Data_Protector_home*\bin 目录中运行。
omniinet.exe	Data Protector 客户机服务，支持 Cell Manager 启动其他系统上的代理。

	Data Protector 单元中的所有系统上都必须运行 Data Protector Inet 服务。 它在 *Data_Protector_home*\bin 目录中运行。
kms.exe	Data Protector Key Management Server (KMS) 服务在 Cell Manager 系统上运行，并且在系统上安装 Cell Manager 软件时启动此服务。 KMS 为 Data Protector 加密功能提供密钥管理。 它在 *Data_Protector_home*\bin 目录中运行。
hpdp-idb	Data Protector Internal Database Service (hpdp-idb) 是 IDB 在其中运行的服务。 需要内部服务器上信息的进程可从 Cell Manager 本地访问该服务。 远程访问此服务，仅获取有关从 Cell Manager 上的 IDB 传输到 Manager-of-Manager (MoM) 上 IDB 的介质管理信息。
hpdp-idb-cp	Data Protector Internal Database Connection Pooler (hpdp-idb-cp) 服务提供了一系列到 hpdb-idb 的开放连接，可以根据需要使用这些连接，无需为每个请求打开一个新连接，从而确保 hpdp-idb 连接的可扩展性。 此服务在 Cell Manager 上运行，并且仅由本地进程访问。
hpdp-as	Data Protector Application Server (hpdp-as) 服务用于通过 HTTPS 连接 (Web 服务)将 GUI 连接到 IDB。 它在 Cell Manager 上运行，并且具有到 hpdp-idb-cp 服务的本地连接。

注意：
如果要使用 Data Protector 用户界面跨平台执行备份或还原，请参见 Data Protector 产品声明、软件说明和参考 了解存在的限制。

提示：
如果 Data Protector GUI 未提供相应的编码，您可以安装附加的代码页转换表来正确显示文件名。 有关详细步骤，请参见操作系统文档。

故障排除

如果安装未成功，请尝试验证由 Setup 自身所检查的安装要求，如果要求未满足，请确定导致安装失败的原因。 请参见先决条件 (第 32 页)。

以下是安装程序 Setup 所检查的要求的列表：

- Service Pack 版本
- nslookup，以便 Data Protector 能够展开主机名
- 磁盘空间
- 管理权限

下面的步骤

在此阶段，将安装 Cell Manager，以及 安装服务器 for Windows(如果已选择)。 下一步的任务是：

1. 为 UNIX 安装 安装服务器，如果具备混合备份环境。 请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。 对于 UNIX 系统，如果不需要 安装服务器，则跳过该步骤。
2. 将软件分发到客户机上。 请参见安装 Data Protector 客户机 (第 49 页)。

安装 安装服务器

安装服务器 可以安装在 Cell Manager 系统上或任何通过 LAN 与 Cell Manager 连接的受支持系统上。 有关 安装服务器 支持的操作系统的详细信息，请参见 https://softwaresupport.softwaregrp.com/。

要将 安装服务器 保留在独立于 Cell Manager 的系统上，请在本地安装相应的软件仓库。 本节介绍详细的过程。

在 UNIX 系统上安装 安装服务器

先决条件

要成为 安装服务器，系统必须满足以下要求：

- 已安装 HP-UX 或 Linux 操作系统。 有关安装服务器支持的操作系统的详细信息，请访问 Data Protector 产品声明、软件说明和参考。
- 已启动并正在运行 `inetd` 或 `xinetd` 后台程序。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 端口号 5555/5565(默认)可用。 如果不属于这种情况，请参见更改默认的 Data Protector Inet 端口 (第 306 页)。
- TCP/IP 协议已安装，并且正在运行。 协议必须能够解析主机名。
- 有足够的磁盘空间可用于完整的 Data Protector 软件仓库。 以下是最低要求：
  - 512 MB 的总 RAM
  - 1.5 GB 可用磁盘空间
- 您需要 `root` 访问权限或具有 root 特权的帐户。
- Data Protector 单元中的 Cell Manager 必须为 10.00 版本。

> **重要：**
> 要将 Data Protector 安装到链接目录中，例如：
>
> `/opt/omni/ -> /prefix/opt/omni/`
>
> `/etc/opt/omni/ -> /prefix/etc/opt/omni/`
>
> `/var/opt/omni/ -> /prefix/var/opt/omni/`
>
> 请在安装之前创建这些链接，并确保目标目录存在。

注意：
要通过网络从某个设备安装软件，需要先在计算机上装载源目录。

建议

使用 UNIX 安装服务器 安装 Data Protector 是适用于 UNIX 客户机的首选方法。

尽管 UNIX 客户机可以本地安装 Data Protector，但是由于不使用 安装服务器 将没有支持过程可修补 UNIX 客户机，因此建议不要这么做。

由于对 UNIX 客户机打补丁需要 安装服务器，因此建议使用同一 安装服务器 在 UNIX 客户机上先安装 Data Protector。

安装过程

在 HP-UX 或 Linux 系统上安装 UNIX 的安装服务器系统

1. 复制 HP-UX 或 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。

   LOCAL_INSTALL

   platform_dir/DP_DEPOT

   其中，*platform_dir* 为：

hpux	对于 HP-UX 系统
linux_x86_64	对于 Linux 系统

2. 转到 LOCAL_INSTALL 目录并执行：

   ./omnisetup.sh -IS

   有关 omnisetup.sh 命令的说明，请参见安装程序包 (tar) *Mount_point*/ 中的 README 文件或安装程序包的 DOCS/C/MAN 目录中的 *Data Protector 命令行界面参考*。

安装完成时，UNIX 的软件仓库位于 /opt/omni/databases/vendor 目录中。

omnisetup.sh 命令会安装安装服务器与所有包。 要仅安装这些包的一部分，请使用 swinstall(适用于 HP-UX)或 rpm(适用于 Linux)。 请参见在 HP-UX 和 Linux 系统上使用本机工具安装 (第 297 页)。

重要：
如果不在网络中为 UNIX 安装安装服务器，则必须从 UNIX 安装程序包 (tar)(对于 HP-UX 或 Linux)本地安装每个 UNIX 客户机。 此外，也无法为 Data Protector 客户机上的组件打补丁。

下面的步骤

至此，您应该已在网络中安装了 UNIX 的 安装服务器。 下一步的任务是：

1. 如果将 安装服务器 安装在不同于 Cell Manager 的系统上，则必须将系统手动添加(导入)到 Data Protector 单元中。 请参见在 UNIX 系统上安装 安装服务器 (第 39 页)。

> **注意：**
> 导入安装服务器后，Cell Manager 上的 `/etc/opt/omni/server/cell/installation_servers` 文件将更新以列出已安装的远程安装包。该文件可用于在 CLI 中检查可用的远程安装包。为保持该文件最新，每当安装或删除远程安装包后应导出再导入安装服务器。即使安装服务器安装在与 Cell Manager 相同的系统上，此方法也适用。

2. 如果 Data Protector 单元中有任何 Windows 系统，请安装 安装服务器 for Windows。请参见在 Windows 系统上安装 安装服务器 (第 41 页)。
3. 将软件分发到客户机上。请参见安装 Data Protector 客户机 (第 49 页)。

在 Windows 系统上安装 安装服务器

先决条件

要成为未来的安装服务器，Windows 系统必须满足以下要求：

- 安装了一种受支持的 Windows 操作系统。有关安装服务器支持的操作系统的详细信息，请参见 https://softwaresupport.softwaregrp.com/。
- 有足够的磁盘空间可用于完整的 Data Protector 软件仓库。以下是最低要求：
  - 512 MB 的总 RAM
  - 2 GB 可用磁盘空间
- 对于 Data Protector 单元中的所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- TCP/UDP 445。对于新的 Data Protector 客户机推送安装(客户机上没有任何 Data Protector 组件)，需要可访问的安装服务器共享。或者，如果无法访问安装服务器库共享，则必须在本地执行初始 Data Protector 客户机安装。
- 5565 — 在 Data Protector 中执行新安装所需的端口。如果不属于这种情况，请参见更改默认的 Data Protector Inet 端口 (第 306 页)。
- 5555 — Data Protector 安装升级期间所需的端口。
- 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。协议必须能够解析主机名。计算机名和主机名必须相同。

限制

由于 Windows 操作系统所施加的安全限制，下列条件之一必须属实：

- 安装服务器和客户机不在同一域中。
- 安装服务器和客户机在同一域中。

> **重要：**
> 如果不在网络上安装适用于 Windows 的安装服务器，则必须通过安装包 (zip) 在本地安装每个 Windows 客户机。

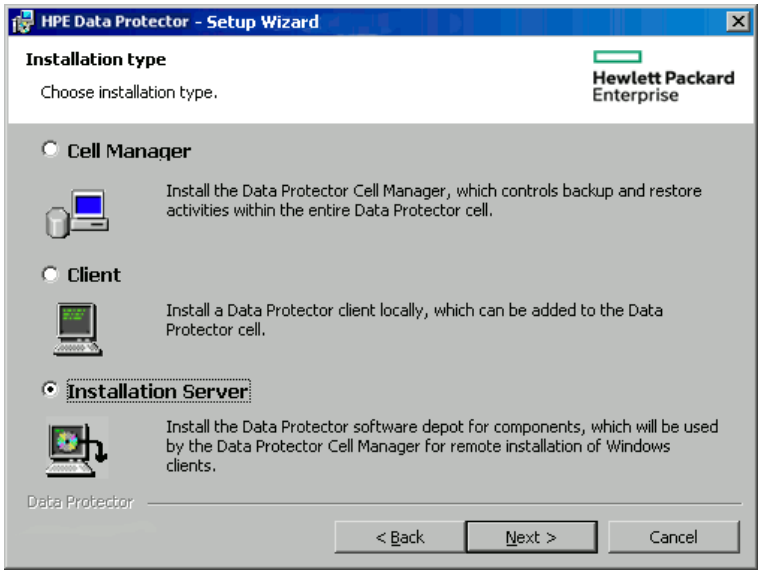
注意：
如果 Windows 系统上已经安装了 安装服务器，那么不可在该系统上远程安装 Data Protector 客户机。要在同一系统上安装 安装服务器 和客户机组件，必须执行本地客户机安装。在安装过程中，选择所有需要的客户机组件和 安装服务器 组件。请参见 安装 Data Protector 客户机 (第 49 页)。

安装过程

安装 **Windows** 的安装服务器系统

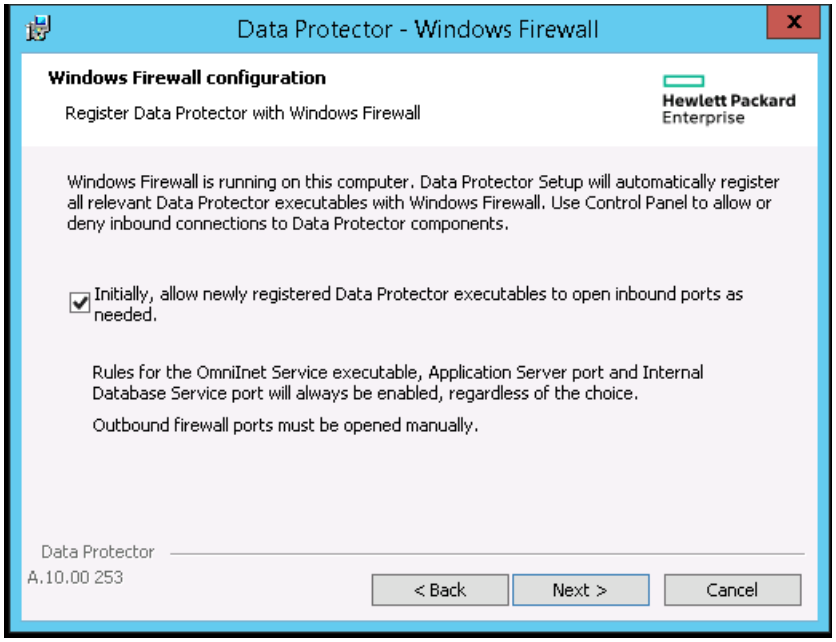
1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。运行适用于平台的文件夹中的 `setup.exe` 文件。
2. 按照安装向导操作，并仔细阅读许可协议。如果接受协议的条款，则单击**下一步**继续。
3. 查看“过时信息”页面中的详细信息，然后单击**我了解对所支持平台的更改**，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在**安装类型**页面中，选择 **安装服务器**，然后单击**下一步**安装 Data Protector 软件仓库。

   选择安装类型

5. 单击**下一步**在默认文件夹中安装 Data Protector。

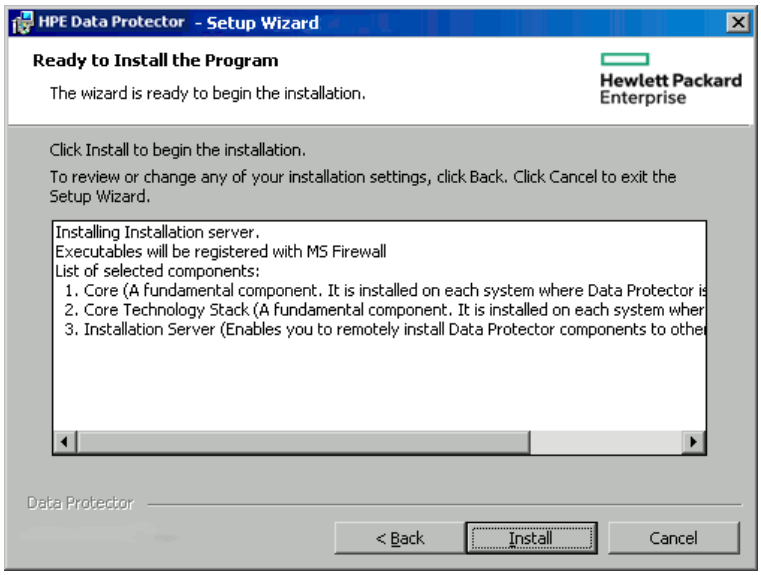
   否则，单击**更改 (Change)** 打开“更改当前目标文件夹 (Change Current Destination Folder)”窗口并输入新的路径。
6. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，**最初，允许新注册的 Data Protector 可执行文件按需打开入站端口**选项已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的 10.00 客户机的 Data Protector，必须启用 Windows 防火墙中的 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。



单击**下一步**。

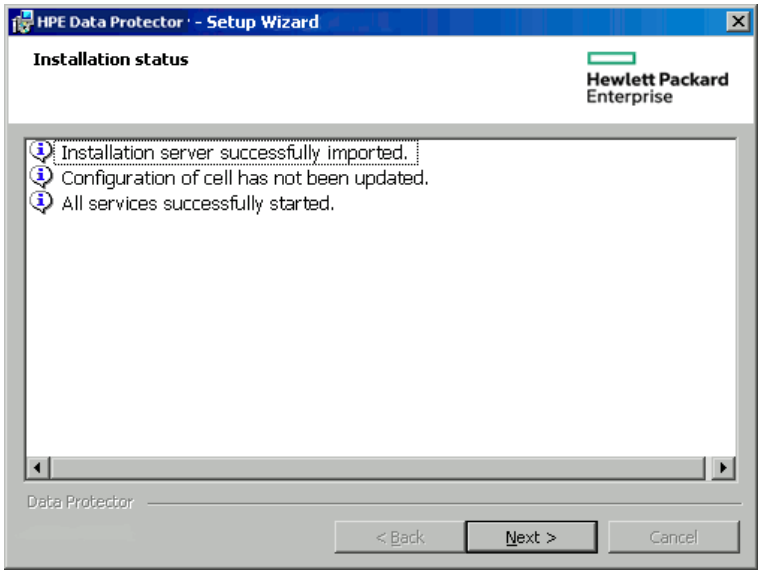
7. 组件摘要列表随即显示。单击**安装**开始安装选定组件。这可能需要几分钟时间。

组件选择摘要页面



8. “安装状态”页随即显示。单击**下一步**。

安装状态页面



9. 单击**完成**。

安装完成后，默认情况下将此软件安装到 *Data_Protector_program_data*\Depot 目录中。该软件设置为共享，以便可以从网络上访问它。

为确保安装文件在从安装服务器复制到新客户机期间不会发生更改，安装服务器和客户机之间的通信使用会话管理块 (Session Management Block, SMB) 网络文件协议。

安装服务器会在第一次远程安装期间设置 SMB 数据包签名。将应用以下策略：

- Microsoft 网络客户机：数字签名通信(始终)
- Microsoft 网络服务器：数字签名通信(始终)

在以下项中，**RequireSecuritySignature** 参数的注册表值将设置为 1：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

远程安装期间会显示以下消息：

```
Verifying SMB signing at Data Protector Installation server and if necessary
starting it...
```

启用 SMB 签名后，如果用户要通过 SMB 从安装服务器主机连接到另一个主机，那么另一个主机也应当启用 SMB 签名。

下面的步骤

此时，您应当已在网络上安装了适用于 Windows 的安装服务器。现在应执行以下任务：

1. 如果已安装独立的安装服务器(例如，不在 Cell Manager 上)，必须将该系统手动添加(导入)到 Data Protector 单元中。
   请参见 在 UNIX 系统上安装 安装服务器 (第 39 页)。
2. 如果具有混合备份环境，则在 HP-UX 或 Linux 上安装适用于 UNIX 的安装服务器。请

参见 在 UNIX 系统上安装 安装服务器 (第 39 页)。

3. 将软件分发到客户机上。请参见 安装 Data Protector 客户机 (第 49 页)。

安装 Data Protector 单服务器版

Data Protector 的单服务器版 (SSE) 针对小型环境而设计，在这种小型环境中，仅对连接到 Cell Manager 的一台设备运行备份。它可用于受支持的 Windows 以及 HP-UX 平台。

要安装 Cell Manager 和 安装服务器(可选)，请遵循安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)中的说明。

适用于 Windows 的 SSE 的限制

- SSE 只支持同时将数据备份到与单个 Cell Manager 连接的一台设备中。
- 仅支持一个 10 插槽的 DDS 自动更换器。
- 不支持 UNIX(以及 HP-UX)客户机和服务器。如果尝试对 UNIX 计算机进行备份，会话会被中止。
- SSE 不支持添加扩展产品。
- SSE 不支持群集。
- SSE 不支持灾难恢复。

Windows 客户机的数量不受限制。

有关受支持的设备，请参见《Data Protector 产品声明、软件说明和参考》。

适用于 HP-UX 的 SSE 的限制

- SSE 只支持同时将数据备份到与单个 Cell Manager 连接的一台设备中。
- 仅支持一个 10 插槽的 DDS 自动更换器。
- 在 UNIX Cell Manager 上，无法备份服务器 - 只能备份 UNIX 客户机、Windows 客户机和 Solaris 客户机。
- SSE 不支持添加扩展产品。
- SSE 不支持群集。

客户机(UNIX、Windows)的数量不受限制。

有关受支持的设备，请参见《Data Protector 产品声明、软件说明和参考》。

安装密码

有关如何在 Cell Manager 上安装密码的逐步指示信息，请参见 Data Protector 密码 (第 268 页) 密码。

验证安装

需要检查 Data Protector 软件组件是否在 Cell Manager 或客户机系统中正常运行时，可以使用 Data Protector 图形用户界面验证安装。

先决条件

必须具有适用于客户机系统类型(UNIX 系统或 Windows 系统)的安装服务器。

步骤

1. 在“上下文列表 (Context List)”中，单击**客户机 (Clients)**。
2. 在范围窗格中，展开**客户机**，右键单击 Cell Manager 或客户机系统，然后单击**检查安装**以打开向导。
3. 此时将列出相同类型(UNIX 系统或 Windows 系统)的所有客户机系统。 选择要验证其安装的客户机，然后单击**完成**开始验证。

验证的结果将显示在“检查安装”窗口中。

关于 Data Protector Inet 服务配置

在 Windows 系统上，通过 Data Protector Inet 服务启动备份和恢复会话，并在默认情况下使用 Windows 本地用户帐户 SYSTEM 运行。 因此，可以使用相同的用户帐户进行备份或恢复会话。

集成

有些 Data Protector 集成要求使用 Windows 域用户帐户启动备份和还原会话。 在 Windows Server 2003 系统上，只需使用不同的用户帐户重新启动 Data Protector Inet 服务就可以实现上述操作。 对于其他受支持的 Windows 操作系统，不再允许执行此操作。 因此，Data Protector 采用备用概念：用户模拟。 这意味着即使使用 Windows 本地用户帐户 SYSTEM 运行 Data Protector Inet 服务，该服务仍可以模拟 Windows 域用户帐户，因此可以使用该用户帐户启动集成代理。

要启用 Data Protector Inet 服务模拟，必须在备份规范或还原向导中指定 Windows 域用户帐户，且必须将用户帐户(包括其密码)保存在 Windows 注册表中。

使用 Windows 域用户帐户运行 Inet 服务

在某些情况下，Data Protector Inet 服务必须使用 Windows 域用户帐户运行：

- **群集环境**

  在群集中，必须为所有群集节点配置 Data Protector Inet 服务。 这表示您需要将 Windows 域用户帐户作为 Inet 帐户使用。

使用 Windows 域用户帐户运行 Inet 服务时，您必须授予其以下 Windows 操作系统安全策略特权：

- Impersonate a client after authentication
- Replace a process level token

为 Data Protector Inet 服务用户模拟设置用户帐户

对于在默认情况下使用 Windows 本地用户帐户 SYSTEM 运行的 Data Protector Inet 服务，可以将其指定为使用其他 Windows 域用户帐户启动会话。

- 如下所示配置用户帐户：
  - 授予用户适当的数据访问权限(例如应用程序数据)。
  - 请确保将此用户添加到 Data Protectoradmin 或 operator 用户组。

使用 Data Protector GUI

步骤

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开 **Data Protector 单元**，然后展开**客户机**。
3. 右键单击客户机，然后单击**添加模拟**。

   > **注意：**
   > 要修改或删除用户，请分别单击**修改模拟**或**删除模拟**。

4. 在“选择客户机系统”页中，选择要配置 Data Protector Inet 服务用户模拟的客户机系统，然后单击**下一步**。
5. 在添加、删除或修改模拟页中，添加一个新的用户帐户，或者修改/删除现有用户帐户，然后单击**完成**。

> **重要：**
> 需要时 Data Protector Inet 服务将使用保存于 Windows 注册表中的用户帐户。

使用 Data Protector CLI

- 要为某个 Data Protector 客户机上的用户模拟设置用户帐户，请使用 omniinetpasswd 命令。

  登录到此客户机并运行：

  ```
  omniinetpasswd -add User@DomainPassword
  ```

- 要为多个 Data Protector 客户机上的用户模拟设置用户帐户，请使用 omnicc 命令。

  登录到 Cell Manager 并运行：

```
omnicc -impersonation -add_user -user User@Domain -host ClientName1 -host
ClientName2 -host ClientName3 -passwd Password
```

有关 omniinetpasswd 和 omnicc 命令的详细信息，请参见《*Data Protector 命令行界面参考*》。

更改 Data Protector Inet 帐户

要确保 Data Protector Inet 服务采用特定用户帐户启动备份和还原所需的进程，必须采用该用户帐户重新启动服务。

先决条件

- Microsoft 群集服务器：在更改帐户之前，使 OBVS_HPDP_AS，OBVS_HPDP_IDB，OBVS_HPDP_IDB_CP 和 OBVS_MCRS 群集组脱机。以其他帐户重新启动 Data Protector Inet 服务后，使群集组再次联机。

在 Windows 系统上

1. 在控制面板中，单击**管理工具**，然后双击**服务**。
2. 双击 **Data Protector Inet**。
3. 在“常规 Data Protector Inet 属性”中，单击**停止**，然后单击**登录**选项卡。
4. 选择**此帐户**按钮。
5. 输入或浏览有正确权限(访问共享磁盘)的帐户。
6. 输入密码，然后确认该密码。
7. 单击**确定**退出这些属性页。
8. 确保仍选择了 Data Protector Inet，右键单击该服务，然后单击**启动**。
9. 退出此对话框。

第 3 章： 安装 Data Protector 客户机

您可以通过使用 安装服务器 进行分发来远程安装 Data Protector 客户机，或者通过相应的安装程序包 (zip/tar) 进行本地安装。

使用 UNIX 安装服务器 安装 Data Protector 是适用于 UNIX 客户机的首选方法。

尽管 UNIX 客户机可以本地安装 Data Protector，但是由于不使用 安装服务器 将没有支持过程可修补 UNIX 客户机，因此建议不要这么做。

由于修补 UNIX 客户机需要 安装服务器，因此建议使用同一 安装服务器 在 UNIX 客户机上先安装 Data Protector。

> **注意：** Windows 安装服务器 在远程安装期间以客户机的端口 445 作为目标，而 HP-UX/Linux 安装服务器 以客户机的端口 22(安全远程安装)或端口 512/514(不安全远程安装)作为目标。在安装服务器端，短端口用于与这些目标端口建立连接。

已经安装完客户机之后，Micro Focus 建议通过在每个客户机上添加命令位置到相应的环境变量来从任何目录调用 Data Protector 命令。Data Protector 文档中的步骤假设变量值已经扩展。`omniintro` 参考页 (*Data Protector 命令行界面参考* 中)和 `omniintro` 手册页中列出了命令位置。

在安装并导入 Data Protector 客户机到单元后，强烈建议对安装进行验证，以防止出现无法保证客户机访问的情况。有关验证客户机安装的过程，请参见验证 Data Protector 客户机安装 (第 287 页)。有关安全保护的详细信息，请参见安全注意事项 (第 174 页)。

安装 Data Protector 客户机系统

客户机系统	安装类型和参考
Windows	远程和本地安装；请参见安装 Windows 客户机 (第 55 页)
HP-UX	远程和本地安装；请参见安装 HP-UX 客户机 (第 64 页)
Solaris	远程和本地安装；请参见安装 Solaris 客户机 (第 67 页)
Linux	远程和本地安装；请参见安装 Linux 客户机 (第 73 页)
ESX Server	远程和本地安装；请参见安装 ESX Server 客户机 (第 75 页)
Mac OS X	远程和本地安装；请参见安装 Mac OS X 客户机 (第 77 页)
IBM AIX	远程和本地安装；请参见安装 IBM AIX 客户机 (第 75 页)
HP OpenVMS	本地安装；请参见安装 HP OpenVMS 客户机 (第 78 页)
其他 UNIX 系统	本地安装；请参见在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)
DAS Media Agent 客户机	远程和本地安装；请参见安装介质代理以使用 ADIC/GRAU 库或 StorageTek 库 (第 93 页)。

客户机系统	安装类型和参考
ACS Media Agent 客户机	远程和本地安装；请参见安装介质代理以使用 ADIC/GRAU 库或 StorageTek 库 (第 93 页)

集成

Data Protector 集成是一些软件组件，可让您通过 Data Protector 备份数据库应用程序。运行数据库应用程序的系统的安装方式与任意 Windows 或 UNIX 客户机系统相同，前提是选择了相应的软件组件(例如，用于备份 Microsoft Exchange Server 数据库的 `MS Exchange Integration` 组件和用于备份 Oracle 数据库的 `Oracle Integration` 组件等)。

安装集成

软件应用程序或磁盘阵列系列	参考
Microsoft Exchange Server	请参见 Microsoft Exchange Server 客户机 (第 101 页)。
Microsoft SQL Server	请参见 Microsoft SQL Server 客户机 (第 107 页)
Microsoft SharePoint Server	请参见 Microsoft SharePoint Server 客户机 (第 108 页)
Microsoft Volume Shadow Copy Service (VSS)	请参见 Microsoft 卷影复制服务客户机 (第 111 页)。
Sybase Server	请参见 Sybase Server 客户机 (第 112 页)
Informix Server	请参见 Informix Server 客户机 (第 112 页)
SAP R/3	请参见 SAP R/3 客户机 (第 112 页)
SAP MaxDB	请参见 SAP MaxDB 客户机 (第 113 页)
SAP HANA Appliance	请参见 SAP HANA Appliance 客户机 (第 113 页)
Oracle Server	请参见 Oracle Server 客户机 (第 113 页)
MySQL	请参见 MySQL 客户机 (第 114 页)
PostgreSQL	请参见 PostgreSQL 客户机 (第 114 页)

软件应用程序或磁盘阵列系列	参考
IBM DB2 UDB	请参见 IBM DB2 UDB 客户机 (第 114 页)
Lotus Notes/Domino Server	请参见 Lotus Notes/Domino Server 客户机 (第 115 页)
VMware	请参见 VMware 客户机 (第 115 页)
Microsoft Hyper-V	请参见 Microsoft Hyper-V 客户机 (第 122 页)
Network Data Management Protocol (NDMP) Server	请参见 NDMP 服务器客户机 (第 123 页)
P4000 SAN 解决方案	请参见 P4000 SAN 解决方案 clients (第 123 页)
P6000 EVA 磁盘阵列系列	请参见 P6000 EVA 磁盘阵列系列 clients (第 123 页)
P9000 XP 磁盘阵列系列	请参见 P9000 XP 磁盘阵列系列 clients (第 129 页)
3PAR StoreServ Storage	请参见 3PAR StoreServ Storage clients (第 134 页)
EMC Symmetrix	请参见 EMC Symmetrix 客户机 (第 134 页)
EMC VNX 存储提供程序	请参见 非 HPE 存储阵列 (第 138 页)
EMC VMAX 存储提供程序	请参见 非 HPE 存储阵列 (第 138 页)
NetApp 存储提供程序	请参见 非 HPE 存储阵列 (第 138 页)

其他安装

安装	参考
Serviceguard	请参见 在 Serviceguard 上安装 Data Protector (第 144 页)。
Symantec Veritas Cluster Server	请参见 在 Symantec Veritas Cluster Server 上安装 Data Protector (第 154 页)。

安装	参考
Microsoft 群集服务器	请参见在 Microsoft 群集服务器上安装 Data Protector (第 157 页)。
IBM HACMP Cluster	请参见在 IBM HACMP Cluster 上安装 Data Protector (第 167 页)。
Microsoft Hyper-V 群集	请参见在 Microsoft Hyper-V 群集上安装 Data Protector (第 167 页)。

Data Protector 组件

有关受支持平台的最新信息，请访问 Data Protector 主页，位于 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

以下是可以选择的 Data Protector 组件，以及它们的说明：

用户界面	用户界面组件包含 Windows 系统上的 Data Protector 图形用户界面和 Windows 与 UNIX 系统上的部分命令行界面。访问 Data Protector Cell Manager 需要使用该软件，必须至少将该软件安装到用于管理单元的系统上。 **注意：** Data Protector 命令行界面的特定命令包含在其他 Data Protector 组件中。有关详细信息，请参见《*Data Protector 命令行界面参考*》。 在异构环境中使用 Data Protector 用户界面之前，请参见 Data Protector 产品声明、软件说明和参考以了解存在的限制。
英语文档(指南、帮助)	这是 Data Protector 英语文档文件集。
法语文档(指南、帮助)	这是 Data Protector 法语文档文件集。
日语文档(指南、帮助)	这是 Data Protector 日语文档文件集。
简体中文文档(指南和帮助)	这是 Data Protector 简体中文文件文件集。
Manager-of-Managers 用户界面	Manager-of-Managers 用户界面包含 Data Protector 图形用户界面。该软件用于访问 Data Protector Manager-of-Managers 功能和控制多单元环境。“Manager-of-Managers 用户界面”和“管理器用户界面”可用作公共应用程序。
磁盘代理	必须在具有需要使用 Data Protector 进行备份的磁盘的系统上安装磁盘代理组件。

常规介质代理	连接了备份设备或有权访问库机械手，并通过 Data Protector 进行管理的系统上必须安装常规介质代理组件。
自动灾难恢复	在需要使用自动灾难恢复方法支持恢复的系统上，以及需要为增强型自动灾难恢复 (EADR) 或一键式灾难恢复 (OBDR) 准备 DR CD ISO 映像来为灾难恢复提供自动准备的系统上，必须安装自动灾难恢复组件。
SAP R/3 集成	具有需要使用 Data Protector 备份的 SAP R/3 数据库的系统上必须安装 SAP R/3 集成组件。
SAP MaxDB 集成	具有需要使用 Data Protector 备份的 SAP MaxDB 数据库的系统上必须安装 SAP MaxDB 集成组件。
SAP HANA 集成	必须在代表或组成您要使用 Data Protector 保护的 SAP HANA Appliance 上安装 SAP HANA Integration 组件。
Oracle 集成	具有需要使用 Data Protector 进行备份的 Oracle 数据库的系统上必须安装 Oracle 集成组件。
MySQL 集成	必须在具有需要使用 Data Protector 进行备份的 MySQL 数据库的系统上安装 MySQL 集成组件。
虚拟环境集成	虚拟环境集成组件必须安装在将用作备份主机的系统上，以使用 Data Protector 虚拟环境集成控制虚拟机的备份和还原。
DB2 集成	必须在具有需要使用 Data Protector 进行备份的 DB2 Server 的所有系统上安装 DB2 集成组件。
Sybase 集成	必须在具有需要使用 Data Protector 进行备份的 Sybase 数据库的系统上安装 Sybase 集成组件。
Informix 集成	必须在具有需要使用 Data Protector 进行备份的 Informix Server 数据库的系统上安装 Informix 集成组件。
MS Exchange 集成	必须将 MS Exchange 集成组件安装到 Microsoft Exchange Server 2007 系统上，并且计划使用 Data Protector Microsoft Exchange Server 2007 集成或 Data Protector Microsoft Exchange Single Mailbox 集成备份该系统。 还必须在将要使用 Data Protector Microsoft Exchange Single Mailbox 集成进行备份的 Microsoft Exchange Server 2010 系统上安装 MS Exchange 集成组件。
MS Exchange Server 2010+ 集成 (MS Exchange Server 2010 Integration)	必须将 MS Exchange Server 2010+ 集成组件安装到计划使用 Data Protector Microsoft Exchange Server 2010 集成进行备份的 Microsoft Exchange Server 2010 或 Microsoft Exchange Server 2013 系统。
MS SQL 集成	具有需要使用 Data Protector 进行备份的 Microsoft SQL Server 数据库的系统上必须安装 MS SQL 集成组件。
MS SharePoint	必须在需要使用 Data Protector 进行备份的 Microsoft SharePoint

2007/2010/2013 集成	Server 2007/2010/2013 系统上安装 MS SharePoint 2007/2010/2013 集成组件。
MS Volume Shadow Copy 集成	在要运行由卷影复制服务协调的备份的 Windows Server 系统上必须安装 MS 卷影复制服务集成组件。
P4000 VSS Agent	P4000 VSS Agent 组件必须同时安装到应用程序系统和备份系统，以将 P4000 SAN 解决方案 与 Data Protector 集成。
P6000/ 3PAR SMI-S 代理	P6000/ 3PAR SMI-S 代理组件必须同时安装在应用程序系统和备份系统上，以将 Data Protector 与 P6000 EVA 磁盘阵列系列集成，或者将 Data Protector 与 3PAR StoreServ Storage 集成。
P9000 XP 代理	P9000 XP 代理组件必须同时安装到应用程序系统和备份系统，以将 Data Protector 与 P9000 XP 磁盘阵列系列 集成。
3PAR VSS 代理	3PAR VSS 代理组件必须同时安装在应用程序系统和备份系统上，以将 Data Protector 与 3PAR StoreServ Storage(在其配置中，应用程序系统和备份系统均为 Windows 系统，并且您要使用卷影复制服务备份及还原数据)集成。
EMC Symmetrix Agent	EMC Symmetrix Agent 组件必须同时安装到应用程序系统和备份系统，以将 Data Protector 与 EMC Symmetrix 集成。
EMC VNX 存储提供程序	应用程序系统和备份系统上的 EMC VNX 存储提供程序，可将 Data Protector 与 EMC VNX 集成。EMC VNX 存储提供程序组件是 Data Protector SMI-S Agent 的插件。
EMC VMAX 存储提供程序	应用程序系统和备份系统上的 EMC VMAX 存储提供程序，可将 Data Protector 与 EMC VMAX 集成。EMC VMAX 存储提供程序组件是 Data Protector SMI-S Agent 的插件。
NetApp 存储提供程序	应用程序系统和备份系统上的 NetApp 存储提供程序，可将 Data Protector 与 NetApp 存储集成。进行虚拟环境集成时，此组件必须仅安装在备份系统上。NetApp Storage Provider 组件是 Data Protector SMI-S 代理的插件。
NDMP 介质代理	必须在需要通过 NDMP 服务器将数据备份到 NDMP 专用驱动器的所有系统上安装 NDMP 介质代理组件。
Lotus 集成	必须在 Data Protector 单元中具有计划使用 Data Protector 进行备份的 Lotus Notes/Domino Server 数据库的所有系统上安装 Lotus 集成组件。
MS Exchange Granular Recovery Extension	要启用精细复原功能，则必须每个 Microsoft Exchange Server 系统上安装适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension。在 Microsoft Exchange Server 的数据库可用性组 (DAG) 环境中，它必须安装在 DAG 的所有 Exchange Server 系统上。
MS SharePoint Granular Recovery Extension	必须在 Microsoft SharePoint Server Central Administration 系统上安装适用于 Microsoft SharePoint Server 的 Data Protector Granular Recovery Extension 。

VMware Granular Recovery Extension 高级 GRE Web 插件	要启用 VMware 虚拟机的精细恢复功能，则必须在 VMware Virtual Server 系统上安装 Data Protector VMware Granular Recovery Extension 高级 GRE Web 插件组件。在使用 Web 插件进行文件恢复操作之前，必须先配置 Data Protector GRE 环境。
VMware Granular Recovery Extension 代理	要启用 VMware 虚拟机的存储和精细复原，则必须在装载代理系统上安装 Data Protector VMware Granular Recovery Extension Agent 组件。仅支持远程安装。

注意：
不能在同一系统上安装常规介质代理和 NDMP 介质代理。

Data Protector 服务

Data Protector 使用以下服务：

Inet	备份客户机服务
CRS	Cell Manager 服务
hpdp-idb	内部数据库服务
hpdp-idb-cp	内部数据库连接池程序
hpdp-as	应用程序服务器

默认情况下，Inet 和 hpdp-* 服务在本地系统帐户下运行，CRS 在管理员帐户下运行。
您可以为其中任一服务更改帐户信息。但是，以下是新帐户必须满足的最低要求：

服务	资源	服务所需的最低资源权限
CRS	*Data_Protector_program_data* HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII	完全访问权限 完全访问权限
Inet	备份和还原 取得所有权	- -

安装 Windows 客户机

有关特定 Windows 操作系统的受支持平台和组件的详细信息，请参见 https://softwaresupport.softwaregrp.com/。

先决条件

要安装 Windows 客户机，必须具有管理员权限。要成为未来的 Data Protector 客户机系统，Windows 系统必须满足以下要求：

- 有足够的磁盘空间可用于 Data Protector 客户机软件。有关详细信息，请参见《Data Protector 产品声明、软件说明和参考》。
- 端口号 5555/5565(默认)可用。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 安装了 TCP/IP 协议的 Microsoft 实现版本，并且协议正在运行。协议必须能够解析主机名。计算机名和主机名必须相同。
- 确保在 Windows 本地安全策略下，为执行安装的帐户设置网络访问用户权限。

限制

- 由于 Windows 操作系统所施加的安全限制，安装服务器只能用于在同一域中远程安装客户机。
- 在 Windows XP Home Edition 上，仅支持本地安装 Data Protector 客户机。
- 当远程安装客户机到 Windows Server 2008 或者 Windows Server 2012 时，可使用以下某个帐户：
  - 远程系统上的内置管理员帐户。必须启用该帐户，并且禁用*管理批准模式*。
  - 域用户帐户，它是远程系统上本地管理员用户组的成员。

建议

- 在安装 Data Protector 之前，检查系统上是否已安装 Microsoft Installer (MSI) 2.0。如果已安装了早期版本，建议先升级到 2.0 版本，再开始 Data Protector 安装。如果事先不升级 MSI，Data Protector 安装向导会自动升级到所需的版本。在这种情况下，Data Protector 会相应地通知您有关 MSI 升级的情况。

  如果 MSI 已升级，强烈建议重新启动系统。

自动灾难恢复

在希望使用增强型自动灾难恢复 (EADR)、一键式灾难恢复 (OBDR) 或者自动系统恢复 (ASR) 进行恢复的系统上，以及需要为 EADR 或 OBDR 准备 DR CD ISO 映像的系统上，必须安装`Automatic Disaster Recovery`组件。

群集感知客户机

对于安装群集感知客户机，还存在一些其他先决条件。有关更多详细信息，请参见安装群集感知客户机 (第 165 页)。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

本地安装

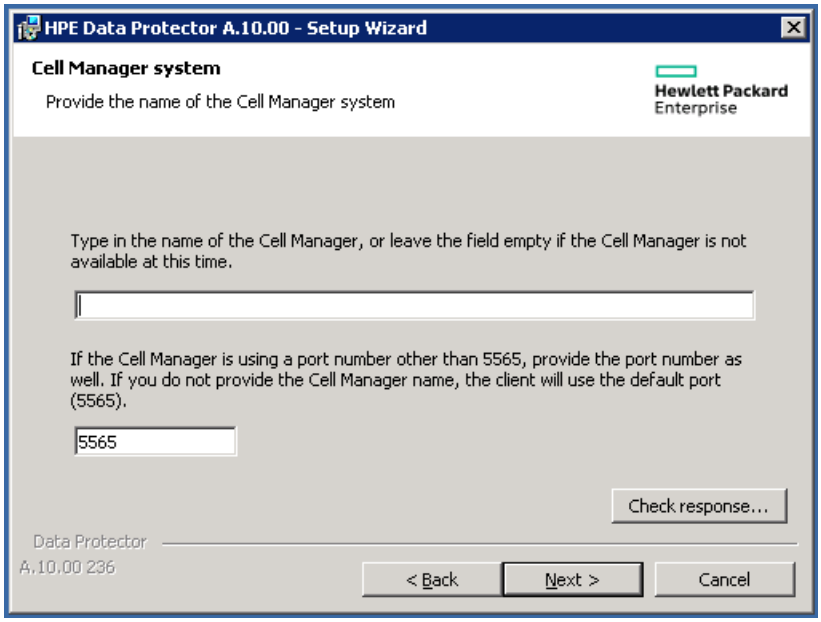
可以通过 Windows 安装包 (zip) 在本地安装 Windows 客户机：

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 `setup.exe` 文件。
2. 按照安装向导操作，并仔细阅读许可协议。单击**下一步 (Next)** 继续。
3. 在“安装类型”页中，选择**客户机**。对于 Itanium 客户机，将会自动选择该类型。
4. 输入 Cell Manager 的名称。

   如果 Cell Manager 使用默认端口 5565 之外的其他端口，请更改端口号。您可以测试 Cell Manager 是否正在工作并使用选定的端口，方法是单击**检查响应**。

   单击**下一步 (Next)**。

   选择 Cell Manager



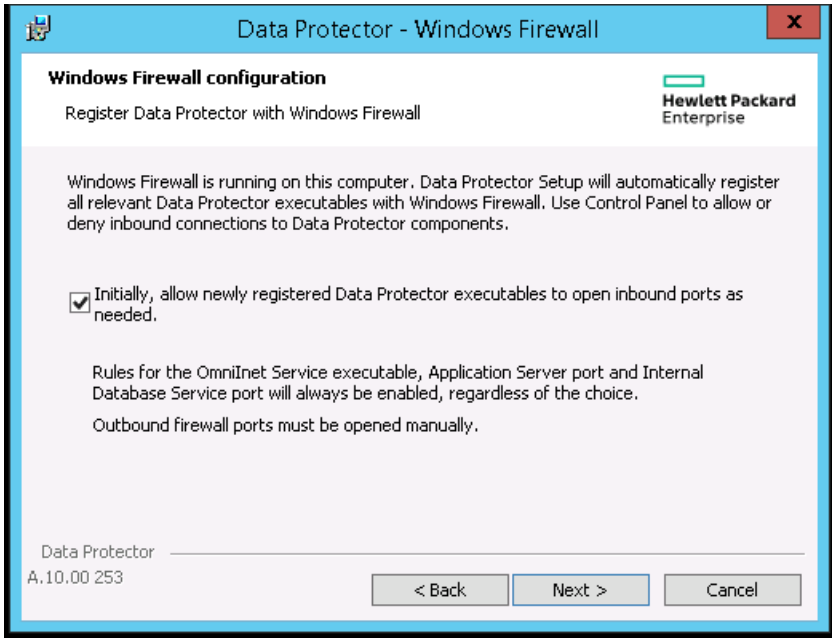
5. 单击**下一步**在默认文件夹中安装 Data Protector。

   否则，单击**更改**打开“更改当前目标文件夹”页面并输入路径。
6. 选择要安装的 Data Protector 组件。

   有关其他 Data Protector 组件的信息，请参见Data Protector 组件 (第 52 页)。

   单击**下一步 (Next)**。
7. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，**最初，允许新注册的 Data Protector 可执行文件按需打开入站端口**选项已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的 10.00 客户机的 Data Protector，必须启用 Windows 防火墙中的 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口

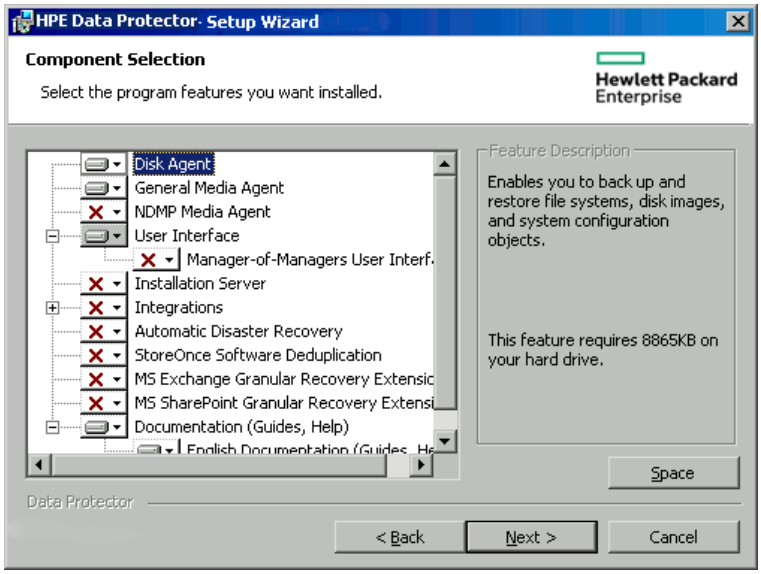
和内部数据库服务端口的规则。



单击**下一步 (Next)**。

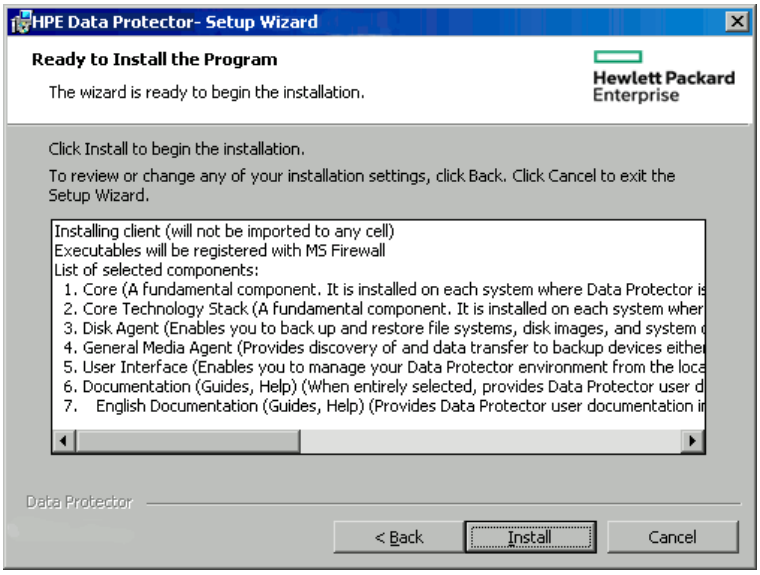
8. 此时会显示组件选择摘要页。单击**安装 (Install)** 安装选定组件。

组件选择摘要页面



9. “安装状态”页随即显示。单击**下一步 (Next)**。

安装摘要页面



10. 如果已安装User Interface组件，要在设置后立即开始使用 Data Protector GUI，请选择**启动 Data Protector GUI**。

    如果已安装English Documentation (Guides, Help)组件，并要在设置之后立即查看 *Data Protector 产品声明、软件说明和参考*，请选择**打开产品声明、软件说明和参考**。
11. 单击**完成**。

导入本地安装的客户机

导入 表示在安装 Data Protector 软件之后手动将计算机添加到单元中。添加到 Data Protector 单元后，系统将变为 Data Protector 客户机。

一个客户机只能是一个单元的成员。如果希望将客户机移动到其他单元，则首先将其从当前单元*导出*，然后将其导入到新单元。有关如何导出客户机的过程，请参见从单元导出客户机 (第 172 页)。

配置客户机以执行导入

此过程仅在本地安装过程中未指定 Cell Manager 名称的情况下适用。

本地安装完成之后，在客户机端执行以下命令：

```
omnicc -secure_comm -configure_peer <Cell manager hostname>
```

此步骤可为客户机配置 Cell Manager 证书。对于本地安装的客户机，这是强制步骤。重新导入删除的客户机也需要此命令。

该命令提示用来显示 Cell Manager 证书指纹的 **y/n** 选项。输入 **y** 将成功完成配置。

如果用户要配置客户机而不执行任何验证，请将 -accept_host 命令附加到以下命令中：

```
omnicc -secure_comm -configure_peer <Cell manager hostname> -accept_host
```

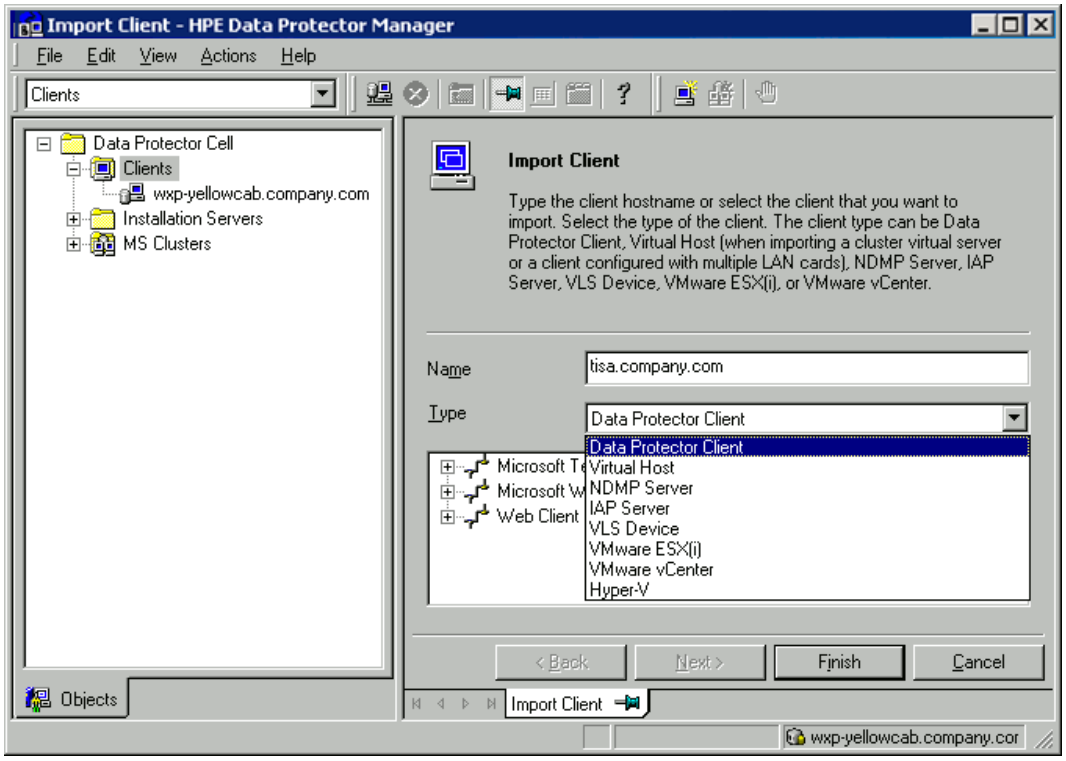
使用 accept_host 命令时，控制台不会提示 **y/n** 选项。

要使用 **GUI** 导入客户机系统，请执行以下操作：

当用户选择**接受指纹**选项时，不会显示指纹窗口，主机会被接受，而无需用户确认。如果不选择此选项，则会显示指纹窗口，用户必须手动接受指纹选项。

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 输入客户机的名称或浏览网络以选择要导入的客户机(仅在 Windows GUI 上)。

将客户机导入到单元



如果导入配置有多个 LAN 卡的客户机，请选择**虚拟主机**选项。选择该选项后，必须导入同一系统的所有名称。

如果导入 NDMP 客户机，请选择 **NDMP 服务器**选项并单击**下一步**。指定 NDMP 服务器的相关信息。

如果要导入 HP OpenVMS 客户机，则在Name文本框中键入 OpenVMS 客户机的 TCP/IP 名称。

如果将导入 Microsoft Exchange Server DAG 虚拟主机以进行 Data Protector Microsoft Exchange Server 2010 集成，请选择**虚拟主机**。

如果要为 Data Protector Virtual 环境集成导入客户机，可以选择适用于独立 VMware ESX (i) Server 系统的 **VMware ESX(i)**、适用于 VMware vCenter Server 系统的 **VMware vCenter**，也可以选择适用于 Microsoft Hyper-V 系统的 **Hyper-V**。单击**下一步**并指定登录凭据。

> **注意：**
> 要能够使用 vCD vStorage 映像备份方法备份虚拟机，请确保导入 Data Protector 单元中用作 VMware vCenter 客户机且由 VMware vCloud Director 使用的所有

> vCenter Server 系统。

4. 单击**下一步 (Next)**。
5. 单击**完成 (Finish)** 以导入客户机。

所导入客户机的名称将显示在结果区域中。

要使用 CLI 导入客户机系统，请执行以下操作：

`omnicc -import_host` 命令用于导入 Data Protector 客户机，而 `omnicc -import_cs` 命令用于导入外部 Cell Manager。将 `-virtual` 添加到命令，以进行虚拟客户机导入。

该命令提示用来显示 Cell Manager 证书指纹的 **y/n** 选项。输入 **y** 将成功完成配置。如果用户要配置客户机而不执行任何验证，请将 `-accept_host` 附加到命令中。

在安装期间指定 Cell Manager

如果在安装期间指定了 Cell Manager，则作为安装的一部分，将在客户机中配置 Cell Manager 证书，但不会执行导入。

要使用 GUI 或 CLI 导入客户机系统，请参见使用 GUI 导入客户机系统和使用 CLI 导入客户机系统部分。

MOM 配置中的 Cell Manager

应遵循以下步骤，以在 MOM 配置中包括 Cell Manager：

1. 应使用以下命令，通过 MOM 服务器配置 Cell Manager：

   ```
   omnicc -secure_comm -configure_peer <MOM server>
   ```

   此操作在 Cell Manager 中配置 MOM 服务器。提示 MOM 服务器指纹，用户需要接受指纹。
2. 从 MOM GUI 导入 Cell Manager。此操作提示 Cell Manager 证书指纹，用户需要接受该指纹。

> **注意：**
> 不得在 MOM 配置中包含不同版本的 Cell Manager。

本地安装 安装服务器

何时添加

如遇下述情况，则必须向单元添加一个 安装服务器：

- 如果作为独立的 UNIX 安装服务器 安装，即未安装在 Cell Manager 上。

  在这种情况下，只有将 安装服务器 添加到单元后，才能在单元中远程安装任何客户机。
- 如果安装在 Cell Manager 上，但是您也想将其用于在其他单元中执行远程安装。那么必须将其添加到其他单元(使用连接到其他单元的 Cell Manager 的 GUI)。

不像客户机，安装服务器 可以是多个单元的成员。因此，不必将其从一个单元删除(导出)，即可添加(导入)到另一个单元。

配置 安装服务器

请运行以下命令配置 安装服务器 主机：

```
omnicc -secure_comm -configure_peer <CM host name>
```

导入 安装服务器

导入 安装服务器 的过程与导入客户机的过程类似。使用 Data Protector GUI(连接到将添加 安装服务器 的单元的 Cell Manager)执行此任务时，请执行以下步骤：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击 **安装服务器s**，然后单击**导入 安装服务器**启动向导。请参见 。
3. 输入或选择要导入的系统的名称。单击**完成 (Finish)** 以导入 安装服务器。

在 Windows/Unix/HP-UX 上将 安装服务器 导入到 Cell Manager 的示例

如果 **hostname1.company.net** 为 Cell Manager，并且 **hostname2.company.net** 为 安装服务器，则在 安装服务器 上运行以下命令：

```
omnicc -secure_comm -configure_peer hostname1.company.net

[root@hostname2 etc]# omnicc -secure_comm -configure_peer hostname1.company.net

- Please use the

fingerprint to validate the certificate manually!

Certificate information:

- Hostname:hostname1.company.net

- Valid: from Sep 24 06:25:52 2016 GMT until Sep 22 06:25:52 2026 GMT

- Fingerprint: e9:2a:3f:ed:af:10:c1:f7:7h:67:69:4b:4d:51:87:25:6h:79:gr:78

Do you want to continue (y/n)?y

Host 'hostname1.company.net' configured for secure configuration successfully.
```

现在在 Cell Manager 上，使用以下命令重新导入 安装服务器，因为必须交换并验证证书。

```
omnicc -import_is HostName [-accept_host]

C:\Program Files\OmniBack\bin>omnicc -import_is hostname2.company.net

- Please use the fingerprint to validate the certificate manually!

Certificate information:

- Hostname:hostname2.company.net

- Valid: from Aug 24 07:26:15 2016 GMT until Aug 22 07:26:15 2026 GMT

- Fingerprint: f5:3b:3h:gb:cf:10:d1:f7:7d:67:60:5b:4d:51:87:76:6h:51:rg:89

Do you want to continue (y/n)?y

Import host successful.
```

将备份设备与 Windows 系统连接

安装介质代理组件之后，可以通过执行以下步骤将备份设备与 Windows 系统进行连接：

1. 为要连接的备份设备的驱动器和控制设备(机械手)查找可用的 SCSI 地址(在 Windows 上称作 *SCSI 目标 ID*。
   请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
2. 为驱动器和控制设备(机械手)设置未使用的 SCSI Target ID。根据设备类型，通常可以通过设备上的开关来完成设置。有关详细信息，请参见设备自带的文档。
   有关受支持的设备的信息，请访问 https://softwaresupport.softwaregrp.com/。
3. 关闭计算机，并将备份设备与系统连接。
4. 开启设备，然后开启计算机，并等待启动过程完成。
5. 要验证系统是否正确识别新的备份设备，可以在 *Data_Protector_home*\bin 目录中运行 devbra -dev 命令。
   查看命令输出列出的新设备。例如，devbra -dev 命令可能会生成以下输出：
   - 如果设备的磁带驱动程序已加载：

     ```
     HP:C1533A
     tape3:0:4:0
     DDS
     ...
     ```

     第一行代表设备规范，第二行是设备文件名。
     路径格式指示 DDS 磁带设备的驱动器实例编号为 3，连接到 SCSI 总线 0，SCSI 目标 ID 4 和 LUN 编号 0。
   - 如果设备的磁带驱动程序未加载：

     ```
     HP:C1533A
     scsi1:0:4:0
     DDS
     ...
     ```

     第一行代表设备规范，第二行提供设备文件名。
     路径格式指示 DDS 磁带设备连接到 SCSI 端口 1、SCSI 总线 0，磁带驱动器具有 SCSI 目标 ID 4 和 LUN 编号 0。

有关加载或卸载适用于设备的本机磁带驱动程序，请参见在 Windows 系统上使用磁带和机械手驱动程序 (第 320 页)。
有关创建设备文件名的详细信息，请参见在 Windows 系统上创建设备文件(SCSI 地址) (第 322 页)。

下面的步骤

在此阶段，您应当已经安装了客户机组件，并连接了备份设备，从而能够配置备份设备和介质池。有关配置任务的信息，请参见 *Data Protector 帮助*索引：“配置, 备份设备”。

安装 HP-UX 客户机

可以使用适用于 UNIX 的 安装服务器 远程安装 HP-UX 客户机，或者从 UNIX 安装程序包 (tar) 本地安装。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。 有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

先决条件

- 此时，您应当已在网络上安装了 Cell Manager 和 安装服务器 for UNIX。 如果未安装，请参见
  安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)以了解相关说明。
- 您将需要 *root* 访问权或具有 *root* 权限的帐户。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 对于 HP-UX 11.11，需要 IPv6NCF11i 软件包或者 TOUR/IPv6 支持来启用 Internet 协议版本 6 (IPv6)。

  有关详细信息，请参见HP-UX 系统补丁 (第 199 页)

UNIX 系统上 Data Protector 客户机组件的 RAM 和磁盘空间要求

下表列出了 Data Protector UNIX 系统上不同客户机组件的最低 RAM 和磁盘空间要求：

RAM 和磁盘空间要求

客户机系统组件	RAM (MB) [1]	可用磁盘空间 (MB) [2]
磁盘代理	每个 64(建议 128)	每个 20
介质代理		
集成组件		
英语文档(指南、帮助)	不适用	100

远程安装

使用 Data Protector 图形用户界面从 UNIX 的 安装服务器 将客户机软件安装到客户机上。 有关用于远程安装软件的逐步式过程，请参见远程安装 (第 83 页)。

进行远程安装之后，客户机系统会自动成为 Data Protector 单元的成员。

[1] 这些数字只表示对组件的要求。 数字不包括操作系统、分页文件或其他应用程序的空间分配。
[2] 这些数字只表示对组件的要求。 数字不包括操作系统、分页文件或其他应用程序的空间分配。

如果在客户机上已安装了介质代理，则必须将备份设备与系统进行物理连接。 要确定对应于您所用设备类型的设备驱动程序是否已构建到内核中，在运行备份之前，请先检查内核配置。

本地安装

在 安装服务器 上

如果在您的环境中未安装适用于 UNIX 的 安装服务器，则必须通过 UNIX 安装程序包 (tar) 执行本地安装。 有关本地安装的步骤，请参见安装服务器的本地安装。

在客户机上

进行本地安装之后，必须将客户机系统手动导入单元中。 请参见导入本地安装的客户机 (第 59 页)。

群集感知客户机

对于安装群集感知客户机，还存在一些其他先决条件和步骤。 有关更多详细信息，请参见安装群集感知客户机 (第 148 页)。

检查 HP-UX 上的内核配置

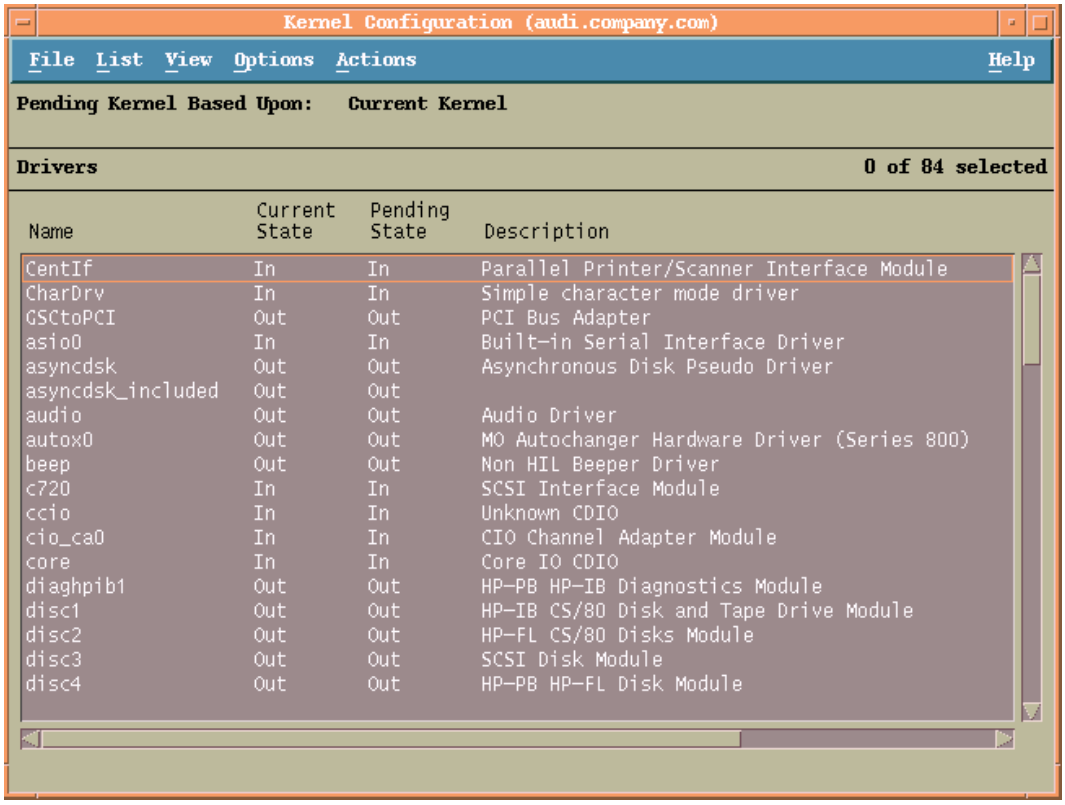
以下过程说明如何使用 *System Administration Manager (SAM)* 实用程序检查和构建 HP-UX 11.x 上的内核配置。 有关如何手动生成内核的说明，请参见在 HP-UX 系统上配置 SCSI 机械手 (第 323 页)。

按照以下过程使用 *System Administration Manager (SAM)* 实用程序构建内核配置：

1. 以 root 用户身份登录，然后打开终端并输入 sam。
2. 在 **System Administration Manager** 窗口中，双击**内核配置 (Kernel Configuration)**，然后双击**驱动程序 (Drivers)**。
3. 在**内核配置 (Kernel Configuration)** 窗口中，验证以下方面：
   - 您将要使用的设备的驱动程序必须列在已安装驱动程序中。 请参见内核配置窗口 (第 66 页)。 如果要查找的驱动程序未列出，则必须使用 /usr/sbin/swinstall 实用程序安装它。 例如：
     - 如果将磁带设备与系统连接，则磁带设备驱动程序对于磁带设备是必需的，因此必须安装它。 例如，对于通用 SCSI 磁带驱动器(如 DLT 或 LTO)，需要使用 stape 驱动程序；对于 DDS 设备，需要使用 tape2 驱动程序。
     - 要控制磁带库设备中的机械手，需要名为 sctl 或 spt 的 SCSI 直通驱动程序，或者名为 schgr 的自动更换器机械手驱动程序(具体取决于硬件)。

       有关详细信息，请参见在 HP-UX 系统上配置 SCSI 机械手 (第 323 页)。

内核配置窗口



- **当前状态 (Current State)** 列中显示的驱动程序状态必须设置为**包含 (In)**。 如果状态值设置为**不包含 (Out)**，则执行以下操作：
  a. 在列表中选择驱动程序。 单击**操作**并选择**将驱动程序添加到内核中**。 在**挂起状态**列中，状态将设置为 In.

     对于**当前状态 (Current State)** 为**包含 (In)** 的每个驱动程序重复该操作。
  b. 单击**操作**并选择**创建新内核**来应用更改，也就是将**挂起内核**构建为**当前内核**。 执行该操作之后，需要重新启动系统。

将所有必需驱动程序构建到内核中之后，您可以继续操作，即将备份设备与系统连接。

将备份设备与 HP-UX 系统连接

1. 确定驱动器和控制设备(机械手)的可用 SCSI 地址。 使用 /usr/sbin/ioscan -f 系统命令。

   有关详细信息，请参见在 HP-UX 系统上查找未使用的 SCSI 地址 (第 329 页)。
2. 在设备上设置 SCSI 地址。 根据设备类型，通常可以通过设备上的开关来完成设置。有关详细信息，请参见设备自带的文档。

   有关受支持的设备的详细信息，请参见 https://softwaresupport.softwaregrp.com/。
3. 将设备与系统连接，开启设备，然后开启计算机，并等待启动过程完成。 设备文件通常在启动过程期间创建。
4. 验证系统是否正确识别新的备份设备。 使用 ioscan 实用程序：

```
/usr/sbin/ioscan -fn
```

从而可以查看针对每个已连接备份设备列出的设备文件。 如果在启动过程期间未自动创建设备文件，则必须手动创建它。 请参见在 HP-UX 系统上创建设备文件 (第 327 页)。

安装过程已完成并且备份设备已正确连接到系统后，请参见《*Data Protector 帮助*》索引："配置，备份设备"以了解有关配置设备和介质池或执行其他 Data Protector 配置任务的信息。

安装 Solaris 客户机

可以使用适用于 UNIX 的安装服务器远程安装 Solaris 客户机，或者从 UNIX 安装程序包 (tar) 本地安装。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。 有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

先决条件

- 安装介质代理时，确保以下条目位于文件 `/etc/system` 中：

  ```
  set semsys:seminfo semmni=100
  ```
- 此时，您应当已在网络上安装了 Cell Manager for UNIX 和安装服务器 for UNIX。

  有关说明，请参见安装 Data Protector Cell Manager 和安装服务器 (第 25 页)。
- 要安装 Solaris 客户机，您需要 *root* 访问权或具有 *root* 权限的帐户。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。

远程安装

使用 Data Protector 图形用户界面从 UNIX 的安装服务器将客户机软件安装到客户机上。有关用于远程安装软件的逐步式过程，请参见远程安装 (第 83 页)。

> **注意：**
> 如果安装`User Interface`组件，则在使用之前应该更新环境变量。 有关详细信息，请参见设置环境变量 (第 31 页)。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

> **重要：**
> 要将 Data Protector 安装到链接目录中，例如：
>
> `/opt/omni/ -> /prefix/opt/omni/`
>
> `/etc/opt/omni/ -> /prefix/etc/opt/omni/`
>
> `/var/opt/omni/ -> /prefix/var/opt/omni/`
>
> 应该在安装前创建链接并确保目标目录存在。

> **注意：**
> 远程安装或升级时，/tmp 和 /var/tmp> 文件夹下的可用磁盘空间应至少为要安装的最大包的大小。

本地安装

如果在您的环境中未安装适用于 UNIX 的安装服务器，则必须通过 UNIX 安装程序包 (tar) 执行本地安装。有关说明，请参见在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)。

群集感知客户机

对于安装群集感知客户机，还存在一些其他先决条件。有关更多详细信息，请参见安装群集感知客户机 (第 156 页)。

安装后配置

配置文件

在客户机系统上安装介质代理组件之后，必须检查配置以确定所需的变更，具体取决于将使用的平台和设备类型。

- 如果您的 Solaris 系统是已打补丁的 Solaris 9 或 Solaris 10 系统，磁带设备驱动程序可能已默认支持您的设备。要对此进行检查，请使用 strings 命令。

  例如，如果要检查您的 DAT-72 设备是否无需额外的配置步骤即可使用，请执行：

  Solaris (SPARC) 系统：

  ```
  strings /kernel/drv/sparcv9/st | grep HP
  ```

  Solaris(x86、x64)系统：

  ```
  strings /kernel/drv/st | grep HP
  ```

  检查命令输出。如果输出中显示了您的设备，则不需要额外的步骤。反之，则按照以下的说明进行操作。

- 对于 DAT(4 毫米)设备，需要在 /kernel/drv/st.conf 文件中添加以下行：

  ```
  tape-config-list =

  "HP HP35470A", "HP DDS 4mm DAT", "HP-data1", "HP HP35480A", "HP DDS-DC 4mm DAT",
  "HP-data1", "HP C1533A", "HP DDS2 4mm DAT", "HP-data2", "HP C1537A", "HP DDS3 4mm
  DAT", "HP-data3", "HP C1553A", "HP DDS2 4mm DATloader", "HP-data2", "HP C1557A",
  "HP DDS3 4mm DATloader", "HP-data3"; HP-data1 =
  1,0x34,0,0x8019,3,0x00,0x13,0x03,2; HP-data2 =
  1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3; HP-data3 =
  1,0x34,0,0x8239,4,0x0,0x13,0x24,0x3,3;
  ```

> **重要：**
> 这些数据条目不同于客户支持人员通常建议的默认条目。请准确指定这些行，否则 Data Protector 将无法使用您的驱动器。

- 对于 DLT、DLT1、SuperDLT、LTO1、LTO2 和 STK9840 设备，需要在 /kernel/drv/st.conf 文件中添加以下行：

  ```
  tape-config-list =

  "HP Ultrium 1-SCSI", "HP Ultrium 1-SCSI", "LTO-data", "HP Ultrium 2-SCSI", "HP_
  LTO", "HP-LTO2", "DEC DLT2000", "Digital DLT2000", "DLT2k-data", "Quantum
  DLT4000","Quantum DLT4000", "DLT4k-data", "QUANTUM DLT7000", "Quantum DLT7000",
  "DLT7k-data", "QUANTUM DLT8000", "Quantum DLT8000", "DLT8k-data", "HP C9264CB-
  VS80","HP DLT vs80 DLTloader","HP_data1" "QUANTUM SuperDLT1", "QUANTUM SuperDLT",
  "SDLT-data", "TANDBERGSuperDLT1", "TANDBERG SuperDLT", "SDL-data", "STK 9840",
  "STK 9840", "CLASS_9840";

  DLT2k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT4k-data =
  1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3; DLT7k-data =
  1,0x38,0,0x8639,4,0x82,0x83,0x84,0x85,3; DLT8k-data =
  1,0x77,0,0x1D639,4,0x84,0x85,0x88,0x89,3; HP_data1 =
  1,0x3a,0,0x8639,4,0x40,0x86,0x87,0x7f,0; LTO-data =
  1,0x7a,0,0x1d679,4,0x00,0x00,0x00,0x40,3; HP-LTO2 =
  1,0x7a,0,0xd639,4,0x00,0x00,0x00,0x42,3; SDLT-data =
  1,0x79,0,0x8639,4,0x90,0x91,0x90,0x91,3; CLASS_9840 = 1,0x78,0,0x1d679,1,0x00,0;
  ```

- 对于 StorageWorks 12000e (48AL) 自动加载器 (HPE C1553A)，除了 /kernel/drv/st.conf 文件中的 HPE 数据条目之外，还需要添加以下条目：

  ```
  name="st" class="scsi" target=ID lun=0; name="st" class="scsi" target=ID lun=1;
  ```

  将 *ID* 符号替换为自动加载器的 SCSI 地址，并将自动加载器选项号设置为 5(开关位于设备的后面板上)，并将驱动器的 DIP 开关设置设为 11111001(开关可以从自动加载器的底部访问)。

> **注意：**
> StorageWorks 12000e 库没有用于拾取器设备的专用 SCSI ID，但它通过相同的 SCSI ID 接收数据驱动器访问命令和拾取器命令。 但是，数据驱动器存取命令必须定向到 SCSI lun=0，拾取器命令必须定向到 SCSI lun=1。

对于所有其他设备，请检查 st.conf.templ 模板(位于 /opt/omni/spt)来确定 st.conf 文件中的必需条目。 它只是一个模板文件，不能代替 st.conf 文件。

- 对于每一个要使用的磁带设备，检查文件 /kernel/drv/st.conf 中是否存在以下行并在必要时添加该行。 用设备地址替换 *ID* 占位符：

  SCSI 设备：

  ```
  name="st" class="scsi" target=ID lun=0;
  ```

  光纤通道设备：

  ```
  name="st" parent="fp" target=ID
  ```

  注意，parent参数的值可能因磁带设备的不同而有所不同。 有关详细信息，请参见您的磁带设备文档。

- 要在 Solaris 9 和更早的 Solaris 版本上控制 SCSI 交换器设备，您必须先安装 SCSI Pass-Through 驱动程序，然后再安装 SCSI 设备。

  通过以下步骤安装 SCSI Pass-Through 驱动程序：

1. 将 sst 模块复制到 /usr/kernel/drv/sparcv9 目录中，并将 sst.conf 配置文件复制到 /usr/kernel/drv 目录中：

   32 位 Solaris 系统：

   ```
   $cp /opt/omni/spt/sst /usr/kernel/drv/sst
   ```

   ```
   $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
   ```

   64 位 Solaris 系统：

   ```
   $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /sst
   ```

   ```
   $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
   ```

2. 在 /etc/devlink.tab 文件中添加以下行：

   > **重要：**
   > 编辑 /etc/devlink.tab 文件时，不要使用“空格 ([space])”字符。 请仅使用 [TAB] 字符。

   “type=ddi_pseudo;name=sst;minor=character rsst\A1”

   这会导致 devlinks (1M) 创建指向设备的链接，名称采用 /dev/rsstX 形式，其中的 X 代表 SCSI 目标编号。

3. 对于每一个要控制的 SCSI 交换器设备，检查文件 /kernel/drv/sst.conf 中是否存在以下行且在必要时添加。 用设备地址替换 *ID* 占位符：

   SCSI 设备：

   ```
   name="sst" class="scsi" target=ID lun=0;
   ```

   光纤通道设备：

   ```
   name="sst" parent=”lpfc” class="scsi" target=ID lun=0;
   ```

   注意，parent参数的值可能因磁带设备的不同而有所不同。 有关详细信息，请参见您的磁带设备文档。

4. 通过输入以下命令在系统上安装驱动程序：

   ```
   add_drv sst
   ```

5. 在此阶段，您已准备好安装 SCSI 设备。 在安装之前，必须为交换器设备的每个驱动器和机械手(拾取器)分配正确的 SCSI 地址。 系统的任何其他设备不能使用所选的地址。

   要检查 SCSI 配置，通过运行以下命令(特定于 Solaris (SPARC) 的步骤)关闭系统：

   ```
   shutdown -i0
   ```

   然后在 ok 提示符处运行 probe-scsi-all 命令来检查所分配的地址：

   ```
   ok probe-scsi-all
   ```

   完成之后，使用以下命令重新启动系统：

   ```
   ok boot -r
   ```

   要准备系统以使用 SCSI 设备，按照下例中所示的步骤执行：

   a. 编辑 /kernel/drv/st.conf 来设置设备参数以使用所分配的 SCSI 端口。 有关详细信息，请参见设备文档。 仅当磁带设备驱动程序默认不支持您的设备时修改 tape-config-list 参数。
   b. 编辑 /kernel/drv/sgen.conf 来设置设备的驱动器参数，以使用所分配的 SCSI 端口(请参见相应设备的文档)。

c. 编辑 /usr/kernel/drv/sgen.conf 来设置 ADIC SCSI 控制设备，以使用所分配的 SCSI 端口 4。 将 ADIC SCSI Exchanger 驱动器的以下数据添加到 /usr/kernel/drv/sst.conf 文件：

```
name=”sst” class= “scsi” target=4 lun=0;
```

- 要在 Solaris 10(SPARC、x86、x64)上控制 SCSI 交换器设备，则应配置内置 sgen 驱动程序，然后安装 SCSI 设备。 请遵循以下步骤：

1. 打开文件 /kernel/drv/sgen.conf。

   如果文件中显示了参数 device-type-config-list，则将更换器设备引用添加到已存在的行中，例如：

   ```
   device-type-config-list=”scanner”, "changer";
   ```

   如果尚未定义参数，则将以下行添加到文件：

   ```
   device-type-config-list="changer";
   ```

2. 对于每一个要控制的 SCSI 交换器设备，检查文件 /kernel/drv/sgen.conf 中是否存在以下行且在必要时添加。 用设备地址替换 *ID* 占位符：

   ```
   name="sgen" class="scsi" target=ID lun=0;
   ```

3. 在此阶段，您已准备好安装 SCSI 设备。 在安装之前，必须为交换器设备的每个驱动器和机械手(拾取器)分配正确的 SCSI 地址。 系统的任何其他设备不能使用所选的地址。

   要检查 SCSI 配置，通过以下命令(特定于 SPARC 系统的步骤)关闭系统：

   ```
   shutdown -i0
   ```

   然后在 ok 提示符处运行 probe-scsi-all 命令来检查所分配的地址：

   ```
   ok probe-scsi-all
   ```

   完成之后，使用以下命令重新启动系统：

   ```
   ok boot -r
   ```

   要准备系统以使用 SCSI 设备，按照下例中所示的步骤执行：

   a. 编辑 /kernel/drv/st.conf 来设置设备参数以使用所分配的 SCSI 端口。 有关详细信息，请参见设备文档。 仅当磁带设备驱动程序默认不支持您的设备时修改 tape-config-list 参数。

   b. 编辑 /kernel/drv/sgen.conf 来设置 ADIC SCSI 控制设备，以使用所分配的 SCSI 端口 4。 将 ADIC SCSI Exchanger 驱动器的以下数据添加到 /kernel/drv/sgen.conf 文件：

      ```
      name="sgen" class= "scsi" target=4 lun=0;
      ```

修改 /kernel/drv/st.conf 文件和 /usr/kernel/drv/sst.conf 文件(Solaris 9 和更早期的 Solaris 版本)或 /kernel/drv/sgen.conf 文件 (Solaris 10) 后，就可以将备份设备与系统进行物理连接了。

将备份设备与 **Solaris** 系统连接

将备份设备与 **Solaris** 系统连接

1. 创建 reconfigure 文件：

   ```
   touch /reconfigure
   ```

2. 通过输入 `$shutdown -i0` 命令关闭系统，然后关闭计算机并将设备与 SCSI 总线进行物理连接。 检查没有任何其他设备正在使用为该设备选择的同一 SCSI 地址。

   有关受支持设备的详细信息，请参见 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

   > **注意：**
   > 在 Solaris 系统上，Data Protector 不会自动识别清洗带。 如果 Data Protector 检测到并在 StorageWorks 12000e (48AL) 设备中插入清洗带，则磁带驱动程序会进入未定义状态，可能需要您重新启动系统。 请在 Data Protector 发出清洗带请求时，手动加载清洗带。

3. 如果您的系统是 Solaris (SPARC)，可通过按 `Stop-A` 键来重新开启系统和中断启动过程。
4. 通过在 `probe-scsi-all` 提示符处输入 `ok` 命令验证是否正确识别了新设备：

   ```
   ok > probe-scsi-all
   ```

   然后，输入：

   ```
   ok > go
   ```

   继续。
5. 在此阶段，设备应当正确工作。 对于驱动器，设备文件必须位于 `/dev/rmt` 目录中；对于 SCSI 控制设备(拾取器)，设备文件必须位于 `/dev` 目录中。

   > **注意：**
   > 在 Solaris 9 和更早期 Solaris 版本上(特别是对于 Solaris 64 位系统)，并不总是会自动创建指向 SCSI 控制设备(拾取器)的链接。 在 Solaris 10 上，从来没有创建过这样的链接。 在这种情况下，创建符号链接以将合适的设备文件加入到 `/dev/rsst`*Num*，其中 *Num* 是您选择的一个数字。 例如：
   >
   > ***当使用 sst 时：***
   >
   > ```
   > ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4
   > ```
   >
   > ***当使用 sgen 时：***
   >
   > ```
   > ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /dev/rsst4
   > ```

   您可以使用 Data Protectoruma 实用程序验证设备。 要检查前面示例的 SCSI 交换器设备的拾取器(使用 SCSI 端口 4)，请输入：

   ```
   echo “inq”|/opt/omni/lbin/uma -ioctl /dev/rsst4
   ```

   拾取器必须将自身标识为 SCSI-2 设备库。 可以通过强制该库初始化自身来检查该库。 命令为：

   ```
   echo “init”|/opt/omni/lbin/uma -ioctl /dev/rsst4
   ```

请确保使用伯克利样式的设备文件；在此例中，对于磁带驱动器使用 `/dev/rmt/0cbn`(不是 `/dev/rmt/0h`))，对于 SCSI 控制文件(拾取器)使用 `/dev/rsst4`。

下面的步骤

完成安装步骤并且将备份设备与 Solaris 客户机正确连接之后，如需有关配置备份设备、介质池和其他配置任务的其他信息，请参见《*Data Protector 帮助*》的索引：“配置，备份设

备”。

安装 Linux 客户机

可以使用适用于 UNIX 的 安装服务器 远程安装 Linux 客户机系统，或者从 UNIX 安装程序包 (tar) 本地安装。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。 有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

先决条件

- 必须在 64 位 Linux 系统 (x86_64) 上安装 32 位 GNU C 库 (glibc) 包。
- 此时，您应当已在网络上安装了 Cell Manager for UNIX 和 安装服务器 for UNIX。
  有关说明，请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。
- 必须安装并设置 rpm 实用程序。 其他打包系统(例如 deb)不受支持。
- 要在远程系统上安装 Data Protector 组件，远程系统必须满足以下先决条件：
  - inetd 或 xinetd 服务必须正在运行或已设置，以使 Data Protector 能够启动它。
  - 应为客户机配置了无密码身份验证或 ssh。
- 确保内核支持 SCSI 设备(模块 SCSI support、SCSI tape support 和 SCSI generic support)。 Probe all LUNs on each SCSI device 参数为可选。
  关于 Linux 内核中 SCSI 支持的详细信息，请参见 Linux 分发文档或者 Linux 内核文档。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。

> **注意：**
> Data Protector 使用默认端口号 5555/5565。 因此，其他程序不应使用该特定端口号。一些 Linux 操作系统分发版本将该端口号用于其他用途。
>
> 如果端口号 5555/5565 已在使用，则应使之可供 Data Protector 使用，或者也可以将默认端口号更改为某个未用端口号。 请参见更改默认的 Data Protector Inet 端口 (第 306 页)。

自动灾难恢复

在希望使用增强型自动灾难恢复 (EADR) 或一键式灾难恢复 (OBDR) 进行恢复的系统上，以及需要为 EADR 或 OBDR 准备 DR CD ISO 映像的系统上，必须安装 Automatic Disaster Recovery 组件。

Serviceguard 群集

对于 Serviceguard 群集， Data Protector 代理(磁盘代理、介质代理)必须单独安装在*每个群集节点*(本地磁盘)而不是共享磁盘上。

安装之后，需要将*虚拟主机*(应用程序包)作为客户机导入单元中。 因此，应用程序包(例如 Oracle)必须使用它的*虚拟 IP* 在群集上运行。 在导入客户机之前，使用命令 `cmviewcl -v` 来检查这一点。

您可以使用被动节点来安装 安装服务器。

Novell Open Enterprise Server (OES)

在 Novell OES 系统上，Data Protector 会自动安装 OES 感知磁盘代理。 但是，存在一些特定于 Novell OES 的方面：

- 如果在 32 位 SUSE Linux Enterprise Server 9.0 (SLES) 上安装 Novell OES，则在系统上安装 Data Protector Linux 客户机之后，必须同时升级 Data Protector 客户机。

  请注意，在升级过程中，新的 Novell OES 感知磁盘代理将被远程安装到客户机系统上。
- 如果从 SLES 中删除了 Novell OES 组件，则必须重新安装 Data Protector 客户机。

远程安装

使用 Data Protector 图形用户界面，通过将 Data Protector 组件从 安装服务器 for UNIX 分发到 Linux 系统来远程安装 Linux 客户机系统。 有关分发软件的逐步过程，请参见远程安装 (第 83 页)。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

本地安装

如果在您的环境中未安装适用于 UNIX 的 安装服务器，则必须通过 UNIX 安装程序包 (tar) 执行本地安装。 有关说明，请参见在 UNIX 系统上安装 安装服务器 (第 39 页)。

将备份设备与 Linux 系统连接

在 Linux 客户机上安装介质代理组件之后，请执行以下步骤将备份设备与系统进行连接：

1. 运行 `cat /proc/scsi/scsi` 命令来确定可用于驱动器和控制设备(机械手)的 SCSI 地址。
2. 在设备上设置 SCSI 地址。 根据设备类型，通常可以通过设备上的开关切换来完成设置。 有关详细信息，请参见设备自带的文档。

   有关受支持的设备的详细信息，请参见 https://softwaresupport.softwaregrp.com/。
3. 将设备与系统连接，开启设备，然后开启计算机，并等待启动过程完成。 设备文件将在启动过程期间创建。

   在 Red Hat Enterprise Linux 系统上，当新设备与系统连接时，启动过程中将会启动应用程序 Kudzu。 按任意键启动该应用程序，然后单击 Configure 按钮。
4. 要验证系统是否正确识别新的备份设备，请先运行 `cat /proc/scsi/scsi`，然后运行 `dmesg |grep scsi`。 此时会列出每个已连接备份设备的设备文件。

   示例

   对于机械手，`dmesg |grep scsi` 命令的输出为：

```
Detected scsi generic sg2 at scsi2, channel 0, id 4, lun 0, type 8
```

对于驱动器，输出为：

```
Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
```

5. 在 /dev 目录中创建设备文件。 要检查是否创建了指向设备文件的链接，请执行：

   ```
   ll /dev | grep device_file
   ```

   例如：

   ```
   ll /dev | grep sg2
   ```

   该命令的输出为：

   ```
   lrwxrwxrwx 1 root root 3 Nov 27 2001 sg2 -> sgc
   ```

   其中，/dev/sg2 是指向设备文件 /dev/sgc 的链接。 这意味着，对于机械手，Data Protector 使用的设备文件为 /dev/sgc，对于驱动器，它使用的设备文件为 /dev/st0。机械手的设备文件为 sga、sgb、sgc、... sgh，驱动器的设备文件为 st0、st1、... st7。

下面的步骤

安装过程已完成并且备份设备已正确连接到 Linux 客户机系统后，请参见《*Data Protector 帮助*》索引："配置, 备份设备"以了解有关配置备份设备和介质池或执行其他配置任务的信息。

安装 ESX Server 客户机

ESX Server 是修改版的 Linux 操作系统。 有关如何在 ESX Server 系统上安装 Data Protector 组件的详细信息，请参见安装 Linux 客户机 (第 73 页)。

安装 IBM AIX 客户机

可以使用适用于 UNIX 的 安装服务器 远程安装 IBM AIX 客户机，或者从 UNIX 安装程序包 (tar) 本地安装。

在启动安装进程之前，先确定需要在客户机系统上安装哪些组件。 有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

先决条件

- 有关系统要求、磁盘空间要求、受支持的平台和 Data Protector 组件，请参见Data Protector 产品声明、软件说明和参考。
- 此时，您应当已在网络上安装了Cell Manager for UNIX 和 安装服务器 for UNIX。
  有关说明，请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。
- 在安装Disk Agent组件之前，请检查端口映射器是否已在选定系统上启动并正在运行。

/etc/rc.tcpip 文件中必须存在用于启动端口映射器的行：

```
start /usr/sbin/portmap "$src_running"
```

如果 srcmstr 后台程序正在运行，则 src_running 标志会设置为 1。 srcmstr 后台程序是系统资源控制器 (System Resource Controller, SRC)。 srcmstr 后台程序可以派生并控制子系统、处理子系统短状态请求、向子系统传递请求，以及处理错误通知。

IBM HACMP Cluster

在适用于 AIX 的 IBM 高可用性群集多处理环境中，在所有群集节点上安装Data ProtectorDisk Agent组件。 有关如何在安装了群集感知应用程序数据库的群集环境中安装 Data Protector 的信息，请参见安装 Data Protector 集成客户机 (第 99 页)。

安装之后，将群集节点和*虚拟服务器*(虚拟环境包 IP 地址)导入 Data Protector 单元。

远程安装

使用 Data Protector 图形用户界面从适用于 UNIX 的安装服务器将 AIX 客户机软件安装到客户机上。 有关用于远程安装软件的逐步式过程，请参见安装 Data Protector 客户机 (第 49 页)。

本地安装

如果在您的环境中未安装适用于 UNIX 的安装服务器，则必须通过 UNIX 安装程序包 (tar) 执行本地安装。 有关说明，请参见安装 Data Protector 客户机 (第 49 页)。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

将备份设备与 AIX 客户机连接

在 AIX 客户机上安装介质代理组件之后，执行以下步骤：

1. 关闭计算机，然后将备份设备连接到 SCSI 总线。 检查是否有任何其他设备正在使用为备份设备选择的同一 SCSI 地址。

   有关受支持的设备的详细信息，请参见 https://softwaresupport.softwaregrp.com/。
2. 开启计算机，并等待启动过程完成。 启动 AIX 系统 smit 管理工具，并验证系统是否正确识别新的备份设备。

   重要：
   使用 smit 将设备的默认块大小更改为 0(可变块大小)。
3. 从 /dev 目录中选择相应的设备文件，并配置 Data Protector 备份设备。

重要：
请仅使用非重绕样式的设备文件。 例如，选择 /dev/rmt0.1 而非 /dev/rmt0。

下面的步骤

安装过程已完成并且备份设备已正确连接到 AIX 系统后，请参见《*Data Protector 帮助*》索引："配置，备份设备"以了解有关配置备份设备和介质池或执行其他 Data Protector 配置任务的信息。

安装 Mac OS X 客户机

可以使用适用于 UNIX 的安装服务器远程安装 Mac OS X 客户机，或者从 UNIX 安装包 (tar) 本地安装 Mac OS X 客户机。

仅支持磁带客户机 (DA)。

先决条件

- 有关系统要求、磁盘空间要求、受支持的操作系统版本和 Data Protector 组件，请参见 RAM 和磁盘空间要求 (第 77 页)、安装 Mac OS X 客户机 (第 77 页)和安装 Mac OS X 客户机 (第 77 页)。
- 以下是在客户机上安装 Windows 用户界面和远程安装的先决条件：
  - 在 Microsoft Windows XP Professional 系统上，必须安装 Service Pack 3 。
  - 在 Microsoft Windows Server 2003 系统上，必须安装 Service Pack 2 。
- 此时，您应当已在网络上安装了Cell Manager for UNIX 和 安装服务器 for UNIX。
  有关说明，请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。

Windows 系统上 Data Protector 客户机组件的 RAM 和磁盘空间要求

下表列出了 Windows 系统上不同 Data Protector 客户机组件的最低 RAM 和磁盘空间要求：

RAM 和磁盘空间要求

客户机系统组件	总 RAM (MB) [1]	可用磁盘空间 (MB) [2]
用户界面	512 [3]	150 [4]

[1] 这些数字只表示组件的要求。数字不包括操作系统、分页文件或其他应用程序的空间分配。
[2] 这些数字只表示组件的要求。数字不包括操作系统、分页文件或其他应用程序的空间分配。
[3] GUI 系统的内存要求随需要同时显示的元素数而大有不同。此注意事项适用于最坏的情况(如展开单一目录)。除非要在查看时展开所有目录，否则无需考虑客户机上的全部目录和文件名。研究显示，每 1000 个元素(目录或文件名)需要 2 MB 内存来显示，加上大约 50 MB 的基础需要。因此，512 MB RAM 足以显示最大数量的文件名。
[4] 关于磁盘空间，要记住页面文件本身应该能增长到物理内存的大约 3 倍。

客户机系统组件	总 RAM (MB) [1]	可用磁盘空间 (MB) [2]
磁带客户机 (Disk Agent)	每个 64(建议 128)	每个 20
介质代理 (Media Agent)		
集成组件		
英语文档(指南、帮助)	不适用	100

这些数字只表示组件的要求。例如，“磁盘空间”的数字不包括操作系统、页面文件或其他应用程序的空间分配。

建议

- 如果增加默认块大小，则 Micro Focus 建议将内核参数 `kern.sysv.shmmax` (最大共享内存段大小)设置为 32 MB。

远程安装

使用 Data Protector 图形用户界面从 UNIX 的安装服务器将 Mac OS X 客户机软件安装到客户机上。有关用于远程安装软件的分步过程，请参见安装 Data Protector 客户机 (第 49 页)。

> **注意：**
> 进行远程安装时，需要基于 UNIX 的安装服务器(Linux 或 HP-UX)以适应 Mac OS X 远程安装包(核心和磁带客户机)。

本地安装

如果在您的环境中未安装 安装服务器 for UNIX，则必须通过 UNIX 安装包 (tar) 执行本地安装。有关说明，请参见安装 Data Protector 客户机 (第 49 页)。

安装客户机组件之后，目标系统会自动成为 Data Protector 单元的成员。

安装 HP OpenVMS 客户机

OpenVMS 客户机的安装过程必须在受支持的 OpenVMS 系统上本地执行。不支持远程安装。

您可以在运行 OpenVMS 7.3-2/IA64 8.2-1 的系统上安装 Data Protector 磁盘代理、常规介质代理和用户界面(仅命令行界面)。您还可以在运行 OpenVMS 7.3-2 或更高版本的系统上安装 Oracle 集成组件。有关 Data Protector 组件的信息，请参见Data Protector 组件 (第 52 页)。

1 这些数字只表示组件的要求。数字不包括操作系统、分页文件或其他应用程序的空间分配。
2 这些数字只表示组件的要求。数字不包括操作系统、分页文件或其他应用程序的空间分配。

有关受支持设备、OpenVMS 平台版本，以及限制、已知问题与变通方法的信息，请参见 Data Protector 产品声明、软件说明和参考。

有关更多特定于 OpenVMS 的信息，请参见 *OpenVMS 发行说明*，它位于 OpenVMS 上的默认帮助文档目录中，例如：SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTES。

先决条件

在 OpenVMS 平台上安装 Data Protector 客户机之前，请检查以下方面：

- 确保装有 TCP/IP 传输协议并正在运行。
- 通过执行以下命令，设置系统的 TIMEZONE 功能：SYS$MANAGER:UTC$TIME_SETUP.COM。
- 登录到 OpenVMS 系统的 SYSTEM 帐户。 请注意，您必须具有相应的权限。
- 确保您有权访问含有 HP OpenVMS 客户机安装程序包的 Data Protector 安装程序包 (zip/tar)。
- 对于 Data Protector 单元中所有 Data Protector 组件，必须在主机名解析过程中执行反向 DNS 查询。

安装过程

安装过程可以通过 Data Protector Windows 安装程序包 (zip) 执行。

在 **OpenVMS** 系统上安装 **Data Protector** 客户机

1. 如果已经有 PCSI 安装文件，则转至 安装 Data Protector 客户机 (第 49 页)。 要获取 PCSI 安装文件，请在 OpenVMS Server 上提取安装程序包，并将其复制到所需位置。 您也可以从 Windows 系统通过 ftp 获取 PCSI 文件。
2. 运行以下命令：

   ```
   $ PRODUCT INSTALL DP /SOURCE=device:[directory]
   ```

   其中，*device*:[*directory*] 是 .PCSI 安装文件的位置。
3. 通过对提示回答 YES 来确认工具包的版本：

   示例

   ```
   The following product has been selected: AXPVMS DP A08.00-xx Layered Product Do
   you want to continue? [YES]
   ```
4. 选择要安装的软件组件。 您可以采用默认选择，这样将会安装磁盘代理、常规介质代理和用户界面。 您也可以单独选择每个组件。

   对于每个选定产品和对于可能安装的任意产品，可能会要求您选择一些选项(如果有)，以满足软件依赖关系要求。

   示例

   ```
   HP IA64VMS DP A08.00-xx: HP OpenVMS IA64 Data Protector V8.00
   COPYRIGHT HEWLETT-PACKARD COMPANY 2013
   Do you want the defaults for all options? [YES] NO
   Do you wish to install Disk Agent for this client node?
   [YES] YES
   ```

```
Do you wish to install Media Agent for this client node?
[YES] YES
Do you wish to install Command Language Interface for this client node?
[YES] YES
Do you wish to install Oracle Integration Agent for this client node?
[YES] YES
Do you want to review the options?
[NO] YES
HP IA64VMS DP X08.00-xx: HP OpenVMS IA64 Data Protector V8.00 [Installed]
Do you wish to install Disk Agent for this client node?
YES
Do you wish to install Media Agent for this client node?
YES
Do you wish to install Command Language Interface for this client node?
YES
Do you wish to install Oracle Integration Agent for this client node?
[YES] YES
Are you satisfied with these options?
[YES] YES
```

Data Protector 目录和文件的默认且唯一的位置为：

```
SYS$SYSDEVICE:[VMS$COMMON.OMNI]
```

目录结构将会自动创建，文件将放在该目录树中。

Data Protector 启动和关闭命令过程将放入

```
SYS$SYSDEVICE:[VMS$COMMON.SYS$STARTUP]
```

对于 OpenVMS 客户机，总是存在四个文件，只有选择 CLI 选项时，才会存在第五个文件。 有关的 5 个文件为：

- SYS$STARTUP:OMNI$STARTUP.COM 它是启动该节点上的 Data Protector 的命令过程。
- SYS$STARTUP:OMNI$SYSTARTUP.COM 它是定义 OMNI$ROOT 逻辑名称的命令过程。 该客户机所需的任何其他逻辑名称可以添加到该命令过程中。
- SYS$STARTUP:OMNI$SHUTDOWN.COM 它是关闭该节点上的 Data Protector 的命令过程。
- OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM 它是用于启动 TCP/IP INET 进程的命令过程，然后该进程会执行由 Cell Manager 发送的命令。
- OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM 它是定义调用 Data Protector CLI 所需符号的命令过程。 只有在安装期间选择 CLI 选项时，系统上才会存在该文件。

  请针对所有将使用 CLI 界面的用户，从 login.com 过程执行该命令过程。 在该过程中会定义几个正确执行 CLI 命令所必需的逻辑名称。

5. 在 SYS$MANAGER:SYSTARTUP_VMS.COM 中插入以下行：

```
@sys$startup:omni$startup.com
```

6. 在 SYS$MANAGER:SYSHUTDWN.COM 中插入以下行：

   ```
   @sys$startup:omni$shutdown.com
   ```

7. 确保可以从 OpenVMS 客户机连接 Cell Manager 的所有可能的 TCP/IP 别名。
8. 使用 Data Protector 图形用户界面将 OpenVMS 客户机导入 Data Protector 单元。

在安装期间会创建名为 OMNIADMIN 的帐户。 OMNI 服务使用该帐户运行。

该帐户的登录目录为 OMNI$ROOT:[LOG]，它保存 Data Protector 组件每次启动的日志文件 OMNI$STARTUP_INET.LOG。 该日志文件包含执行请求的进程的名称、所用 Data Protector 映像的名称，以及请求的选项。

任何意外错误都记录在该目录中的 DEBUG.LOG 中。

> **注意：**
> 在 OpenVMS 8.3 和更高版本上， Data Protector 安装会显示以下消息：
>
> ```
> %PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0800
> -XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
> is not signed and therefore has no manifest file
> ```
>
> 要避免发出该警告，请使用 /OPTION=NOVALIDATE_KIT 运行产品安装命令。

在群集环境中安装

如果使用公用系统磁盘，则客户机软件只需安装一次。 但是，对于每个节点，需要执行 OMNI$STARTUP.COM 过程，节点才可用作 Data Protector 客户机。 如果使用的不是公用系统磁盘，则需要在每台客户机上安装客户机软件。

如果使用群集 TCP/IP 别名，并且如果使用群集公用系统磁盘，则可以为别名定义客户机。 定义别名客户机后，不需要配置各个客户机节点。 您可以选择客户机定义或别名定义以在群集中运行备份和还原。 根据您的配置，保存或还原可能可以使用，也可能不能使用到磁带设备或磁带库的直接路径。

磁盘代理配置

OpenVMS 上的 Data Protector 磁盘代理支持装载的 FILES-11 ODS-2 和 ODS-5 磁盘卷。 不需要配置 OpenVMS 磁盘代理。 但是，在设置将使用它的备份规范时，需要记住几点。 下面介绍这几点：

- 输入 GUI 或传递给 CLI 的文件规范必须使用 UNIX 样式语法，例如：

  ```
  /disk/directory1/directory2/.../filename.ext.n
  ```

  - 字符串必须以斜杠开头，后跟磁盘、目录和文件名，中间用斜杠分隔。
  - 不要在磁盘名称后面加冒号。
  - 版本号前面应该用句点，而不是分号。
  - OpenVMS 文件的文件规范不区分大小写，驻留在 ODS-5 磁盘上的文件除外。

示例

OpenVMS 文件规范：

```
$1$DGA100:[USERS.DOE]LOGIN.COM;1
```

必须使用以下形式指定给 Data Protector：

```
/$1$DGA100/USERS/DOE/LOGIN.COM.1
```

> **注意：**
> 没有隐式版本号。 必须始终指定版本号，且仅备份指定的文件版本。
>
> 对于一些允许使用通配符的选项，可以将版本号替换为星号“*”。
>
> 要在备份中包括文件的所有版本，则应在 GUI 中进行选择，或者在 CLI 中在 `-only` 选项下包括文件规范，并使用通配符作为版本号，如下：
>
> ```
> /DKA1/dir1/filename.txt.*
> ```

介质代理配置

您应根据 OpenVMS 和硬件文档的指导，配置 OpenVMS 系统上的设备。 必须先使用 SYSMAN 创建磁带库的伪设备，如下：

```
$ RUN SYS$SYSTEM:SYSMAN

SYSMAN&gt; IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER
```

其中：

- c = K，代表直接连接的 SCSI 磁带库。
- a = A,B,C, ...代表 SCSI 控制器的适配器字符。
- n = 磁带库的机械手控制设备的单元号。

> **注意：**
> 必须在系统启动之后执行该命令序列。

对于 SAN 连接的磁带库，在根据 SAN 指南配置 SAN 设备之后，磁带驱动器和机械手设备名称将会在 OpenVMS 下自动显示。

如果要安装磁带介质库供 Data Protector 使用，则应在 Data Protector 中配置它之前验证硬件是否正确工作。 您可以使用 Media Robot Utility(MRU，可从惠普公司获取)来验证硬件。

> **注意：**
> 您通常可以使用 Data Protector GUI 来手动配置或自动配置这些设备。
>
> 但是，一些较旧的磁带库和所有与 HSx 控制器连接的磁带库无法进行自动配置。 请使用手动配置方法将这些设备添加到 Data Protector。

群集中的介质代理

处理与群集系统连接的设备时：

1. 配置每个磁带设备和磁带库，使之可从每个节点进行访问。
2. 将节点名称添加到设备名称末尾，以区分不同设备。
3. 对于磁带设备，在 `Devices/Properties/Settings/Advanced/Other` 下设置常见的 `Device Lock Name`。

示例

在带有节点 A 和 B 的群集中，一个 TZ89 与节点 A 连接，并通过 MSCP 供应给节点 B。配置名为 TZ89_A 的设备，使用节点 A 作为客户机；配置名为 TZ89_B 的设备，使用节点 B 作为客户机。两个设备获得一个公用设备锁名称 TZ89。现在，Data Protector 可以通过任一路径使用设备(知道它实际上只是一台设备)。如果在节点 B 上使用 TZ89_A 运行备份，Data Protector 会将数据从节点 B 移动到节点 A 上的设备。如果在节点 B 上使用 TZ89_B 运行备份，OpenVMS MSCP 服务器会将数据从节点 B 移动到节点 A 上的设备。

> **注意：**
> 对于群集中通过 MSCP 供应的磁带设备，对于通过 HSx 控制器连接的所有磁带设备，以及对于通过光纤通道连接的所有磁带设备，请遵循 *Data Protector 帮助* 索引中有关 SAN 配置的指导：“SAN, 配置设备于”。

命令行界面

在 OpenVMS 上使用 Data Protector 命令行界面之前，必须先运行 CLI 命令设置过程，如下：

```
$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM
```

有关可用 CLI 命令的说明，请参见 *Data Protector 命令行界面参考*。

Oracle 集成

按照 *Data Protector 集成指南* 中的说明安装 Oracle 集成并进行配置之后，请验证 OMNI$ROOT:[CONFIG.CLIENT]omni_info 中是否存在 -key Oracle8 条目，例如：

```
-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath
“““ -uxpath “““ -version 9.00
```

如果不存在该条目，请从 OMNI$ROOT:[CONFIG.CLIENT]omni_format 复制它。否则，Oracle 集成在 OpenVMS 客户机上不会显示为已安装。

下面的步骤

有关其他配置任务的信息，请参见 *Data Protector 帮助* 索引：“HP OpenVMS”。

远程安装

本节介绍使用 安装服务器 将 Data Protector 软件分发到客户机上的过程(远程安装或升级)。

使用 Data Protector 用户界面将软件分发到客户机上。支持跨平台客户机安装。

先决条件

- 有关安装的先决条件和建议，请参见介绍特定客户机安装过程的章节。参考列在 安装 Data Protector 客户机系统 (第 49 页) 和 安装集成 (第 50 页) 中。
- 有关受支持平台、Data Protector 组件和磁盘空间要求的信息，请参见 https://softwaresupport.softwaregrp.com/ 和 远程安装 (第 83 页)。

- 此时，您应当已在网络上安装了 Cell Manager 和 安装服务器。
- 关于全新远程安装，Windows 的 安装服务器必须驻留在共享目录中，从而在网络上可见。
- ***Windows 2012：*** 要远程安装到 Windows 2012 系统，请完成以下任一步骤：
  在**安装服务器主机**上配置作为远程主机 (omniinetpasswd -inst_srv_user) 管理员的域用户。 在此帐户下启动远程安装，并在无其他用户干预的情况下建立到远程主机的连接。

  或者

  在**远程主机**上的防火墙内阻止以下服务。

  ◦ 远程服务管理 (RPC)

  ◦ 远程服务管理 (RPC-EPMAP)

  或者

  在**安装服务器主机**上关闭 RPC/TCP(客户机端)。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

  DWORD SCMApiConnectionParam = 0x80000000

  合并 SCMApiConnectionParam 注册表值和掩码值 0x80000000。

  > **注意：** 不需要重新启动系统。

为成功的远程安装配置防火墙

用安装服务器安装新的 Data Protector 客户机或升级较旧的 Data Protector 客户机时，将在远程计算机上启动安装代理。 安装服务器随即通过 Data Protector 单元端口 (默认是 5555/5565) 连接到该代理。 但是，如果客户机上正在运行 Microsoft 防火墙或任何第三方防火墙软件，就无法建立连接，安装将失败。 要解决此问题，请执行以下步骤之一：

- 将 Windows 防火墙配置为允许通过特定端口连接。
- 对于 Microsoft 防火墙：如果在安装服务器上设置了 omnirc 选项 OB2FWPASSTHRU，则安装代理将自动注册 Windows 防火墙，安装继续正常进行。

建议

- ***UNIX 系统：*** 出于安全原因，建议使用安全 shell 进行 Data Protector 远程安装。 配置 SSH 时，将使用无密码身份验证，否则将提示用户输入凭据。

  要使用安全 shell，请在客户机和 安装服务器 上都安装并设置 OpenSSH。 如果私钥要加密，请在 安装服务器 上安装并设置 keychain。 请参见安装 Data Protector 客户机 (第 49 页)。

> **注意：**
> 您无法将软件分发到另一个 Data Protector 单元中的客户机上。 但是，如果具有独立的 安装服务器，可以将它导入多个单元。 然后，可以通过依次使用与每个 Cell Manager 连接的 GUI 在每个不同单元中分发软件。

- ***管理员帐户：*** 要使用属于**远程主机**上管理员组成员的本地用户 (远程主机已启用 UAC)，则在远程主机上完成以下任一步骤：

禁用用户帐户控制 (UAC)

> **注意：** 需要重新启动系统。

或

设置注册表值：

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
DWORD LocalAccountTokenFilterPolicy = 1
```

> **注意：** 不需要重新启动系统。

使用安全 shell 进行远程安装

通过安全 shell 以安全方式安装 Data Protector 组件，可以帮助您保护客户机和 安装服务器。 通过以下方式实现高级保护：

- 通过公钥-私钥对机制以安全的方式为客户机验证 安装服务器 用户。
- 通过网络发送加密的安装包。

> **注意：**
> 只有 UNIX 系统支持安全 shell 安装。

设置 OpenSSH

在客户机和 安装服务器 上都安装并设置 OpenSSH：

1. 确保系统上安装了 OpenSSH。 有关详细信息，请参见操作系统文档或分发文档。

   如果 OpenSSH 包不是 OS 分配的一部分，则需要从 http://www.openssh.org 下载 OpenSSH，然后同时在 Data Protector 客户机和 安装服务器 上安装。

   或者，在 HP-UX 上，可以使用 HP-UX Secure Shell。

   > **注意：**
   > 安全 shell 安装的默认位置为 /opt/ssh。

2. 在 安装服务器 上，运行 ssh-keygen 生成公钥-私钥对。 将私钥保存在 安装服务器 上，同时将公钥传输到客户机上。 请注意，如果使用加密私钥(即受密码片语保护)，则需要在 安装服务器 上设置 keychain(有关详细信息，请参见安装 Data Protector 客户机 (第 49 页))。

   有关 ssh-keygen 的信息，请参见 http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen&sektion=1。

3. 使用名称 $HOME/.ssh 将公钥存储在客户机的 authorized_keys 目录中。

   > **注意：**
   > $HOME/.ssh 通常是 root 用户的主目录。

   要设置 SSH 协议版本(SSH1 或 SSH2)，请修改以下文件中的 protocol 参数：

   a. ***在 安装服务器 上：***

      ssh_install_directory /ssh/etc/ssh_config

ssh 命令将使用该文件。

b. ***在客户机上：***

ssh_install_directory /ssh/etc/sshd_config

ssh 后台程序 (sshd) 将使用该命令。

请注意，这两个文件必须同步。

> **注意：**
> 默认的 SSH 协议版本为 SSH2。

4. 在客户机上，启动 ssh 后台程序：

ssh_install_directory /ssh/sbin/sshd

5. 将客户机添加到已知主机列表中(位于 安装服务器 上的 $HOME/.ssh/known_hosts 中)，方法是运行：

ssh root@*client_host*

其中，*client_host* 必须为完全限定 DNS 名称，例如：

ssh root@client1.company.com

设置 keychain

keychain 是一个工具，利用它可以在解密私钥时无需手动提供通行密码。 只有私钥进行加密的情况下才需要它。

设置 keychain：

1. 将 keychain 从 http://www.gentoo.org/proj/en/keychain/index.xml 下载到 安装服务器。
2. 在 $HOME/.profile 中添加以下两行：

HP-UX 和 Solaris 系统：

keychain_install_directory /keychain-*keychain_version*/keychain $HOME/.ssh/*private_key*

. $HOME/.keychain/'hostname'-sh

Linux 系统：

/usr/bin/keychain $HOME/.ssh/*private_key*

. $HOME/.keychain/'hostname'-sh

3. 在 安装服务器 上，将 OB2_ENCRYPT_PVT_KEY omnirc 选项设置为 1。 有关 omnirc 选项的详细信息，请参见 *Data Protector 故障诊断指南*。

如果因执行此命令失败而无法执行安全 shell 安装，将发出一个警告。 但是，将使用标准 Data Protector 远程安装方法继续安装。

下面的步骤

设置 OpenSSH 和 keychain 后，按 安装 Data Protector 客户机 (第 49 页) 中所述使用 GUI，或使用 CLI 通过运行 ob2install 命令向单元中添加客户机。 有关 CLI 命令及其参数的信息，请参见 *Data Protector 命令行界面参考*。

注意：
如果因为执行命令发生失败而无法执行安全 shell 安装，则会发出一条警告消息。但是，安装将继续使用标准 Data Protector 远程安装方法。

向单元添加客户机

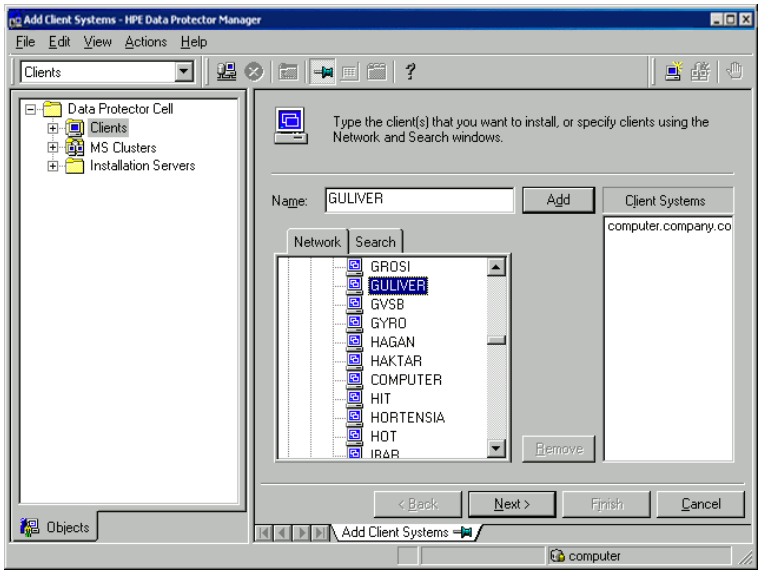
将 **Data Protector** 软件分发到不在 **Data Protector** 单元中的客户机上

1. 通过单击**开始 > 程序 > Data Protector > Data Protector 管理器**，启动 Data Protector GUI。

   注意：
   有关 Data Protector 图形用户界面的详细信息，请参见Data Protector 图形用户界面 (第 23 页)和*Data Protector 帮助*。

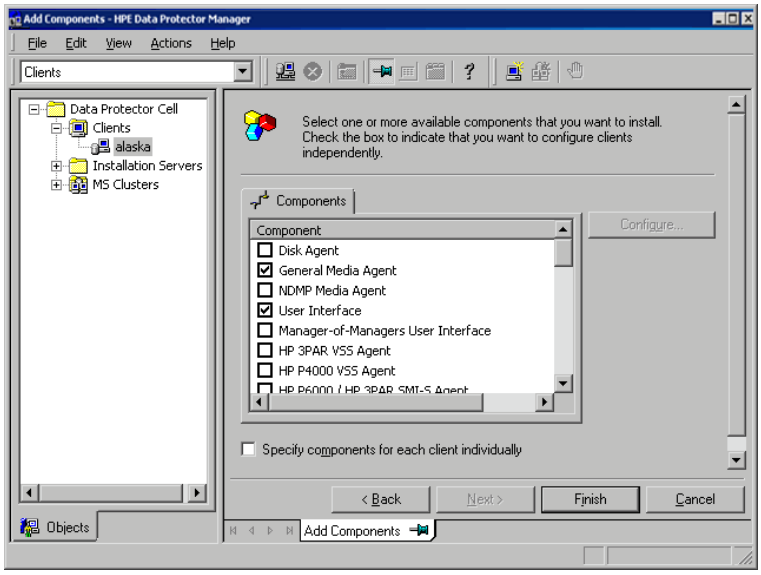
2. 在 Data Protector Manager 中，切换到**客户机**环境。
3. 在“范围窗格”中，右键单击**客户机**，然后单击**添加客户机**。
4. 如果配置了多个安装服务器，则选择要安装客户机的平台(UNIX 或 Windows)和要用于安装客户机的安装服务器。单击**下一步 (Next)**。
5. 键入客户机的名称，或搜索要安装的客户机(仅限于 Windows GUI 中)，如安装 Data Protector 客户机 (第 49 页)中所示。单击**下一步 (Next)**。

   选择客户机



6. 选择要安装的 Data Protector 组件，如安装 Data Protector 客户机 (第 49 页)中所示。请注意，您只能选择一种介质代理。请参见Data Protector 组件 (第 52 页)。

选择组件



7. 要更改安装的默认用户帐户和目标目录(仅限于 Windows 中)，请单击**选项 (Options)**。
8. 如果已选择多个客户机并且要在每个客户机上安装不同组件，请单击**为各个客户机分别指定组件**，然后单击**下一步**。 单独为每个客户机选择要安装的组件。
9. 单击**下一步 (Next)**。
10. 单击**完成 (Finish)** 开始安装。
11. 在安装过程中和受到请求时，提供所需的数据(用户名、密码和(在 Windows 上还需提供)域)来访问特定客户机系统，然后单击**确定**。

在系统上安装 Data Protector 软件并将系统添加到 Data Protector 单元中之后，它会成为 Data Protector 客户机。

> **注意：**
> 在客户机系统上开始使用 Data Protector GUI 之前，将该系统的某个用户添加到相应的 Data Protector 用户组。 有关步骤和可用用户权限的说明，请参见《*Data Protector 帮助*》。

故障排除

完成远程安装时，可以使用 GUI 通过单击**操作 (Actions)** 和**重新启动失败的客户机 (Restart Failed Clients)** 来重新启动任意失败的安装过程。 如果安装再次失败，请参见安装和升级故障诊断 (第 279 页)。

向客户机中添加组件

您可以在现有客户机和 Cell Manager 上安装其他 Data Protector 软件组件。 组件可以从远程或本地添加。 对于本地安装，请参见更改 Data Protector 软件组件 (第 207 页)。

先决条件

相应的 安装服务器 必须可用。

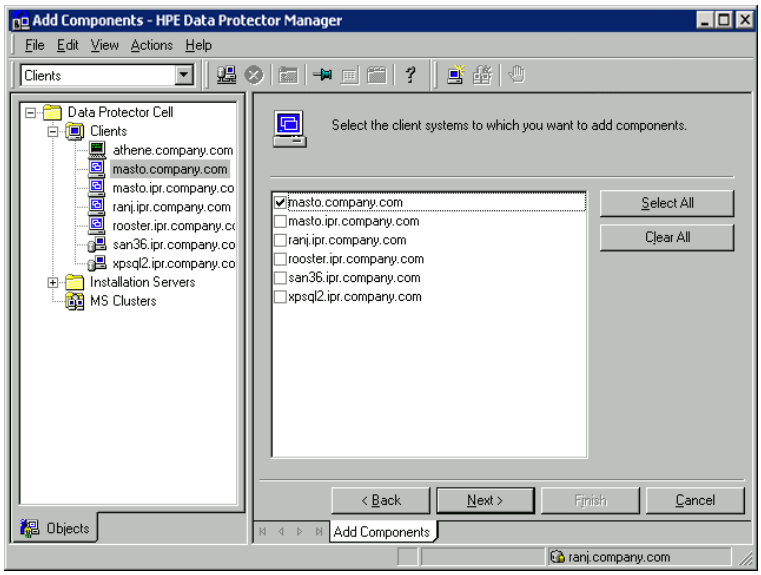
Serviceguard 客户机

在 Serviceguard 群集环境中，请确保要添加组件的节点处于活动状态。

将 Data Protector 软件分发到 Data Protector 单元中的客户机上

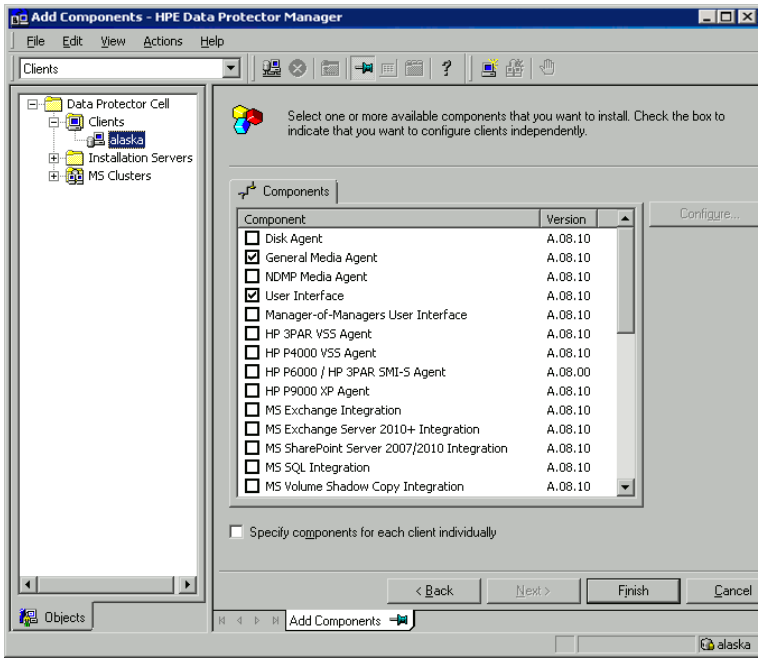
1. 在 Data Protector Manager 中，切换到**客户机 (Clients)** 环境。
2. 在“范围窗格 (Scoping Pane)”中，展开“客户机 (Clients)”，右键单击某个客户机，然后单击**添加组件 (Add Components)**。
3. 如果配置了多个 安装服务器，则选择要安装组件的客户机的平台(UNIX 或 Windows)和要用于安装组件的 安装服务器。 单击**下一步 (Next)**。
4. 选择要在其中安装组件的客户机，如选择客户机 (第 89 页)中所示。 单击**下一步 (Next)**。

   选择客户机



5. 选择要安装的 Data Protector 组件，如安装 Data Protector 客户机 (第 49 页)中所示。 请注意，您只能选择一种介质代理。 请参见Data Protector 组件 (第 52 页)。

选择组件



如果已选择多个客户机，并且希望在各个客户机上安装不同组件，请单击**为各个客户机分别指定组件**，然后单击**下一步**。 单独为每个客户机选择组件。

单击**完成 (Finish)** 开始安装。

在 UNIX 和 Mac OS X 系统上进行本地安装

如果不在网络中安装适用于 UNIX 的安装服务器，或者如果由于某些原因无法远程安装客户机系统，可以从 UNIX 安装程序包 (tar) 本地安装 Data Protector 客户机。

在启动安装程序之前，先确定需要在客户机系统上安装哪些组件。 有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

> **注意：**
> Windows XP Home Edition 和 HP OpenVMS 客户机可以本地安装。 不支持远程安装。

先决条件

- 有关系统要求、磁盘空间要求、受支持的平台、处理器和 Data Protector 组件的信息，请参见《Data Protector 产品声明、软件说明和参考》。
- 您必须具有每个目标系统上的 root 权限。
- 安装必须使用 POSIX shell (sh)。

> **注意：**
> 您也可以使用以下步骤在本地升级 UNIX 客户机。 脚本将会检测先前的安装，并提示您执行升级。

安装过程

本地安装 UNIX 和 Mac OS X 客户机

1. 复制 HP-UX 或 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 在 LOCAL_INSTALL 目录中，执行 omnisetup.sh 命令。

   命令的语法如下：

   omnisetup.sh [-source *directory*] [-server *name*] [-install *component_list*]

   其中：

   - *目录*是提取安装包所在的位置。 如果未指定，则使用当前目录。
   - *name* 是要将客户机导入到的 Cell Manager 单元的完整主机名。 如果未指定，则不会自动将客户机导入单元。

     > **注意：**
     > 在升级 Cell Manager 或安装服务器上的客户机时，不需要指定 -install *component_list*。 在此情况下，安装程序在升级前将选择与系统上已安装的组件相同的组件，而不会发出提示。

   - *component_list* 是要安装的组件代码的逗号分隔列表。 不允许有空格。 如果未指定 -install 参数，则安装程序会对于在系统上安装每个可用组件分别给出提示。

     > **注意：**
     > 在升级客户机的情况下，安装程序在升级前将选择与系统上已安装的组件相同的组件，而不会发出提示。

     下表显示了组件的列表。 准确的组件列表取决于组件在特定系统上是否可用。 有关组件的说明，请参见Data Protector 组件 (第 52 页)。

Data Protector component codes

组件代码	组件
cc	用户界面
da	磁盘代理
ma	常规介质代理
ndmp	NDMP 介质代理
informix	Informix 集成
lotus	Lotus 集成

组件代码	组件
oracle8	Oracle 集成
mysql	MySQL 集成
postgresql	PostgreSQL 集成
vepa	虚拟环境集成
sybase	Sybase 集成
sap	SAP R/3 集成
sapdb	SAP MaxDB 集成
saphana	SA HANA 集成
db2	DB2 集成
emc	EMC Symmetrix Agent
smisa	P6000/ 3PAR SMI-S 代理
ssea	P9000 XP 代理
emcvnx	EMC VNX 存储提供程序
emcvmax	EMC VMAX 存储提供程序
netapp	NetApp 存储提供程序
StoreOnceSoftware	StoreOnce Software Deduplication
autodr	自动灾难恢复
docs	英语文档(指南、帮助)

示例

以下示例显示了如何在客户机上安装Disk Agent、General Media Agent、User Interface和 Informix Integration组件，并且使用 Cell Managercomputer.company.com 将该客户机自动导入到单元中：

```
./omnisetup.sh -server computer.company.com -installda,ma,cc,informix
```

3. 如果安装完成，并且客户机导入到 Data Protector 单元中，安装程序将会通知您。

   CORE 组件在首次选择安装任意软件组件时安装。

   CORE-INTEG 组件在首次选择安装或重新安装任意集成软件组件时安装。

从硬盘运行安装

要将安装程序包复制到计算机，并且从硬盘运行 UNIX 和 Mac OS X 客户机的安装或升级，则至少要复制 hpux/DP_DEPOT 和 LOCAL_INSTALL 目录。

> **注意：**
> Linux 仓库不支持本地安装。 即使在 Linux 系统上，也必须复制 HP-UX 仓库。

例如，如果将安装包复制到 /var/dp80，则目录必须是 /var/dp10 的子目录：

```
# pwd
/var/dp80
# ls
DP_DEPOT
LOCAL_INSTALL
```

将其复制到硬盘之后，更改为 LOCAL_INSTALL 目录并执行以下命令：

```
omnisetup.sh [-server name] [-install component_list]
```

例如：

```
./omnisetup.sh -install da
```

请注意，如果将 DP_DEPOT 目录复制到其他目录(例如，由于硬盘空间限制)，则还需要使用 -source 选项。

下面的步骤

如果在安装期间未指定 Cell Manager 的名称，客户机将不会被导入单元中。 在这种情况下，应使用 Data Protector 图形用户界面导入它。 有关步骤，请参见 。有关其他配置任务的信息，请参见*Data Protector 帮助*。

安装介质代理以使用 ADIC/GRAU 库或 StorageTek 库

Data Protector 提供了专用的 ADIC/GRAU 和 StorageTek ACS 库 策略，用于将 ADIC/GRAU 库或 StorageTek ACS 库配置为 Data Protector 备份设备。 您需要在将与 ADIC/GRAU 或 StorageTek 库中的驱动器物理连接的每个系统上安装 Data Protector 介质代理(常规介质代理或 NDMP 介质代理)。 此外，对于多主机配置，必须在控制 ADIC/GRAU 或 StorageTek 库机械手的系统上安装 Data Protector 介质代理。 请注意，多主机配置是库和驱动器不连接到同一计算机的配置。

对于 ADIC/GRAU 库，安装了介质代理软件并通过 GRAU/ADIC DAS 服务器访问库机械手的每个系统称作 **DAS 客户机**。 对于 STK ACS 集成，安装了介质代理软件并通过 STK ACS 服务器访问库机械手的每个系统称作 **ACS 客户机**。

注意：
您需要特别的许可证，具体取决于在 StorageTek 库中使用的驱动器和插槽数量。 有关详细信息，请参见Data Protector 许可 (第 243 页)。

连接库驱动器

将库驱动器与要安装介质代理软件的系统进行物理连接。

有关受支持的 ADIC/GRAU 或 STK 库的详细信息，请参见 https://softwaresupport.softwaregrp.com/。

有关如何将备份设备与系统进行物理连接的信息，请参见 安装 Data Protector 客户机 (第 49 页) 和 ADIC/GRAU 或 StorageTek 库随附的文档。

有关如何将备份设备与受支持的 Windows 系统进行物理连接的信息，请参见 安装 Data Protector 客户机 (第 49 页) 和 ADIC/GRAU 或 StorageTek 库随附的文档。

准备 Data Protector 客户机以使用 ADIC/GRAU 库

以下步骤与配置 ADIC/GRAU 库有关，应在安装介质代理软件之前完成它们：

1. 如果 DAS 服务器基于 OS/2，则在配置 Data Protector ADIC/GRAU 备份设备之前，请创建/更新 DAS 服务器计算机上的 `C:\DAS\ETC\CONFIG` 文件。 在该文件中，必须定义所有 DAS 客户机的列表。 对于 Data Protector，这意味着必须在文件中定义每个可以控制库机械手的 Data Protector 客户机。

   每个 DAS 客户机都用唯一的客户机名称(无空格)进行标识，例如 `DP_C1`。 例如，`C:\DAS\ETC\CONFIG` 文件的内容应类似如下：

   ```
   client client_name = DP_C1, # hostname = AMU,"client1" ip_address =
   19.18.17.15, requests = complete, options = (avc,dismount), volumes = ((ALL)),
   drives = ((ALL)), inserts = ((ALL)), ejects = ((ALL)), scratchpools = ((ALL))
   ```

2. 在安装有需要访问 ADIC/GRAU DAS 库机械手的 Data Protector 介质代理的 Data Protector 客户机上，编辑 `omnirc` 文件并设置以下选项：

`DAS_CLIENT`	在 DAS 服务器上定义的唯一 GRAU 客户机名称。 例如，如果客户机名称为 “DP_C1”，则 `omnirc` 文件中的相应行为 `DAS_CLIENT=DP_C1`。
`DAS_SERVER`	DAS 服务器的名称。

3. 您必须确定 ADIC/GRAU 库插槽分配策略的配置方式(静态或动态)。 有关如何检查所用分配策略是何种类型的信息，请参见*AMU 参考手册*。

   静态策略对于每个 volser 具有专用的插槽，而动态分配策略则随机分配插槽。 根据已设置的策略，您需要相应地配置 Data Protector。

   如果配置了静态分配策略，则需要向控制库机械手的系统中添加以下 omnirc 选项：

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

   注意：
   它适用于 HP-UX 和 Windows。

有关 ADIC/GRAU 库配置的更多问题，请与当地 ADIC/GRAU 支持人员联系，或者查看 ADIC/GRAU 文档。

安装介质代理来使用 ADIC/GRAU 库

先决条件

在系统上安装介质代理之前，必须满足以下安装先决条件：

- ADIC/GRAU 库必须已配置，并且正在运行。 请参见 ADIC/GRAU 库随附的文档。
- 必须安装并配置 Data Protector。 有关说明，请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。
- DAS 服务器必须已启动并正在运行。

  要控制 ADIC/GRAU 库，DAS 软件是必需的。 每个 DAS 客户机上必须安装 DAS 客户机软件。 由 Data Protector 启动的每个介质和设备相关操作首先从 DAS 客户机传送到 DAS 服务器。 然后，它被传递给 ADIC/GRAU 库的内部部分 (AMU - AML Management Unit)，该部分控制机械手和移动或加载介质。 操作完成之后，DAS 服务器会答复 DAS 客户机。 请参见 ADIC/GRAU 库随附的文档。
- 安装介质代理之前，必须先获取以下信息：
  - DAS 服务器(在 OS/2 主机上运行的应用程序)的主机名。
  - 可用驱动器的列表，以及驱动器相应的 DAS 名称。 获取的驱动器名称将在 Data Protector 中配置 ADIC/GRAU 驱动器时使用。

    如果已经为 ADIC/GRAU 系统定义了 DAS 客户机，则可以使用以下 `dasadmin` 命令之一获取该列表：

    ```
    dasadmin listd2 client
    dasadmin listd client
    ```

    其中，*`client`* 是要显示所保留驱动器的 DAS 客户机。

    `dasadmin` 命令可以从 OS/2 主机上的 `C:\DAS\BIN` 目录中调用；或者，如果安装在其他系统上，则可以从安装了 DAS 客户机软件的目录中调用。 在 UNIX 客户机系统上，该目录通常为 `/usr/local/aci/bin` 系统目录。
  - 可用“插入/弹出区域”的列表，以及相应的格式规范。

    在 OS/2 主机上，可以在 AMS (AML Management Software) 的“图形配置”中获得可用“插入/弹出区域”的列表：

    1. 从菜单 `Admin > Configuration` 启动该配置。
    2. 通过双击 **I/O 单元**图标，打开 **EIF 配置**窗口,然后单击**逻辑范围**字段。 在文本框中，将会列出可用的“插入/弹出区域”。

    > **注意：**
    > 一个 Data Protector 库设备只能处理一种介质类型。 记住哪种介质类型属于每个指定的“插入/弹出区域”非常重要，因为稍后将需要该数据来为 Data Protector 库配置“插入/弹出区域”。

- 驱动器的 UNIX 设备文件列表(如果要在 UNIX 系统上安装介质代理)。
  在系统上运行 `ioscan -fn` 系统命令以显示所需的信息。
  有关 UNIX 设备文件的详细信息，请参见安装 Data Protector 客户机 (第 49 页)。
- 驱动器的 SCSI 地址的列表(如果要在 Windows 系统上安装介质代理)。 例如，`scsi4:0:1:0`。
  有关 SCSI 地址的详细信息，请参见安装 Data Protector 客户机 (第 49 页)。

安装过程

安装过程包含以下步骤：

1. 使用 Data Protector 图形用户界面和 安装服务器 将介质代理组件分发到客户机上。 请参见安装 Data Protector 客户机 (第 49 页)。
2. 安装 ADIC/GRAU 库：
   - 在 Windows 系统上，执行以下操作：
     a. 将 `aci.dll`、`winrpc32.dll` 和 `ezrpc32.dll` 库复制到 *`Data_Protector_home`*`\bin` 目录。 (这三个库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。 在安装介质上或 AMU-PC 上的 `C:\DAS\AMU\` 目录中可以找到它们。)
     b. 同时将这三个文件复制到 *`%SystemRoot%`*`\system32` 目录中。
     c. 将 `Portinst` 和 `Portmapper service` 复制到 DAS 客户机上。 (这些必需文件是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。 在安装介质上可以找到它们。)
     d. 在“控制面板”中，转至 `Administrative Tools, Services`，并启动 `portinst` 来安装 `portmapper`。 DAS 客户机需要重新启动才能运行 `portmapper` 服务。
     e. 重新启动系统之后，检查是否 `portmapper` 和两个 `rpc services` 都在运行(在“控制面板”中，转至**管理工具、服务**，并检查服务的状态。
   - 在 HP-UX 系统上，将 `libaci.sl` 共享库复制到 `/opt/omni/lib` 目录中。 您必须具有访问该目录的权限。 请确保共享库对于所有用户(root、组和其他对象)都具有读取和执行权限。 `libaci.sl` 共享库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。 在安装介质上可以找到它。
   - 在 AIX 系统上，将 `libaci.o` 共享库复制到 `/usr/omni/lib` 目录中。 您必须具有访问该目录的权限。 请确保共享库对于所有用户(root、组和其他对象)都具有读取和执行权限。 `libaci.o` 共享库是随 ADIC/GRAU 库提供的 DAS 客户机软件的一部分。 在安装介质上可以找到它。

在此阶段，应已连接了硬件并正确安装了 DAS 软件。

从默认的 Data Protector 管理命令位置，执行 `devbra -dev` 命令来检查库驱动器是否与系统正确连接。

查看库驱动器和列表中显示的相应设备文件。

下面的步骤

安装介质代理并将 ADIC/GRAU 库物理连接到系统后，请参见 *Data Protector 帮助* 索引："配置, 备份设备"，了解有关其他配置任务的信息，如配置备份设备和介质池。

准备 Data Protector 客户机来使用 StorageTek 库

先决条件

安装介质代理之前，必须满足以下安装先决条件：

- StorageTek 库必须已配置，并且正在运行。 请参见 StorageTek 库随附的文档。
- 必须安装并配置 Data Protector。 请参见安装 Data Protector Cell Manager 和 安装服务器 (第 25 页)。
- 开始安装介质代理软件之前，必须先获取以下信息：
  - 运行 ACSLS 的主机的*主机名*。
  - 要用于 Data Protector 的 ACS 驱动器 ID 的列表。 获取的驱动器 ID 在 Data Protector 中配置 StorageTek 驱动器时使用。 要显示列表，请登录运行 ACSLS 的主机，并执行以下命令：

    ```
    rlogin "ACSLS hostname" -l acssa
    ```

    您需要输入终端类型并等待命令提示符。 在 ACSSA 提示符处，输入以下命令：

    ```
    ACSSA> query drive all
    ```

    ACS 驱动器的格式规范必须为以下形式：

    ```
    ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
    ```

  - 可用 ACS CAP ID 的列表和 ACS CAP 格式规范。 要显示列表，请登录运行 ACSLS 的主机，并执行以下命令：

    ```
    rlogin "ACSLS hostname" -l acssa
    ```

    输入终端类型并等待命令提示符。 在 ACSSA 提示符处，输入以下命令：

    ```
    ACSSA> query cap all
    ```

    ACS CAP 的格式规范必须为以下形式：

    ```
    ACS CAP: ID:#,#,# - (ACS num, LSM num, CAP num)
    ```

  - 驱动器的 UNIX 设备文件列表(如果要在 UNIX 系统上安装介质代理)。

    在系统上运行 `ioscan -fn` 系统命令以显示所需的信息。

    有关 UNIX 设备文件的详细信息，请参见安装 Data Protector 客户机 (第 49 页)。

  - 驱动器的 SCSI 地址的列表(如果要在 Windows 系统上安装介质代理)。 例如，`scsi4:0:1:0`。

    有关 SCSI 地址的详细信息，请参见安装 Data Protector 客户机 (第 49 页)。

- 确保将用于 Data Protector 的驱动器处于 online 状态。 如果某个驱动器不处于 online 状态，则在 ACSLS 主机上使用以下命令更改状态： `vary drive drive_id online`
- 确保将用于 Data Protector 的 CAP 处于online状态，并处于manual工作模式。

  如果某个 CAP 未处于 online 状态，则使用以下命令更改状态：

  `vary cap cap_id online`

  如果某个 CAP 未处于 manual 工作模式，则使用以下命令更改模式：

  `set cap manual cap_id`

安装介质代理来使用 StorageTek 带库

安装介质代理来使用 StorageTek 库

1. 使用 Data Protector 图形用户界面和 UNIX 的安装服务器系统将介质代理组件分发到客户机上。 请参见安装 Data Protector 客户机 (第 49 页)。
2. 为每个 ACS 客户机启动 ACS ssi 后台程序：

   Windows 系统：

   安装 LibAttach 服务。 有关详细信息，请参见 ACS 文档。 请确保在 LibAttach 服务配置期间输入相应的 ACSLS 主机名。 成功配置之后，LibAttach 服务将自动启动，并且每次系统重新启动之后也会自动启动。

   HP-UX、Solaris 和 Linux 系统：

   运行以下命令：

   `/opt/omni/acs/ssi.sh start ACS_LS_Hostname`

   AIX 系统：

   运行以下命令：

   `/usr/omni/acs/ssi.sh start ACS_LS_Hostname`

   > **注意：**
   > 安装 LibAttach 服务之后，检查 libattach\bin 目录是否已自动添加到系统路径。 如果未添加，则手动添加它。

   有关 LibAttach 服务的详细信息，请参见 StorageTek 库随附的文档。
3. 从默认的 Data Protector 管理命令位置，执行 devbra -dev 命令来检查库驱动器是否正确连接到系统。

   可以看到列表中显示库驱动器和相应的设备文件/SCSI 地址。

下面的步骤

安装了介质代理并且 StorageTek 库已与系统建立物理连接之后，请参见《*Data Protector 帮助*》索引：“配置, 备份设备”以了解有关其他配置任务(例如配置备份设备和介质池)的信息。

第 4 章： 安装 Data Protector 集成客户机

Data Protector集成是一些软件组件，通过它们可以使用 Data Protector运行数据库应用程序(例如 Oracle Server 或 Microsoft Exchange Server)的联机备份。Data Protector ZDB 集成是一些软件组件，通过它们可以运行使用磁盘阵列(例如 P6000 EVA 磁盘阵列系列)的零宕机时间备份和即时恢复。

运行数据库应用程序的系统称作**集成客户机**；使用 ZDB 磁盘阵列备份和存储数据的系统称作**ZDB 集成客户机**。按照 Windows 或 UNIX 系统上的任何其他客户机的相同安装过程安装此类客户机，假设已选择合适的软件组件(例如，用于备份 Microsoft Exchange Server 数据库的 `MS Exchange Integration` 组件、ZDB 和带 P6000 EVA 磁盘阵列系列的 IR 或 StoreServ Storage 的 `P6000 / 3PAR SMI-S Agent` 组件等)。

先决条件

- 有关系统要求、磁盘空间要求、受支持的平台、处理器和 Data Protector 组件的信息，请参见《Data Protector 产品声明、软件说明和参考》。
- 您需要具有许可证才能使用数据库应用程序的 Data Protector 集成(VSS 集成除外)。有关许可的信息，请参见Data Protector 产品结构和许可证 (第 267 页)。
- 此时，您应当已在网络上安装了 Cell Manager 和安装服务器(可选，用于进行远程安装)。

  有关说明，请参见安装 Data Protector Cell Manager 和安装服务器 (第 25 页)。

在开始安装步骤之前，请确定要与集成组件一起在客户机上安装哪些其他 Data Protector 软件组件。有关 Data Protector 软件组件及其说明的列表，请参见Data Protector 组件 (第 52 页)。

请注意，对于下面说明的情形，需要安装以下 Data Protector 组件：

- `Disk Agent` 组件，以便能够通过 Data Protector 备份文件系统数据。您可以将磁盘代理用于以下用途：
  - 对*无法*使用数据库应用程序备份进行备份的重要数据运行文件系统备份。
  - 对数据库应用程序服务器(例如，Oracle Server 或 Microsoft SQL Server)运行文件系统测试备份。在配置数据库应用程序的 Data Protector 集成之*前*，您需要对文件系统备份进行测试，并解决通信和与应用程序及 Data Protector 有关的其他问题。
  - 运行文件系统或磁盘映像的零宕机时间备份。
  - 对于 SAP R/3 ZDB 集成，从备份介质将数据还原到 LAN 上的应用程序系统中。
- `User Interface` 组件，用于访问 Data Protector 集成客户机上的 Data Protector GUI 和 Data Protector CLI。
- `General Media Agent` 组件，如果有与 Data Protector 集成客户机连接的备份设备。在用于通过 NDMP 服务器访问 NDMP 专用驱动器的 Data Protector 客户机上，需要 `NDMP Media Agent`。

可以使用适用于 Windows 或 UNIX 的安装服务器远程安装集成客户机，或者从 Windows 或 UNIX 安装程序包 (zip/tar) 本地安装。

有关特定集成客户机的详细信息，请参见以下相应章节：

- Microsoft Exchange Server 客户机 (第 101 页)
- Microsoft SQL Server 客户机 (第 107 页)
- Microsoft SharePoint Server 客户机 (第 108 页)
- Microsoft 卷影复制服务客户机 (第 111 页)
- Sybase Server 客户机 (第 112 页)
- Informix Server 客户机 (第 112 页)
- SAP R/3 客户机 (第 112 页)
- SAP MaxDB 客户机 (第 113 页)
- SAP HANA Appliance 客户机 (第 113 页)
- Oracle Server 客户机 (第 113 页)
- MySQL 客户机 (第 114 页)
- PostgreSQL 客户机 (第 114 页)
- IBM DB2 UDB 客户机 (第 114 页)
- Lotus Notes/Domino Server 客户机 (第 115 页)
- VMware 客户机 (第 115 页)
- Microsoft Hyper-V 客户机 (第 122 页)
- NDMP 服务器客户机 (第 123 页)
- P4000 SAN 解决方案 clients (第 123 页)
- P6000 EVA 磁盘阵列系列 clients (第 123 页)
- P9000 XP 磁盘阵列系列 clients (第 129 页)
- 3PAR StoreServ Storage clients (第 134 页)
- EMC Symmetrix 客户机 (第 134 页)
- 非 HPE 存储阵列 (第 138 页)

已经安装完集成客户机之后，Micro Focus 建议通过在每个客户机上将命令位置添加到相应的环境变量来从任何目录调用 Data Protector 命令。Data Protector 文档中的步骤假设变量值已经扩展。omniintro 参考页(*Data Protector 命令行界面参考* 中)和 omniintro 手册页中列出了命令位置。

安装后，另请参见《*Data Protector 集成指南*》、《*Data Protector 零宕机时间备份管理员指南*》或《*Data Protector 零宕机时间备份集成指南*》配置 Data Protector 集成客户机。

远程安装

使用 Data Protector图形用户界面从安装服务器将客户机软件安装到客户机上。有关用于远程安装软件的分步过程，请参见远程安装 (第 83 页)。

进行远程安装之后，客户机系统会自动成为 Data Protector 单元的成员。

本地安装

如果所在环境中未安装相应操作系统的安装服务器，则必须通过 Windows 或 UNIX 安装程序包 (zip/tar) 执行本地安装，具体取决于客户机要安装到的平台。

如果在安装期间未选择 Cell Manager，则必须在本地安装之后将客户机系统手动导入单元中。请参见导入本地安装的客户机 (第 59 页)。

安装群集感知集成

Data Protector 群集感知集成客户机必须在每个群集节点上通过安装程序包在本地进行安装。在本地客户机设置和安装的过程中，除了安装其他客户机软件组件之外，还要安装相应的集成软件组件(如 `Oracle Integration` 或 `P6000 / 3PAR SMI-S Agent`)。

您还可以在 Data Protector Cell Manager 上安装群集感知数据库应用程序和 ZDB 代理。在 Cell Manager 安装期间，请选择相应的集成软件组件。

安装过程取决于安装集成客户机的群集环境。请参见对应于您所用操作系统的群集相关章节：

- 在 Serviceguard 上安装 Data Protector (第 144 页)
- 在 Symantec Veritas Cluster Server 上安装 Data Protector (第 154 页)
- 在 Microsoft 群集服务器上安装 Data Protector (第 157 页)
- 在 Microsoft Hyper-V 群集上安装 Data Protector (第 167 页)
- 在 IBM HACMP Cluster 上安装 Data Protector (第 167 页)

有关群集化的详细信息，请参见 *Data Protector 帮助*索引：“群集、Serviceguard”和 *Data Protector 概念指南*。

下面的步骤

安装完成后，请参见《*Data Protector 集成指南*》了解有关配置集成的信息。

Microsoft Exchange Server 客户机

需要在 Microsoft Exchange Server 系统上安装的 Data Protector 组件会因您要使用的备份和还原解决方案而异。可以从下列解决方案中选择：

- Data Protector Microsoft Exchange Server 2007 integration (第 102 页)
- Data Protector Microsoft Exchange Server 2010 integration (第 104 页)
- Data Protector Microsoft Exchange Server Single Mailbox 集成 (第 104 页)
- Data Protector Microsoft 卷影复制服务集成 (第 105 页)
- Data Protector 适用于 Microsoft Exchange Server 的 Granular Recovery Extension (第 105 页)

Data Protector Microsoft Exchange Server 2007 integration

要能够备份 Microsoft Exchange Server 数据库，请将 `MS Exchange Integration` 组件安装到 Microsoft Exchange Server 系统。

Microsoft Exchange Single Mailbox 集成代理将作为 Data Protector Microsoft Exchange Server 集成组件的一部分安装。

先决条件

- 假设 Microsoft Exchange Server 已启动并正在运行。
- 需要熟悉 Microsoft Exchange Server 的基本体系结构。 有关 Microsoft Exchange Server 的信息，请参见 *Microsoft Exchange Server 联机帮助*。
- 必须具有适当的 Data Protector 联机扩展使用许可证 (LTU)，才能使用 Data Protector Microsoft Exchange Server 集成。
- 如果要在磁盘阵列上使用 Microsoft Exchange Server 集成，则要在应用程序系统的磁盘阵列源卷上安装 Exchange Server 的各种服务 - Information Store、Key Management Service(可选)和 Site Replication Service(可选)。

步骤

1. 在 Exchange Server 系统上，将 *Exchange_Server_home*\bin 目录添加到系统路径。
   a. 在 Windows 桌面上，右键单击**我的电脑**，然后单击**属性**。
   b. 在“系统属性”窗口中，单击**高级**，然后单击**环境变量**。
   c. 在“系统变量”组框的变量列表中，找到 **Path** 条目，然后单击**编辑**。
   d. 在“编辑系统变量”窗口的“变量值”文本框中，添加 *Exchange_Server_home*\bin 目录。 单击**确定**。

   > **重要：**
   > 如果 Exchange Server 可群集感知，则在所有群集节点上将此目录添加到系统路径。

2. 在 Exchange Server 系统(Data Protector 客户机)上从安装程序包本地安装或使用 Data Protector GUI 远程安装 Microsoft Exchange Server 集成软件。

   > **重要：**
   > 如果 Exchange Server 可群集感知，则在所有群集节点上从安装程序包本地安装软件组件。

   如果已在 Exchange Server 系统上安装了 Data Protector，或者要向尚未安装 Data Protector 的 Exchange Server 系统进行远程安装，则使用 Data Protector GUI 安装所需的软件组件。

如果尚未在 Exchange Server 系统上安装 Data Protector，并且要执行本地安装，则启动 Data Protector 安装向导。 安装向导将指导您完成整个安装过程，此过程与安装 Data Protector Cell Manager 和安装 Data Protector 客户机的过程不同。

需要安装以下 Data Protector 软件组件：

- MS Exchange 集成
- 常规介质代理(如果已将设备连接到 Exchange Server 客户机系统)

建议还要安装：

- 用户界面
- Disk Agent(如果要执行 Exchange Server 客户机系统的文件系统备份用于测试)

3. 如果 Exchange Server 可群集感知，则在所有群集节点上将群集服务帐户分配给 Data Protector Inet 服务。
   a. 在 Windows 桌面上，右键单击**我的电脑**，然后单击**管理**。
   b. 在“计算机管理”窗口中，展开**服务和应用程序**，然后单击**服务**。
   c. 在服务列表中，找到 **Data ProtectorInet** 条目，右键单击该条目，然后单击**属性**。 此时将显示“Data Protector Inet 的属性”窗口。
   d. 在“登录”属性页中，单击**此帐户**。
   e. 在“此帐户”文本框中，输入群集服务帐户名。 (可选)通过单击**浏览**可用浏览方式查找特定名称。
   f. 在“密码”和“确认密码”文本框中，输入群集服务帐户的密码。
   g. 单击**确定**。
   h. 在“文件”菜单中，单击**退出**。

验证 Data Protector Microsoft Exchange Server 集成安装

- 检查环境变量 Path 是否还包含 *Exchange_Server_home*\bin 目录。
  如果不包含，则将此目录的完整路径添加到 Path 变量。
- 检查是否在 Data Protector 客户机系统中正确设置了 Cell Manager 名称。 请执行以下操作：
  1. 搜索以下注册表项：
     HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site
  2. 验证注册表项的名称和数据是否分别为 CellServer 和 *Cell_Manager_host_name*。 如果不是，则在此客户机上重新安装 Data Protector。

验证 Microsoft Exchange Server

- 检查以下 Microsoft Exchange Server 服务是否正在运行：
  - Microsoft Exchange 系统助理 (MSExchangeSA)
  - Microsoft Exchange 信息存储 (MSExchangeIS)

  如果未运行，则重新启动 Exchange Server。
- 使用 Windows 的备份实用程序(Microsoft Windows 备份)而非 Data Protector 执行 Exchange Server Information Store 的备份和还原。 如果发生失败，则尝试通过验证 Exchange Server 安装和配置找出问题。

Data Protector Microsoft Exchange Server 2010 integration

假设 Microsoft Exchange Server 环境已启动并正在运行。

要能够备份 Microsoft Exchange Server 2010 或 Microsoft Exchange Server 2013 数据库，请将以下 Data Protector 组件安装到所有 Microsoft Exchange Server 系统：

- MS Exchange Server 2010+ Integration
- MS Volume Shadow Copy Integration
- 相应的 Data Protector 磁盘阵列代理(如果 Microsoft Exchange Server 数据位于磁盘阵列上)

> **注意：**
> 对于 VSS 可传输备份会话，必须在备份系统上安装 MS Volume Shadow Copy Integration 组件和相应的 Data Protector 磁盘阵列代理。

在 DAG 环境中，DAG 虚拟系统(主机)还必须导入到 Data Protector 单元中。 关于如何将客户机导入至 Data Protector 单元，请参见 *Data Protector 帮助* 索引：“导入, 客户机系统”。

> **注意：**
> - 因为 Data Protector Microsoft Exchange Server 2010 集成以 VSS 技术为基础，在安装 MS Exchange Server 2010+ Integration 组件时，Data Protector 将自动安装 MS Volume Shadow Copy Integration 组件。 如果已经安装了 MS Volume Shadow Copy Integration 组件，则将对该组件进行升级。
> - 如果从系统中删除 MS Exchange Server 2010+ Integration 组件，MS Volume Shadow Copy Integration 组件不会自动删除。 另请注意，不能从安装有 MS Exchange Server 2010+ Integration 组件的系统中删除 MS Volume Shadow Copy Integration 组件。

Data Protector Microsoft Exchange Server Single Mailbox 集成

假设 Microsoft Exchange Server 已启动并正在运行。

为了能够备份 Microsoft Exchange Server 邮箱和公共文件夹项目，请在 Microsoft Exchange Server 系统上安装 MS Exchange Integration 组件。 在 DAG 环境中，在所有属于 DAG 一部分的 Microsoft Exchange Server 系统上安装该组件。

在 Microsoft Exchange Server 2007 系统上，还需要另外安装一个软件包来支持 Data Protector Microsoft Exchange Single Mailbox 集成的功能。 该软件包称作 Microsoft Exchange Server MAPI Client and Collaboration Data Objects (ExchangeMapiCdo.EXE)，可以从 Microsoft 网站 http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en 免费下载。

Data Protector Microsoft 卷影复制服务集成

请参见Microsoft 卷影复制服务客户机 (第 111 页)。

Data Protector 适用于 Microsoft Exchange Server 的 Granular Recovery Extension

使用 Data Protector 扩展能够恢复单个 Microsoft Exchange Server 邮箱项。 根据 Microsoft Exchange Server 的环境配置在以下对象上安装 Data Protector 组件：

- 单个 Microsoft Exchange Server 系统：此系统
- 多个 Microsoft Exchange Server 系统：配置了 Mailbox Server 角色的每个 Exchange Server 系统
- Microsoft Exchange Server 的数据库可用性组 (DAG) 环境：DAG 中的所有 Exchange Server 系统

先决条件

- 将以下对象安装到所选的 Microsoft Exchange Server 系统：
  - Data ProtectorMS Exchange Server 2010+ Integration 组件
  - Data ProtectorUser Interface 组件
  - 所有必需的非 Data Protector 组件
- 将 TCP/IP 端口 60000(默认)在所选 Microsoft Exchange Server 系统上保持空闲。

Microsoft Exchange Server 软件

安装以下各项：

- Microsoft Exchange Server

  确保已正确安装和配置 Microsoft Exchange Server 环境。

  有关受支持版本、平台、设备和其他信息，请参见 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword= 上的最新支持矩阵。

  有关安装、配置和使用 Microsoft Exchange Server 的信息，请参见 Microsoft Exchange Server 文档。
- Microsoft 管理控制台 (MMC) 3.0 或更高版本

- .NET Framework 3.5.1
- Internet Information Services (IIS) 6.0 或更高版本

Data Protector 软件

安装以下 Data Protector 组件：

- Data Protector`User Interface` 组件
- 所有 Microsoft Exchange Server 系统上的 Data Protector`MS Exchange Server 2010+ Integration` 组件

确保已安装和配置 Data Protector 备份解决方案，如 *Data Protector 安装指南* 和 *Data Protector 集成指南* 中所述。

其他非 Data Protector 软件和服务

- 安装 Windows PowerShell 1.0 或更高版本(Windows Management Framework Core 包)
- 不支持除英语以外的 PowerShell 本地化(Windows OS 必须使用英语本地化)。
- 将 TCP/IP 端口 60000(默认)在 Granular Recovery Web 服务上保持空闲。
- 将防火墙配置为允许新端口。

支持的环境

该扩展可与不同 Microsoft Exchange Server 环境中的 Microsoft Exchange Server 集成。

- 独立的 Microsoft Exchange Server 系统(独立环境)
- 多个 Microsoft Exchange 邮箱服务器系统(多个服务器系统)
- Microsoft Exchange Server 的数据库可用性组环境(DAG 环境)

根据 Microsoft Exchange Server 环境，按如下方式安装扩展：

独立环境

所有 Microsoft Exchange Server 服务和数据均安装在单个 Microsoft Exchange 邮箱服务器上，这在小规模环境中已足够。 将 `MS Exchange Granular Recovery Extension` 组件安装到 Exchange 邮箱服务器系统。

多个 Exchange Server 系统的环境

您的环境包含多个 Microsoft Exchange Server 数据库。 将 `MS Exchange Granular Recovery Extension` 组件安装到要恢复单个项目的 Exchange 邮箱服务器系统中。

DAG 环境

您的环境最多包含 16 个 Microsoft Exchange 邮箱服务器系统。 将 `MS Exchange Granular Recovery Extension` 组件安装到任何 Microsoft Exchange Server 邮箱角色的系统节点。 安装该组件之后，Granular Recovery Extension 图形用户界面 (GUI) 将为 DAG 环境中的所有邮箱服务器节点显示所有邮箱数据库对象。 该扩展将自动考虑 DAG 环境的动态行为。

CCR 环境

在邮箱服务器节点上安装 `MS Exchange 2010 Granular Recovery Extension` 组件。

LCR 环境

在活动和被动邮箱数据库所处的服务器上安装 `MS Exchange 2010 Granular Recovery Extension` 组件。

有关 Microsoft Exchange Server 概念的详细信息，请参见 Microsoft Exchange Server 文档。

安装扩展

适用于 Microsoft Exchange Server 的 Data Protector Granular Recovery Extension 作为 Data Protector 组件提供。 MS Exchange Granular Recovery Extension 组件包含 Granular Recovery Extension 图形用户界面、命令行选项、Web 服务组件和上下文相关 (F1) 帮助。 所有这些内容安装在一起。

> **注意：**
> 在 Microsoft Exchange 组织中，只能将该扩展安装在 Microsoft Exchange Server 邮箱角色系统上。 这些系统包含 Microsoft Exchange Server 邮箱数据库和恢复技术，例如，还原完整的 Microsoft Exchange Server 数据库和邮箱项所需的恢复数据库 (RDB)。

步骤

使用 Data Protector 图形用户界面 (GUI) 安装扩展：

> **重要：**
> 确保拥有 Windows 本地用户帐户 SYSTEM 或在 Microsoft Exchange Server 邮箱角色系统上授予的 Windows 域用户帐户管理特权。 您必须能够创建注册表项并将文件或文件夹安装到 Program Files 目录。

1. 通过以下方式远程安装客户机：
   - 添加客户机
   - 导入客户机
2. 将 MS Exchange Granular Recovery Extension 组件添加到 Data Protector 客户机系统。

有关 Data Protector 安装的详细信息，请参见 Data Protector中的“安装客户机系统”、“导入客户机系统”和“添加 Data Protector 安装指南 组件”。

删除扩展

执行以下某个操作：

- 使用 Data Protector GUI 远程删除已安装扩展组件的客户机。
  有关删除 Data Protector 客户机的详细信息，请参见 *Data Protector 帮助* 索引：“卸载, 客户机”。
- 手动删除 MS Exchange Granular Recovery Extension 组件。
  有关删除 Data Protector 软件组件的详细信息，请参见 *Data Protector 帮助*索引：“卸载, Data Protector 软件”

Microsoft SQL Server 客户机

假设 Microsoft SQL Server 已启动并正在运行。

为了能够备份 Microsoft SQL Server 数据库，您需要在安装过程中选择 MS SQL Integration 组件。

Microsoft SharePoint Server 客户机

需要在 Microsoft SharePoint Server 环境中安装的 Data Protector 组件会因您要使用的备份和恢复解决方案而异。 可以从下列解决方案中选择：

- Data Protector Microsoft SharePoint Server 2007/2010/2013 integration (第 108 页)
- Data Protector 基于 Microsoft SharePoint Server VSS 的解决方案 (第 108 页)
- Data Protector Microsoft Volume Shadow Copy Service 集成 (第 109 页)
- Data Protector 适用于 Microsoft SharePoint Server 的 Granular Recovery Extension (第 109 页)

Data Protector Microsoft SharePoint Server 2007/2010/2013 integration

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。

为了能够备份 Microsoft SharePoint Server 对象，请安装以下 Data Protector 组件：

- Microsoft SharePoint Server 2007/2010/2013 集成 – 在 Microsoft SharePoint Server 系统上 (Microsoft SQL Server 系统除外)
- MS SQL Integration – 在 Microsoft SQL Server 系统上

> **注意：**
> 如果系统已安装 Microsoft SQL Server 和 Microsoft SharePoint Server，则在其上安装所有 Data Protector 组件。

Data Protector 基于 Microsoft SharePoint Server VSS 的解决方案

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。

为了能够备份 Microsoft SharePoint Server 对象，请安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration 在 Microsoft SQL Server 系统和至少启动了以下服务之一的 Microsoft SharePoint Server 系统上：

  Microsoft Office SharePoint Server 2007：

  - Windows SharePoint Services Database
  - Windows SharePoint Services Help Search
  - Office SharePoint Server Search

  Microsoft SharePoint Server 2010：

- SharePoint Foundation Database
- SharePoint Foundation Help Search
- SharePoint Server Search

Microsoft SharePoint Server 2013：

- SharePoint Foundation Database
- SharePoint Server Search

- 在安装了 Data ProtectorMS Volume Shadow Copy Integration 组件并且计划要在其上配置和启动备份的 Microsoft SharePoint Server 系统之一上安装 Data ProtectorUser Interface组件。

Data Protector Microsoft Volume Shadow Copy Service 集成

请参见Microsoft 卷影复制服务客户机 (第 111 页)。

Data Protector 适用于 Microsoft SharePoint Server 的 Granular Recovery Extension

假设 Microsoft SharePoint Server 和相关的 Microsoft SQL Server 实例已启动并正在运行。

为了能够恢复各个 Microsoft SharePoint Server 对象，请在 Microsoft SharePoint Server Central Administration 系统上安装 MS SharePoint Granular Recovery Extension。

- 本地安装该组件时，Data Protector 安装向导将显示“MS SharePoint GRE 选项”对话框。 指定场管理员用户名和密码。
- 要远程安装此组件，请选择 MS SharePoint Granular Recovery Extension，单击**配置**，并在“MS SharePoint GRE 选项”对话框中指定场管理员用户名和密码。

> **注意：**
> - 您只可以将 Granular Recovery Extension 安装到已安装 Microsoft SharePoint Server 的系统上。
> - 确保备份 Microsoft SharePoint Server 数据所需的 Data Protector 组件也安装在 Microsoft SharePoint Server 环境中。

先决条件

- **Microsoft 软件包：**

  安装以下 Windows Management Framework Core 软件包：
  - Microsoft PowerShell 2.0 或更高版本

- **Microsoft SQL Server 包：**

安装以下适用于 Microsoft SQL Server 2005 或 Microsoft SQL Server 2008 的包：

- Microsoft SQL Server Native Client
- Microsoft Core XML Services (MSXML) 6.0
- Microsoft SQL Server 2008 管理对象集合

安装以下适用于 Microsoft SQL Server 2012 的包：

- Microsoft SQL Server Native Client
- Microsoft Core XML Services (MSXML) 6.0 或更高版本
- Microsoft SQL Server 2012 管理对象集合

必须在所有已至少启用以下其中一项服务的 Microsoft SharePoint Server 系统上安装这些包：

- 管理中心
- Windows SharePoint Services Web 应用程序 (Microsoft Office SharePoint Server 2007)
- Microsoft SharePoint Foundation Web 应用程序 (Microsoft SharePoint Server 2010/2013)

可以从以下网站下载包： http://www.microsoft.com/downloads/en/default.aspx。

搜索 **Feature Pack for Microsoft SQL Server 2008** 或 **Feature Pack for Microsoft SQL Server 2012**。

- **Data Protector 组件：**

  确保您已按照以下信息源中所述安装和配置 Data Protector 备份解决方案：

  - *Data Protector 安装指南*
  - 的相应章节 *Data Protector 集成指南*
  - *Data Protector 零宕机时间备份集成指南*
  - *适用于 Microsoft 卷影复制服务的 Data Protector 集成指南*

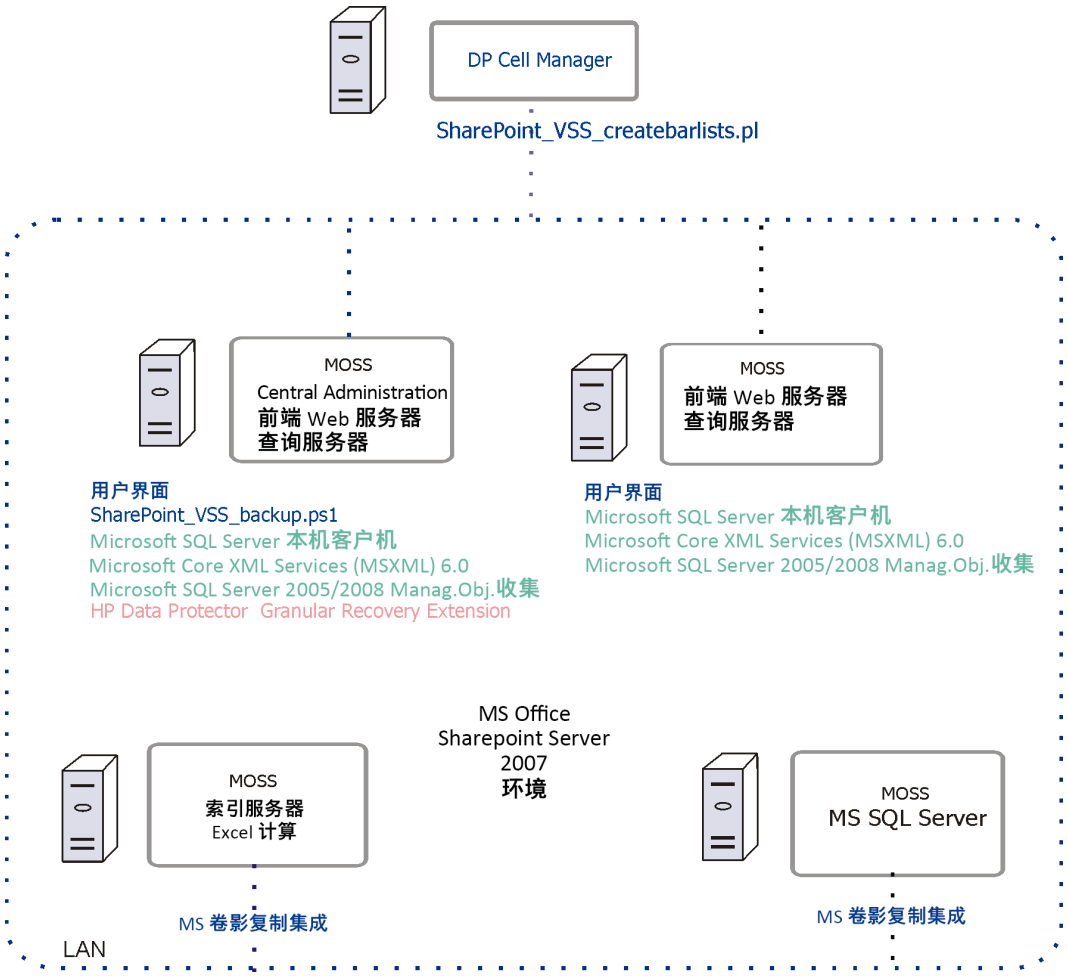
  此外，请确保在所有已至少启用以下服务之一的 Microsoft SharePoint Server 系统上安装 Data Protector`User Interface`组件：

  - 管理中心
  - Windows SharePoint Services Web 应用程序 (Microsoft Office SharePoint Server 2007)
  - Microsoft SharePoint Foundation Web 应用程序 (Microsoft SharePoint Server 2010/2013)

GRE 环境

在使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案安装介质场(示例)(第 111 页)中，Data Protector 组件显示为蓝色，Microsoft SQL Server 安装包显示为绿色，Data Protector Granular Recovery Extension 组件显示为红色。

使用基于 Data Protector Microsoft SharePoint Server VSS 的解决方案安装介质场(示例)



Microsoft 卷影复制服务客户机

要备份 VSS 写入程序或者只有文件系统使用 VSS，请在应用程序系统(本地备份)或同时在应用程序和备份系统(可传输备份)上安装以下 Data Protector 软件组件：

- MS Volume Shadow Copy Integration.
- 如果要使用磁盘阵列(包含硬件提供程序)，则相应的磁盘阵列代理为： P4000 VSS Agent、 P6000 / 3PAR SMI-S Agent、P9000 XP Agent 或 3PAR VSS Agent。

安装 VSS 集成之后，如果要执行 ZDB 到磁盘和 ZDB 到磁盘 + 磁带会话(支持即时恢复的会话)，则需要解析应用程序系统上的源卷。 如下从单元中的任何 VSS 客户机上运行解析操作：

```
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

但是，如果不进行解析或未能解析应用程序系统，则只要 omnirc 文件中的 OB2VSS_DISABLE_AUTO_RESOLVE 选项设置为 0(默认值)，就会自动对它进行解析。 在这种情况下，创建复本的备份时间会延长。

有关详细信息，请参见 *Data Protector 零宕机时间备份集成指南*。

Sybase Server 客户机

假设 Sybase Backup Server 正在运行。

要备份 Sybase 数据库，需要在安装期间选择以下 Data Protector 组件：

- `Sybase Integration` - 为了能够备份 Sybase 数据库
- `Disk Agent` - 出于两个原因而安装磁带客户机：
  - 运行 Sybase Backup Server 的文件系统备份。 请在配置 Data Protector Sybase 集成之*前*执行该备份，并解决与 Sybase Backup Server 和 Data Protector 有关的所有问题。
  - 对*无法*使用 Sybase Backup Server 备份的重要数据运行文件系统备份。

Informix Server 客户机

假设 Informix Server 已启动并正在运行。

要备份 Informix Server 数据库，需要在安装期间选择以下 Data Protector 组件：

- `Informix Integration` - 为了能够备份 Informix Server 数据库
- `Disk Agent` - 出于两个原因而安装磁带客户机：
  - 运行 Informix Server 的文件系统备份。 请在配置 Data Protector Informix Server 集成之*前*执行该备份，并解决与 Informix Server 和 Data Protector 有关的所有问题。
  - 对*无法*使用 ON-Bar 进行备份的重要 Informix Server 数据(例如， ONCONFIG 文件、`sqlhosts` 文件、ON-Bar 紧急引导文件、`oncfg_`*`INFORMIXSERVER.SERVERNUM`* 和配置文件等)运行文件系统备份。

IBM HACMP Cluster

如果 Informix Server 安装在 IBM HACMP 群集环境中，请在所有群集节点上安装 `Informix Integration`组件。

SAP R/3 客户机

先决条件

- 确保安装并配置以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 软件

- SQL*Plus

- 假设 SAP R/3 Database Server 已启动并正在运行。

> **注意：**
> Data Protector SAP R/3 集成备份规范与先前版本的 Data Protector 完全兼容。 Data Protector 可以运行由先前 Data Protector 版本创建的所有备份规范。 在较早版本的 Data Protector 上，无法使用由当前版本的 Data Protector 创建的备份规范。

为了能够备份 SAP R/3 数据库，在安装过程中请选择以下组件：

- `SAP R/3 Integration`
- `Disk Agent`

  Data Protector 要求在 Backup Server(具有需要备份的文件系统数据的客户机)上安装磁带客户机。

SAP MaxDB 客户机

假设 SAP MaxDB 服务器已启动并正在运行。

为了能够备份 SAP MaxDB 数据库，您需要在安装期间选择以下 Data Protector 组件：

- `SAP MaxDB Integration` - 为了能够运行 SAP MaxDB 数据库的集成联机备份
- `Disk Agent` - 为了能够运行 SAP MaxDB 数据库的文件系统备份

SAP HANA Appliance 客户机

要将 Data Protector 与 SAP HANA Appliance (SAP HANA) 集成，请在 SAP HANA 系统上安装以下 Data Protector 软件组件：

- `SAP HANA Integration`

  该组件支持完整 SAP HANA 数据库和 SAP HANA 重做日志的集成备份。
- `Disk Agent`

  该组件支持使用 Data Protector 文件系统备份功能对 SAP HANA 配置文件进行非集成备份。 发生灾难后，SAP HANA 配置文件的备份映像可以帮助您更轻松地识别和恢复更改。

在分布式 SAP HANA 环境中，在组成该环境的每个 SAP HANA 系统上安装上述组件。

Oracle Server 客户机

假设 Oracle Server 已启动并正在运行。

为了能够备份 Oracle 数据库，您需要在安装过程中选择 `Oracle Integration`组件。

HP OpenVMS

在 HP OpenVMS 上，按照*Data Protector 集成指南*中所述安装并配置 Oracle 集成之后，请验证 OMNI$ROOT:[CONFIG.CLIENT]omni_info 中是否存在 -key Oracle8 条目，例如：

```
-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath
“” -uxpath “” -version 9.08
```

如果不存在该条目，请从 OMNI$ROOT:[CONFIG.CLIENT]omni_format 复制它。 否则，Oracle 集成在 OpenVMS 客户机上不会显示为已安装。

MySQL 客户机

要将 Data Protector 与 MySQL 数据库管理系统集成并且希望能够备份 MySQL 实例和数据，请在 MySQL 主机上安装以下 Data Protector 组件：

- MySQL Integration
  此组件可用于执行 MySQL 数据库的集成备份和还原。
- Disk Agent
  此组件可用于备份和还原 MySQL 二进制日志，以满足执行 MySQL 数据库恢复的前提条件。 它还可以用于执行 MySQL 数据的非集成备份，以便解决安装了 MySQL 的 Data Protector 客户机所存在的问题。

PostgreSQL 客户机

要将 Data Protector 与 PostgreSQL 数据库服务器系统集成并且希望能够备份 PostgreSQL 实例和数据，请在 PostgreSQL 主机上安装以下 Data Protector 组件：

- PostgreSQL Integration
  此组件可用于执行 PostgreSQL 数据库的集成备份和还原。

IBM DB2 UDB 客户机

假设 DB2 服务器已启动并正在运行。

为了能够备份 DB2 数据库，您需要在安装过程中选择 DB2 Integration和 Disk Agent组件。

在物理分区的环境中，在数据库所驻留的每个物理节点(系统)上安装 DB2 Integration和 Disk Agent组件。

> **注意：**
> 以 root 用户身份登录，以执行安装。

Lotus Notes/Domino Server 客户机

假设 Lotus Notes/Domino Server 已启动并正在运行。

为了能够备份 Lotus Notes/Domino Server 数据库，您需要在安装过程中选择 Lotus Integration和 Disk Agent组件。 为了能够将 Data Protector 备份文件系统数据用于以下目的，您需要Disk Agent组件：

- 备份*无法*使用 Lotus 集成代理备份的重要数据。 它们是所谓的非数据库文件，需要备份这些文件(notes.ini、desktop.dsk 和所有 *.id files)才能为 Lotus Notes/Domino Server 提供完整的数据保护解决方案。
- 测试文件系统备份，以解决通信和其他与应用程序及 Data Protector 有关的问题。

Lotus Domino Cluster

在将用于备份的 Domino 服务器上安装 Lotus Integration和Disk Agent组件，并且如果计划将 Domino 数据库还原到包含这些数据库的复本的其他 Domino 服务器上，请同时在这些 Domino 服务器上安装这两个组件。

VMware 客户机

需要在 VMware 系统上安装的 Data Protector 组件会因您要使用的还原和恢复解决方案而异。

本节指南将为您提供以下几个方面的帮助：

- GRE 环境
- 安装 Data Protector GRE
- 卸载 Data Protector GRE

适用于 VMware vSphere 的 Data Protector GRE

Data Protector Granular Recovery Extension 使用 Data Protector 虚拟环境集成恢复数据；此扩展只是一款恢复解决方案。 GRE 环境(包括装载代理)和 vCenter Server 必须满足特定的要求，然后才能安装这两种 GRE 插件。

GRE 插件可通过高级 GRE Web 插件用户界面进行访问。

本节指南提供创建此环境所必需的信息。

GRE 环境

在下图中

- Data Protector 组件用蓝色表示。
- VMware 组件用黑色表示。

安装 Data Protector Granular Recovery Extension

装载代理系统

适用于 VMware vSphere 的 Data Protector Granular Recovery Extension 需要一个装载代理系统，此系统在 VMware vCenter Server 系统上用作原始位置与目标位置之间的临时还原或恢复位置。 任何受支持的系统(也称为虚拟机)均可用作装载代理系统。

虚拟机磁盘未立即装载。 当您以 VMware vCenter 用户身份在 vCenter 环境中使用集成的扩展开始浏览这些文件时，装载会话将启动。

装载代理系统需要为已恢复的数据提供足够的磁盘空间。 此外，您还可以通过附加额外的磁盘或添加其他装载代理系统按需调整磁盘空间。

> **注意：**
> 建议将专用的系统配置为装载代理系统。

系统要求

装载代理系统必须满足以下系统要求：

- **Windows 系统：**
  (可选)如果要使用 VIX API 恢复文件，请确保安装以下实用程序。 当网络共享不可用时，VIX 可用作回退选项。
  - VMware VIX API 1.14
- **Linux 系统：**
  确保安装以下操作系统组件和实用程序：
  - FUSE 2.7.3 或更高版本*
  - cifs-utils 包(用于在 Linux 装载代理系统上装载 Windows 虚拟机磁盘)

- ntfs-3g 包(用于在 Linux 装载代理系统上装载 Windows 虚拟机磁盘)
- NFS 服务
- VMware VIX API 1.14(可选；用于恢复文件，当网络共享不可用时还可用作回退选项)
- 具有 LVM 分区的磁盘需要 kpartx
- Samba 服务器，在恢复期间，Data Protector 使用 Samba 服务器创建共享。 确保 Samba 共享具有读写权限。 如果已在 Linux 系统中部署增强安全机制的 Linux (SELinux) 内核安全模块，请执行 `# setsebool -P samba_export_all_rw on` 命令来启用对 Samba 共享的读写权限。
- 使用以下命令将介质代理主机的用户添加到 Samba 密码数据库：`smbpasswd –a <user>`。 您可以使用以下命令验证用户是否已添加到密码数据库：`pdbedit -w -L`。
- 应配置 Windows 防火墙。 要了解更多有关配置的信息，请参见*Data Protector Granular Recovery Extension 用户指南*中的“配置 Windows 防火墙例外”部分。

> **注意：**
> 1. 要了解配置智能缓存设备的详细信息，请参见《*Data Protector* 管理员指南》中的“配置智能缓存”部分。
> 2. 要了解配置 StoreOnce 设备的详细信息，请参见《*Data Protector 管理员指南*》中的“配置智能缓存”部分。

*对于 SUSE Linux Enterprise Server (SLES)，请使用 FUSE 2.7.2

*对于 SUSE Linux Enterprise Server 12 (SLES 12)，请使用 FUSE 2.9.3

装载代理系统上所需的 **Data Protector** 组件

安装 Data Protector 客户机。 然后，继续在装载代理系统上远程安装以下 Data Protector 组件：

- **`Virtual Environment Integration`**
- **`VMware Granular Recovery Extension Agent`**

请参见组件选择屏幕。 您需在安装期间选择此组件。 请参见安装 Data Protector 客户机 (第 49 页)。

如果远程安装失败，请在本地系统上安装扩展。 请参见 *Data Protector Granular Recovery Extension 用户指南*中的“本地安装变通方法”一节。 但是，对于补丁更新，必须远程安装 GRE 代理。

有关导入过程的详细信息，请参见《*Data Protector 集成指南*》中的“配置集成”一节。

RHEL 7.0 和 SLES 12 默认未创建 Linux 循环设备。 确保装载代理系统上具有足够的 Linux 循环设备。 由于要装载大量磁盘才能使整个逻辑卷组可用，因此需要足够的循环设备。

> **注意：**
> 如果已添加或删除任意 Data Protector 组件或 VMware VDDK，请在安装 VMware Granular Recovery Extension Agent 之前重新启动系统。

> **注意：**
> 在装载代理系统上安装 VMware Granular Recovery Extension Agent 组件期间，系统可能会在安装会话输出中通知用户，指出必须重新启动目标主机才能完成安装。

> **注意：**
> 您打算作为备份主机使用的客户机不必安装 VMware Consolidated Backup (VCB) 软件。

VMware vCenter Server(VirtualCenter 服务器)

适用于 VMware vSphere 的 Data Protector Granular Recovery Extension (GRE) 可集成至 VMware vCenter Server 中。 您可使用 VMware vSphere Web 客户机访问虚拟机。 Data Protector 选项卡将添加到 VMware vSphere Web 客户机界面中。

> **注意：**
> GRE 的高级 GRE Web 插件支持 5.5.0 U2 及以上版本的 VMware vSphere Web 客户机。

VMware vCenter Server Appliance (VCSA) 6.0 环境

先决条件

需要在 VCSA 服务器上执行以下命令：

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
```

安装适用于 VMware vSphere Web 客户机的 Data Protector GRE

注意事项

1. 您计划用于执行恢复操作的虚拟机必须安装 VMware 工具 4.x 或更高版本。 可以从 http://www.vmware.com/download 网页下载 VMware 工具安装包。
2. 仅支持远程安装适用于 VMware vSphere 的 Data Protector Granular Recovery Extension Web 客户机。
3. 为确保扩展的功能正常，请不要在同一客户机系统上同时安装和配置 VMware vCenter Server 系统和装载代理系统。
4. 确保 VMware Granular Recovery Extension Agent、Virtual Environment Integration Agent 和 Data Protector Cell Manager 为同一版本。 不支持混合代理版本。

要求

要使用扩展，需要安装和配置以下系统：

- **Data Protector** 单元和客户机
- VMware vCenter Server 系统
- 装载代理系统

GRE 插件可通过高级 GRE Web 插件用户界面进行访问。

全新安装

完成以下步骤以安装适用于 VMware vSphere Web 客户机的 GRE。

环境： Data Protector 版本(9.02 或更新版本)、vCenter(参见受支持版本的虚拟化支持矩阵)，以及高级 GRE Web 插件。

步骤 1： 设置 Cell Manager.

Cell Manager 可以位于 Windows 和 Linux 系统中。

步骤 2： 设置安装服务器:

默认情况下，会在安装 Cell Manager 过程中添加安装服务器。

- 如果已在 Windows 中安装 Windows Installation Server 以及 Cell Manager(默认选项)，则可跳过此步骤，并继续安装装载代理。
- 如果已在 Linux 上安装 Cell Manager，则需要设置 Windows Installation Server 并将其导入到 Linux 上的 Cell Manager 中。

步骤 3： 安装装载代理。

- 可在 Windows 和/或 Linux 系统中完成。
- 建议在 Cell Manager 以外的其他专用计算机上安装装载代理。
- 必须在已安装以下组件的装载代理计算机上安装 Data Protector 客户机：
  1. `Virtual Environment Integration`
  2. `VMware Granular Recovery Extension Agent.`

步骤 4： 设置 vCenter Server。

- vCenter 可以位于 Windows 或 Linux 环境中。
- 不需要 Data Protector 客户机。

步骤 5： 在 vCenter Server 上安装高级 GRE Web 插件。

1. 要将 vCenter 计算机作为 vCenter 客户机导入到 Data Protector Cell Manager 中，请执行以下操作。
   a. 右键单击**客户机**，并选择**导入客户机**。
   b. 输入 vCenter 的主机名并选择类型 **VMware vCenter**。 单击**下一步 (Next)**。
   c. 输入 vCenter 的凭据(用于登录 vCenter Web 客户机的相同凭据)。 选中**高级 GRE Web 插件**复选框并单击**完成**。

注意：
您可以分别使用 omnicc -import_vcenter 和 omnicc -export_host 命令注册和取消注册高级 GRE Web 插件。有关详细信息，请参见《*Data Protector 命令行界面参考指南*》。

注意：
您可以将多个 vCenter 导入 Data Protector Cell Manager中。

升级

确定适合您的环境并继续执行升级步骤，参见下表：

Data Protector		**插件**		
从	**至**	**升级自**	**至**	**请参见**
以前的任何版本	DP 9.02 或更高版本	Web 插件	Advanced GRE Web Plug-in	选项 1
DP 9.02 或更高版本	最新版本	Advanced GRE Web Plug-in	Advanced GRE Web Plug-in	选项 2

选项 1

环境：如果正在 vCenter 5.5 U2 或更高版本上，从包含 Web 插件的之前 Data Protector 版本升级到包含高级 GRE Web 插件的 Data Protector 新版本(9.02 版或更高版本)(请参见受支持版本的虚拟化支持矩阵)。

如果已完成 Data Protector 升级过程，则直接执行步骤 2。

请执行以下操作：

1. 使用本机(所需的版本)Data Protector 安装程序升级 Data Protector Cell Manager
2. 右键单击 Cell Manager 中的 **vCenter** 客户机，然后单击**升级**。由于用户已安装 Web 插件，因此 vCenter 计算机必须已作为 Data Protector 客户机导入。此步骤将删除 vCenter 上的现有 Web 插件并将 vCenter 上的 Data Protector 客户机升级到所需的版本。

   注意：
   现有的请求文件将被删除，您必须创建新请求。

3. 右键单击 Cell Manager 中的客户机，然后单击**升级**。对所有装载代理和其他客户机重复此步骤。

   要将 vCenter 计算机作为 vCenter 客户机导入到 Data Protector Cell Manager 中，请执行以下操作。

   a. 右键单击**客户机**，并选择**导入客户机**。
   b. 输入 vCenter 的主机名并选择类型 **VMware vCenter**。单击**下一步 (Next)**。
   c. 输入 vCenter 的凭据(用于登录 vCenter Web 客户机的相同凭据)。选中**高级 GRE Web 插件**复选框并单击**完成**。

> **注意：**
> 如果需要，Data Protector 客户机可以保留在该 vCenter 上。

选项 2

环境：如果有包含 Data Protector 高级 GRE Web 插件的 Data Protector 9.02 版或更高版本，要借助最近更新来获得高级 GRE Web 插件的更新功能，请完成以下步骤：

1. 要从 Data Protector 取消注册高级 GRE Web 插件，请取消选中**高级 GRE Web 插件**复选框并单击**应用**。 确保从高级 GRE Web 插件主机列表删除所有 Cell Manager。
2. 要注册高级 GRE Web 插件，请选中**高级 GRE Web 插件**复选框并单击**应用**。

> **注意：**
> 确保 Cell Manager 和所有代理服务器都已升级。

卸载高级 GRE Web 插件

如果在启动这些插件时遇到任何问题，则完成以下步骤并根据您的环境重新启动之前提供的升级过程。

卸载高级 GRE Web 插件

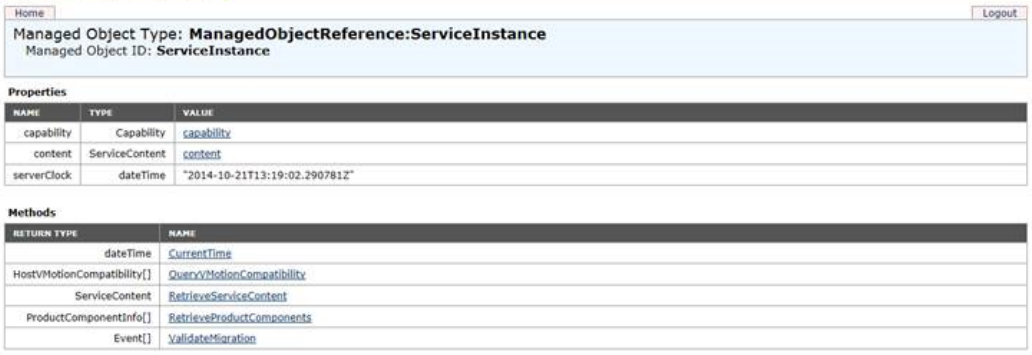
要卸载高级 GRE Web 插件，请取消选中 VMware vCenter 客户机的“登录”选项卡中的**高级 GRE Web 插件**复选框，然后单击**应用**。

> **注意：**
> 如果您已卸载一个 Cell Manager 或多个 Cell Manager，而没有取消注册高级 GRE Web 插件，那么您将在 VMware vSphere Web 客户机中看到“Data Protector”选项卡，但您不能连接它。 您必须手动取消注册高级 GRE Web 插件。有关详细信息，请参见手动取消注册 VMware vSphere 托管对象引用

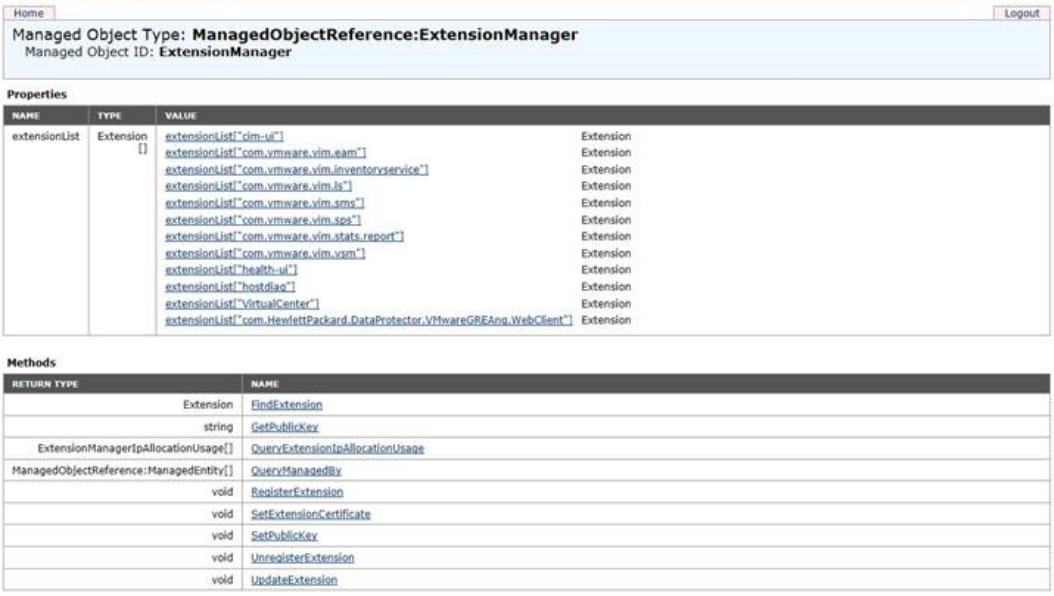
手动取消注册 VMware vSphere 托管对象引用

完成以下步骤，以删除 vCenter 中注册的一个或多个单元管理器。

1. 转至 VMware vSphere 托管对象引用 URL，https://<vcenter>/mob



2. 单击**内容**，然后单击 **ExtensionManager**。
3. 选择密钥 com.HewlettPackardEnterprise.DataProtector.VMwareGREAng.WebClient


Home Logout

Managed Object Type: **ManagedObjectReference:ExtensionManager**
Managed Object ID: **ExtensionManager**

Properties

NAME	TYPE	VALUE	
extensionList	Extension []	extensionList["cim-ui"]	Extension
		extensionList["com.vmware.vim.eam"]	Extension
		extensionList["com.vmware.vim.inventoryservice"]	Extension
		extensionList["com.vmware.vim.ls"]	Extension
		extensionList["com.vmware.vim.sms"]	Extension
		extensionList["com.vmware.vim.sps"]	Extension
		extensionList["com.vmware.vim.stats.report"]	Extension
		extensionList["com.vmware.vim.vsm"]	Extension
		extensionList["health-ui"]	Extension
		extensionList["hostdiag"]	Extension
		extensionList["VirtualCenter"]	Extension
		extensionList["com.HewlettPackard.DataProtector.VMwareGREAng.WebClient"]	Extension

Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

4. 单击页面底部的 **UnregisterExtension**。

Microsoft Hyper-V 客户机

需要在 Microsoft Hyper-V 系统上安装的 Data Protector 组件会因您要使用的备份和还原解决方案而异。 可以从下列解决方案中选择：

- Microsoft Hyper-V 客户机 (第 122 页)
- Data Protector Microsoft Volume Shadow Copy Service integration (第 123 页)

Data Protector 虚拟环境集成

假设您打算安装组件的所有系统已启动并正在运行。

在应当控制备份和恢复会话(**备份主机**)的系统上安装以下 Data Protector 组件：

- Virtual Environment Integration
- MS Volume Shadow Copy Integration
- Disk Agent

> **注意：**
> Disk Agent 组件使您在备份主机上恢复到某目录时能够使用**浏览**按钮。 如果没有安装组件，您必须自行键入目标目录。

在 Microsoft Hyper-V 系统上，安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration

> **注意：**
> 如果您的 Microsoft Hyper-V 系统在群集中配置，它们必须像群集感知客户机那样安装。 有关详细信息，请参见在 Microsoft Hyper-V 群集上安装 Data Protector (第 167

> 页)。

在备份系统(适用于 VSS 可传输备份)上，安装以下 Data Protector 组件：

- MS Volume Shadow Copy Integration

> **注意：**
> *备份主机*和*备份系统*不是同一个系统。

Data Protector Microsoft Volume Shadow Copy Service integration

有关需要在 Microsoft Hyper-V 系统上安装哪些组件的详细信息，请参见Microsoft Hyper-V 客户机 (第 122 页)。

NDMP 服务器客户机

假设 NDMP 服务器已启动并正在运行。

在安装过程中，请选择 NDMP Media Agent，并将它安装到所有访问 NDMP 专用驱动器的 Data Protector 客户机上。

> **注意：**
> 如果某个 Data Protector 客户机不用于通过 NDMP 服务器访问 NDMP 专用驱动器，而仅用于控制库的机械手，则可以在此类客户机上安装 NDMP Media Agent或General Media Agent。

请注意，一台 Data Protector 客户机上只能安装一个介质代理。

P4000 SAN 解决方案 clients

要将 P4000 SAN 解决方案与 Data Protector 进行集成，请在应用程序和备份系统上安装以下 Data Protector 软件组件：

- MS Volume Shadow Copy Integration
- P4000 VSS Agent

要执行“ZDB 到磁盘 + 磁带”或“ZDB 到磁带”会话，请在备份系统上另外安装以下 Data Protector 软件组件：

- General Media Agent

P6000 EVA 磁盘阵列系列 clients

要将 P6000 EVA 磁盘阵列系列与 Data Protector 进行集成，请在应用程序和备份系统上安装以下 Data Protector 软件组件：

- P6000 / 3PAR SMI-S Agent
- General Media Agent

  在备份系统上安装 General Media Agent 组件来备份批量数据。 将它安装在应用程序系统上，以备份归档日志或执行到应用程序系统的还原。
- Disk Agent

  在应用程序和备份系统上安装 Disk Agent 组件来运行文件系统或者磁盘映像的零宕机时间备份。 在创建 ZDB 备份规范时， Application system 和 Backup system 下拉列表中不会列出未安装磁盘代理的客户机。

> **重要：**
> 在 Microsoft Windows Server 2008 系统上，必须安装两个 Windows Server 2008 修补程序，才能支持 Data Protector P6000 EVA 磁盘阵列系列集成的正常工作。 您可以从 Microsoft 网站 (http://support.microsoft.com/kb/952790 和 http://support.microsoft.com/kb/971254)中下载所需的修补程序包。
>
> 这个额外的要求不适用于 Windows Server 2008 R2 系统。

在群集中安装

您可以在群集环境中安装 P6000 EVA 磁盘阵列系列集成。 有关受支持的群集配置和特定安装要求，请参见《*Data Protector 零宕机时间备份管理员指南*》。

与其他应用程序集成

要安装 P6000 EVA 磁盘阵列系列与数据库应用程序的集成，请在应用程序系统和备份系统上安装特定于特定集成的 Data Protector 组件，并执行特定于该集成的安装任务。 您可以安装 P6000 EVA 磁盘阵列系列与 Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server 和 Microsoft 卷影复制服务的集成。

P6000 EVA 磁盘阵列系列 与 Oracle Server 的集成

先决条件

- 在应用程序系统上，以及使用备份集 ZDB 方法的备份系统上，必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus

  备份系统上的 Oracle 软件必须安装在与应用程序系统相同的目录中。 二进制文件应与应用程序系统上的二进制文件相同。 实现方法有，从应用程序系统将文件和系统环境复制到备份系统，或者使用与应用程序系统上相同的安装参数在备份系统上全新安装 Oracle 二进制文件。
- 应用程序系统上的 Oracle 数据文件必须安装在将使用已安装的 SMI-S 代理进行复制的源

卷上。

根据 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 的位置，有以下两个可能选项：

- Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于**不同于** Oracle 数据文件的其他卷组(如果使用了 LVM)或源卷。

  默认情况下，此类配置启用即时恢复。

- Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于与 Oracle 数据文件**相同**的卷组(如果使用了 LVM)或源卷。

  默认情况下，此类配置*不*启用即时恢复。 可以通过设置 ZDB_ORA_INCLUDE_CF_OLF、ZDB_ORA_INCLUDE_SPF 和 ZDB_ORA_NO_CHECKCONF_IR omnirc 选项。 有关详细信息，请参见 *Data Protector 零宕机时间备份集成指南*。

Oracle 归档重做日志文件不一定要位于源卷上。

如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

安装过程

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。 最好将它安装在独立系统、非镜像磁盘上。 使恢复编目保持为未注册状态。 有关如何安装数据库的详细信息，请参见 Oracle 文档。
2. 安装以下 Data Protector 软件组件：
   - P6000 / 3PAR SMI-S Agent – 在应用程序系统和备份系统上
   - Oracle Integration – 在应用程序系统和备份系统上

> **注意：**
> - 只有对于备份集 ZDB 方法，备份系统上才需要 Data ProtectorOracle Integration 组件。 对于代理复制 ZDB 方法则不需要它。
> - 在 RAC 群集环境中，Oracle 应用程序数据库通过多个 Oracle 实例进行访问。 因此，请在运行 Oracle 实例的所有系统上安装 Data ProtectorOracle Integration 和 P6000 / 3PAR SMI-S Agent 组件。
> - 如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

P6000 EVA 磁盘阵列系列 与 SAP R/3 的集成

先决条件

- 在应用程序系统上必须安装以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话(BRBACKUP 在备份系统上启动，而不是在应用程序系统上)，请配置备份系统。 有关详细信息，请参见 Oracle 的 SAP 数据库指南(分割镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件*必须*位于磁盘阵列上。
  - 对于*联机备份*，控制文件和联机重做日志不一定要位于磁盘阵列上。 *联机* SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须位于磁盘阵列上。
  - 对于*脱机备份*，控制文件和联机重做日志*必须*位于磁盘阵列上。
  - 归档重做日志文件不一定要位于磁盘阵列上。

  如果 Oracle 控制文件、联机重做日志和 Oracle SPFILE 位于与 Oracle 数据文件相同的 LVM 卷组或源卷上，请设置 Data Protector`ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF` 和 `ZDB_ORA_INCLUDE_SPFomnirc` 选项。 否则，将无法运行“ZDB 到磁盘”和“ZDB 到磁盘 + 磁带”会话。 有关详细信息，请参见*Data Protector 零宕机时间备份集成指南*。

  > **注意：**
  > 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。
  >
  > ***UNIX 系统：*** 如果 Oracle 数据库安装在原始分区(原始磁盘或原始逻辑卷)上，请确保应用程序系统和备份系统上的卷/磁盘组名称是相同的。
- 在 UNIX 系统上，确保应用程序系统上存在以下用户：
  - `ora`*`ORACLE_SID`* 具有主组 `dba`
  - *`ORACLE_SID`* `adm` 在 UNIX 组中 `sapsys`
- SAP R/3 软件必须正确安装在应用程序系统上。

  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  > **注意：**
  > 目录的位置取决于环境(UNIX 系统)或注册表(Windows 系统)变量。 有关详细信息，请参见 SAP R/3 文档。

- *ORACLE_HOME* /dbs (UNIX 系统)*ORACLE_HOME*\database(Windows 系统)- Oracle 和 SAP 配置文件
- *ORACLE_HOME* /bin (UNIX 系统)*ORACLE_HOME*\bin(Windows 系统)- Oracle 二进制文件
- *SAPDATA_HOME* /sapbackup (UNIX 系统)*SAPDATA_HOME*\sapbackup(Windows 系统)- 带有 BRBACKUP 日志文件的 SAPBACKUP 目录
- *SAPDATA_HOME* /saparch (UNIX 系统)*SAPDATA_HOME*\saparch(Windows 系统)- 带有 BRARCHIVE 日志文件的 SAPARCH 目录
- *SAPDATA_HOME* /sapreorg (UNIX 系统)*SAPDATA_HOME*\sapreorg(Windows 系统)
- *SAPDATA_HOME* /sapcheck (UNIX 系统)*SAPDATA_HOME*\sapcheck(Windows 系统)
- *SAPDATA_HOME* /saptrace (UNIX 系统)*SAPDATA_HOME*\saptrace(Windows 系统)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIX 系统)

  c:\Oracle*ORACLE_SID*\sys\exe\run (Windows 系统)

  > **注意：**
  > 如果计划执行即时恢复，请确保 sapbackup、saparch 和 sapreorg 目录位于不同于 Oracle 数据文件的其他源卷上。

UNIX 系统

在 UNIX 系统上，如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。

在 UNIX 系统上，目录 /usr/sap/*ORACLE_SID*/SYS/exe/run 必须由 UNIX 用户 ora*ORACLE_SID* 所有。 SAP R/3 文件的所有者必须为 UNIX 用户 ora*ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba。 例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID*adm 所有。

UNIX 示例

如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于：

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

安装过程

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：
   - P6000 / 3PAR SMI-S Agent
   - SAP R/3 Integration
   - Disk Agent

注意：
只有计划运行 SAP 兼容 ZDB 会话(在该会话中，BRBACKUP 在备份系统上启动)时，才需要在备份系统上安装 SAP R/3 Integration 集成。

在 Windows 系统上，必须使用 SAP R/3 管理员用户帐户安装 Data Protector 软件组件，并且该帐户必须包含在运行 SAP R/3 实例的系统的 ORA_DBA 或 ORA_*SID*_DBA 本地组中。

P6000 EVA 磁盘阵列系列 与 Microsoft Exchange Server 的集成

先决条件

在应用程序系统源卷上必须安装 Microsoft Exchange Server 数据库。 以下对象必须位于源卷上：

- Microsoft Information Store (MIS)
- (可选)Key Management Service (KMS)
- (可选)Site Replication Service (SRS)

为了能够备份事务日志，请禁用 Microsoft Exchange Server 上的“循环日志记录”。

安装过程

安装以下 Data Protector 软件组件：

- P6000 / 3PAR SMI-S Agent – 在应用程序系统和备份系统上
- MS Exchange Integration – 仅在应用程序系统上

P6000 EVA 磁盘阵列系列 与 Microsoft SQL Server 的集成

先决条件

应用程序系统上必须安装 Microsoft SQL Server。 用户数据库*必须*位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。 但是，如果系统数据库也安装在磁盘阵列上，它们*必须*安装在*不同于*用户数据库的其他源卷上。

安装过程

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- P6000 / 3PAR SMI-S Agent – 在应用程序系统和备份系统上
- MS SQL Integration – 仅在应用程序系统上

P9000 XP 磁盘阵列系列 clients

要将 P9000 XP 磁盘阵列系列与 Data Protector 进行集成，请在应用程序和备份系统上安装以下 Data Protector 软件组件：

- P9000 XP Agent
- General Media Agent

  在备份系统上安装 General Media Agent 组件来备份批量数据。将它安装在应用程序系统上，以备份归档日志或执行到应用程序系统的恢复。
- Disk Agent

  在应用程序和备份系统上安装 Disk Agent 组件来运行文件系统或者磁盘映像的零宕机时间备份。在创建 ZDB 备份规范时，Application system 和 Backup system 下拉列表中不会列出未安装磁带客户机的客户机。

> **重要：**
> 在 Microsoft Windows Server 2008 系统上，必须安装两个 Windows Server 2008 修补程序，才能支持 Data Protector P9000 XP 磁盘阵列系列集成的正常工作。您可以从 Microsoft 网站(http://support.microsoft.com/kb/952790 和 http://support.microsoft.com/kb/971254)中下载所需的修补程序包。
>
> 这个额外的要求不适用于 Windows Server 2008 R2 系统。

在群集中安装

您可以在群集环境中安装 P9000 XP 磁盘阵列系列集成。有关受支持的群集配置和特定安装要求，请参见《*Data Protector 零宕机时间备份管理员指南*》。

与其他应用程序集成

要安装数据库应用程序的 P9000 XP 磁盘阵列系列集成，请在应用程序系统和备份系统上安装特定于特定集成的 Data Protector 组件，并执行特定于该集成的安装任务。您可以安装 P9000 XP 磁盘阵列系列与 Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server 和 Microsoft 卷影复制服务的集成。

P9000 XP 磁盘阵列系列 与 Oracle Server 的集成

先决条件

- 在应用程序系统上，以及使用备份集 ZDB 方法的备份系统上，必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务

- SQL*Plus

备份系统上的 Oracle 软件必须安装在与应用程序系统相同的目录中。 二进制文件应与应用程序系统上的二进制文件相同。 实现方法有，从应用程序系统将文件和系统环境复制到备份系统，或者使用与应用程序系统上相同的安装参数在备份系统上全新安装 Oracle 二进制文件。

- 应用程序系统上的 Oracle 数据文件必须安装在镜像到备份系统的 P9000 XP 磁盘阵列系列 LDEV 上。

  在使用备份集方法的情况下，如果一些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

  根据 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 的位置，有以下两个可能选项：

  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于**不同于** Oracle 数据文件的其他卷组(如果使用了 LVM)或源卷。

    默认情况下，此类配置启用即时恢复。

  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于与 Oracle 数据文件**相同**的卷组(如果使用了 LVM)或源卷。

    默认情况下，此类配置*不*启用即时恢复。 可以通过设置 `ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPF` 和 `ZDB_ORA_NO_CHECKCONF_IR` omnirc 选项。 有关详细信息，请参见 *Data Protector 零宕机时间备份集成指南*。

  Oracle 归档重做日志文件不一定要位于源卷上。

安装过程

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。 最好将它安装在独立系统、非镜像磁盘上。 使恢复编目保持为未注册状态。 有关如何安装数据库的详细信息，请参见 Oracle 文档。
2. 安装以下 Data Protector 软件组件：
   - `P9000 XP Agent` – 在应用程序系统和备份系统上
   - `Oracle Integration` – 在应用程序系统和备份系统上

> **注意：**
> - 只有对于备份集 ZDB 方法，备份系统上才需要 Data Protector `Oracle Integration` 组件。 对于代理复制 ZDB 方法则不需要它。
> - 在 RAC 群集环境中，Oracle 应用程序数据库通过多个 Oracle 实例进行访问。 因此，请在运行 Oracle 实例的所有系统上安装 Data Protector、`Oracle Integration` 和 `P9000 XP Agent` 组件。
> - 如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

P9000 XP 磁盘阵列系列 与 SAP R/3 的集成

先决条件

- 在应用程序系统上必须安装和配置以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话(BRBACKUP 在备份系统上启动，而不是在应用程序系统上)，请配置备份系统。 有关详细信息，请参见 Oracle 的 SAP 数据库指南(分割镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件*必须*位于磁盘阵列上。
  - 对于*联机备份*，控制文件和联机重做日志不一定要位于磁盘阵列上。 *联机* SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须位于磁盘阵列上。
  - 对于*脱机备份*，控制文件和联机重做日志*必须*位于磁盘阵列上。
  - 归档重做日志文件不一定要位于磁盘阵列上。

  如果 Oracle 控制文件、联机重做日志和 Oracle SPFILE 位于与 Oracle 数据文件相同的 LVM 卷组或源卷上，请设置 Data Protector`ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF` 和 `ZDB_ORA_INCLUDE_SPFomnirc` 选项。 否则，将无法运行“ZDB 到磁盘”和“ZDB 到磁盘 + 磁带”会话。 有关详细信息，请参见《*Data Protector 零宕机时间备份集成指南*》。

  > **注意：**
  > 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。
  >
  > ***UNIX 系统：*** 如果 Oracle 数据库安装在原始分区(原始磁盘或原始逻辑卷)上，请确保应用程序系统和备份系统上的卷/磁盘组名称是相同的。
- 在 UNIX 系统上，确保应用程序系统上存在以下用户：
  - `ora`*`ORACLE_SID`* 具有主组 `dba`
  - *`ORACLE_SID`* `adm` 在 UNIX 组中 `sapsys`
- SAP R/3 软件必须正确安装在应用程序系统上。

  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  > **注意：**
  > 目录的位置取决于环境(UNIX 系统)或注册表(Windows 系统)变量。 有关详细信息，请参见 SAP R/3 文档。

- *ORACLE_HOME* /dbs (UNIX 系统)
  ORACLE_HOME\database(Windows 系统)- Oracle 配置文件和 SAP R/3 配置文件)
- *ORACLE_HOME* /bin or (UNIX 系统)
  ORACLE_HOME\bin(Windows 系统)- Oracle 二进制文件
- *SAPDATA_HOME* /sapbackup (UNIX 系统)
  SAPDATA_HOME\sapbackup(Windows 系统)-
  带有 BRBACKUP 日志文件的 SAPBACKUP 目录
- *SAPDATA_HOME*/saparch(UNIX 系统)
  SAPDATA_HOME\saparch(Windows 系统)-
  带有 BRARCHIVE 日志文件的 SAPARCH 目录
- *SAPDATA_HOME* /sapreorg (UNIX 系统)
  SAPDATA_HOME \sapreorg(Windows 系统)
- *SAPDATA_HOME* /sapcheck (UNIX 系统)
  SAPDATA_HOME \sapcheck(Windows 系统)
- *SAPDATA_HOME* /saptrace (UNIX 系统)
  SAPDATA_HOME \saptrace(Windows 系统)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIX 系统)
  c:\Oracle*ORACLE_SID*\sys\exe\run (Windows 系统)

  > **注意：**
  > 如果计划执行即时恢复，请确保 sapbackup、saparch 和 sapreorg 目录位于不同于 Oracle 数据文件的其他源卷上。

UNIX 系统

在 UNIX 系统上，如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。

在 UNIX 系统上，目录 /usr/sap/*ORACLE_SID*/SYS/exe/run 必须由 UNIX 用户 ora*ORACLE_SID* 所有。 SAP R/3 文件的所有者必须为 UNIX 用户 ora*ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba。 例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID*adm 所有。

UNIX 示例

如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于：

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

安装过程

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：
   - P9000 XP Agent
   - SAP R/3 Integration
   - Disk Agent

> **注意：**
> 只有计划运行 SAP 兼容 ZDB 会话(在该会话中，BRBACKUP 在备份系统上启动)时，才需要在备份系统上安装 SAP R/3 Integration 集成。
>
> 在 Windows 系统上，必须使用 SAP R/3 管理员用户帐户安装 Data Protector 软件组件，并且该帐户必须包含在运行 SAP R/3 实例的系统的 ORA_DBA 或 ORA_*SID*_DBA 本地组中。

P9000 XP 磁盘阵列系列 与 Microsoft Exchange Server 的集成

先决条件

镜像到备份系统的 P9000 XP 磁盘阵列系列 卷 (LDEV) 上的应用程序系统上必须安装 Microsoft Exchange Server 数据库。 镜像可以是 Business Copy P9000 XP 或 Continuous Access P9000 XP，并且数据库安装在文件系统上。 以下对象必须位于被镜像的卷上：

- Microsoft Information Store (MIS)
- (可选)Key Management Service (KMS)
- (可选)Site Replication Service (SRS)

为了能够备份事务日志，请禁用 Microsoft Exchange Server 上的“循环日志记录”。

安装过程

安装以下 Data Protector 软件组件：

- P9000 XP Agent – 在应用程序系统和备份系统上
- MS Exchange Integration – 仅在应用程序系统上

P9000 XP 磁盘阵列系列 与 Microsoft SQL Server 的集成

先决条件

应用程序系统上必须安装 Microsoft SQL Server。 用户数据库*必须*位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。 但是，如果系统数据库也安装在磁盘阵列上，它们*必须*安装在*不同于*用户数据库的其他源卷上。

安装过程

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- P9000 XP Agent
- MS SQL Integration

3PAR StoreServ Storage clients

要将 3PAR StoreServ Storage 与 Data Protector 集成，请在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- P6000 / 3PAR SMI-S Agent

如果要使用卷影复制服务备份和恢复对象，您还需要具备以下组件：

- MS Volume Shadow Copy Integration
- 3PAR VSS Agent

不论是何种操作系统，要执行“ZDB 到磁盘 + 磁带”或“ZDB 到磁带”会话，则还要在备份系统上安装以下 Data Protector 软件组件：

- General Media Agent

EMC Symmetrix 客户机

要将 EMC Symmetrix 与 Data Protector 进行集成，请在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- EMC Symmetrix Agent (SYMA)

  在远程安装 EMC Symmetrix Agent 组件之前，请安装以下两个 EMC 组件：
  - EMC Solution Enabler
  - EMC Symmetrix TimeFinder 或 EMC Symmetrix Remote Data Facility (SRDF) 微代码和许可证。
- General Media Agent

在备份系统上安装 General Media Agent 组件来备份批量数据。 将它安装在应用程序系统上，以备份归档日志或执行到应用程序系统的恢复。

- Disk Agent

  在应用程序系统和备份系统上安装Disk Agent组件来运行磁盘映像和文件系统 ZDB。 在创建 ZDB 备份规范时， Application system 和 Backup system 下拉列表中不会列出未安装磁带客户机的客户机。

在群集中安装

您可以在群集环境中安装 EMC Symmetrix 集成。 有关受支持的群集配置和特定安装要求，请参见《*Data Protector 零宕机时间备份管理员指南*》。

与其他应用程序集成

要安装数据库应用程序的 EMC Symmetrix 集成，请在应用程序系统和备份系统上安装特定于特定集成的 Data Protector 组件，并执行特定于该集成的安装任务。 您可以安装 Oracle 和 SAP R/3 的 EMC Symmetrix 集成。

Oracle 的 EMC Symmetrix 集成

先决条件

- 在应用程序系统上必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 应用程序系统使用的 Oracle 数据库文件必须安装在镜像到备份系统的 EMC Symmetrix 设备上。

  数据库可以安装在磁盘映像、逻辑卷或文件系统上。 以下 Oracle 文件必须进行镜像：
  - 数据文件
  - 控制文件
  - 联机重做日志文件

  归档重做日志文件必须位于非镜像磁盘上。

安装过程

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。 最好将它安装在独立系统、非镜像磁盘上。 使恢复编目保持为未注册状态。 有关如何安装数据库的详细信息，请参见 Oracle 文档。

2. 安装以下 Data Protector 软件组件：
   - EMC Symmetrix Agent – 在应用程序系统和备份系统上
   - Oracle Integration – 在应用程序系统和备份系统上

> **注意：**
> - 只有对于备份集 ZDB 方法，备份系统上才需要 Data ProtectorOracle Integration 组件。 对于代理复制 ZDB 方法则不需要它。
> - 在 RAC 群集环境中，Oracle 应用程序数据库通过多个 Oracle 实例进行访问。 因此，请在运行 Oracle 实例的所有系统上安装 Data ProtectorOracle Integration 和 EMC Symmetrix Agent 组件。
> - 如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

SAP R/3 的 EMC Symmetrix 集成

先决条件

- 在应用程序系统上必须安装和配置以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 软件
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话(BRBACKUP 在备份系统上启动，而不是在应用程序系统上)，请配置备份系统。 有关详细信息，请参见 Oracle 的 SAP 数据库指南(分割镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件*必须*位于磁盘阵列上。
  - 对于*联机备份*，控制文件和联机重做日志不一定要位于磁盘阵列上。 *联机* SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须位于磁盘阵列上。
  - 对于*脱机备份*，控制文件和联机重做日志*必须*位于磁盘阵列上。
  - 归档重做日志文件不一定要位于磁盘阵列上。

> **注意：**
> 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。
> ***UNIX 系统：*** 如果 Oracle 数据库安装在原始分区(原始磁盘或原始逻辑卷)上，请确保应用程序系统和备份系统上的卷/磁盘组名称是相同的。

- 在 UNIX 系统上，确保应用程序系统上存在以下用户：

- ora*ORACLE_SID* 具有主组 dba
- *ORACLE_SID* adm 在 UNIX 组中 sapsys

- SAP R/3 软件必须正确安装在应用程序系统上。
  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  注意：
  目录的位置取决于环境变量。 有关详细信息，请参见 SAP R/3 文档。

  - *ORACLE_HOME* /dbs - Oracle 配置文件和 SAP R/3 配置文件
  - *ORACLE_HOME* /bin - Oracle 二进制文件
  - *SAPDATA_HOME* /sapbackup - 带有 BRBACKUP 日志文件的 SAPBACKUP 目录
  - *SAPDATA_HOME* /saparch - 包含 BRARCHIVE 日志文件的 SAPARCH 目录
  - *SAPDATA_HOME* /sapreorg
  - *SAPDATA_HOME* /sapcheck
  - *SAPDATA_HOME* /saptrace
  - /usr/sap/*ORACLE_SID*/SYS/exe/run

    注意：
    如果计划执行即时恢复，请确保 sapbackup、saparch 和 sapreorg 目录位于不同于 Oracle 数据文件的其他源卷上。

  如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。

  目录 /usr/sap/*ORACLE_SID*/SYS/exe/run 必须归 UNIX 用户 ora*ORACLE_SID* 所有。 SAP R/3 文件的所有者必须为 UNIX 用户 ora*ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba。 例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID*adm 所有。

  示例

  如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于：

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011 brrestore -rwsr-xr-x 1
orapro dba 188629 Apr 17 2011 brtools
```

安装过程

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- EMC Symmetrix Agent
- SAP R/3 Integration
- Disk Agent

> **注意：**
> 只有计划运行 SAP 兼容 ZDB 会话(在该会话中，BRBACKUP 在备份系统上启动)时，才需要在备份系统上安装 SAP R/3 Integration 集成。

Microsoft SQL Server 的 EMC Symmetrix 集成

先决条件

应用程序系统上必须安装 Microsoft SQL Server。用户数据库*必须*位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。但是，如果系统数据库也安装在磁盘阵列上，它们*必须*安装在*不同于*用户数据库的其他源卷上。

安装过程

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- EMC Symmetrix Agent
- MS SQL Integration

非 HPE 存储阵列

Data Protector 使用适用于非 HPE 存储阵列的存储提供程序与以下 ZDB 存储阵列集成：NetApp Storage、EMC VNX 和 EMC VMAX Storage 系列。此存储提供程序组件是 Data Protector SMI-S Agent 的插件。它通过 SMI-S Agent 启用相应存储的 ZDB 功能。

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- 根据所使用的存储(NetApp Storage Provider、EMC VNX Storage Provider 或 EMC VMAX Storage Provider)安装适用于非 HPE 存储阵列的存储提供程序组件之一

要执行“ZDB 到磁带”会话，请在备份系统上安装以下 Data Protector 软件组件：

- General Media Agent

与其他应用程序集成

要安装与数据库应用程序的 Data Protector 非 HPE 存储阵列集成或虚拟环境集成，请在适用的系统上安装特定于特定集成的 Data Protector 组件，并执行特定于该集成的安装任务。您可以安装与 VMware、Oracle Server、SAP R/3 和 Microsoft SQL Server 的非 HPE 存储阵列集成。请参见 https://softwaresupport.softwaregrp.com/ 上最新的支持列表，以检查非 HPE 存储阵列与特定数据库应用程序或虚拟环境集成的哪些组合受支持。

与 VMware 虚拟环境的非 HPE 存储阵列集成

限制

- 仅支持 VMware vCenter 环境。
- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

先决条件

假设您打算安装组件的所有系统已启动并正在运行。

安装过程

在应当控制备份和还原会话(备份系统)的系统上安装以下 Data Protector 组件：

- Virtual Environment Integration
- 非 HPE 存储阵列的存储提供程序(NetApp Storage Provider)
- General Media Agent
- Disk Agent

> **注意：**
> - Disk Agent 组件使您在备份主机上还原到某目录时能够使用**浏览**按钮。如果没有安装组件，您必须自行键入目标目录。
> - 您打算作为备份主机使用的客户机不必安装 VMware Consolidated Backup (VCB) 软件。

与 Oracle Server 的非 HPE 存储阵列集成

限制

- 不支持 RAC 群集环境。
- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

先决条件

- 在应用程序系统上，以及使用备份集 ZDB 方法的备份系统上，必须安装和配置以下软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务

- SQL*Plus

备份系统上的 Oracle 软件必须安装在与应用程序系统相同的目录中。二进制文件应与应用程序系统上的二进制文件相同。实现方法有，从应用程序系统将文件和系统环境复制到备份系统，或者使用与应用程序系统上相同的安装参数在备份系统上全新安装 Oracle 二进制文件。

- 应用程序系统上的 Oracle 数据文件必须安装在将使用已安装的 Storage Provider(通过 SMI-S 代理)进行复制的源卷上。

  根据 Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 的位置，有以下两个可能选项：

  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于**不同于** Oracle 数据文件的其他卷组(如果使用了 LVM)或源卷。
  - Oracle 控制文件、联机重做日志文件和 Oracle SPFILE 位于与 Oracle 数据文件**相同**的卷组(如果使用了 LVM)或源卷。

  Oracle 归档重做日志文件不一定要位于源卷上。

  如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。

安装过程

执行以下安装任务：

1. 安装 Oracle 恢复编目数据库。最好将它安装在独立系统、非镜像磁盘上。使恢复编目保持为未注册状态。有关如何安装数据库的详细信息，请参见 Oracle 文档。
2. 安装以下 Data Protector 软件组件：
   - 在应用程序系统和备份系统上安装适用于非 HPE 存储阵列(NetApp Storage Provider、EMC VNX Storage Provider 或 EMC VMAX Storage Provider)的存储提供程序
   - Oracle Integration – 在应用程序系统和备份系统上

> **注意：**
> - 只有对于备份集 ZDB 方法，备份系统上才需要 Data ProtectorOracle Integration 组件。对于代理复制 ZDB 方法则不需要它。
> - 如果将 Oracle 恢复编目数据库安装在独立的系统上，则不需要在该系统上安装任何 Data Protector 软件组件。

与 SAP R/3 的非 HPE 存储阵列集成

限制

- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

先决条件

- 在应用程序系统上必须安装以下 Oracle 软件：
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net 服务
  - SQL*Plus
- 如果计划运行 SAP 兼容 ZDB 会话(BRBACKUP 在备份系统上启动，而不是在应用程序系统上)，请配置备份系统。有关详细信息，请参见 Oracle 的 SAP 数据库指南(分割镜像备份、软件配置)。
- 应用程序系统上的数据库可以安装在磁盘映像、逻辑卷或文件系统上。
  - Oracle 数据文件*必须*驻留在存储系统上。
  - 对于*联机备份*，控制文件和联机重做日志不必驻留在存储系统上。*联机* SAP 兼容 ZDB 会话属于例外，对于这些会话，控制文件必须驻留在存储系统上。
  - 对于*脱机备份*，控制文件和联机重做日志*必须*位于存储系统上。
  - 归档重做日志文件不必驻留在存储系统上。

  > **注意：**
  > 如果某些 Oracle 数据文件安装在符号链接上，则必须也在备份系统上创建这些链接。
  >
  > ***UNIX 系统：***如果在原始分区(原始磁盘或原始逻辑卷)上安装 Oracle 数据库，请确保应用程序系统和备份系统上的卷/磁盘组名称相同。
- 在 UNIX 系统上，确保应用程序系统上存在以下用户：
  - ora*ORACLE_SID* 具有主组 dba
  - *ORACLE_SID* adm 在 UNIX 组中 sapsys
- SAP R/3 软件必须正确安装在应用程序系统上。

  以下是安装 SAP R/3 之后，必须在应用程序系统上安装的标准目录的列表：

  > **注意：**
  > 目录的位置取决于环境(UNIX 系统)或注册表(Windows 系统)变量。有关详细信息，请参见 SAP R/3 文档。

  - *ORACLE_HOME* /dbs(UNIX 系统)*ORACLE_HOME*\database(Windows 系统)- Oracle 和 SAP 配置文件
  - *ORACLE_HOME* /bin(UNIX 系统)*ORACLE_HOME*\bin(Windows 系统)- Oracle 二进制文件
  - *SAPDATA_HOME* /sapbackup(UNIX 系统)*SAPDATA_HOME*\sapbackup(Windows 系统)- 带有 BRBACKUP 日志文件的 SAPBACKUP 目录

- *SAPDATA_HOME* /saparch(UNIX 系统)*SAPDATA_HOME*\saparch(Windows 系统)- 带有 BRARCHIVE 日志文件的 SAPARCH 目录
- *SAPDATA_HOME* /sapreorg(UNIX 系统)*SAPDATA_HOME*\sapreorg(Windows 系统)
- *SAPDATA_HOME* /sapcheck(UNIX 系统)*SAPDATA_HOME*\sapcheck(Windows 系统)
- *SAPDATA_HOME* /saptrace(UNIX 系统)*SAPDATA_HOME*\saptrace(Windows 系统)
- /usr/sap/*ORACLE_SID*/SYS/exe/run(UNIX 系统)
  c:\Oracle*ORACLE_SID*\sys\exe\run(Windows 系统)

UNIX 系统

在 UNIX 系统上，如果最后 6 个目录不是位于以上指定目标中，请创建指向它们的相应链接。

在 UNIX 系统上，目录 /usr/sap/*ORACLE_SID*/SYS/exe/run 必须由 UNIX 用户 ora*ORACLE_SID* 所有。SAP R/3 文件的所有者必须为 UNIX 用户 ora*ORACLE_SID* 和包含 setuid 位组 (chmod 4755 ...) 的 UNIX 组 dba。例外情况是文件 BRRESTORE，该文件必须由 UNIX 用户 *ORACLE_SID*adm 所有。

UNIX 示例

如果 *ORACLE_SID* 为 PRO，那么目录 /usr/sap/PRO/SYS/exe/run 中的权限应类似于：

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011

brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

安装过程

1. 在应用程序系统上安装 SAP R/3 BRTOOLS。
2. 在应用程序系统和备份系统上安装以下 Data Protector 软件组件：
   - 非 HPE 存储阵列的存储提供程序(NetApp Storage Provider)
   - SAP R/3 Integration
   - Disk Agent

> **注意：**
> 只有计划运行 SAP 兼容 ZDB 会话(在该会话中，BRBACKUP 在备份系统上启动)时，才需要在备份系统上安装 SAP R/3 Integration。
>
> 在 Windows 系统上，必须使用 SAP R/3 管理员用户帐户安装 Data Protector 软件组件，并且该帐户必须包含在运行 SAP R/3 实例的系统的 ORA_DBA 或 ORA_*SID*_DBA 本地组中。

与 Microsoft SQL Server 的非 HPE 存储阵列集成

限制

- 不支持即时恢复。
- 仅支持 ZDB 到磁带的备份。

先决条件

应用程序系统上必须安装 Microsoft SQL Server。用户数据库*必须*位于磁盘阵列源卷上，而系统数据库可以安装在任意位置。但是，如果系统数据库也安装在磁盘阵列上，它们*必须*安装在*不同于*用户数据库的其他源卷上。

安装过程

在应用程序系统和备份系统上安装以下 Data Protector 软件组件：

- 在应用程序和备份系统上安装适用于非 HPE 存储阵列(NetApp Storage Provider、EMC VNX Storage Provider 或 EMC VMAX Storage Provider)的存储提供程序
- MS SQL Integration — 仅在应用程序系统上

第 5 章： 在群集上安装 Data Protector

在 Serviceguard 上安装 Data Protector

Data Protector 支持 Serviceguard (SG) for HP-UX 和 HP Serviceguard (HP SG) for Linux。有关所支持的操作系统版本的详细信息，请参见Data Protector产品声明、软件说明和参考。

如果 Cell Manager 需要以群集感知模式运行，请注意应对许可证使用虚拟服务器 IP 地址。

配置阶段

1. 配置主 Cell Manager
2. 配置辅助 Cell Manager
3. 配置 Cell Manager 包

安装群集感知 Cell Manager

先决条件

在 Serviceguard 上安装 Data Protector Cell Manager 之前，请检查以下各项：

- 确定哪些系统将作为主 Cell Manager 和辅助 Cell Manager。它们全部都必须安装 Serviceguard，并且必须配置为群集成员。
- 在主节点和每个辅助节点上，都必须安装 Data Protector Cell Manager(带有建议的补丁)，以及要在群集中部署的集成的所有其他 Data Protector 软件组件。
- 用户组 hpdp 和专用用户帐户 hpdp 在两个节点上必须具有相同 ID。
- 在此群集环境中，Data Protector Cell Manager 应有自己的包。在 Serviceguard 中安装 Data Protector Cell Manager 之前，需要从网络管理员处获得以下信息：
  - 虚拟服务器名称(群集包中指定的主机名)
  - 包 IP 或虚拟 IP 地址

  此外，还将需要在共享磁盘上创建卷组。有关详细信息，请参见卷组创建示例 (第 148 页)。
- 确保群集节点和包 IP(虚拟 IP)位于相同的子网上。
- 如果环境中有 DNS，则确保将群集中的所有节点和包 IP 都注册到 DNS 服务器。

配置主 Cell Manager

步骤

1. 启动群集：

   ```
   cmruncl
   ```

2. 激活卷组。

   HP-UX：

   ```
   vgchange -a e vg_name
   ```

   Linux：

   ```
   vgchange -a y vg_name
   ```

3. 将逻辑卷装载到装载点目录(例如， /omni_shared)。

   ```
   mount lv_path /omni_shared
   ```

4. 修改 /etc/opt/omni/server/sg/sg.conf 模板文件。

   > **注意：**
   > SHARED_DISK_ROOT 选项应包含装载点目录的名称(例如 SHARED DISK ROOT=/omni_shared)。
   >
   > CS_SERVICE_HOSTNAME 选项应包含虚拟 Cell Manager 的名称，因为网络已知该名称。群集中的每个包都需要有自己的虚拟 IP 地址及其网络名称(例如 CS_SERVICE HOSTNAME=ob2cl.company.com)。

5. 配置主 Cell Manager。运行脚本时，确保当前位置不在 /etc/opt/omni/ 或 /var/opt/omni/ 目录或其子目录中。还要确保 /etc/opt/omni/ 或 /var/opt/omni/ 中没有装载的子目录。运行：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary
   ```

   注意，运行此脚本之后，已停止 Data Protector 服务，并且随后将重新启动该服务。

6. 卸载装载点目录：

   ```
   umount dirname
   ```

7. 停用卷组：

   ```
   vgchange -a n vg_name
   ```

配置辅助 Cell Manager

步骤

1. 激活卷组。

   HP-UX：

   ```
   vgchange -a e vg_name
   ```

   Linux：

```
vgchange -a y vg_name
```

2. 将逻辑卷装载到装载点目录。

   ```
   mount lv_path /omni_shared
   ```

3. 配置辅助 Cell Manager：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname
   ```

   其中 *dirname* 表示装载点或共享目录(例如 `/omni_shared`)。

4. 卸载装载点目录：

   ```
   umount /omni_shared
   ```

5. 停用卷组：

   ```
   vgchange -a n vg_name
   ```

配置 Cell Manager 包

先决条件

- 在两个群集节点上都应安装并配置了 Data Protector Cell Manager。
- 配置 Data Protector 群集包之前，应创建并编辑一个群集配置文件。

旧包配置始终包括 2 个文件，包配置文件和包控制脚本。旧包配置文件作为 ASCII 文件创建，然后使用 `cmapplyconf` 命令存储在二进制 Serviceguard 配置中。模块化包配置文件将所有包文件系统、装载点和服务定义包含在单个文件中，该文件使用 `cmapplyconf` 命令存储在二进制 Serviceguard 配置中。

> **注意：**
> 任何一个群集节点上都不再运行 Data Protector 后台程序。

步骤

在主 Cell Manager 节点上执行以下步骤：

1. 检查群集配置文件(例如 `cluster.conf`)是否有错误：

   ```
   cmcheckconf -C /etc/cmcluster/cluster.conf
   ```

   如果有错误，则修复这些错误。

   如果没有错误，则启用该配置：

   ```
   cmapplyconf -C /etc/cmcluster/cluster.conf
   ```

2. 启动群集(如果尚未启动)：

   ```
   cmruncl
   ```

3. 创建和修改 Data Protector 群集包文件(配置和控制)。对于模块化包，创建并修改单个群集包文件(配置)。

   a. 在 `/etc/cmcluster` 目录中创建将容纳 Data Protector 包的目录：

      ```
      mkdir /etc/cmcluster/ob2cl
      ```

   b. 更改为 `/etc/cmcluster/ob2cl` 目录：

```
cd /etc/cmcluster/ob2cl
```

c. 对于旧包，在 Data Protector 包目录中创建包配置文件：

```
cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf
```

对于模块化包，使用该命令：

```
cmmakepkg -m sg/all ob2cl.conf
```

d. 只需要针对旧包执行此步骤。在 Data Protector 包目录中创建包控制文件：`cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl`。

e. 修改 Data Protector 包配置文件(例如，`/etc/cmcluster/ob2cl/ob2cl.conf`)。有关详细信息，请参见修改 Data Protector 包配置文件 (第 151 页)。

f. 只需要针对旧包执行此步骤。修改 Data Protector 包控制文件(例如，`/etc/cmcluster/ob2cl/ob2cl.cntl`)。有关详细信息，请参见修改 Data Protector 包控制文件 (第 153 页)。

4. 检查和传播 Data Protector 群集包文件。

a. 对于旧包，将包控制文件复制到群集中称为 system2 的另一个节点：

```
remsh system2 "mkdir /etc/cmcluster/ob2cl" rcp
/etc/cmcluster/ob2cl/ob2cl.cntl system2: /etc/cmcluster/ob2cl/ob2cl.cntl
```

b. 在所有群集节点上将 Data Protector 共享磁盘作为(先前创建的)群集卷组：

HP-UX：

```
vgchange -c y vg_name
```

Linux：

```
vgchange -a y vg_name
```

c. 检查 Data Protector 包：

```
cmcheckconf -P /etc/cmcluster/ob2cl/ob2cl.conf
```

如果检查成功，则添加 Data Protector 包：

```
cmapplyconf -P /etc/cmcluster/ob2cl/ob2cl.conf
```

d. 启动包：

```
cmrunpkg ob2cl
```

此时应形成群集，并且 Data Protector Cell Manager 包应正常运行。

5. 在主节点上，更新应用程序服务器的 IDB 和 Data Protector 域客户机中的群集主机名。在第一个活动节点上运行以下命令一次：

```
#omnidbutil -config_unixCluster -clusterHost  <clusterHostName>
```

在群集节点上安装安装服务器

如果进行远程安装，则可以在辅助 Serviceguard 节点上安装 安装服务器 并使用。在 UNIX 系统上安装 安装服务器 (第 39 页)。

> **注意：**
> 如果在将主节点配置为群集感知 Cell Manager 之前对安装服务器进行安装，请确保将安装服务器安装在每个辅助群集节点上。在配置主节点期间，会使用虚拟服务器名称导入安装服务器。如果安装服务器并未在每个群集节点上安装，则必须从安装

> 服务器的列表中导出安装服务器的虚拟服务器名称。另外，在群集感知 Cell Manager 的配置完成之后，必须导入每个相应的物理群集节点名称。

安装群集感知客户机

> **重要：**
> 所有群集节点上都必须安装 Data Protector 群集感知客户机。

安装过程是在 UNIX 客户机上安装 Data Protector 的标准过程。有关详细说明，请参见 安装 HP-UX 客户机 (第 64 页)和 安装 Linux 客户机 (第 73 页)。

下面的步骤

完成安装之后，必须将虚拟服务器(在群集包中指定的主机名)导入 Data Protector 单元。请参见将群集感知客户机导入到单元 (第 170 页)。

有关如何配置备份设备、介质池或任何其他 Data Protector 配置任务的详细信息，请参见 *Data Protector 帮助*索引：“配置”。

卷组创建示例

在两个 Cell Manager 均可访问的共享磁盘上创建卷组。

> **注意：**
> 如果要使用 ob2 磁盘作为群集锁磁盘，则应已为其创建了卷组。

主节点步骤

在主节点上执行以下步骤：

1. a. 为新卷组创建一个目录：

   ```
   mkdir vg_name
   ```

   > **注意：**
   > vg_name 是 /dev 目录的一个子目录中的卷组的路径名。

   b. 列出系统中现有的所有卷组，以检查哪些次要编号正在使用中：

   ```
   ll /dev/*/group
   ```

   c. 为卷组创建组文件：

   ```
   mknod vg_name/group c 64 0xNN0000
   ```

   > **注意：**
   > NN 是可用的次要编号。

   d. 在 Data Protector Cell Manager 使用的磁盘上创建物理卷：

   ```
   pvcreate -f pv_path ...
   ```

> **注意：**
> pv_path 与 pvcreate 命令一起使用，引用 /dev/rdsk 目录的子目录中的物理卷的字符(原始)设备路径名称(例如物理卷 c0t1d0 的 character pv_path 为 /dev/rdsk/c0t1d0)。

e. 创建新的卷组：

```
vgcreate vg_name pv_path ...
```

> **注意：**
> pv_path 与 vgcreate 命令一起使用，引用分配到新卷组的物理卷的块设备路径名称。位于 /dev/dsk 目录的子目录中(例如物理卷 c0t1d0 的 block pv_path 为 /dev/dsk/c0t1d0)。

2. 为此组创建逻辑卷。
   a. 为卷组创建新的逻辑卷：

```
lvcreate -L lv_size -n lv_name vg_name
```

> **注意：**
> 此处提供 /etc/opt/omni 和 /var/opt/omni Data Protector 目录。
> *lv_size* 是表示分区大小的数字(以 MB 为单位)。
> *lv_name* 是逻辑卷的名称。

   b. 在逻辑卷上创建日记文件系统：

```
newfs -F FStype lv_path
```

> **注意：**
> *FStype* 指定要在其上进行操作的文件系统类型。
> *lv_path* 是逻辑卷的字符(原始)特殊设备路径名称。

3. 根据群集文档设置卷组属性。

HP-UX：

   a. 从常规模式取消激活卷组：

```
vgchange -a n vg_name
```

   b. 标记供群集使用的卷组：

```
vgchange -c y vg_name
```

> **注意：**
> 如果这是群集锁磁盘，并且您正在使用新版的 Serviceguard(例如，11.09)，则自动标记群集的卷组。

   c. 以独占模式使用卷组：

```
vgchange -a e vg_name
```

Linux：

   a. 从常规模式取消激活卷组：

```
vgchange -a n vg_name
```

b. 标记供群集使用的卷组：

```
vgchange -a y vg_name
```

4. 创建一个装载点目录(例如 /omni_shared)，然后将逻辑卷装载到此目录：
   a. `mkdir shared_dirname`
   b. `mount lv_path shared_dirname`
5. 卸载装载点目录：

   ```
   umount shared_dirname
   ```
6. 取消激活所创建的卷组：

   ```
   vgchange -a n vg_name
   ```
7. 导出在主 Cell Manager 上创建的卷组。
   a. 从 system1 导出 LVM 配置信息：

   ```
   vgexport -p -m mapfile vg_name
   ```

   > **注意：**
   > 在这里，*mapfile* 指定必须将逻辑卷名称和编号写入到的文件的路径名。

   b. 将映射文件传输到 system2：

   ```
   rcp mapfile second_system: mapfile
   ```

辅助节点步骤

在辅助节点上执行以下步骤：

1. 创建要导入的卷组，并将其导入。
   a. 为新卷组创建一个目录：

   ```
   mkdir vg_name
   ```

   > **注意：**
   > *vg_name* 是位于 /dev 目录的一个子目录中的卷组的路径名。

   b. 列出系统中现有的所有卷组，以检查哪些次要编号正在使用中：

   ```
   ll /dev/*/group
   ```

   c. 为卷组创建组文件：

   ```
   mknod vg_name/group c 64 0xNN0000
   ```

   > **注意：**
   > NN 是可用的次要编号。

   d. 导入卷组：

   ```
   vgimport -m mapfile -v vg_name pv_path ...
   ```

   > **注意：**
   > *mapfile* 是要从中读取逻辑卷名称和编号的文件的名称。
   > *pv_path* 是物理卷的块设备路径名称。

2. 设置卷组属性。

HP-UX：

a. 从常规模式取消激活卷组：

```
vgchange -a n vg_name
```

b. 标记供群集使用的卷组：

```
vgchange -c y vg_name
```

> **注意：**
> 如果这是群集锁磁盘，并且您正在使用新版的 Serviceguard(例如， 11.09)，则自动标记群集的卷组。

c. 以独占模式使用卷组：

```
vgchange -a e vg_name
```

Linux：

a. 从常规模式取消激活卷组：

```
vgchange -a n vg_name
```

b. 标记供群集使用的卷组：

```
vgchange -a y vg_name
```

3. 创建装载点目录(与主 Cell Manager 上创建的相同)，然后将逻辑卷装载到此目录。
4. 卸载装载点目录：

```
umount shared_dirname
```

5. 取消激活所导入的卷组：

```
vgchange -a n vg_name
```

修改 Data Protector 包配置文件

在 Data Protector 模块化包配置文件中，修改以下字段：

例如：

package_name	ob2cl
run_script_timeout	600
halt_script_timeout	600
script_log_file	/usr/local/cmcluster/conf/ob2cl/ob2cl.log

子网设置如下所示：

例如：

monitored_subnet	10.81.0.0
ip_subnet	10.81.0.0
ip_address	10.81.8.46

> **注意：**
> monitored_subnet 是包括群集节点的子网。
>
> ip_subnet 是包括 Data Protector Cell Manager 虚拟服务器 IP 的子网。
>
> ip_address 是 Data Protector Cell Manager 虚拟服务器 IP。

Data Protector 服务设置如下所示：

例如：

service_name	dp_svc
service_cmd	/opt/omni/sbin/csfailover.ksh start
service_restart	None
service_fail_fast_enabled	no
service_halt_timeout	300

> **注意：**
> service_cmd 必须设置为 /opt/omni/sbin/csfailover.ksh start。

Data Protector 共享的文件系统信息如下所示：

例如：

vg	DP
fs_name	/dev/DP/vol
fs_directory	/DPCLUS
fs_type	ext3
fs_mount_opt	-o rw
fs_umount_opt	""
fs_fsck_opt	""

在 Data Protector 旧包配置文件中，修改以下字段：

PACKAGE_NAME

NODE_NAME

RUN_SCRIPT(与 Data Protector 包控制文件相同。)

HALT_SCRIPT(与 Data Protector 包控制文件相同。)

MONITORED_SUBNET

SERVICE_NAME(您可以输入任何名称，但在控制文件中也必须使用相同名称。)

SERVICE_FAIL_FAST_ENABLED

SERVICE_HALT_TIMEOUT

例如：

PACKAGE_NAME	ob2cl
NODE_NAME	onca
NODE_NAME	pardus
RUN_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
HALT_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
MONITORED_SUBNET	10.17.0.0
SERVICE_NAME	omni_sv
SERVICE_FAIL_FAST_ENABLED	NO
SERVICE_HALT_TIMEOUT	300

修改 Data Protector 包控制文件

在 Data Protector 旧包控制文件中，修改以下字段：

VG [n]

LV [n]

FS [n]

FS_MOUNT_OPT [n]

IP

SUBNET

SERVICE_NAME(与配置文件中使用的相同。)

SERVICE_CMD(必须为： /opt/omni/sbin/csfailover.ksh start)

例如：

VG[0]	vg_dp
LV[0]	/dev/vg_dp/dp_share
FS[0]	/DP_SHARE
FS_MOUNT_OPT[0]	-o rw
FS_TYPE[0]	vxfs
IP[0]	10.17.17.69
SUBNET[0]	10.17.0.0
SERVICE_NAME[0]	omni_sv

SERVICE_CMD[0]	/opt/omni/sbin/csfailover.ksh start

在 Symantec Veritas Cluster Server 上安装 Data Protector

Data Protector 支持适用于 Linux 的 Symantec Veritas Cluster Server (VCS)。 有关支持的操作系统版本的详细信息，请参见最新的*Data Protector 平台和集成支持矩阵*。

> **注意：**
> 如果您已配置 Data Protector 服务组 IP，使用该 IP 进行许可。 如果您在配置 Data Protector 服务组时未使用 IP 地址，使用 Veritas Cluster IP 进行许可。

配置阶段

1. 配置主 Cell Manager
2. 配置辅助 Cell Manager
3. 配置 Cell Manager 群集服务组

安装群集感知 Cell Manager

先决条件

在 VCS 上安装 Data Protector Cell Manager 之前，请检查以下各项：

- 确定主和辅助 Cell Manager 系统。 它们全部都必须安装 Symantec Veritas Cluster Server，并且必须配置为群集成员。
- 在主节点和每个辅助节点上，都必须安装 Data Protector Cell Manager(带有建议的补丁)，以及要在群集中部署的集成的所有其他 Data Protector 软件组件。
- 用户组 hpdp 和专用用户帐户 hpdp 在两个节点上必须具有相同 ID。
- 在群集环境中，Data Protector Cell Manager 必须具备其自己的群集服务组，该服务组必须在群集感知的 Cell Manager 配置之前创建和准备。 在 VCS 中安装 Data Protector Cell Manager 之前，您需要获取虚拟服务器名称及相应的 IP。 之后，该服务器名称或 IP 用作 Data Protector Cell Manager 虚拟服务器名称或 Data Protector 服务组 IP。
- 确保群集节点和 Data Protector 服务组 IP(虚拟 IP)位于相同的子网上。

  > **注意：**
  > 确保 Data Protector 服务组 IP 和 Veritas Cluster IP 不同。

- 如果环境中有 DNS，则确保将群集中的所有节点和 Data Protector 服务组 IP 都注册到 DNS 服务器。
- 完成安装之后，必须对已安装的主 Cell Manager 和辅助 Cell Manager，以及 Cell Manager 程序包进行配置。

为 Data Protector Cell Manager 准备群集服务组

您可以通过以下资源创建群集 (Data Protector) 服务组：

- IP 群集资源 — 是指用于 IP 资源配置的虚拟 IP。
- 装载群集资源 — 是指带有相应从属资源的装载资源，用于控制共享卷，在共享磁盘上创建，可通过所有节点访问，其中可能运行 Data Protector。 该共享卷用于节点之间共享的 Data Protector 配置和数据文件。

配置主 Cell Manager

步骤

1. 在主节点上启动 Data Protector 服务组。
2. 修改 /etc/opt/omni/server/sg/sg.conf 模板文件。

   注意：
   SHARED_DISK_ROOT 选项应包含装载点目录的名称(例如 SHARED_DISK_ROOT=/omni_shared)。

   CS_SERVICE_HOSTNAME 选项必须包含虚拟 Cell Manager 的名称，因为网络已知该名称。 (例如 CS_SERVICE_HOSTNAME=dpvcs.company.com)。
3. 配置主 Cell Manager。 确保不从 /etc/opt/omni/ 或 /var/opt/omni/ 目录或其子目录执行脚本。 还要确保 /etc/opt/omni/ 或 /var/opt/omni/ 目录中未装载子目录。 请执行以下命令：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary
   ```

   注意：
   运行此脚本之后，已停止 Data Protector 服务，并且随后将重新启动该服务。

配置辅助 Cell Manager

步骤

1. 将 Data Protector 服务组切换到辅助节点。
2. 配置辅助 Cell Manager：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname
   ```

   其中 *dirname* 表示装载点或共享目录(例如 /omni_shared)。

配置 Cell Manager 群集服务组

步骤

1. 将 Data Protector 服务组切换回到主节点。
2. 添加群集应用程序资源，该资源将用于监控和控制 Data Protector 服务至 Data Protector 服务组并使用 vcsfailover.ksh 脚本作为应用程序监控或控制程序。 例如，

```
Application dpapp (
StartProgram = "/opt/omni/sbin/vcsfailover.ksh start"
StopProgram = "/opt/omni/sbin/vcsfailover.ksh stop"
CleanProgram = "/opt/omni/sbin/vcsfailover.ksh stop"
MonitorProgram = "/opt/omni/sbin/vcsfailover.ksh monitor"
 )
```

> **注意：**
> 如果 vcsfailover.ksh 脚本需要自定义，必须创建该脚本的副本并用作监控或控制程序。 在升级或更新期间，原始脚本被覆盖，必须通过新引入的更改(如有)手动更新自定义的脚本。

3. 创建 Data Protector 应用程序资源。

> **注意：**
> 使 Data Protector 应用程序资源依赖于装载和虚拟服务器 IP 字段。

4. 启用并启动 Data Protector 应用程序资源。

在群集节点上安装安装服务器

可以在辅助 Symantec Veritas Cluster Server 节点上安装 安装服务器 并使用，以进行远程安装。 在 UNIX 系统上安装 安装服务器 (第 39 页)。

> **注意：**
> 如果在将主节点配置为群集感知 Cell Manager 之前对安装服务器进行安装，请确保将安装服务器安装在每个辅助群集节点上。 在配置主节点期间，会使用虚拟服务器名称导入安装服务器。 如果安装服务器并未在每个群集节点上安装，则必须从安装服务器的列表中导出安装服务器的虚拟服务器名称。 另外，在群集感知 Cell Manager 的配置完成之后，必须导入每个相应的物理群集节点名称。

安装群集感知客户机

此安装步骤是在客户机系统上安装 Data Protector 的标准步骤。 有关详细说明，请参见安装 Data Protector 客户机 (第 49 页)。

下面的步骤

完成安装之后：

- 要备份虚拟服务器，应该将其导入到单元。
- 要备份物理节点，也应该将其导入单元。

请参见将群集感知客户机导入到单元 (第 170 页)。有关如何配置备份设备、介质池或任何其他 Data Protector 配置任务的详细信息，请参见《*Data Protector 帮助*》的索引："配置"。

在 Microsoft 群集服务器上安装 Data Protector

有关 Microsoft 群集服务器集成的最新受支持操作系统，请参见 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword= 上最新的支持矩阵。

> **注意：**
> 如果 Cell Manager 需要以群集感知模式运行，请对许可证使用 Cell Manager 的虚拟服务器 IP 地址。

安装群集感知 Cell Manager

先决条件

安装群集感知 Data Protector Cell Manager 之前，必须满足以下先决条件：

- 必须在所有群集节点上都正确安装了群集功能。例如，必须能够根据需要多次将组从一个节点移动到另一个节点，而不会产生有关共享磁盘的问题。
- 确保群集上不存在具有以下名称的资源：

  OBVS_MCRS、OBVS_HPDP_AS、OBVS_HPDP_IDB、OBVS_HPDP_IDB_CP 和 OmniBack_Share。

  Data Protector 将这些名称用于 Data Protector 虚拟服务器。如果存在此类资源，请删除或重命名它们。

  可以通过以下步骤完成该操作：

  1. 单击**开始 > 程序 >管理工具 > 群集管理员**。
  2. 检查资源列表，并根据需要删除或重命名这些资源。
- 至少应为群集中的一个组定义文件群集资源。Data Protector 会将其某些数据文件安装在此文件群集资源中的某个特定文件夹下。

  Windows Server 2008、Windows Server 2012： 数据文件安装在用户安装时选择的共享文件夹下的*文件服务器*资源中。

  其他 Windows 系统： 数据文件安装在创建文件群集资源时指定的文件夹下的*文件共享*资源中。

  有关如何定义文件群集资源的说明，请参见特定于群集的文档。请注意，文件群集资源的文件共享名称不能为 OmniBack。
- 如果与文件群集资源相同的组中不存在虚拟服务器，则使用免费注册的 IP 地址和与之

关联的网络名称来创建新的虚拟服务器。

- Data Protector 要安装到的文件群集资源必须在文件群集资源依赖关系中设置 IP Address、Network Name和Physical Disk。这可确保 Data Protector 群集组能够在独立于任何其他组的任意节点上运行。
- 应当只有群集管理员有权访问文件群集资源的共享文件夹，并且它们应具有对于共享文件夹的完全访问权。
- 在所有群集节点上，Data Protector 将安装在相同的位置(驱动器和路径名)。请确保这些位置可供使用。
- 如果要从网络共享启动群集感知 Cell Manager 安装，则必须具有从所有群集节点访问此共享的权限。
- 请确保在任何群集节点上，不运行任何其他基于 Microsoft Installer 的安装。
- 群集的每个系统(节点)应正在运行，并且正常工作。
- 为了能够在服务器群集(具有在 Windows Server 2008 或 Windows Server 2012 上运行的 Microsoft Cluster Service (MSCS))上安装群集感知 Data Protector Cell Manager，请执行准备在运行 Windows Server 2008 或 Windows Server 2012 的 Microsoft 服务器群集上安装 Data Protector (第 308 页)中所述的过程。

注意事项

- 安装程序必须使用文件群集资源处于活动状态的系统(节点)上的群集服务帐户启动，以便可以直接访问文件群集资源的共享文件夹。可以使用群集管理器确定资源所有者(其中资源处于活动状态的系统)。
- 要正确安装和配置群集感知 Data ProtectorCell Manager，在安装期间必须提供具有以下用户权限的域帐户：
  - Cell Manager 系统上的管理员权限
  - 群集中的群集管理员权限
  - 密码永不过期
  - 作为服务登录
  - 用户无法更改密码
  - 允许所有登录时间

  > **重要：**
  > 对于 Microsoft 群集服务器安装，需要在所有群集系统(节点)上都具有管理员权限的帐户。您还应使用此帐户来安装 Data Protector。否则会导致 Data Protector 服务以普通模式而非群集感知模式运行。

- 在所有群集节点上必须赋予用于 Inet 服务的 Windows 域用户帐户以下 Windows 操作系统安全策略特权：
  - 身份验证后模拟客户机

- 替换进程级别令牌

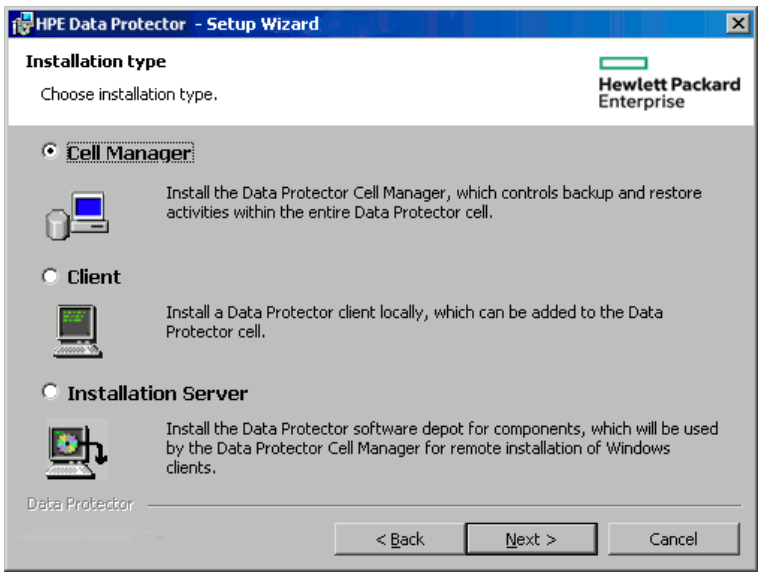
请参见 *Data Protector 帮助*索引：“Inet 用户模拟”。

本地安装过程

群集感知 Data Protector Cell Manager 必须从安装包进行本地安装。请执行以下操作：

1. 将下载的安装程序包 (zip) 复制到 Windows 系统上，然后将文件提取到本地目录。从适用于您平台的文件夹运行 `setup.exe` 文件。
2. 按照安装向导操作，并仔细阅读许可协议。如果接受协议的条款，则单击**下一步 (Next)** 继续。
3. 查看“过时信息”页面中的详细信息，然后单击**我了解对所支持平台的更改**，前提是您接受 Data Protector 对支持的硬件和软件版本列表所做的更改。
4. 在“安装类型”页中，选择 **Cell Manager**，然后单击**下一步**安装 Data ProtectorCell Manager 软件。

   选择安装类型

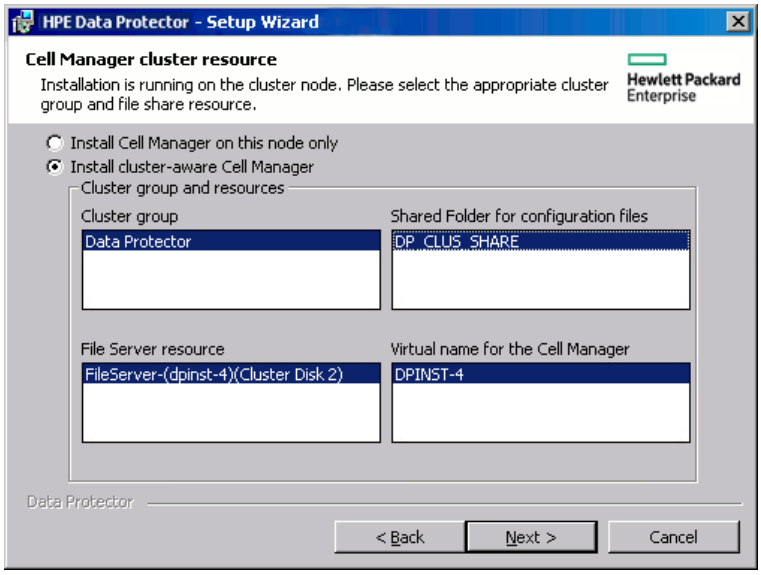
   

5. 安装程序会自动检测它是否是在群集环境中运行。选择**安装群集感知 Cell Manager** 来支持群集安装。

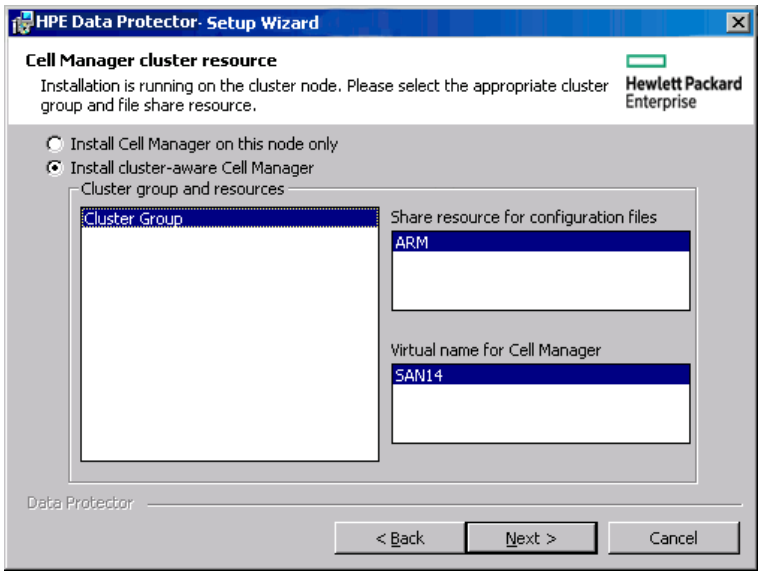
   选择群集组、虚拟主机名，以及 Data Protector 共享文件和数据块将驻留的文件群集资源。

   > **注意：**
   > 如果选择**仅在该节点安装 Cell Manager**，Cell Manager 将*不是*以群集感知模式运行。请参见安装 Windows Cell Manager (第 32 页)。

   在 Windows Server 2008 上选择群集资源

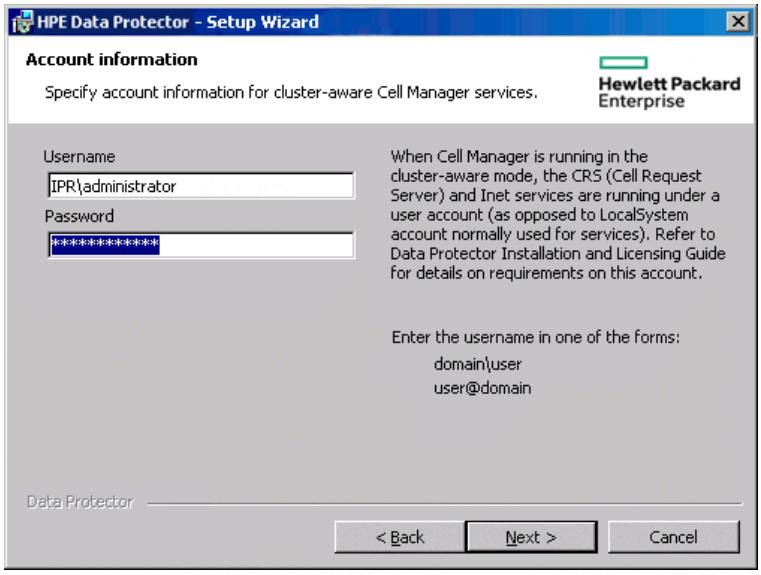


在其他 Windows 系统上选择群集资源



6. 输入将用于启动 Data Protector 服务的帐户的用户名和密码。

输入帐户信息



7. 单击**下一步 (Next)** 将 Data Protector 安装到默认安装文件夹中。

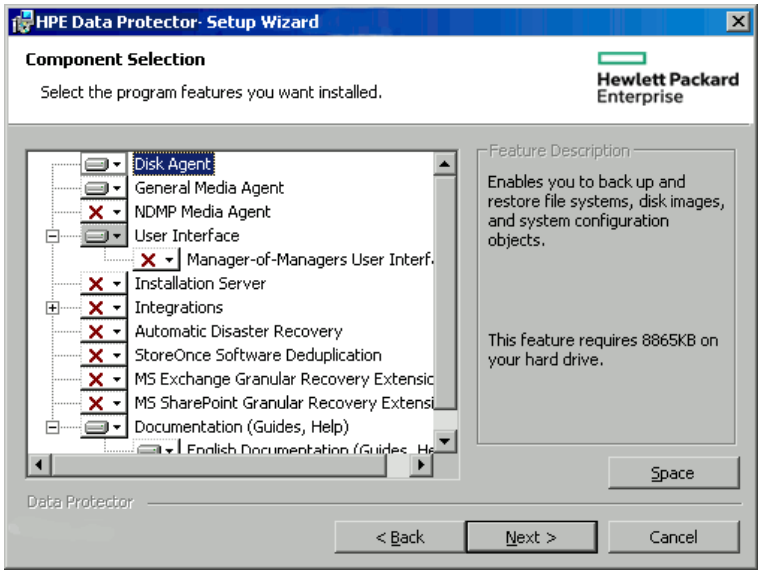
   或者单击**更改 (Change)** 打开“更改当前目标文件夹 (Change Current Destination Folder)”或“更改当前程序数据目标文件夹 (Change Current Program Data Destination Folder)”对话框，然后根据需要更改安装文件夹。指向程序数据安装文件夹的路径不得超过 80 个字符。

8. 在“组件选择”窗口中，选择要在所有群集节点和群集虚拟服务器上安装的组件。单击**下一步 (Next)**。

   此时将自动安装 MS 群集支持文件。

   选定组件将安装到所有群集节点上。

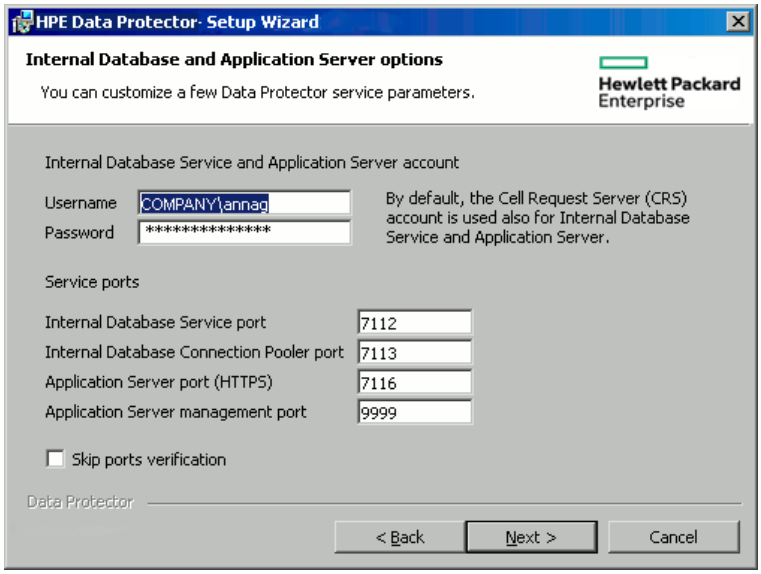
   组件选择页面



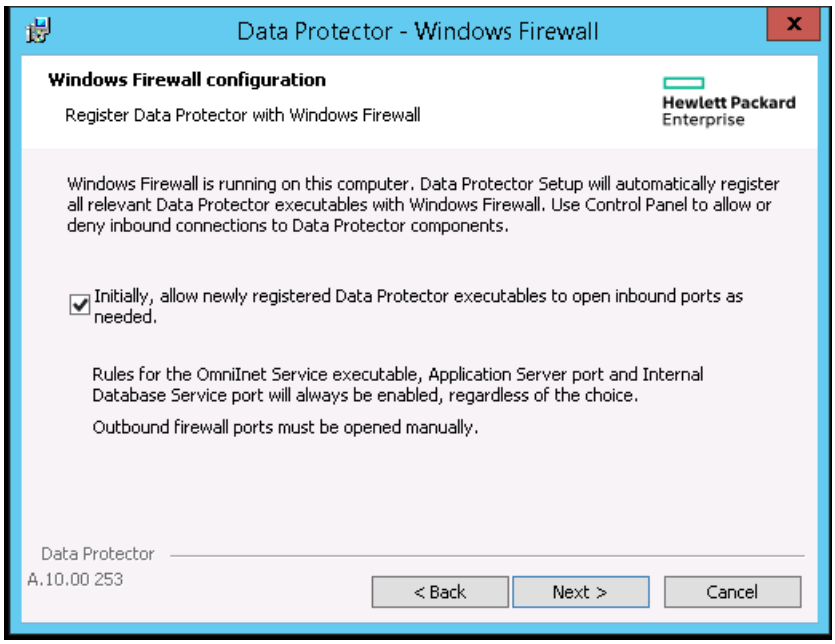
9. 此外，还可以更改用户帐户或 Data Protector 服务内部数据库服务和应用程序服务器所使用的端口。

单击**下一步 (Next)**。

更改 IDB 和应用程序服务器选项



10. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，**最初，允许新注册的 Data Protector 可执行文件按需打开入站端口**选项已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的 10.00 客户机的 Data Protector，必须启用 Windows 防火墙中的 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。

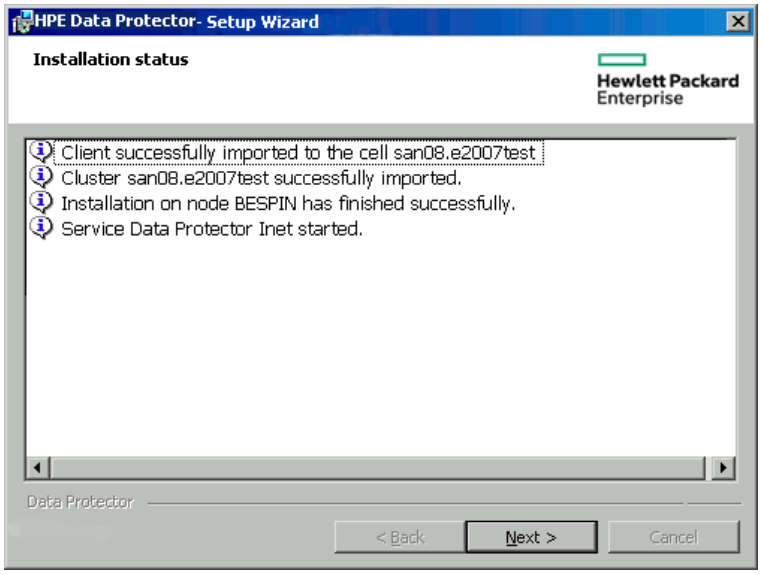


单击**下一步 (Next)**。

11. 此时会显示组件选择摘要页。单击**安装 (Install)**。

12. 此时会显示“安装设置”页。单击**下一步 (Next)**。

    安装状态页面



13. 如果已安装User Interface组件，要在设置后立即开始使用 Data Protector GUI，请选择**启动 Data Protector GUI**。

    如果已安装English Documentation (Guides, Help)组件，并要在设置后立即查看Data Protector产品声明、软件说明和参考，请选择**打开产品声明、软件说明和参考**。

14. 单击**完成 (Finish)** 完成安装。

安装适用于 Windows 2012 和 Windows 2012 R2 群集的群集感知 Cell Manager

要安装群集感知 **Cell Manager**，请执行以下操作：

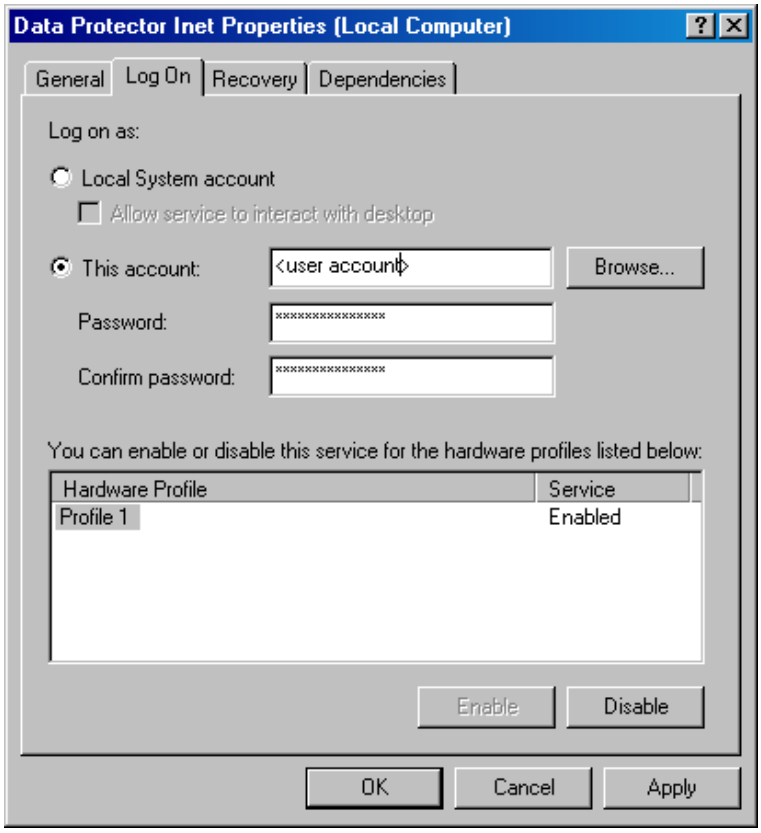
1. 在不属于群集一部分的计算机上安装 Data Protector 安装服务器。
2. 在其上应用最新的补丁。安装服务器的‘\DP_Program_data\Depot’中的仓库可用于在 Windows 2012 和 2012 R2 系统中安装群集感知 Cell Manager。
3. 将仓库复制到任一群集节点，并从本地磁盘开始安装。
4. 或者，也可以使用网络共享访问仓库，并从该共享开始安装。对于此步骤，需要考虑以下各项：
   - 安装服务器应当与群集位于相同的域中。
   - 不应使用管理(隐藏)共享(\\hostname or IP address of IS\c$\...)，因为在某些情况下，它们不可从其他群集节点访问。因此，应当使用正常路径(\\hostname or IP address of IS\depot)，且所有群集节点均应共享该路径。
   - 群集节点应当无需任何密码即可连接到正常的网络路径。
   - 正常的网络路径应当可从浏览器访问，且无需提供凭据。如果提示需要凭据，请输入凭据并选择“记住凭据”。

检查安装

完成安装过程之后，可以检查 Data Protector 软件是否已正确安装。请执行以下操作：

1. 检查在每个群集节点上，是否为 Data Protector Inet 服务分配了 Cluster 服务帐户。确保 Data Protector admin 用户组中也添加了同一用户。登录帐户类型应设置为This account，如Data Protector 用户帐户 (第 164 页)中所示。

   Data Protector 用户帐户



2. 请执行以下命令：

   `omnirsh` *host* `INFO_CLUS`

   其中，*host* 是群集虚拟服务器的名称(区分大小写)。输出将会列出群集中的系统的名称，以及虚拟服务器的名称。如果输出返回 `0 "NONE"`，则表明不是在群集感知模式下安装的 Data Protector。

3. 启动 Data Protector GUI，选择**客户机 (Clients)** 上下文，然后单击**MS 群集 (MS Clusters)**。可以看到"结果区域"中列出新安装的系统。

Data Protector Inet 和 CRS 服务

如果需要，请更改运行 Data Protector Inet 和 CRS 服务的帐户。

安装群集感知客户机

先决条件

安装群集感知 Data Protector 客户机之前，必须满足以下先决条件：

- 必须在所有群集节点上都正确安装了群集功能。例如，必须能够根据需要多次将组从一个节点移动到另一个节点，而不会产生有关共享磁盘的问题。
- 群集的每个系统应正在运行，并且正常工作。
- 为了能够在服务器群集(具有在 Windows Server 2008 或 Windows Server 2012 上运行的 Microsoft Cluster Service (MSCS))上安装群集感知 Data Protector 客户机，请执行准备在运行 Windows Server 2008 或 Windows Server 2012 的 Microsoft 服务器群集上安装 Data Protector (第 308 页)中所述的过程。

本地安装过程

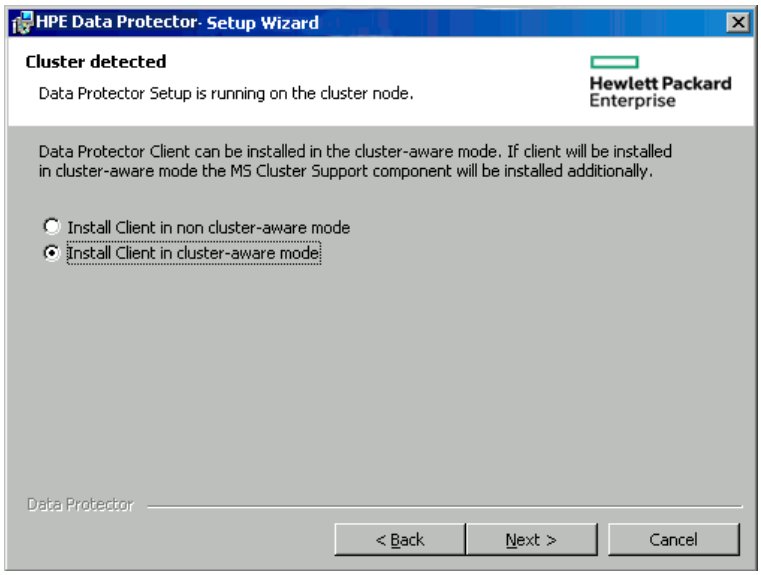
群集感知的 Data Protector 客户机必须在每个群集节点上通过安装包在本地进行安装。群集节点(Data Protector 群集客户机)会在安装期间被导入指定的单元。之后，您需要导入虚拟服务器名称。

执行安装需要群集 Administrator 帐户。除此之外，群集客户机安装与普通 Windows 客户机的安装方式相同。此时将自动安装 MS 群集支持文件。

有关如何在本地安装 Data Protector Windows 客户机系统的信息，请参见安装 Windows 客户机 (第 55 页)。

Data Protector 安装会报告检测到群集。选择**以群集感知模式安装客户机 (Install client in cluster-aware mode)**。

选择群集感知安装模式



如果要安装 Data Protector Oracle 集成，则必须在所有群集节点上和 Oracle 资源组的虚拟服务器上执行安装步骤。

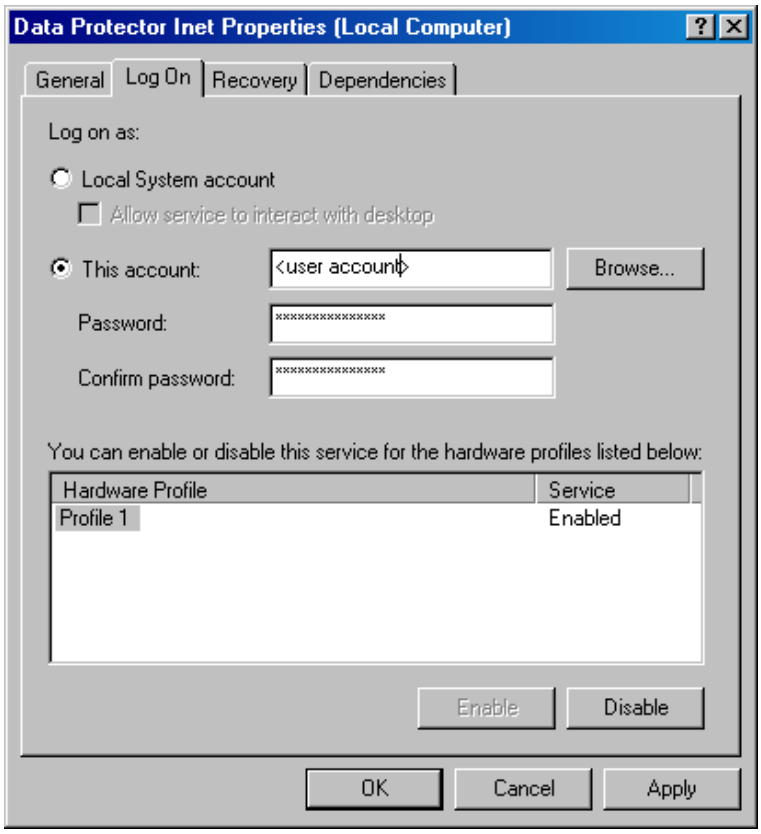
> **注意：**
> 您可以将群集感知客户机导入使用标准 Cell Manager 或群集感知 Cell Manager 管理的 Data Protector 单元。

检查安装

完成安装过程之后，可以检查 Data Protector 软件是否已正确安装。请执行以下操作：

1. 检查在每个群集节点上，是否为 Data Protector `Inet` 服务分配了 Cluster 服务帐户。确保 Data Protector `admin` 用户组中也添加了同一用户。登录帐户类型应设置为**本帐户**，如Data Protector 用户帐户 (第 166 页)中所示。

   Data Protector 用户帐户

2. 执行：

   `omnirsh` *`host`* `INFO_CLUS`

   其中，*host* 是群集客户机系统的名称。输出将会返回群集感知客户机系统的名称。如果输出返回 `0 "NONE"`，则表明不是在群集感知模式下安装的 Data Protector。

Veritas Volume Manager

如果在群集中安装了 Veritas Volume Manager，则在 Microsoft Cluster Server 上完成 Data Protector 的安装之后，还需要执行另外一些步骤。有关应执行的其他步骤，请参见在带 Veritas Volume Manager 的 Microsoft 群集服务器上安装 Data Protector (第 310 页)。

下面的步骤

完成安装之后，必须将虚拟服务器主机名(群集感知应用程序)导入 Data Protector 单元。请参见将群集感知客户机导入到单元 (第 170 页)。

有关如何配置备份设备、介质池或任何其他 Data Protector 配置任务的详细信息，请参见 *Data Protector 帮助*索引：“配置”。

更改 **Inet** 和 **CRS** 帐户

如果需要，请更改运行 Data Protector `Inet` 和 `CRS` 服务的帐户。

在 IBM HACMP Cluster 上安装 Data Protector

Data Protector 支持适用于 AIX 的 IBM 高可用性群集多处理。

> **重要：**
> 在所有群集节点上安装 Data Protector 磁带客户机组件。

安装群集感知客户机

要在群集节点上安装 Data Protector 组件，请使用在 UNIX 系统上安装 Data Protector 的标准步骤。有关详细信息，请参见远程安装 (第 83 页)或在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)。

下面的步骤

安装之后，将群集节点和虚拟服务器(虚拟环境包 IP 地址)导入 Data Protector 单元。请参见将群集感知客户机导入到单元 (第 170 页)。

有关如何配置备份设备、介质池或任何其他 Data Protector 配置任务的信息，请参见《*Data Protector 帮助*》的索引：“配置”。

在 Microsoft Hyper-V 群集上安装 Data Protector

在集群中使用 Microsoft 故障转移群集功能配置的 Microsoft Hyper-V 系统上安装 Data Protector，与在 Microsoft Cluster Server 上安装 Data Protector 是相似的；Microsoft Hyper-V 系统必须成为 Data Protector 群集感知客户机。有关详细信息，请参见在 Microsoft 群集服务器上安装 Data Protector (第 157 页)。

> **注意：**
> 一旦 Microsoft Hyper-V 系统成为群集感知客户机，您便可以使用 Data Protector 安装服务器远程安装任何其他 Data Protector 组件。

第 6 章： 维护安装

本章描述了最常用的修改备份环境配置的步骤。 各节将提供以下相关信息：

- 使用维护模式的方式和时间
- 如何使用图形用户界面将客户机导入到单元。
- 如何使用图形用户界面将 安装服务器 导入到单元。
- 如何使用图形用户界面导入群集/虚拟服务器。
- 如何使用图形用户界面导出客户机。
- 如何使用图形用户界面保证安全性。
- 如何在 Data Protector 中配置用于用户身份验证的 LDAP。
- 使用证书生成实用程序的方式和时间
- 如何管理 Data Protector 补丁包和识别已安装的 Data Protector 补丁
- 如何卸载 Data Protector 软件
- 如何添加或删除 Data Protector 软件组件

Data Protector 维护模式

在 Cell Manager 上执行维护任务期间，应阻止对内部数据库进行写入操作，需要 Data Protector 进入维护模式。此类任务包含升级 Data Protector 安装、安装补丁和重要修补程序、升级硬件或操作系统。在本章中，只有特定的步骤需要使用维护模式。但事实上，维护模式同样适用于整个文档在其他部分描述的任务。

进入维护模式过程可自动启动一系列任务，例如停止调度程序、重命名备份规范目录、中止正在运行的进程和释放锁定的资源。单个单元、MoM 和群集环境中支持维护模式。

启动维护模式

维护模式可以由具有管理权限的用户通过命令行界面进行启动。要启动维护模式，请执行以下命令：

在单个单元中：

```
omnisv -maintenance [GracefulTime]
```

在 MoM 环境中：

```
omnisv -maintenance -mom
```

Cell Manager 指示运行会话一次全部停止，同时 MoM 环境中的单元逐一进入维护模式。

要自定义 Cell Manager 进入维护模式的方式，请修改相应的全局选项。 MaintenanceModeGracefulTime 选项反映了用于中止运行会话的 Data Protector 服务的秒数，而 MaintenanceModeShutdownTime 选项则反映了等待会话中止所需要的秒数。两个选项的默认值均为 300。如果使用 *GracefulTime* 选项，则它将覆盖 MaintenanceModeGracefulTime 全局选项。如果在执行此选项后恢复会话仍在运行，则维护模式初始化失败。

如果 MoM 环境中任何单元未能进入维护模式，模式会恢复。

要检查 Data Protector 是否以维护模式运行，请通过执行 omnisv -status 或检查 GUI 状态栏查看 CRS 服务状态。注意，GUI 只有连接到 Cell Manager 时才能可靠地显示维护模式，这有时可能会导致即使在 Cell Manager 切换回正常模式后状态栏上依旧显示维护模式。

在维护模式期间，Cell Manager 拒绝所有将数据写入内部数据库的操作，例如创建新设备、备份和恢复会话或其预览、清除、复制和合并会话。

在群集环境中，维护模式处于活动状态时只能执行手动群集的相关活动，例如关闭群集包、停止 Data Protector 服务，或者手动装载卷。

维护模式处于活动状态时允许所有只读 IDB 操作。Data Protector 服务均已启动并正在运行。当 Cell Manager 处于维护模式时，只有具有管理 Data Protector 用户权限的用户可以连接到单元或 MoM。

退出维护模式

要使用 CLI 退出 Cell Manager 上的维护模式，请执行：

- 在单个单元中：

  ```
  omnisv -maintenance -stop
  ```

- 在 MoM 环境中：

  ```
  omnisv -maintenance –mom_stop
  ```

处于 MoM 环境中时，单个单元不能退出维护模式。只能从 MoM 服务器调用 MoM 维护。

要使用 GUI 退出维护模式，请执行以下操作：

1. 在“上下文列表 (Context List)”中，选择**客户机 (Clients)**。
2. 在**操作**菜单中，单击**停止维护模式**。

正常模式恢复后，可以重新启动已中止和拒绝的会话，因为它们已记录到 maintenance.log 文件中，该文件位于默认的 Data Protector 日志文件目录中。

以下两个示例显示了已中止和拒绝会话的 maintenance.log 条目：

```
10.5.2013 10:52:45  OMNISV.2492.9936
["/cli/omnisv/omnisv.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2
Session was aborted - graceful period expired!
session id:        2013/05/10-8
session type:      0
datalist:          large_backup
start date:        2013-05-10 10:52:45
owned by:          JOHN.JOHNSON@company.com

10.5.2013 10:48:45  CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $ $Date:: 2013-
03-22 18:00:03":142] X.99.01 b2
CRS is in maintenance mode - session rejected
session id:        R-2013/05/10-200
session type:      dbsm
session desc:      Database
start date:        2013-05-10 10:48:45
owned by:          .@ pid=0
```

当维护模式处于活动状态时，试图启动的会话将被记录为已中止。要运行中止后的会话，请执行以下操作：

1. 在上下文列表中，单击**内部数据库**。
2. 在“范围窗格”中，展开**设备**。
3. 右键单击会话，然后从上下文菜单中选择**重新启动失败的对象 (Restart Failed Objects)**

当 Cell Manager 进入维护模式时，会话在尝试启动时被记录为拒绝。要在随后运行被拒绝的会话，请手动重新启动每个会话。

将群集感知客户机导入到单元

在群集感知客户机上本地安装 Data Protector 软件后，将代表群集感知客户机的虚拟服务器导入到 Data Protector 单元。

先决条件

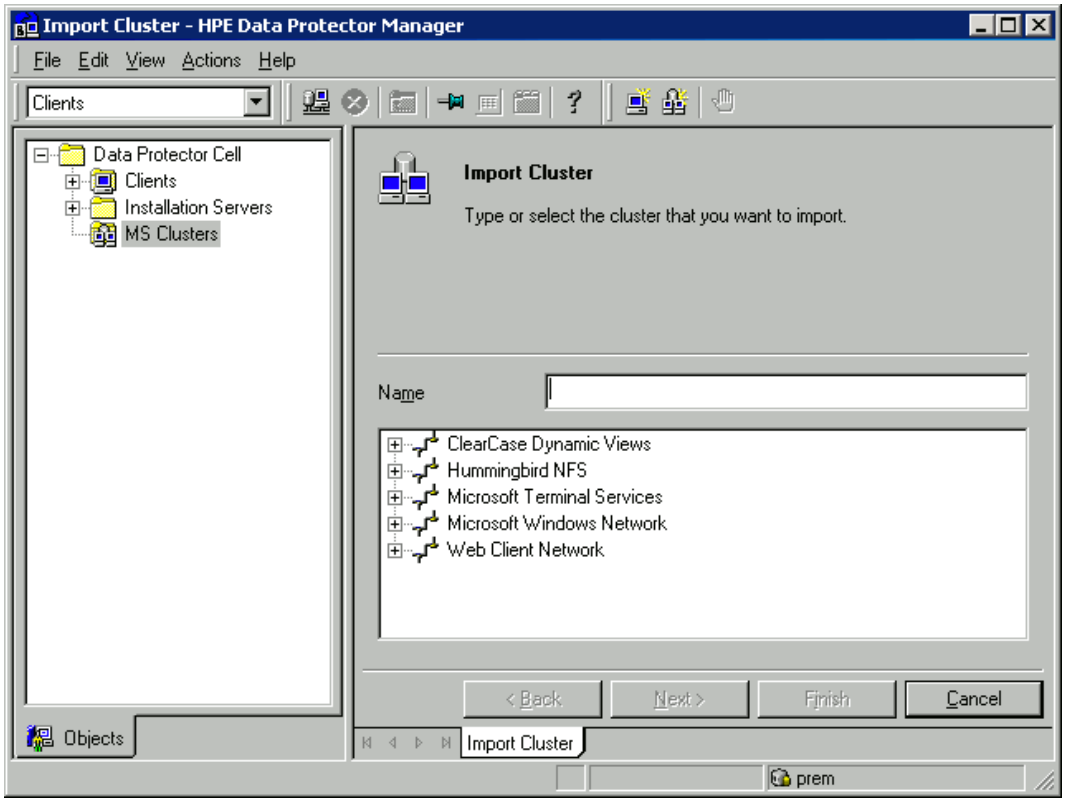
- 必须在所有群集节点上都安装 Data Protector。
- 所有群集包必须正在群集内运行。

Microsoft 群集服务器

将 Microsoft Cluster Server 客户机导入到 Data Protector 单元

1. 在 Data Protector Manager 中，切换到客户机上下文。
2. 在“范围窗格”中，右键单击 **MS 群集**，然后单击**导入群集**。
3. 输入代表要导入的群集客户机的虚拟服务器的名称，或浏览网络以选择虚拟服务器。

将 Microsoft Cluster Server 客户机导入到单元



4. 单击**下一步 (Next)**。
5. 单击**完成 (Finish)** 以导入群集客户机。

> **提示：**
> 要导入特定的群集节点或虚拟服务器，请在“范围窗格 (Scoping Pane)”中右键单击其群集并单击**导入群集节点 (Import Cluster Node)** 或**导入群集虚拟服务器 (Import Cluster Virtual Server)**。

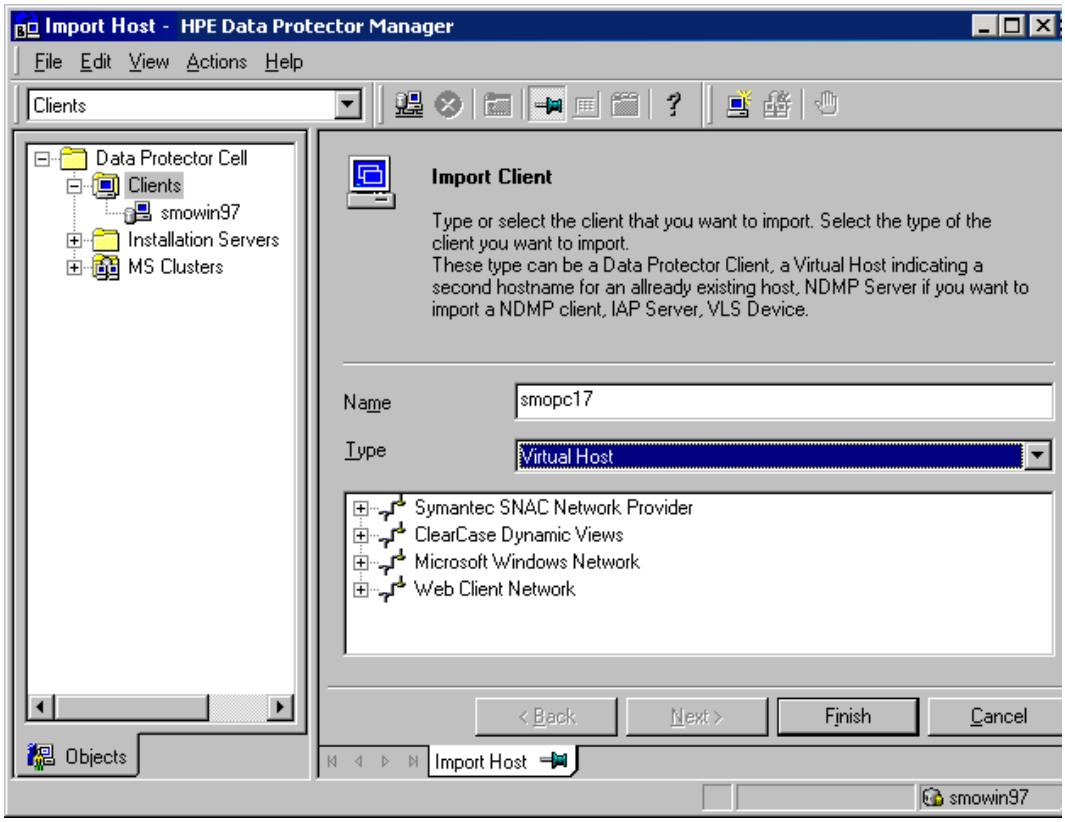
其他群集

将一个 **Serviceguard**、**Veritas** 或 **IBM HACMP** 群集客户机导入到 **Data Protector** 单元

1. 在 Data Protector Manager 中，切换到客户机上下文。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 键入虚拟服务器的主机名(如应用程序群集包中所指定)，或浏览网络以选择要导入的虚拟服务器(仅限 Windows GUI 中)。

   选择**虚拟主机**选项指明这是一个群集虚拟服务器。

将 Serviceguard 或 Veritas 客户机导入到单元



4. 单击**完成 (Finish)** 以导入虚拟服务器。

> **提示：**
> 要在群集节点的本地磁盘上配置数据备份，需要导入代表 Data Protector 客户机的群集节点。

从单元导出客户机

从 Data Protector 单元导出客户机的意思是从 Cell Manager 上的 IDB 中删除其引用，而未从客户机卸载软件。 这可以使用 Data Protector GUI 来完成。

如果您要执行以下操作，则可以使用导出功能：

- 要将客户机移动到其他单元
- 希望从不再属于网络的 Data Protector 单元配置中删除客户机
- 希望解决有关许可的问题

  通过从单元导出客户机，许可证将对其他某个系统可用。

先决条件

在导出客户机前，请检查以下内容：

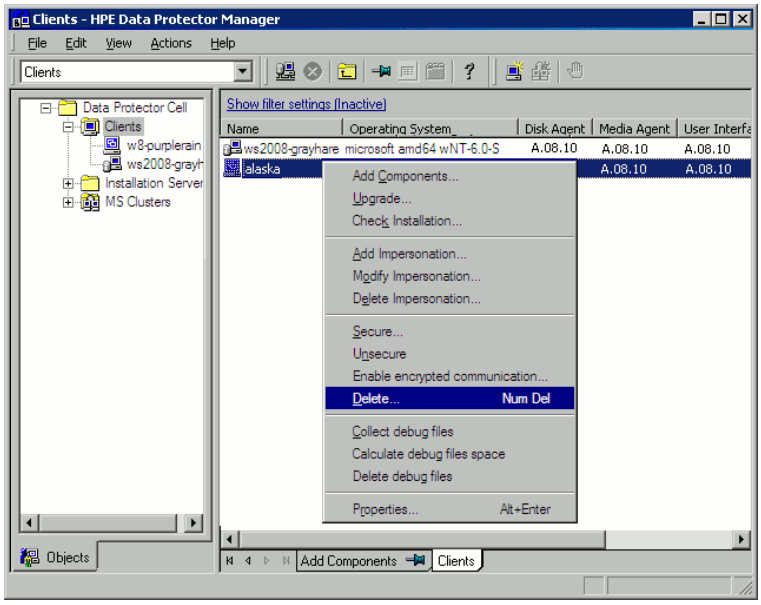
- 客户机的所有实例都已从备份规范中删除。 否则，Data Protector 将尝试备份未知的客户机，而此部分备份规范将会失败。 有关如何修改备份规范的说明，请参见《*Data Protector 帮助*》的索引：“修改, 备份规范”。
- 客户机没有已连接和配置的备份设备或磁盘列阵。 导出系统后，Data Protector 不再能够使用原单元中的备份设备或磁盘列阵。

导出客户机

使用 **Data Protector GUI** 导出客户机

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，单击**客户机**，右键单击要导出的客户机系统，然后单击**删除**。

   导出客户机系统



3. 此时会询问您是否要同时卸载 Data Protector 软件。 单击**否 (No)** 以导出客户机，然后单击**完成 (Finish)**。

客户机将从“结果区域”的列表中删除。

> **注意：**
> 如果 Cell Manager 安装在与要导出的客户机相同的系统上，则无法导出或删除 Data Protector 客户机。 但是，可以从仅安装了客户机和 安装服务器 的系统中导出客户机。 在这种情况下，安装服务器 也从单元中删除。

Microsoft Cluster Server 客户机

从 **Data Protector** 单元导出 **Microsoft** 群集服务器客户机

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开 **MS 群集**，右键单击要导出的群集客户机，然后单击**删除**。

3. 此时会询问您是否要同时卸载 Data Protector 软件。 单击**否 (No)** 仅导出群集客户机。

群集客户机将从“结果区域”的列表中删除。

> **提示：**
> 要导出特定的群集节点或虚拟服务器，请在“范围窗格 (Scoping Pane)”中右键单击群集节点或虚拟服务器并单击**删除 (Delete)**。

安全注意事项

本节描述了 Data Protector 的安全性元素。它描述了可用于提高 Data Protector 安全性的高级设置，以及必须考虑的先决条件和注意事项。

因为在整个环境中提高安全性需要进行其他设置，所以许多安全性功能无法在默认情况下启用。

本章描述的注意事项不仅在更改安全性设置时适用，而且在配置新用户、添加客户机、配置应用程序代理或进行其他更改时也必须遵守。任何对安全设置的更改都可能对整个单元有效，应小心地计划这些更改。

安全性层

必须在不同的安全性关键层上计划、测试和实施安全性，以确保 Data Protector 的安全性操作。这样的层是 Data Protector 客户机、Cell Manager 和用户。本节说明了如何在这些层上配置安全性。

客户机安全性

安装在单元的客户机上的 Data Protector 代理程序提供了许多强大的功能，例如访问系统上的所有数据。这些功能仅对在**单元授权机构** (Cell Manager 和 安装服务器)上运行的进程可用，而其他所有请求都被拒绝，这一点是很重要的。

在保证客户机的安全性前，确定受信任主机列表是很重要的。此列表必须包括：

- Cell Manager
- 相关的 安装服务器
- 对于某些客户机，还要包括将远程访问机械手的客户机列表。

> **重要：**
> 列表必须包含所有可能发出连接的主机名(或 IP 地址)。如果以上任意客户机是多宿主的(有多个网络适配器和/或多个 IP 地址)或是群集，则可能需要多个主机名。
>
> 如果单元中的 DNS 配置不统一，则可能需要考虑其他注意事项。

虽然并不总是需要保证单元中每个客户机的安全性，但是保证其他客户机将信任的计算机自身的安全性却很重要：

- Cell Manager / Manager-of-Managers
- 安装服务器s
- 介质代理客户机

注意：
不需要将用户界面客户机添加到受信任客户机的列表中。您可以使用 GUI 访问完整的 Data Protector 功能或仅访问特定环境，具体取决于用户权限。

Data Protector 用户

配置 Data Protector 用户时请考虑以下重要方面：

- 某些用户权限非常强大。例如，User configuration 和 Clients configuration 用户权限可以让用户更改安全性设置。 Restore to other clients 用户权限也非常强大，尤其是(但不仅限于)与 Back up as root 或 Restore as root 用户权限结合使用时。
- 甚至不太强大的用户权限也有内在的风险与自身相关。可以配置 Data Protector 以限制某些用户权限，从而降低这些风险。本章稍后将描述这些设置。另请参见 “启动备份规范”用户权限 (第 177 页)。
- Data Protector 仅带有几个预定义的用户组。建议在 Data Protector 环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。
- 除了按用户组成员资格分配用户权限以外，可能要进一步将某些用户组的操作设定为仅限于 Data Protector 单元的特定系统。可以通过配置 user_restrictions 文件来实施该策略。有关详细信息，请参见 *Data Protector 帮助*。
- 用户配置与用户验证相关联(请参见 严格主机名检查 (第 176 页))。增强的验证如果没有详细的用户配置也没有价值，反之亦然 - 即使最详细的用户配置如果没有增强的验证也没有意义。
- 在 Data Protector 用户列表中没有“薄弱”的用户，这一点很重要。

  注意：
  用户规范的主机部分是最强的部分(尤其在有增强验证的情况下)，而用户和组部分则无法可靠地进行验证。具有强大用户权限的用户应配置给特定的客户机，他们将用于 Data Protector 管理。如果使用了多个客户机，则应为每个客户机添加一个入口，而不是将这种用户指定为用户、组、<任意>。不应允许不受信任的用户登录任何此类系统。

有关配置用户的详细信息，请参见 *Data Protector 帮助*索引：“配置, 用户”。

Cell Manager 安全性

Cell Manager 安全性很重要，因为 Cell Manager 能访问单元中的所有客户机和所有数据。

Cell Manager 的安全性可以通过严格的主机名检查功能来增强。但是，像保证客户机的安全性一样来保证 Cell Manager 的安全性以及仔细配置 Data Protector 用户也很重要。

虽然并不总是需要保证单元中每个客户机的安全性，但是保证其他客户机将信任的计算机自身的安全性却很重要：这些客户机除了 Cell Manager 之外，还包括安装服务器和介质代理客户机。

有关详细信息，请参见《严格主机名检查 (第 176 页)》。

其他安全性方面

还有其他一些安全性相关的方面应考虑到：

- 用户应无权访问任何受信任的客户机(Cell Manager、安装服务器、MA 和机械手客户机)。甚至授予 anonymous 登录或 ftp 访问权限也可能会给整体安全性带来严重的风险。
- 实际上必须严防未授权或不受信任的人员访问介质和磁带库(以及它们连接的客户机)。
- 备份、还原、对象或介质复制、对象合并或对象验证期间，通常会通过网络传输数据。如果使用网络分段无法完全分离不受信任的网络，请使用本地连接的设备、Data Protector 加密技术或自定义的编码库。请注意，更改编码库后应执行完整备份。

有关其他安全性方面，请参见《*Data Protector 帮助*》和《*Data Protector 概念指南*》。

严格主机名检查

默认情况下，Cell Manager 使用相对简单的方法进行用户验证。它使用已启动用户界面或应用程序代理的客户机已知的主机名。此方法配置起来较简单，在将安全性视为“咨询”(例如，不期望恶意攻击)的环境中提供了合理的安全性级别。

而另一方面，严格主机名检查设置提供了增强的用户验证。该验证使用 Cell Manager 从在连接中获取的 IP 进行反向 DNS 查询来解析的主机名。这施加了以下限制和注意事项：

限制

- 基于 IP 的用户验证的强度仅相当于网络中的防欺骗保护。安全性设计人员必须确定现有网络提供的防欺骗安全性级别是否足以满足特定的安全性要求。通过使用防火墙、路由器、VPN 等对网络分段可以增强防欺骗保护。
- 特定客户机内用户间的分离不如客户机间的分离强大。在高度安全的环境中，在同一客户机内一定不能将普通用户与强大用户混合在一起。
- 用户规范中使用的主机无法配置为使用 DHCP，除非将它们绑定到固定 IP 并在 DNS 中进行配置。

请意识到这些限制，以便正确地评估使用严格主机名检查可以达到的安全性级别。

主机名解析

在以下情况下，Data Protector 用于验证的主机名可能在默认用户验证与严格主机名检查间有所区别：

- 反向 DNS 查询返回不同的主机名。这可能是有意所为，或表明客户机或反向 DNS 表配置错误。
- 客户机是多宿主的(有多个网络适配器和/或多个 IP 地址)。该注意事项是否适用于特定的多宿主客户机，取决于它在网络中的角色及在 DNS 中对其进行配置的方式。
- 客户机是群集。

通过此设置启用的检查的性质可能要求重新配置 Data Protector 用户。您必须检查 Data Protector 用户的现有规范，以查看他们是否可能受到以上某种原因的影响。根据不同情况，可能需要更改现有规范，或添加新规范，以包含所有可能发出连接的 IP。

请注意，如果启用严格的主机名检查时必须修改用户规范，则当恢复到默认用户验证时也必须重新配置用户。因此，建议确定想要使用的用户验证并坚持使用下去。

可靠的反向 DNS 查询的先决条件是安全性的 DNS 服务器。您必须防止对所有未授权人员的物理访问和登录。

用 IP 而不是主机名配置用户，您可以避免一些 DNS 相关的验证问题，但是这种配置更难以维持。

要求

增强的验证不会自动对某些内部连接授予访问权限。因此，使用此验证后，必须为以下每种程序添加新用户：

- Windows 客户机中的任何应用程序代理 (OB2BAR)。针对 Windows 客户机，要求为安装了应用程序代理的每个客户机添加用户 SYSTEM、NT AUTHORITY、*client*。请注意，如果某客户机上的 Inet 配置为使用特定帐户，则该帐户必须已配置。有关详细信息，请参见 *Data Protector 帮助*索引：“严格主机名检查”。

有关用户配置的详细信息，请参见 *Data Protector 帮助*索引：“配置, 用户”。

启用功能

要启用严格主机名检查，请将 StrictSecurityFlags 全局选项设置为 0x0001。

有关全局选项的详细信息，请参见《*Data Protector 故障诊断指南*》。

“启动备份规范”用户权限

有关 Data Protector 用户和用户权限的常规信息，请参见 *Data Protector 帮助*索引：“用户”。

Start backup specification 用户权限不能使用户使用 GUI 中的备份上下文。用户可从命令行使用 omnib 与 -datalist 选项启动备份规范。

> **注意：**
> 通过结合 Start Backup Specification 和 Start Backup 用户权限，用户可在 GUI 中查看配置的备份规范并能够启动备份规范或交互式备份。

并不总是希望允许用户执行交互式备份。要仅允许还拥有保存备份规范权利的用户进行交互式备份，请将 StrictSecurityFlags 全局选项设置为 0x0200。

有关全局选项的详细信息，请参见《*Data Protector 故障诊断指南*》。

隐藏备份规范的内容

在高安全环境中，可能会将所保存备份规范的内容视为敏感甚至保密信息。可以将 Data Protector 配置为对所有用户隐藏备份规范的内容，除具有 Save backup specification 用户权限的用户之外。为此，请将 StrictSecurityFlags 全局选项设置为 0x0400。

有关全局选项的详细信息，请参见《*Data Protector 故障诊断指南*》。

主机信任

主机信任功能仅需在有限数量的客户机内将数据从一个客户机恢复到其他客户机，从而减小了将“恢复到其他客户机”用户权限授予用户的需要。可以定义一组主机，彼此信任对方的数据。

主机信任通常在以下情况下使用：

- 用于群集中的客户机(节点和虚拟服务器)。
- 如果客户机的主机名已更改且旧备份对象的数据需要恢复。
- 如果由于 DNS 问题导致客户机主机名与备份对象不匹配。
- 如果用户拥有多个客户机且需要将数据从一个客户机恢复到另一个客户机。
- 将数据从一个主机迁移到另一个主机时。

配置

要配置主机信任，请在 Cell Manager 上创建文件 *Data_Protector_program_data*\Config\Server\cell\host_trusts(Windows 系统)或 /etc/opt/omni/server/cell/host_trusts(UNIX 系统)。

彼此信任的主机组定义为包含在波形括号中的主机名列表。例如：

示例

```
GROUP="cluster.domain.com"
{
    cluster.domain.com
    node1.domain.com
    node2.domain.com
}
GROUP="Bajo"
{
    computer.domain.com
    anothercomputer.domain.com
}
```

监控安全性事件

如果在使用 Data Protector 时遇到问题，可使用日志文件中的信息来确定问题。例如，记录的事件可帮助您确定配置错误的用户或客户机。

客户机安全性事件

客户机安全性事件将记录在单元中每个客户机上默认的 Data Protector 日志文件目录下的 inet.log 文件中。

Cell Manager 安全性事件

Cell Manager 安全性事件将记录在默认 Data Protector 服务器日志文件目录中的 security.log 文件中。

用户验证和 **LDAP**

应在企业用户管理基础设施中结合将 Data Protector 作为企业系统进行认证和授权的功能。此连接允许向企业用户目录中配置的用户和组授予访问 Data Protector 服务的权限。

将在安全连接上执行用户身份验证，并将轻型目录访问协议 (LDAP) 用作基础技术。 因此，用户可以使用其企业凭据访问 Data Protector 服务而无需单独保存密码。 此外，可以在企业目录中将管理员或操作员保留为组，从而符合已建立的授权和审批流程。

使用 Java 验证和授权服务 (JAAS) 登录模块在 Data Protector 嵌入式应用程序服务器 (WildFly) 的安全域中配置 LDAP 集成。 可选的 LDAP 登录模块可提供 LDAP 验证和授权服务，可将这些服务通过必需的 Data Protector 登录模块映射到 Data Protector 权限。 如果未配置 LDAP 集成，Data Protector 将按照以前版本中的流程运行。

Data Protector 使用登录模块堆栈中的登录模块验证用户。 如果用户使用 Data Protector GUI 连接 Cell Manager，则以下登录模块将执行用户验证：

1. LDAP 登录模块：针对现有 LDAP 服务器验证用户凭据，如用户名和密码。 请参见初始化并配置 LDAP 登录模块。
2. Data Protector 登录模块：针对 Data Protector 用户列表和 Web 访问密码验证用户凭据。 请参见授予 LDAP 用户或组 Data Protector 权限。
3. 执行 LDAP 初始化和配置所需的所有步骤后，还可以检查配置。 请参见检查 LDAP 配置。

> **注意：** 如果已在 Data Protector 中配置用户或客户机以允许执行经典的 CLI 访问方式， Data Protector GUI 不会使用 LDAP 功能。

初始化并配置 LDAP 登录模块

LDAP 登录模块位于 WildFly 应用程序服务器 (随 Data Protector 一起安装) 的安全域中。 必须在首次使用 LDAP 安全功能前初始化并配置 LDAP 登录模块。

1. 初始化 LDAP 登录模块。
2. 配置 LDAP 登录模块。

初始化 LDAP 登录模块

要初始化 LDAP 登录模块，请使用 `jboss-cli` 实用程序 (也随 Data Protector 一起安装)

1. `jboss-cli` 实用程序位于：`%Data_Protector_home%/AppServer/bin`。 请执行以下命令：
   - **Windows**： `jboss-cli.bat --file=ldapinit.cli`
   - **UNIX**： `jboss-cli.sh --file=ldapinit.cli`

   此命令将在 WildFly 配置中创建一个 LDAP 登录模块，并将使用默认值来填充这一新的登录模块。 `standalone.xml` 配置文件中的命令行生成的默认值为：

```
<security-domain name="hpdp-domain">
<authentication>
<login-module code="LdapExtended" flag="optional">
<module-option name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory"/>
<module-option name="java.naming.security.authentication" value="simple"/>
```

```
<module-option name="roleFilter" value="(member={1})"/>
<module-option name="roleAttributeID" value="memberOf"/>
<module-option name="roleNameAttributeID" value="distinguishedName"/>
<module-option name="roleAttributeIsDN" value="true"/>
<module-option name="searchScope" value="SUBTREE_SCOPE"/>
<module-option name="allowEmptyPasswords" value="true"/>
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
<login-module code="com.hp.im.dp.cell.auth.DpLoginModule" flag="required">
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
</authentication>
</security-domain>
```

注意：
如果 Cell Manager 安装在 UNIX 环境中并使用 LDAP 身份验证，则 standalone.xml 配置文件中通过命令行生成的默认值将会更改。 更改如下：

```
<login-module code="LdapExtended" flag="optional">
<module-option name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory"/>
<module-option name="java.naming.security.authentication" value="simple"/>
<module-option name="roleFilter" value="(member={1})"/>
<module-option name="roleAttributeID" value="memberOf"/>
<module-option name="roleNameAttributeID" value="distinguishedName"/>
<module-option name="roleAttributeIsDN" value="true"/>
<module-option name="searchScope" value="SUBTREE_SCOPE"/>
<module-option name="allowEmptyPasswords" value="false"/>
<module-option name="password-stacking" value="useFirstPass"/>
<module-option name="java.naming.provider.url" value="ldap://<IP_of_
Active_Directory_host>"/>
<module-option name="baseCtxDN" value="OU=_Benutzer,DC=godyo,DC=int"/>
<module-option name="rolesCtxDN" value="OU=_Gruppen,DC=godyo,DC=int"/>
<module-option name="bindDN" value="CN=backup-service,OU=_Service_
Accounts,DC=godyo,DC=int"/>
<module-option name="bindCredential" value="password"/>
```

```
<module-option name="baseFilter" value="(userPrincipalName={0})"/>
</login-module>
```

主要是配置参数 baseCtxDN 和 rolesCtxDN。 组织单位 (OU) 参数用于对 UNIX Cell Manager 进行身份验证。

2. 要从远程客户机访问 Cell Manager 上的 WildFly 管理控制台，请启用对 WildFly 管理控制台的远程访问。 为此，请使用文本编辑器，在 standalone.xml 文件的接口部分中将管理接口的绑定地址从 127.0.0.1 更改为 0.0.0.0：

```
<interfaces>
<interface name="management">
<inet-address value="${jboss.bind.address.management:0.0.0.0}"/>
</interface>
<interface name="public">
<inet-address value="0.0.0.0"/>
</interface>
<interface name="unsecure">
<inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"/>
</interface>
</interfaces>
```

3. 重新启动 Data Protector 服务：

```
omnisv stop
omnisv start
```

配置 LDAP 登录模块

要配置 LDAP 登录模块，请使用 WildFly 应用程序服务器的基于 Web 的管理控制台，该控制台随 Data Protector 一起安装。 请执行以下操作：

1. 要访问 WildFly 管理控制台，请创建一个 WildFly 用户。 要创建 WildFly 用户，请运行 add-user 实用程序：
   - **Windows**： add-user.bat，位于 %Data_Protector_home%/AppServer/bin
   - **UNIX**： add-user.sh，位于 /opt/omni/AppServer/bin
2. 为以下参数提供输入内容：
   - **要添加的用户类型**：选择“管理用户”。
   - **领域**：将此字段留空，因为实用程序将选择默认值 ManagementRealm。
   - **用户名**：添加一个用户名。

- **密码**：添加一个密码。
- **组**：无。

3. 要访问 WildFly 管理控制台，请使用浏览器打开 URL：<http://cell-manager-name:9990/console>
4. 在“身份验证”屏幕中，指定由 add-user 实用程序创建的**用户名**和**密码**。
5. 单击**登录**。 WildFly 应用程序服务器的管理控制台随即显示。
6. 在 WildFly 管理控制台中，选择**配置文件**选项卡。
7. 在**配置文件**选项卡中，展开**安全**节点，然后单击**安全域**。
8. 在已注册的安全域的列表中，对 hpdp-domain 单击**视图**。 为安全域 hpdp-domain 定义了以下登录模块：
   - LdapExtended
   - Com.hp.im.dp.cell.auth.DpLoginModule
9. 选择 **LdapExtended** 模块。
10. 在“详细信息”部分中，单击**模块选项**选项卡。 **模块选项**选项卡中列出了所有预定义的模块选项。
11. 要自定义和使用 LDAP 登录模块，需要添加其他模块选项。 单击**添加**并为每个模块选项指定**名称**和**值**。 有关详细信息，请参见下表：

模块选项	名称	值	说明
提供程序 URL	`java.naming.provider.url`	使用以下格式指定 LDAP 服务器的 URL：`ldap://<server>:<port>`	标准属性名称
基本上下文判别名称 (DN)	`baseCtxDN`	指定含有用户的 LDAP 位置的 DN。	从中启动用户搜索操作的上下文的固定 DN
Base 过滤器	`baseFilter`	按照以下格式在 LDAP 设置中指定与用户登录名匹配的属性： `(<user-login-name-attribute>={0})` 。其中，`<user-login-name-attribute>` 需要由相应的 LDAP 属性名称替换。	用于定位要验证的用户的上下文的搜索过滤器
角色上下文 DN	`rolesCtxDN`	指定含有用户组的 LDAP 位置的 DN。	要搜索用户组的上下文的固定 DN
绑定 DN	`bindDN`	指定由登录模块用于执行初始 LDAP 绑定的 LDAP 用户	用于为用户和角色查询绑定

模块选项	名称	值	说明
		DN。 必须拥有所需权限以搜索用户和组的 LDAP 位置，来获取用户及其组。 这些位置在 baseCtxDN 和 rolesCtxDN 模块选项中进行定义。	LDAP 服务器的 DN。 这是一个对 baseCtxDN 和 rolesCtxDN 值具有读取/搜索权限的 DN
绑定凭据	bindCredential	为在 BindDN 模块选项中提供的 LDAP 用户指定密码。	bindDN 的密码。

有关其他模块选项的更多信息，请访问以下 URL：

- https://community.jboss.org/wiki/LdapExtLoginModule
- http://technet.microsoft.com/en-us/library/cc773354 (v=ws.10).aspx

12. 在重新加载 WildFly 应用程序服务器配置后更改将生效。 要重新加载配置，请使用 jboss-cli 实用程序，该实用程序位于：%Data_Protector_home%/AppServer/bin。
13. 请执行以下命令：
    - **Windows**： jboss-cli.bat -c :reload
    - **UNIX**： jboss-cli.sh -c :reload

> **注意：** 在 MoM 环境中配置 LDAP 登录模块时，请确保在每个 Cell Manager 上执行上述步骤。 MoM 环境中的每个 Cell Manager 需具有相同的 LDAP 登录模块配置。

向 LDAP 用户或组授予 Data Protector 权限

LDAP 用户仅在被授予 Data Protector 权限后才能连接到 Cell Manager。 配置 LDAP 登录模块后，可以为 LDAP 用户授予所需的 Data Protector 权限。

要授予 Data Protector 权限，请执行以下步骤：

1. 启动 Data Protector GUI 并向 LDAP 用户或组授予 Data Protector 权限。
   - 向 Data Protector 用户组添加 LDAP 用户。
   - 向 Data Protector 用户组添加 LDAP 组。
2. 使用 LDAP 凭据登录。

向用户组添加 LDAP 用户

要将 LDAP 用户添加至 Data Protector 用户组，请执行以下步骤：

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**，然后右键单击要向其添加 LDAP 用户的用户组。
3. 单击**添加/删除用户**打开向导。

4. 在“添加/删除用户”对话框的**手动**选项卡中，提供以下详细信息：
   - **类型**：选择 LDAP。
   - **名称**：以 LDAP 用户主体名称格式指定 LDAP 用户。
   - **实体**：输入 LDAP 用户。
   - **说明**：这是可选字段。
5. 单击**完成**退出向导。

向用户组添加 LDAP 组

要将 LDAP 组添加至 Data Protector 用户组，请执行以下步骤：

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**，然后右键单击要向其添加 LDAP 组的用户组。
3. 单击**添加/删除用户**打开向导。
4. 在“添加/删除用户”对话框的**手动**选项卡中，提供以下详细信息：
   - **类型**：选择 LDAP。
   - **名称**：按照判别名称 (DN) 格式指定 LDAP 组名。
   - **实体**：输入 LDAP 组。
   - **说明**：这是可选字段。
5. 单击**完成**退出向导。

> **注意**：将自动授予 LDAP 用户与其所属 LDAP 组相同级别的权限。

使用 LDAP 凭据登录

要使用 LDAP 凭据登录，请执行以下步骤：

1. 启动 Data Protector GUI 并连接 Cell Manager。
2. 在“LDAP 验证 (LDAP Authentication)”屏幕中，提供 LDAP 凭据以访问 Data Protector。LDAP 用户可属于任何可用的 Data Protector 用户组。

检查 LDAP 配置

以下过程讲解如何检查是否为特定 LDAP 用户或组正确设置了用户权限，方法是从 Web 浏览器中查询 Data Protector 登录提供程序服务 `getDpAcl`。

要获取指定用户的 Data Protector 访问控制列表 (ACL)，请执行以下步骤：

1. 使用浏览器连接 Data Protector 登录提供程序 Web 服务。
2. 浏览器可能会提示您接受服务器证书。 单击**接受**确认请求。

3. 将显示一个对话框，提示您提供登录凭据。 提供已使用 Data Protector 配置的有效 LDAP 用户名和密码。 请参见配置 LDAP 登录模块。
4. 浏览器将返回以下访问控制列表 (ACL)： `https://<server>:7116/dp-loginprovider/restws/dp-acl`
5. 使用 ACL 检查所分配的权限是否与为对应 Data Protector 用户组指定的 Data Protector 用户权限相匹配。

证书生成实用程序

X.509 证书生成实用程序 (omnigencert.pl) 可生成证书颁发机构 (CA)、服务器和客户机证书。它负责执行以下任务：

- 设置单级 root CA
- 生成 CA、服务器和客户机证书
- 创建用于存储密钥、证书、配置和密钥库文件所需的目录结构
- 在 CM 上的预定义位置中存储所生成的证书
- 生成 Web 服务角色的属性文件

> **注意：** omnigencert.pl 实用程序只能由管理员用户 (Windows) 或 root 用户 (UNIX) 运行。

omnigencert.pl 实用程序以脚本形式开发，并随 Cell Manager (CM) 安装套件一起安装。作为 CM 安装过程的一部分，首先运行此脚本，然后生成证书并将其存储在预定义的位置。

omnigencert.pl 脚本存在于以下位置：

Windows：%Data_Protector_home%\bin

Unix：/opt/omni/sbin

如果需要，Data Protector 管理员可在安装后随时运行此实用程序，以使用新的密钥对或 CA 安装重新生成证书。但是，并非必须对基于证书的身份验证过程使用由此实用程序生成的证书。您可以改为使用现有的 CA 安装，以生成所需的证书。

语法

作为 Cell Manager 安装过程的一部分，此实用程序最初由安装程序执行，并生成所需证书并将其存储到预定义的位置。

此实用程序仅限管理员使用，并用于通过使用新密钥对(即使包括新 CA 安装)重新生成证书。Windows 平台上的“管理员”用户和 UNIX 平台上的 "root" 用户可执行此脚本。

omnigencert.pl 脚本存在于以下位置：

Windows：%Data_Protector_home%\bin

Unix：/opt/omni/sbin

可使用以下语法和选项运行 omnigencert.pl 实用程序：

使用情况

[-no_ca_setup]

[-server_id ServerIdentityName]

[-user_ID UserIdentityName]

[-store_password KeystorePassword]

[-cert_expire CertificateExpireInDays]

[-ca_dn CertificateAuthorityDistinguishedName]

[-server_dn ServerDistinguishedName]

[-client_dn ClientDistinguishedName]

[-server_san]

omnigencert.pl 实用程序支持多个选项，这些选项可为生成证书提供灵活性。如果未指定选项，此实用程序将使用默认值生成证书。

omnigencert.pl 实用程序支持以下选项：

选项	说明
-no_ca_setup	为现有 CA 安装生成客户机和服务器证书。如果 CA 安装不存在，则此选项无效。
-server_id	指定服务器证书的判别名称 (DN) 部分中的公用名称 (CN) 实体的值。此选项的默认值是 CM 完全限定的域名 (FQDN)。
-user_id	指定客户机证书 DN 部分 CN 实体的值。此选项的默认值是 WebService 用户。
-store_password	定义密钥库或信任库(在其中保存服务器和客户机证书，包括其密钥)的密码。如果未提供此选项，将使用默认密码创建库。
-cert_expire	定义所生成的证书的有效期限(以天为单位)。此选项的默认值为 8760 天(24 年)。
-ca_dn	定义 CA 的 DN 字符串。DN 格式如下所示：“CN=<value>, O=<value>, ST=<value>, C=<value>” CN = 公用名称， O= 组织名称， ST= 州名称， C= 国家名称。O、ST 和 C 参数的默认值如下所示：CN = CA <CM 服务器的 FDQN 名称> O = HEWLETT-PACKARD ST = CA C= US
-server_dn	定义服务器证书的 DN 字符串。DN 格式如下所示：“CN=<value>, O=<value>, ST=<value>, C=<value>” CN = 公用名称， O= 组织名称， ST= 州名称， C= 国家名称。O、ST 和 C 参数的默认值如下所示：CN = <CM 服务器的

选项	说明
	FDQN 名称> O = HEWLETT-PACKARD ST = CA C= US
-client_dn	定义客户机或用户证书的 DN 字符串。DN 格式如下所示：“CN=<value>, O=<value>, ST=<value>, C=<value>” CN = 公用名称， O= 组织名称， ST= 州名称， C= 国家名称。O、ST 和 C 参数的默认值如下所示：CN = WebService User O = HEWLETT-PACKARD ST = CA C= US
-server_san	指定服务器证书中的使用者替代名称 (SAN)。但是，在 Cell Manager 安装期间生成的服务器证书在 SAN 部分中具有 DNS 类型的条目。这些 SAN 条目将基于 Cell Manager 中的可用 IP 数量自动生成。要覆盖服务器证书中默认情况下自动生成的 SAN 条目，请在使用证书生成实用程序生成证书时指定该选项。 支持 DNS 和 IP类型的 SAN 条目。 此选项的值格式如下所示： santype:value,santype:value 每个 SAN 条目由逗号 (",") 分隔，且包括两个部分： 1) SAN 类型， 2) SAN 类型的值。 **示例：** dns:myserver1.mycompany.com、dns:myserver2.mycompany.com ip:10.218.1.100, ip:10.218.1.200, ip:10.218.1.155 dns:myserver1.mycompany.com, ip:10.218.1.100

> **注意：**
> 此实用程序不支持以下选项组合：
>
> - -server_id 和 -server_dn
> - -user_id 和 -client_dn
> - -no_ca_setup 和 -ca_dn.

示例

以下部分列出了用于在 Windows 和 UNIX 上运行 omnigencert.pl 实用程序的示例命令。

omnigencert.pl 脚本存在于以下位置：

Windows：%Data_Protector_home%\bin

Unix：/opt/omni/sbin

Windows 和 **Unix** 命令

任务	Windows 命令	Unix 命令
使用默认值设置 CA 并生成 CA、客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl	/opt/omni/bin/perl omnigencert.pl
使用指定的公用名称值设置 CA 并生成 CA、客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl -server_id <value> -user_id <value>	/opt/omni/bin/perl omnigencert.pl -server_id <value> -user_id <value>
使用指定的库密码设置 CA 并生成 CA、客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl -store_password <value>	/opt/omni/bin/perl omnigencert.pl -store_password <value>
使用指定的证书有效期限设置 CA 并生成 CA、客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl -cert_expire <value>	/opt/omni/bin/perl omnigencert.pl -cert_expire <value>
通过默认值生成将使用现有 CA 安装(在安装过程中创建)的客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl –no_ca_setup	/opt/omni/bin/perl omnigencert.pl –no_ca_setup
使用指定的 DN 设置 CA 并生成 CA、客户机和服务器证书	%Data_Protector_home% \bin\perl.exe omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>
通过指定 DN	%Data_Protector_	/opt/omni/bin/perl

任务	Windows 命令	Unix 命令
生成将使用现有 CA 安装的客户机和服务器证书	home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>	omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>
使用 SG-CLUSTER 环境中的现有 CA 证书生成客户机和服务器证书	1.从 <DP_DATA_DIR>\Config\client\components\webservice.properties 检索现有的密钥库密码。 2.从 <DP_SDATA_DIR>\server\idb\idb.config 检索 **PGOSUSER** 值。 3.对群集虚拟系统名称运行 omnigencert.pl 实用程序，如下所示： %Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd	1.从 /etc/opt/omni/client/components/webservice.properties 检索现有的密钥库密码。 2.从 /etc/opt/omni/server/idb/idb.config. 检索 **PGOSUSER** 值 3.对群集虚拟系统名称运行 omnigencert.pl 实用程序，如下所示： /opt/omni/bin/perl omnigencert.pl –no_ca_setup -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd
在 SG-CLUSTER 环境中生成 CA、客户机和服务器证书：	1.从 <DP_DATA_DIR>\Config\client\components\webservice.properties 检索现有的密钥库密码。 2.从 <DP_SDATA_DIR>\server\idb\idb.config 检索 **PGOSUSER** 值。 3.对群集虚拟系统名称运行	1.从 /etc/opt/omni/client/components/webservice.properties 检索现有的密钥库密码。 2.从 /etc/opt/omni/server/idb/idb.config 检索 **PGOSUSER** 值。 3.对群集虚拟系统名称运行

任务	Windows 命令	Unix 命令
	omnigencert.pl 实用程序，如下所示： %Data_Protector_home% \bin\perl.exe omnigencert.pl -server_id cm_virtual_ name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd	omnigencert.pl 实用程序，如下所示： /opt/omni/bin/ perl omnigencert.pl -server_id cm_virtual_ name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd
为特定的 Cell Manager 服务器生成含 DNS 类型的 SAN 条目的服务器证书。	%Data_Protector_home% \ bin\perl.exe omnigencert.pl -no_ca_setup -server_dn iwf11160123.dprnd.hpe.com -server_san "dns:iwf11160123.dprnd.hpe.com, dns:iwf11160123.dp.hpe.com"	/opt/omni/ bin/perl omnigencert.pl -no_ca_setup -server_dn myserver4.mycompany.com -server_san "dns:myserver4.mycompany.com, dns:myserver4.mycompany.com"
为特定的 Cell Manager 服务器生成含 IP 类型的 SAN 条目的服务器证书。	%Data_Protector_home%\ bin\perl.exe omnigencert.pl -no_ca_setup -server_dn 10.218.1.100 -server_san “ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116”	/opt/omni/bin/ perl omnigencert.pl -no_ca_setup -server_dn 10.218.1.100 -server_san "ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"
为特定的 Cell Manager 服务器生成含 DNS 和 IP 类型的 SAN 条目的服务器证书。	%Data_Protector_home%\bin\ perl.exe omnigencert.pl -no_ca_setup -server_dn myserver3.mycompany.com	/opt/omni/bin/ perl omnigencert.pl -no_ca_setup -server_dn

任务	Windows 命令	Unix 命令
	-server_san "dns:myserver3.mycompany.com, myserver3.mycompany.com, ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"	myserver3.mycompany.com -server_san "dns:myserver3.mycompany.com, myserver3.mycompany.com, ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"

目录结构

以下部分列出了用于存储证书的目录。

Windows 目录	Unix 目录	说明
ProgramData\Omniback\Config\Server\certificates	/etc/opt/omni/server/certificates	包含 CA 证书文件 cacert.pem (其中包含 CA 公钥)。
ProgramData\Omniback\Config\Server\certificates\ca	/etc/opt/omni/server/certificates /ca	包含 CA 功能所需的配置、输入和其他文件。
ProgramData\Omniback\Config\Server\certificates\ca\keys	/etc/opt/omni/server/certificates /ca/keys	包含 CA 私钥文件 cakey.pem。
ProgramData\Omniback\Config\Server\certificates\server	/etc/opt/omni/server/certificates /server	包含两种类型的库：密钥库和信任库。这些库由 Java 实用程序和密钥工具创建，用于保护服务器证书及其密钥。这些库通过库密码进行保护。包括以下库：

Windows 目录	Unix 目录	说明
		ca.truststore server.keystore server.truststore
ProgramData\Omniback\Config\Server\certificates\client	/etc/opt/omni/server/certificates /client	包含两种类型的库：密钥库和信任库。这些库由 Java 实用程序和密钥工具创建，用于保护客户机证书及其密钥。这些库通过库密码进行保护。包括以下库： • client.keystore • client.truststore
ProgramData\Omniback\Config\Server\AppServer	/etc/opt/omni/server/AppServer	包含由此实用程序创建的属性文件。除以下属性文件外，此目录还包括其他一些文件： • jce-webservice-roles.properties • dp-webservice-roles.properties

覆盖现有的证书

要使用由现有 CA 安装生成的证书覆盖现有证书(在 CM 安装期间由实用程序生成)，可使用以下选项之一：

- 覆盖现有密钥库和信任库文件中的证书
- 通过创建新密钥库和信任库文件覆盖证书

> **注意：**重新生成证书或使用新证书后，必须重新启动 CM 上的 Data Protector 服务。必须在执行任何将使用证书的操作前完成此步骤，因为重新启动此服务将确保新证书生效。

覆盖现有密钥库和信任库文件中的证书

要覆盖现有密钥库和信任库文件中的证书，请完成以下任务：

- 替换现有服务器和客户机库文件
- 替换 CA 证书
- 更新判别名称 (DN) 字符串

替换现有服务器和客户机库文件

要替换现有服务器和客户机库文件，请执行以下步骤：

1. 从位于以下位置的 webservice.properties 和 standalone.xml 配置文件检索密钥库和信任库文件的库密码：

   Windows

   - ProgramData\OmniBack\Config\client\components\webservice.properties
   - ProgramData\OmniBack\Config\server\AppServer\standalone.xml

   UNIX

   - /etc/opt/omni/client/components/webservice.properties
   - /etc/opt/omni/server/AppServer/standalone.xml

2. 从现有服务器和客户机存储文件(server.keystore、 server.truststore、client.keystore 和 client.truststore)中删除所有条目，这些文件位于：

   服务器

   - Windows： ProgramData\Omniback\Config\Server\certificates\server
   - Unix： /etc/opt/omni/server/certificates/server

   客户机

- Windows： ProgramData\Omniback\Config\Server\certificates\client
- UNIX： /etc/opt/omni/server/certificates/client

要执行这些更改，可使用位于以下位置的 Java 密钥工具实用程序：

Windows： Program Files\Omniback\jre\bin

UNIX： /opt/omni/jre/bin

3. 使用 Java 密钥工具实用程序将生成的证书导入以下库：
   - 服务器和 CA 证书 server.keystore
   - CA 和客户机证书 server.truststore
   - CA 证书 ca.truststore
   - 客户机和 CA 证书 client.keystore
   - CA 和服务器证书 client.truststore

替换 CA 证书

要替换 CA 证书，请执行以下步骤：

1. 请注意现有 CA 证书文件 cacert.pem 的权限，该文件位于：
   - **Windows**： ProgramData\Omniback\Config\Server\certificates
   - **UNIX**： /etc/opt/omni/server/certificates
2. 将现有 CA 证书文件 cacert.pem 替换为生成的 CA 证书。

更新判别名称 (DN) 字符串

将 jce-webservice-roles.properties 和 dp-webservice-roles.properties 文件中的现有判别名称 (DN) 字符串替换为用于客户机证书的 DN 字符串。这些文件位于：

Windows： ProgramData\Omniback\Config\Server\AppServer

UNIX： /etc/opt/omni/server/AppServer

> **注意**：在 DN 字符串中，在空格和 "=" 字符前加上反斜杠 (\) 字符。

通过创建新密钥库和信任库文件覆盖证书

要覆盖新密钥库和信任库文件中的证书，请完成以下任务：

- 替换现有服务器和客户机库文件
- 替换 CA 证书
- 更新判别名称 (DN) 字符串
- 使用库密码更新配置文件

> **注意：**必须为服务器和客户机库保留密码。

替换现有服务器和客户机库文件

要替换现有服务器和客户机库文件，请执行以下步骤：

1. 请注意现有服务器和客户机存储文件(server.keystore、server.truststore、client.keystore 和 client.truststore)的权限，这些文件位于：

   服务器

   - Windows：ProgramData\Omniback\Config\Server\certificates\server
   - UNIX：/etc/opt/omni/server/certificates/server

   客户机

   - Windows： ProgramData\Omniback\Config\Server\certificates\client
   - UNIX： /etc/opt/omni/server/certificates/client

2. 删除服务器和客户机库文件。
3. 创建具有相同文件名和权限的库。
4. 使用 Java 密钥工具实用程序将生成的证书导入以下库：
   - 服务器和 CA 证书 server.keystore
   - CA 和客户机证书 server.truststore
   - CA 证书 ca.truststore
   - 客户机和 CA 证书 client.keystore
   - CA 和服务器证书 client.truststore

> **注意：**在 Windows 中，Java 密钥工具实用程序位于：Program Files\Omniback\jre\bin 和 UNIX：/opt/omni/jre/bin。

替换 CA 证书

要替换 CA 证书，请执行以下步骤：

1. 请注意现有 CA 证书文件 cacert.pem 的权限，该文件位于：

   Windows

   ProgramData\Omniback\Config\Server\certificates

   UNIX

   /etc/opt/omni/server/certificates

2. 将现有 CA 证书文件 cacert.pem 替换为生成的 CA 证书。

更新判别名称 (DN) 字符串

将 jce-webservice-roles.properties 和 dp-webservice-roles.properties 文件中的现有判别名称 (DN) 字符串替换为用于客户机证书的 DN 字符串。这些文件位于：

Windows

ProgramData\Omniback\Config\Server\AppServer

UNIX

/etc/opt/omni/server/AppServer

注意： 在 DN 字符串中，在空格和 "=" 字符前加上反斜杠 (\) 字符。

使用库密码更新配置文件

要使用库密码更新配置文件，请执行以下步骤：

注意： 只有在使用新密码创建了新库的情况下才需要执行此任务。

1. 使用在创建存储文件(如 server.keystore、server.truststore、 ca.truststore、client.keystore 和 client.truststore)时采用的存储密码更新 webservice.properties 和 standalone.xml 配置文件。

   配置文件位于：

   Windows

   •ProgramData\OmniBack\Config\client\components\webservice.properties

   •ProgramData\OmniBack\Config\server\AppServer\standalone.xml

   UNIX

   •/etc/opt/omni/client/components/webservice.properties

   • /etc/opt/omni/server/AppServer/standalone.xml

2. 在 standalone.xml 文件中，更新存储密码(以粗体突出显示)：

   ```
   <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
   file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
   verify-client="want" ca-certificate-
   file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
   password="M6.pOino06L3w"/>
   ```

3. 在 webservice.properties 文件中，更新密码(以粗体突出显示)：

   ```
    <jsse keystore-password="M6.pOino06L3w" keystore-
   url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
   password="M6.pOino06L3w" truststore-
   url="/etc/opt/omni/server/certificates/server/server.truststore"/>

   <jsse keystore-password="M6.pOino06L3w" keystore-
   url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
   ```

```
password="M6.pOino06L3w" truststore-
url="/etc/opt/omni/server/certificates/server/server.truststore"/>

 <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
verify-client="want" ca-certificate-
file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
password="M6.pOino06L3w"/>
```

管理 Data Protector 补丁

Data Protector 补丁由支持提供，并且可从在线软件支持网站下载，网址为：https://softwaresupport.softwaregrp.com/。Data Protector提供单独补丁和补丁包。

验证已安装哪些 Data Protector 补丁

您可以在单元中的系统上验证已安装哪些 Data Protector补丁。要在单元中的特定系统上验证已安装哪些 Data Protector 补丁，请使用 Data Protector GUI 或 CLI。

> **注意：**
> 安装站点特定的补丁或补丁包后，它将始终列在补丁报告中，即使以后的补丁已包括该补丁。

先决条件

- 要使用这个功能，应安装 User Interface 组件。

限制

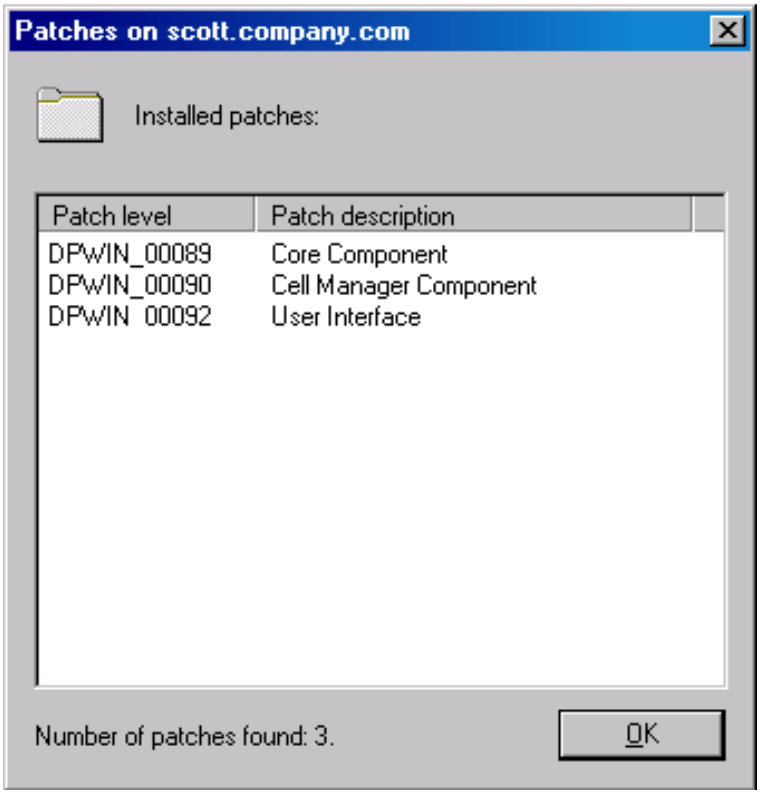
- 补丁验证只能在同一单元的系统上检查已安装哪些补丁。

使用 GUI 验证 Data Protector 补丁

使用 Data Protector GUI 验证特定客户机上已安装哪些补丁

1. 在“上下文列表 (Context List)”中，选择**客户机 (Clients)**。
2. 在“范围窗格 (Scoping Pane)”中，展开**客户机 (Clients)** 并选择单元中要验证已安装补丁的系统。
3. 在“结果区域 (Results Area)”中，单击**补丁 (Patches)** 打开**安装的补丁 (Patches on)** 窗口。

验证安装的补丁



如果在系统中找到了补丁，则验证返回每个补丁的级别和说明以及安装的补丁数。

如果系统上没有 Data Protector 补丁，则验证将返回一个空列表。

如果验证的系统不是单元的成员、不可用或发生错误，则验证将报告错误消息。

4. 单击**确定 (OK)** 关闭窗口。

使用 CLI 验证 Data Protector 补丁

要使用 Data Protector CLI 验证特定客户机上安装了哪些补丁，请执行 `omnicheck -patches -host` *`hostname`* 命令，其中，*hostname* 是要验证的系统的名称。

有关 `omnicheck` 命令的详细信息，请参见 `omnicheck` 手册页。

Data Protector 所需的补丁

对于 Data Protector 补丁，请参见 https://softwaresupport.softwaregrp.com/ 了解最新信息。

Windows 系统补丁

对于运行 Windows 的系统，请联系 Microsoft Corporation 了解最新的 Microsoft Windows Service Pack。

HP-UX 系统补丁

有关运行 HP-UX 操作系统的系统补丁，请参见 https://softwaresupport.softwaregrp.com/ 了解最新信息，或与响应中心联系以了解当前的补丁号。 在寻求支持前，请先安装最新的补丁。 列出的补丁可以由更新的补丁所替代。

Micro Focus 建议定期安装适用于 HP-UX 的 Extension Software Package。 其中涵盖了许多建议的补丁，下面列出的是其中一部分。 请联系客户支持人员，了解当前版本的 HP-UX Extension Software Package。

HP-UX 11.11

Data Protector 需要以下 HP-UX 11.11 补丁包：

服务包	包名称	说明
使用最新版	GOLDQPK11i	适用于 HP-UX 11.11 的最新补丁包
使用最新版	HWEnable11i	必需的硬件启用补丁

建议在 Data Protector 单元的所有系统安装以下 HP-UX 11.11 单个补丁：

补丁名称	硬件平台	说明
PHCO_40310	s700、s800	libc 累计补丁
PHSS_41214	s700、s800	ld(1) 和连接器工具累计补丁
KRNG11i	s700、s800	强随机数生成器

建议为 Data Protector 单元的所有 HP-UX 11.11 客户机安装 HP-UX 11.11 单个补丁：

补丁名称	硬件平台	说明
使用最新版	s700、s800	适用于您所使用版本的 Serviceguard 补丁

以下产品和 HP-UX 11.11 补丁必须安装到每个 Data Protector 磁盘代理系统上。在该系统上，数据将以 AES 256 位加密形式备份：

产品号或补丁名称	硬件平台	说明
KRNG11I	s700、s800	HP-UX 强随机数生成器
PHKL_27750	s700、s800	启用 vpar、krng

此外，要使用 HP-UX 11.11 上的 IPv6，Data Protector 需要以下包和补丁：

包或补丁名称	硬件平台	说明
IPv6NCF11i 包或 TOUR 转换补丁	s700、s800	传输转换补丁

HP-UX 11.23

Data Protector 需要以下 HP-UX 11.23 补丁包：

服务包	包名称	说明
使用最新版	QPK1123	适用于 HP-UX 11.23 的最新补丁包

建议为 Data Protector 单元的所有 HP-UX 11.23 客户机安装 HP-UX 11.23 单个补丁：

补丁名称	硬件平台	说明
PHKL_32272 [1]	s700、s800	用于修复 getacl/setacl 中间歇性故障的更改。
PHSS_41178	s700、s800	连接器和 fdp 累计补丁

HP-UX 11.31

Data Protector 需要以下 HP-UX 11.31 补丁包：

服务包	包名称	说明
使用最新版	QPK1131	适用于 HP-UX 11.31 的最新补丁包

Data Protector 需要以下 HP-UX 11.31 单个补丁：

补丁名称	硬件平台	说明
PHCO_38050	Itanium、PA-RISC	pthread 库累计补丁
PHKL_38055	Itanium、PA-RISC	调度程序累计补丁
PHSS_41179	Itanium、PA-RISC	连接器和 fdp 累计补丁

SUSE Linux Enterprise Server 系统补丁

使用推荐的最新系统补丁，由 SUSE 提供。

Red Hat Enterprise Linux 系统补丁

使用推荐的最新系统补丁，由 Red Hat 提供。

[1] 此补丁是支持访问控制列表 (ACL) 功能所必需的。

安装补丁

Cell Manager 补丁可以本地安装。 但是，修补客户机需要 安装服务器。 安装服务器 修补后，可以远程修补客户机。

> **重要：**
> 在 HP-UX 系统上，在使用 Cell Manager (CS) 补丁修复 Cell Manager 时，使用 Data Protector omnisv 命令停止 Data Protector 服务，然后在完成修复过程后重新启动。

如果单个补丁包括在补丁包中，您只能安装整个包。 有关详细信息，请参见随补丁提供的安装说明。

要验证系统上安装的补丁类型，可以使用 Data Protector GUI 或 CLI。 请参见验证已安装哪些 Data Protector 补丁 (第 197 页)

在 Symantec Veritas Cluster Server 中配置的 Cell Manager 中安装补丁

为 Cell Manager 组件(CS 补丁和补丁包)安装补丁时，补丁必须首先在本地应用于每个节点。 在 Symantec Veritas Cluster Server 上执行的群集感知的 Cell Manager 的修补程序与升级类似(请参见升级在 Symantec Veritas Cluster Server 中配置的 Cell Manager)，但以下方面例外：

1. 必须跳过配置步骤。 (即，不得执行 omniforsg.ksh。)
2. 在补丁安装之前，不得启动 Data Protector 服务。

在本地安装好补丁后(如果需要)，非 Cell Manager 组件和核心组件必须从已修补的安装服务器推动升级。 对于非群集感知的 Cell Manager，这也是正常补丁安装程序。

安装和删除 Data Protector 补丁包

如果已在系统上安装 Data Protector，则还可以在此系统上安装 Data Protector 补丁包(一组 Data Protector 补丁)。

要在 UNIX 系统上安装一个 Data Protector 补丁包，可以使用 omnisetup.sh 脚本。 在 Windows 系统上，补丁包安装作为可执行文件提供。

也可以删除此补丁包。 在删除补丁包之后，系统中仍会保留上一个 Data Protector 发行版本。 有关详细信息，请参见随补丁包提供的安装说明。

在 UNIX 系统上安装和删除 Data Protector 补丁包

要安装 Data Protector 补丁包，请使用随补丁包文件一起提供的 tar 归档中的 omnisetup.sh 命令。 使用 -bundleadd 选项。

遥测订阅

要选择收集遥测数据，请接受遥测许可协议，并使用omnisetup.sh命令-telemetry选项输入所需的详细信息。

用于遥测的命令选项有：-compname、-proxyhost、-proxyport、-proxyuser、-proxypasswd、-no_telemetry 和 -accept_obsolescence。

有关 omnisetup.sh 命令的更多信息，请参见《Data Protector CLI 参考指南》。

> **注意：**
> 如果在安装过程中未配置遥测订阅，则可以稍后使用 Data Protector GUI 进行配置。

仅可以在安装服务器和 Cell Manager 上安装一个 Data Protector 补丁包。如果安装失败或停止安装，可以继续使用该安装并安装补丁的剩余部分(仅 Linux 系统支持)，将已安装的补丁回滚到之前的补丁级别，或退出安装而不安装所有补丁。

要删除 Data Protector 补丁包，请使用 omnisetup.sh -bundlerem 命令。

有关详细信息，请参见随此补丁或补丁包提供的安装说明。

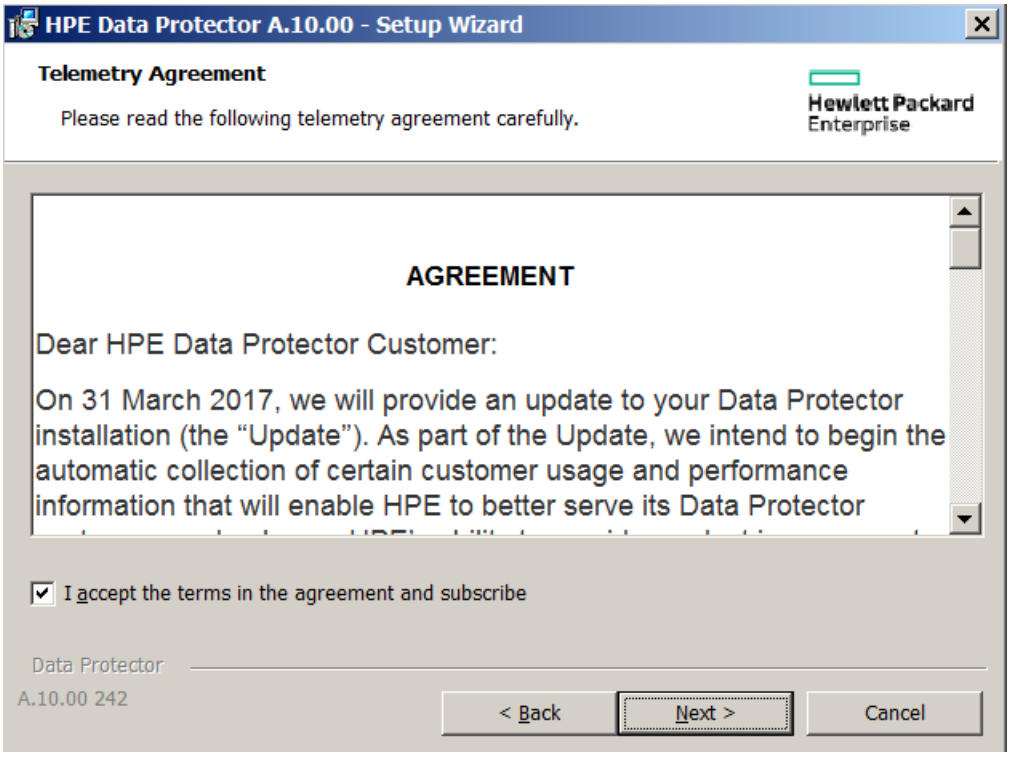
在 Windows 系统上安装和删除 Data Protector 补丁包

适用于 Windows 的 Data Protector 补丁包作为可执行文件(例如 DPWINBDL_00701.exe)提供。可以在安装服务器、Cell Manager 或者客户机系统上安装一个 Data Protector 补丁包。

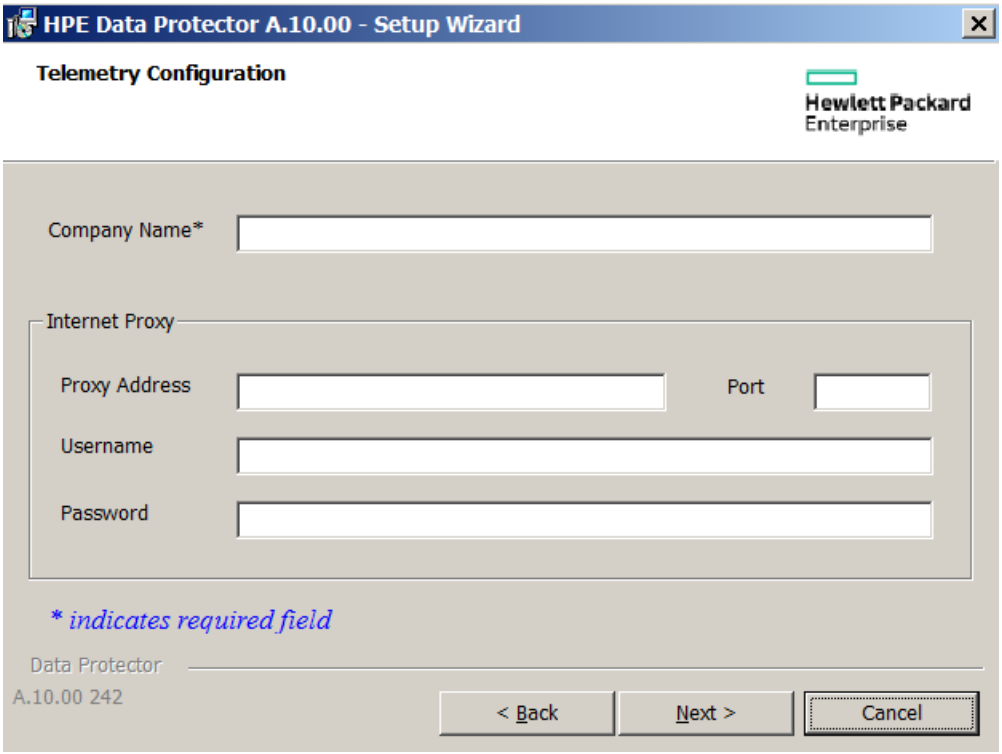
要在 Windows 系统上安装补丁包，请执行 *BundleName*.exe 命令。

遥测订阅

- **遥测协议**：要选择收集遥测数据，请接受遥测许可协议，并输入所需的详细信息。有关遥测的更多信息，请参见《Data Protector 管理指南》。



- **遥测配置**：接受协议后，您需要更新以下参数：



- 公司名称：公司的名称。
- 代理地址：代理服务器的地址。
- 端口：代理服务器的端口。
- 用户名：用于连接代理服务器的用户名。
- 密码：给定用户名的密码。

> **注意：**
> 将 Cell Console (CC) 客户机的遥测数据加载到 Data Protector 基础架构需要代理配置。

> **注意：**
> 如果在安装过程中不选择配置遥测订阅，则可以稍后使用 Data Protector GUI 进行配置。

此命令可识别在系统上安装的组件并将其升级到最新的补丁。

要删除 Data Protector 补丁包，可使用 `remove_patch.bat` 命令，该命令位于 `utilns` 目录中的默认 Data Protector 命令位置。

`remove_patch`*BundleNameDPInstallationDepot* 其中 *DPInstallationDepot* 是安装了 Data Protector (非补丁包)的位置。 例如，要删除补丁包 `b701`，其中 Data Protector 从 `D:\WINDOWS_OTHER` 进行安装，请执行：

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

可以从Data Protector、安装服务器 或者客户机系统中删除 Cell Manager 补丁包。

> **注意：**
> 在 Windows 系统上，还可以使用 `remove_patch.bat` 命令删除单个补丁。 但是，请确保在其他单独补丁仍然安装在系统上之前，不要删除核心补丁。 否则，将无法在之后删除其他单个补丁。
>
> 在系统上安装一些在主要版本后引入的 Data Protector 组件时，确保此系统上的产品已更新回至补丁级别，在该级别，此类组件已知，或者在卸载核心补丁或补丁包之前，删除此类组件。 有关删除 Data Protector 组件的信息，请参见 更改 Data Protector 软件组件 (第 207 页) 部分。

有关详细信息，请参见随此补丁或补丁包提供的安装说明。

下载内部数据库补丁

对于 Data Protector 9.07 和更高版本，在删除补丁之前，IDB 需要降级。

要降级 IDB 补丁，请执行以下操作：

1. 通过执行以下命令，停止除 IDB 以外的所有服务：

   ```
   omnisv stop
   omnisv start -idb_only
   ```
2. 执行 IDB 降级至 Data Protector 9.04 级别：

   Windows 系统：

   ```
   cd %DP_HOME_DIR%bin\dbscripts
   omnidbutil -run_script CPE\downgrade_to_904.sql
   ```

   GNU/Linux 或 UNIX 系统：

   ```
   cd /opt/omni/sbin/dbscripts
   omnidbutil -run_script CPE/downgrade_to_904.sql
   ```
3. 继续删除补丁并删除所有补丁，直到 Data Protector 版本可升级至且早于 DP 9.04。
4. 删除补丁后，执行备份或还原前，立即重新升级至最低 9.04 或更高版本。

管理站点特定补丁和热修复

站点特定补丁 (SSP) 和热修复 (HF) 将手动应用于受影响的客户机或 Cell Manager。

准备用于远程安装 SSP 或 HF 的安装服务器

Data Protector SSP 或 HF 包由客户支持提供。必须将 SSP 或 HF 包复制到位于以下位置的安装服务器仓库：

UNIX： `/opt/omni/databases/vendor/ssphf`

Windows： `Data_Protector_program_data\depot\ssphf`(例如：`C:\ProgramData\Omniback\depot\ssphf`)

> **注意：**
> 修补程序以 ZIP 文件的方式提供。在安装服务器上使用 SSP 或 HF 之前，必须对这些文件进行解压缩。对于 Windows，可以将提取的 zip 文件复制到 `Data_Protector_program_data\depot\ssphf`。对于 Linux/UNIX，在将 SSP 或 HF 复制到安装服务器之后，必须在 Linux/UNIX 上对提取的 tar.gz 文件进行解压缩(使用 gzip)。安装服务器上预期的 SSP 或 HF 格式对于 Windows 系统为 ZIP，对于 Linux/UNIX 系统为 TAR。

要检查安装服务器上可用于远程安装的 SSP/HF 包，请执行以下操作：

1. 在“上下文 (Context)”列表中，选择**客户机 (Clients)**。
2. 在“范围 (Scoping)”窗格中，展开**安装服务器 (Installation Servers)** 并选择单元中要进行 SSP/HF 推送安装的目标系统。
3. 在“结果 (Results)”区域中，单击 **SSP 和 HF (SSPs and HFs)...** 打开 SSP/HF 弹出窗口。
   如果在系统中找到了 SSP/HF，则需要查看安装服务器上的 SSP/HF ID 和 SSP/HF 数量。
4. 单击**确定**关闭窗口。

在客户机上安装站点特定补丁或热修复

在将 SSP/HF 包复制到安装服务器后，可以使用 Data Protector GUI 中提供的 SSP/HF 选择列表来选择用于安装的 SSP/HF。如果选择了 SSP/HF，则所有其他 Data Protector 组件将被禁止选中，因为一次只能安装一个 SSP/HF 包。SSP/HF 可提供各种 Data Protector 组件的二进制文件，只有已安装的 Data Protector 组件的二进制文件才会应用于系统。但由于所有适用的二进制文件都会应用于系统，因此 SSP/HF 包的状态仍显示为已安装。

> **注意：**
> 也可以在 MoM-GUI 中进行 SSP/HF 包的远程安装。

SSP/HF 包的远程安装指的是在远程系统上部署 SSP/HF 包，提取包，并将适用的二进制文件复制到其目标位置。这样，它就不会处理替换在使用文件所需的特殊过程。

要在客户机上手动安装 SSP/HF，请执行以下操作：

- 将 SSP/HF 存档包复制到目标主机并进行提取。
- 停止 Data Protector 服务。只能停止受影响的服务或进程。
- 按以下方式应用 SSP/HF 二进制文件：
  - 将文件从提取的 SSP/HF 包复制到适用的目标位置。(仅复制为其安装 Data Protector 组件的文件)。
  - 将 `CII_<SSPHFNAME>` 复制到其相应的位置。
    例如：
    Windows： `Data_Protector_program_data\config\Client\ssphf`
    其他平台： `\etc\opt\omni\client\ssphf`

此外，还可以使用 `ob2install` 命令在客户机上安装 SSP/HF。有关 `ob2install` 命令的详细信息，请参见 `ob2install` 手册页。

多数情况下，需要手动安装 SSP/HF 包，其中提供了所列的一些二进制文件：

- 单元服务器二进制文件 - 尤其是服务和会话管理器二进制文件。
- CORE 二进制文件 - **Windows**： Inet 服务二进制文件和编目消息。例如 OmniInet.exe、OmniEnu.dll 等等。
- GUI 二进制文件 - 当在需要应用此类 SSP/HF 的主机上使用 Data Protector GUI 时。

> **注意：**
> 将禁止把组件添加到正在 MS 群集服务器上运行的群集感知型 Cell Manager，因为这样无法远程安装 SSP/HF，而必须手动将其应用于所有适用的群集节点。

恢复被 SSP/HF 替换的二进制文件

在远程安装 SSP/HF 二进制文件期间，当前文件进行备份并留在系统上供以后使用。

例如，

Windows： Data_Protector_program_data\tmp\ssphf\<SSPHFNAME>\<DATE_TIME>

其他平台： /var/opt/omni/tmp/ssphf/<SSPHFNAME>/<DATE_TIME>。(确切的位置取决于平台)。

要恢复被 SSP/HF 推送安装替换的二进制文件，请考虑以下方法之一：

- 手动恢复已备份的二进制文件。
- 将受影响的组件重新安装到系统。(首选方法)
- 从 Data Protector GUI 升级系统。(**客户机**上下文)
- 从 Data Protector 安装向导执行修复操作。(仅适用于 Windows 系统)
- 安装任何其他 SSP/HF 包，其中包含了正在打包的作为将要替换的旧 SSP/HF 一部分的所有二进制文件。

每个 SSP/HF 推送操作都会在以下位置创建自己的日志，该日志可用于对失败的操作进行故障诊断：

Windows： Data_Protector_program_data\log\ssphf_install_<DATE_TIME>.log

Unix： /var/opt/omni/log/ssphf_install_<PID>.log(确切的位置取决于平台)。

验证已安装的 SSP 或 HF

可以使用 Data Protector GUI 或 CLI 验证在单元中的系统上安装了哪些 Data Protector 站点特定补丁或热修复。

> **注意：**
> 成功安装 SSP/HF 后，SSP 和 HF 将安装状态显示为Installed。在失败的情况下，将会恢复二进制文件，并且不列出此类 SSP/HF 的状态。

SSP/HF 的远程安装仅安装已在目标主机上安装的组件的二进制文件。SSP/HF 包可能显示以下状态之一：

- 已安装 - 已复制在系统上安装的 Data Protector 组件的所有 SSP/HF 二进制文件。
- 部分 - 未安装 SSP/HF 包中对应已在系统上安装的 Data Protector 组件的少量二进制文件。由于两种原因可能发生这种情况：

1. 如果安装了完整的 SSP/HF 包，SSP/HF 将被标记为Installed。但在某个时间点，如果来自原始安装的另一个 SSP/HF 或 Data Protector 组件被推送到系统，覆盖了 SSP/HF 提供的部分二进制文件，则这类包的状态将更改为Partly安装。
2. 如果 SSP/HF 包提供了用于多个 Data Protector 组件(例如：da 和 ma)的二进制文件，并且系统中仅安装了其中很少的组件(例如：da)，则仅在系统中应用已安装组件(即 da)的二进制文件。这类包的安装状态将显示为Installed。稍后，如果在系统上安装了 ma 组件，该包的状态将变为Partly安装。

> **注意：**
> 如果 SSP/HF 包安装的所有二进制文件都被其他某些二进制文件替换，则这类 SSP/HF 不再被视为已安装，也不会显示在 SSP/HF 状态列表中。

要查看已更改的 SSP/HF 二进制文件列表，请执行以下操作：

- 使用调试选项运行 Inet 服务。
- 检查已安装的 SSP/HF 包的状态。
- 检查已更改的二进制文件的 Inet 日志。

使用 GUI 验证 SSP 或 HF 包

使用 **Data Protector GUI** 验证特定客户机上已安装哪些 **SSP/HF**：

1. 在“上下文 (Context)”列表中，选择**客户机 (Clients)**。
2. 在“范围 (Scoping)”窗格中，展开**客户机 (Clients)** 并选择单元中要验证已安装 SSP/HF 的系统。
3. 在“结果 (Results)”区域中，单击 **SSP 和 HF (SSPs and HFs)...** 打开 SSP/HF 弹出窗口。
   如果在系统上找到了 SSP/HF，验证操作将返回 SSP/HF ID 和每个 SSP/HF 的状态以及已安装的 SSP/HF 数量。
4. 单击**确定**关闭窗口。

使用 CLI 验证 SSP 或 HF

要使用 Data Protector CLI 验证特定客户机上安装了哪些 SSP/HF，请执行 `omnicheck -ssphf -host` *`hostname`* 命令，其中，*hostname* 是要验证的系统的名称。

有关 omnicheck 命令的详细信息，请参见 omnicheck 手册页。

更改 Data Protector 软件组件

本节描述了在 Windows、HP-UX、Solaris 和 Linux 系统中删除和添加 Data Protector 软件组件的步骤。有关特定操作系统支持的 Data Protector 组件的列表，请参见Data Protector 产品声明、软件说明和参考。

Data Protector 软件组件可在 Cell Manager 或客户机上使用 Data Protector GUI 添加。使用 安装服务器 功能远程安装选定组件。有关详细过程，请参见远程安装 (第 83 页)。

Data Protector 组件可在 Cell Manager、安装服务器 或客户机本地删除。

在 Windows 系统中

在 **Windows** 系统上添加或删除 **Data Protector** 软件组件。

仅当具有相同补丁级别的 Data Protector 安装仓库可用时，方可执行此过程。在某些情况下，需要设置安装仓库的路径，例如：**\\<DP_IS_SYSTEM>\Omniback\x8664**。

1. 在 Windows 控制面板中，单击**添加或删除程序/程序和功能**。
2. 选择 **Data Protector 10.00** 并单击**更改**。
3. 单击**下一步 (Next)**。
4. 在“程序维护”窗口中，单击**修改**，然后单击**下一步**。
5. 在“自定义设置”窗口中，选择要添加的组件和/或取消选择要删除的软件组件。单击**下一步 (Next)**。
6. 单击**安装 (Install)** 开始安装或删除软件组件。
7. 安装完成后，单击**完成 (Finish)**。

群集感知客户机

如果是在群集感知客户机上更改 Data Protector 软件组件，则必须在每个群集节点从安装包本地完成此操作。然后，必须使用 GUI 手动将虚拟服务器主机名导入到 Data Protector 单元中。

在 HP-UX 系统中

可以使用 安装服务器 功能添加新组件。

要删除组件，请使用 swremove 命令。

步骤

删除 Data Protector 软件组件

1. 以 root 身份登录并运行 swremove 程序。
2. 依次双击 **B6960MA**、**DATA-PROTECTOR**、**OB2-CM** 以显示 Data Protector 组件的列表。
3. 选择要删除的组件。
4. 在**操作**菜单中，单击**标记以删除**来标记要删除的组件。
5. 标记完要删除的组件后，单击**操作**菜单中的**删除**，然后单击**确定**。

> **注意：**
> 在标记要删除的 Data Protector 组件时，如果剩余组件无法正常操作，则会弹出**依赖性消息对话 (Dependency Message Dialog)** 框，显示有依赖性的组件列表。

Oracle Server 详细信息

在 Oracle Server 系统上卸载 Data ProtectorOracle Server 集成后，Oracle Server 软件仍链接到 Data ProtectorDatabase Library。您必须删除此链接，否则删除该集成后将无法启动 Oracle Server。有关详细信息，请参见《*Data Protector 集成指南*》。

在 Linux 系统上

可以使用 安装服务器 功能添加新组件。在 Linux 系统上，某些 Data Protector 组件互相依赖，如果删除某一个，则无法正常操作。下表显示了组件及它们之间的依赖关系。

Linux 上的 Data Protector 软件组件依赖关系

组件	依赖
Cell Manager	
OB2-CC、OB2-DA、OB2-MA 和 OB2-DOCS	OB2-CORE 和 OB2-TS-CORE
OB2-CS	OB2-CORE、OB2-TS-CORE 和 OB2-CC
OB2-TS-CS、OB2-TS-JRE、OB2-TS-AS、OB2-WS、OB2-JCE-DISPATCHER、OB2-JCE-SERVICEREGISTRY	OB2-CORE、OB2-TS-CORE 和 OB2-CC
安装服务器	
OB2-CORE-IS	OB2-CORE
OB2-CF-P 和 OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	OB2-CORE-IS、OB2-CF-P 和 OB2-TS-CFP
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP、OB2-CORE-IS、OB2-CF-P 和 OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

步骤

从 **Linux** 系统删除 **Data Protector** 组件

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 输入 `rpm | grep OB2` 命令列出已安装的所有 Data Protector 组件。
3. 以与安装顺序相反的顺序，使用 `rpm -e` *`package name`* 命令删除步骤 2 中提到的组件并按提示继续。

在其他 **UNIX** 系统上

手动从 UNIX 系统(而不是 HP-UX 或 Linux)上的 Data Protector 客户机删除组件时，更新 `/usr/omni/bin/install` 中的 `omni_info` 文件。

对于每个删除的组件，请从 `omni_info` 文件中删除相关的组件版本字符串。

如果仅从 Data Protector 客户机中删除组件而没有从单元中导出客户机，则需要更新 `cell_info` 文件中的单元配置(在 Cell Manager 上)。方法是在安装有单元控制台的单元中的系统上执行以下命令：

```
omnicc -update_host HostName
```

验证安装

需要检查 Data Protector 软件组件是否在 Cell Manager 或客户机系统中正常运行时，可以使用 Data Protector 图形用户界面验证安装。

先决条件

必须具有适用于客户机系统类型(UNIX 系统或 Windows 系统)的安装服务器。

步骤

1. 在“上下文列表 (Context List)”中，单击**客户机 (Clients)**。
2. 在范围窗格中，展开**客户机**，右键单击 Cell Manager 或客户机系统，然后单击**检查安装**以打开向导。
3. 此时将列出相同类型(UNIX 系统或 Windows 系统)的所有客户机系统。 选择要验证其安装的客户机，然后单击**完成**开始验证。

验证的结果将显示在“检查安装”窗口中。

卸载 **Data Protector** 软件

如果您的系统配置更改，则可能要从系统中卸载 Data Protector软件或删除部分软件组件。

卸载就是从系统中删除所有 Data Protector 软件组件，包括 Cell Manager 计算机上的 IDB 对此系统的*所有*参考。但是，默认情况下，Data Protector 配置数据会保留在系统中，因为将来升级 Data Protector 时可能需要这些数据。要在卸载 Data Protector 软件后删除配置数据，请删除安装了 Data Protector 的目录。

如果 Data Protector 安装目录中有其他数据，请确保在卸载 Data Protector 前将这些数据复制到其他位置。否则，卸载过程中将删除这些数据。

从单元中卸载 Data Protector 软件需要以下步骤：

1. 使用 GUI 卸载 Data Protector 客户机软件。请参见卸载 Data Protector 客户机 (第 211 页)。
2. 卸载 Data Protector Cell Manager 和 安装服务器。请参见卸载 Cell Manager 和 安装服务器 (第 212 页)。

您也可以不用卸载 Cell Manager 或客户机即可卸载 Data Protector 软件组件。请参见更改 Data Protector 软件组件 (第 207 页)。

在 UNIX 上，还可以手动删除 Data Protector 软件。请参见在 UNIX 上手动删除 Data Protector 软件 (第 218 页)。

先决条件

从计算机中卸载 Data Protector 软件前，请检查以下内容：

- 确保计算机的所有相关参考都已从备份规范中删除。否则，Data Protector 将尝试备份未知的系统，而此部分备份规范将会失败。有关如何修改备份规范的说明，请参见 *Data Protector 帮助*索引：“修改, 备份规范”。
- 确保要卸载的系统上没有连接和配置备份设备或磁盘阵列。导出系统后，Data Protector 不再能够使用原单元中的备份设备或磁盘列阵。
- 在卸载之前，确保关闭所有未处理的 GRE 开机请求。此外，确保完成或中止正在进行中的实时迁移会话。

卸载 **Data Protector** 客户机

> **注意：**
> 远程卸载过程要求为正在卸载其 安装服务器 软件的平台安装 Data Protector。

在 **Data Protector GUI** 中远程卸载客户机

1. 在“上下文列表 (Context List)”中，切换到**客户机 (Clients)** 上下文。
2. 在“范围窗格”中，展开**客户机**，右键单击要卸载的客户机，然后单击**删除**。此时会询问您是否要同时卸载 Data Protector 软件。
3. 单击**是 (Yes)** 从客户机中卸载所有软件组件，然后单击**完成 (Finish)**。

客户机将从“结果区域 (Results Area)”的列表中删除，Data Protector 软件将从硬盘中删除。

请注意，Data Protector 配置数据将保留在客户机系统中。要删除配置数据，请删除安装了 Data Protector 的目录。

卸载群集客户机

如果您的 Data Protector环境中具有群集感知客户机且要卸载它们，则必须在本地执行此操作。过程与卸载 Cell Manager 或 安装服务器 相同。请参见卸载 Cell Manager 和 安装服务器 (第 212 页)。

群集客户机将从“结果区域 (Results Area)”的列表中删除，Data Protector 软件将从硬盘中删除。

TruCluster

要卸载 TruCluster 客户机，请首先导出虚拟节点。然后从节点卸载 Data Protector 客户机。

HP OpenVMS 客户机

无法使用 安装服务器 远程删除 Data Protector OpenVMS 客户机。必须在本地卸载它。

从 OpenVMS 系统中卸载 Data Protector 客户机

1. 如从单元导出客户机 (第 172 页)中所述，首先使用 Data Protector GUI 从 Data Protector 单元中导出该客户机。

   当询问是否要同时卸载 Data Protector 软件时，选择**否**。
2. 要删除实际的 Data Protector 客户机软件，请登录到 OpenVMS 客户机上的 SYSTEM 帐户并执行以下命令：`$ PRODUCT REMOVE DP`。对于出现的提示请选择YES。

   > **重要：**
   > 这将关闭 Data Protector 服务并删除 OpenVMS 系统上所有与 Data Protector 关联的目录、文件和帐户。

卸载 Cell Manager 和 安装服务器

本节描述了从 Windows、HP-UX 和 Linux 系统上卸载Data ProtectorCell Manager 和 安装服务器 软件的步骤。

从 Windows 系统中卸载

从 Microsoft Server 群集中卸载

从 Windows 系统中卸载 Data Protector 软件

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 在 Windows 控制面板中，单击**添加/删除程序**。
3. 根据您是否希望在系统上留下配置数据，将应用不同的操作：

   > **重要：**
   > 如果卸载后将 Data Protector 配置数据保留在系统中，以后又安装了低于卸载版本的 Data Protector Cell Manager，则注意，这些配置数据将不可用。
   >
   > 要成功安装较低版本，请在安装期间选择将删除配置数据的选项。

- 要卸载 Data Protector 并将 Data Protector 配置数据保留在系统中，请选择 **Data Protector 10.00** 并单击**删除**。
- 要卸载 Data Protector 并删除 Data Protector 配置数据，请选择 **Data Protector10.00**，单击**更改**，然后单击**下一步**。在“程序维护 (Program Maintenance)”对话框中，选择**删除 (Remove)**。选择**永久删除配置数据**并单击**下一步**。

4. 卸载完成后，单击**完成**退出向导。

从 HP-UX 系统中卸载

适用于 HP-UX 的 Cell Manager 始终使用 `omnisetup.sh` 命令在本地安装。因此，必须使用 `swremove` 实用程序 在本地将其卸载。

> **重要：**
> 如果卸载后将 Data Protector 配置数据保留在系统中，以后又安装了低于卸载版本的 Data Protector Cell Manager，则注意，这些配置数据将不可用。
>
> 要成功安装较低版本，请在卸载后从系统中删除剩余的 Data Protector 目录。

先决条件

- 使用 `omnisetup.sh -bundlerem` 命令删除已安装的所有 Data Protector 补丁包。请参见在 UNIX 系统上安装和删除 Data Protector 补丁包 (第 201 页)。

步骤

开始卸载 Data Protector 软件前，先关闭 Data Protector 和/或 Cell Manager 系统上运行的 安装服务器 进程：

1. 以根身份登录并执行 `omnisv -stop`。
2. 输入 `ps -ef | grep omni` 命令以验证是否所有进程都已关闭。执行 `ps -ef | grep omni` 后，此时不应再列出任何 Data Protector 进程。

   如果有任何 Data Protector 进程在运行，则应在继续进行卸载之前，使用 `kill` *`process_ID`* 命令将其停止。
3. 运行 `/usr/sbin/swremove DATA-PROTECTOR` 以卸载 Data Protector 软件。

要删除您系统上剩余的 Data Protector 目录，请参见在 UNIX 上手动删除 Data Protector 软件 (第 218 页)。

卸载 Serviceguard 上配置的 Cell Manager 和/或 安装服务器

如果您的 Cell Manager 和/或 安装服务器 是在 Serviceguard 群集上配置的，请执行以下步骤来卸载软件。

主节点

登录到主节点，并执行以下步骤：

1. 停止 Data Protector 包：

   `cmhaltpkg` *`PackageName`*

   其中 *`PackageName`* 表示群集包名称。

例如：

```
cmhaltpkg ob2cl
```

2. 停用卷组的群集模式：

   ```
   vgchange -c n vg_name
   ```

   (其中*vg_name*代表位于 /dev 目录的子目录中的卷组的路径名)。

   例如：

   ```
   vgchange -c n /dev/vg_ob2cm
   ```

3. 激活卷组：

   ```
   vgchange -a y -q y vg_name
   ```

   例如：

   ```
   vgchange -a y -q y /dev/vg_ob2cm
   ```

4. 将逻辑卷装载为共享磁盘：

   ```
   mount  lv_path shared_disk
   ```

   (其中 *lv_path* 代表逻辑卷的路径名，*shared_disk* 代表装载点或共享目录)。

   例如：

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

5. 使用 swremove 实用程序删除 Data Protector。
6. 删除软链接：

   ```
   rm /etc/opt/omni
   rm /var/opt/omni
   ```

7. 删除备份目录：

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```

8. 删除 Data Protector 目录及其内容：

   ```
   rm -rf /opt/omni
   ```

9. 卸载共享磁盘：

   ```
   umount shared_disk
   ```

   例如：

   ```
   umount /omni_shared
   ```

10. 停用卷组：

    ```
    vgchange -a n vg_name
    ```

    例如：

    ```
    vgchange -a n /dev/vg_ob2cm
    ```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 激活卷组：

   ```
   vgchange -a y vg_name
   ```

2. 装载共享磁盘：

   mount *lv_pathshared_disk*
3. 使用 swremove 实用程序删除 Data Protector。
4. 删除软链接：

   rm /etc/opt/omni

   rm /var/opt/omni
5. 删除备份目录：

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save
6. 删除 Data Protector 目录及其内容：

   rm -rf /opt/omni
7. 删除共享文件系统中的目录：

   rm -rf *shared_disk*/etc_opt_omni

   rm -rf *shared_disk*/var_opt_omni

   例如：

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/etc_opt_omni
8. 卸载共享磁盘：

   umount*shared_disk*
9. 停用卷组：

   vgchange -a n *vg_name*

已将 Data Protector 从系统中完全删除。

卸载在 Symantec Veritas Cluster Server 中配置的 Cell Manager 和/或 安装服务器

如果您的 Cell Manager 和/或 安装服务器 是在 Symantec Veritas Cluster Server 上配置的，请执行以下步骤来卸载软件。

主节点

登录到主节点，并执行以下步骤：

1. 使 Data Protector 应用程序资源脱机。
2. 禁用 Data Protector 应用程序资源。
3. 卸载 Data Protector。
4. 删除软链接：

   rm /etc/opt/omni

   rm /var/opt/omni
5. 删除备份目录：

   rm -rf /etc/opt/omni.save

```
rm -rf /var/opt/omni.save
```

6. 删除 Data Protector 目录及其内容：

```
rm -rf /opt/omni
```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到辅助节点。
2. 卸载 Data Protector。
3. 删除软链接：

```
rm /etc/opt/omni
rm /var/opt/omni
```

4. 删除备份目录：

```
rm -rf /etc/opt/omni.save
rm -rf /var/opt/omni.save
```

5. 删除 Data Protector 目录及其内容：

```
rm -rf /opt/omni
```

6. 删除共享文件系统中的目录：

```
rm -rf shared_disk/etc_opt_omni
rm -rf shared_disk/var_opt_omni
```

例如：

```
rm -rf /omni_shared/etc_opt_omni
rm -rf /omni_shared/var_opt_omni
```

已将 Data Protector 从系统中完全删除。

从 Linux 系统中卸载

先决条件

- 使用 `omnisetup.sh -bundlerem` 命令删除已安装的所有 Data Protector 补丁包。请参见在 UNIX 系统上安装和删除 Data Protector 补丁包 (第 201 页)。

Cell Manager

适用于 Linux 的 Cell Manager 始终使用 `omnisetup.sh` 命令在本地安装。因此，必须使用 `rpm` 实用程序 在本地将其卸载。

> **重要：**
> 如果卸载后将 Data Protector 配置数据保留在系统中，以后又安装了低于卸载版本的 Data Protector Cell Manager，则注意，这些配置数据将不可用。
>
> 要成功安装较低版本，请在卸载后从系统中删除剩余的 Data Protector 目录。

要卸载 Data Protector Cell Manager，请按如下方式继续操作：

1. 确保已终止所有 Data Protector 会话并退出图形用户界面。
2. 输入 `rpm -qa | grep OB2` 命令以列出 Cell Manager 上安装的所有 Data Protector 组件。
   与 Cell Manager 关联的组件如下：

OB2-CORE	Data Protector 核心软件
OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-DISPATCHER	作业控制引擎调度程序
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。
OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 指南和 WebHelp 格式的 *Data Protector 帮助*。

   如果系统上还安装了 Data Protector 客户机或 安装服务器，则其他组件也将列出。

   > **注意：**
   > 要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 `rpm -e package name` 命令删除上一步中提到的组件并按提示继续。

安装服务器

适用于 Linux 上的 UNIX 的 安装服务器 始终使用 `omnisetup.sh` 命令在本地安装。因此，必须使用 `rpm` 实用程序 在本地将其卸载。

要卸载 Data Protector 安装服务器，请按如下方式继续操作：

1. 确保已终止所有 Data Protector 会话并退出 GUI。
2. 输入 `rpm -qa | grep OB2` 命令以列出所有 Data Protector 组件和 安装服务器 系统上存储的远程安装包。
   与 安装服务器 关联的组件和远程安装包如下：

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装 安装服务器，则已安装该子产品包。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器 核心软件。
OB2-CFP	适用于所有 UNIX 平台的公用 安装服务器 核心软件。
OB2-TS-CFP	适用于所有 UNIX 平台的公用 安装服务器 技术堆栈软件
OB2-DAP	适用于所有 UNIX 系统的磁盘代理远程安装包。
OB2-MAP	适用于所有 UNIX 系统的介质代理远程安装包。
OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于所有 UNIX 系统的单元控制台远程安装包。

如果系统上安装了其他 Data Protector 组件，则其他组件也将列出。

有关组件和依赖关系的完整列表，请参见Linux 上的 Data Protector 软件组件依赖关系 (第 209 页)。

> **注意：**
> 要保留任何其他已安装的 Data Protector 组件，则必须保留已安装的 OB2-CORE 组件，因为其他组件都依赖于它。

3. 以与安装顺序相反的顺序，使用 `rpm -e` *`package name`* 命令删除上一步中提到的组件并按提示继续。

在 UNIX 上手动删除 Data Protector 软件

卸载 UNIX 客户机前，应先将其从单元中导出。有关相应的过程，请参见从单元导出客户机 (第 172 页)。

HP-UX 系统

要手动从 HP-UX 系统中删除文件，请执行以下操作：

1. 运行 `/usr/sbin/swremove DATA-PROTECTOR` 以删除 Data Protector 软件。
2. 使用 `rm` 命令删除以下目录：

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   至此，系统中不再有 Data Protector 参考。

Linux 系统

要手动从 Linux 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Solaris 系统

要手动从 Solaris 系统中删除文件，请使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

其他 UNIX 系统和 Mac OS X 系统

使用 rm 命令从以下目录中删除文件，然后删除目录：

```
rm -fr /usr/omni
```

第 7 章： 升级 Data Protector

本章提供执行 Data Protector 升级和迁移任务的指示信息。

> **注意：**
> 在安装期间，需要为 Inet 打开以下端口：
> - Data Protector 全新安装 - 5565
> - Data Protector 升级安装 - 5555

升级概述

升级现有产品版本之前，请考虑以下几点：

- 有关支持的和不再支持的平台和版本的信息，请参见 https://softwaresupport.softwaregrp.com/ 和 Data Protector 产品声明、软件说明和参考。

  在不再支持 Cell Manager 的平台上，首先将 Cell Manager 迁移至支持的平台，然后将其升级到 Data Protector10.00。有关详细信息，请参见将 Cell Manager 迁移到其他平台 (第 224 页)。

  作为不受支持的功能区，Data Protector10.00 中不提供 Data Protector Java 图形用户界面。如果已安装 Data Protector Java 图形用户界面的 Data Protector 单元中存在 UNIX 系统，则在单元升级过程中，您需要选择其他系统来担任 Data Protector 图形用户界面客户机的角色。这些客户机应该在初始(原始)Data Protector 图形用户界面支持的操作系统上运行。
- 为 Data Protector10.00 之前的版本发布的许可证密码将不再支持此版本。

  您需要具有有效的支持协议，才能按照支持协议中列出的许可证类型和数量获取新许可证密码。

  在开始升级之前，请检查已在 Data Protector 环境中安装的许可证密钥数量和类型，并将其与支持协议中列出的许可证数量和类型进行比较。

  如果支持协议中列出的许可证少于或不同于在环境中实际安装的许可证，您将不能开始升级。否则，由于缺少许可证密钥，将存在 Data Protector 环境不再能运行的风险。首先，联系您的销售代表或合作伙伴，以确定需执行哪些步骤来消除支持合同所涵盖的功能许可证与当前使用的实际许可证(在早于 Data Protector 9.00 的 Data Protector 版本中使用的许可证)之间的差异。

  有关许可的详细信息，请参见Data Protector 许可 (第 243 页)。
- 升级后，Cell Manager 和安装服务器必须安装相同的 Data Protector 版本。尽管同一单元中支持旧版 Data Protector 磁带客户机和介质代理，但强烈建议客户机另外安装同一版本的 Data Protector 组件。

  有关在升级之后旧版磁带客户机和介质代理存在的限制，请参见*Data Protector 产品声明、软件说明和参考*。
- 升级多单元(MoM)环境后，所有 Cell Manager 必须安装相同的 Data Protector 版本。
- 借助 Data Protector 10.00，基本计划程序和高级计划程序已过时，被基于 Web 的新计划程序所替代。所有现有的调度程序会自动迁移至新的调度程序。迁移不需要任何用户交互。

  如果在升级过程中迁移失败，您可以手动运行以下命令，以便将现有调度程序成功迁移到新的调度程序：

```
omnidbutil -migrate_schedules
```

- 借助 Data Protector 10.00，JBoss 7.1 替换为 WildFly 10。在 Data Protector 升级过程中，以下 JBoss 配置会自动迁移到 WildFly：
  - 日志记录器级别和格式
  - LDAP 配置
  - PostgreSQL 凭据

> **重要：**
> 升级之后，除上面列出的配置以外，在 JBoss 7.1 `standalone.xml` 文件中所做的任何更改都必须手动添加到 WildFly 配置文件中。

请注意，在升级过程中，Data Protector 会为 *Data_Protector_program_data* 文件夹中的旧 JBoss 配置文件创建备份。默认情况下，这些文件可从以下位置获取：

- Linux：`/etc/opt/omni/server/AppServer_<versionNo>`
- Windows：`C:\ProgramData\OmniBack\Config\Server\AppServer_<versionNo>`

先决条件

- 在升级之前对现有 IDB 运行数据库一致性检查，以验证数据一致性。
- 备份现有 Cell Manager 系统和内部数据库 (IDB)。
- 升级之前，确保所有 GRE Power On 打开请求均已关闭。此外，确保完成或中止正在进行中的实时迁移会话。

限制

- 不支持在升级过程中更改 Cell Manager 平台。仅支持在相同 Cell Manager 平台 (HP-UX 对 HP-UX，Linux 对 Linux，以及 Windows 对 Windows) 上进行升级。

  如果平台不再受支持，则先将 Cell Manager 迁移到受支持的平台，然后再升级到新版本。请参见将 Cell Manager 迁移到其他平台 (第 224 页)。
- 在 UNIX 环境中：在执行升级之前，只能通过 Data Protector 服务运行 Data Protector 进程。为此，请停止 Data Protector 服务、终止任何正在运行的进程并重新启动服务。
- 仅从相同的次要-次要 Data Protector 版本支持内部数据库恢复，在该版本中，内部数据库已备份。这是由于新版本中的内部数据库架构更改。
- 如果您想要恢复早期 Data Protector 版本中已备份的内部数据库，请重新安装该特定版本，导入内部数据库备份介质，然后执行恢复。

升级顺序

若要从早期版本的产品升级单元，请执行如下步骤：

1. 将 Cell Manager 和安装服务器升级到 Data Protector 10.00。UNIX 平台和 Windows 平台上的升级步骤并不相同。

必须先升级当前单元中的 Cell Manager，然后才能升级 安装服务器。

2. 升级 GUI 客户机。
3. 升级已安装联机应用程序集成的客户机，如 Oracle、SAP R/3、Informix Server、Microsoft SQL Server、Microsoft Exchange Server 等等。
4. 升级已安装 Data Protector 介质代理的 (MA) 的客户机。在与 Cell Manager 同平台的所有 MA 客户机上升级 MA 之后，即可立即执行备份。
5. Micro Focus 建议在接下来的两周内升级装有 Data Protector 磁带客户机 (DA) 的客户机。

在 MoM 环境中升级

若要将 MoM 环境升级到 Data Protector 10.00，需要先升级 MoM Manager 系统。完成此升级后，所有尚未升级的以前版本的 Cell Manager 仍能访问中央 MMDB 和中央许可，以及执行备份，但是不能使用其他 MoM 功能。请注意，不支持 Data Protector 10.00 MoM 单元与装有早期版本产品的单元之间的设备共享。在 MoM 环境中进行升级期间，MoM 环境中的任何 Cell Manager 都不应处于运行状态。

支持早期代理版本

只要可能，Data Protector 单元中所有客户机上的 Data Protector 组件都应在定期升级过程中升级到版本 10.00。这可确保客户在单元内的所有系统上都能够从 Data Protector 10.00 的完整功能中受益。

在 10.00 单元中支持早期 Data Protector 版本的磁带客户机和介质代理组件，但有以下限制：

- 仍支持将更早产品版本作为独立产品。要检查产品公布的支持结束日期，请参见网页 https://softwaresupport.softwaregrp.com/。
- 支持受早期 Data Protector 版本的功能集限制。
- 若正在执行涉及不同系统上的客户机的操作，则所有同类型客户机(例如介质代理)必须是同一版本。
- 不支持早期版本的介质代理组件与 NDMP 服务器结合使用。
- 文件系统备份可来源于多个不同版本的磁带客户机，不同版本的介质代理支持备份服务器重复数据删除。磁盘和介质代理版本可能低于或等于 Cell Manager 版本。但是，源重复数据删除需要相同版本的磁带客户机和介质代理，可能低于或等于 Cell Manager 版本。
- 对于 Data Protector StoreOnce 软件存储，磁带客户机和介质代理必须为相同版本。但是，该版本可能低于或等于 Cell Manager 版本。
- 如果客户机上的某个 Data Protector 组件升级到 10.00，则所有其他组件也必须升级到 10.00。
- 最新的 Cell Manager 版本不支持较低版本的集成代理。

如果在与早期产品版本的代理建立连接时出现问题，请首先考虑升级到 9.08。

从单服务器版升级

可以从以下某个版本执行升级：

- 从早期版本的单服务器版 (SSE) 升级到 Data Protector 10.00 单服务器版。有关详细信息，请参见从早期版本的 SSE 升级到 Data Protector 10.00 SSE。
- 从 Data Protector 10.00 单服务器版升级到 Data Protector 10.00。有关详细信息，请参见从 Data Protector 10.00 SSE 升级到 Data Protector 10.00

从早期版本的 SSE 升级到 Data Protector 10.00 SSE

从早期版本的 SSE 升级到 Data Protector 10.00 SSE 的过程与从早期版本的 Data Protector 升级到 Data Protector 10.00 的过程相同。

从 Data Protector 10.00 SSE 升级到 Data Protector 10.00

您必须拥有许可证才能执行从 Data Protector 10.00 单服务器版到 Data Protector 10.00 的升级。有关许可的详细信息，请参见Data Protector 许可 (第 243 页)。

对于以下两种可能的场景，可进行从 Data Protector 10.00 单服务器版到 Data Protector 10.00 的升级：

- Data Protector 单服务器版只安装在一台系统(Cell Manager)上。请参见升级 Cell Manager (第 223 页)。
- Data Protector 单服务器版安装在多台系统上，并且您要合并这些单元。请参见从多个安装升级 (第 223 页)。

> **注意：**
> 要从以前版本的单服务器版升级到 Data Protector 完整安装，请先将该单服务器版升级到同一版本级别的完整安装。

升级 Cell Manager

为了升级单服务器版 Cell Manager，请执行以下步骤：

1. 删除单服务器版许可证：

   Windows 系统：

   ```
   del Data_Protector_program_data\Config\server\Cell\lic.dat
   ```

   UNIX 系统：

   ```
   rm /etc/opt/omni/server/cell/lic.dat
   ```

2. 启动 Data Protector GUI 并添加永久密码。

从多个安装升级

为了升级安装在多台系统上的 Data Protector单服务器版，请执行如下步骤：

1. 选择要作为新 Cell Manager 的某个现有单服务器版系统。请参见选择 Cell Manager 系统 (第 22 页)。
2. 执行以下操作来升级选定的 Cell Manager：

a. 删除单服务器版许可证：

del *Data_Protector_program_data*\Config\server\Cell\lic.dat (在 Windows 系统中)或

rm /etc/opt/omni/server/cell/lic.dat(在 UNIX 系统上)

b. 启动 Data Protector GUI 并添加永久密码。

3. 使用 GUI 将其他单服务器版系统作为客户机导入新创建的 Cell Manager 系统。
4. 从其他系统上卸载 Data Protector 单服务器版。请参见 。
5. 将介质导入到新的 Cell Manager。

有关导入介质的信息，请参见 *Data Protector 帮助*索引：“导入, 介质”。

将 Cell Manager 迁移到其他平台

从 PA-RISC HP-UX 系统迁移到 Intel Itanium HP-UX 系统

Data Protector 不再支持将基于 PA-RISC 架构的 HP-UX 11.11/11.23 系统作为 Cell Manager 平台。因此，在升级之前，必须将基于 PA-RISC 架构的 HP-UX 11.11/11.23 系统从 Cell Manager 迁移到 Intel Itanium 2 架构的 HP-UX 11.23/11.31 系统。

有关迁移步骤的信息，请参见相应产品版本中的《*Data Protector 安装指南*》。

从 32 位/64 位 Windows 迁移到 64 位 Windows/Windows Server 2008 或 Windows Server 2012

Data Protector 不再支持 32 位 Windows 系统作为 Cell Manager 平台。因此，必须在开始升级到 Data Protector 10.00 或更高版本之前，将 Cell Manager 迁移到 64 位 Windows 系统。有关迁移步骤的信息，请参见相应产品版本的《*Data Protector 安装指南*》。

从 Solaris 迁移到 Linux

此部分描述将现有 Cell Manager 从 Solaris 系统迁移到 Linux 系统的过程。

> **重要：**
> Data Protector 10.00 不再支持 Solaris 作为 Cell Manager 平台。因此，使用已安装的 Data Protector 版本升级到 Data Protector 10.00 或更改版本之前，必须先将 Cell Manager 迁移到新平台。

步骤

1. 使用现有的 Data Protector 安装，导出当前 Cell Manager 上的所有介质编目：
   a. 在上下文列表中，单击**设备和介质**。
   b. 在范围窗格中，展开**介质**，然后展开**池**。
   c. 展开要复制其编目的介质所在的介质池。

d. 选择并右键单击介质，然后单击**将编目复制到文件 (Copy Catalog to File)**。
e. 指定 MCF 文件的输出目录，此文件将包含与介质相关的编目数据。
f. 单击**完成**以开始复制，然后退出向导。有关详细信息，请参见《*Data Protector 帮助*》主题*"将编目介质数据复制到 MCF 文件"*。

2. 在将成为新 Cell Manager 的 Linux 系统上安装 Data Protector。有关详细信息，请参见 安装 UNIX Cell Manager (第 26 页)。
3. 如果更改了旧 Cell Manager 上的默认 Data Protector Inet 端口，那么在新 Cell Manager 上也设置相同的 Inet 端口。请参见 更改默认的 Data Protector Inet 端口 (第 306 页)。
4. 将 MCF 文件导入新 Cell Manager：
   a. 在上下文列表中，单击**设备和介质**。
   b. 在范围窗格中，展开**介质**，右键单击**池**，然后单击**从 MCF 文件导入编目**以打开向导。
   c. 指定要导入的 MCF 文件。
   d. 指定会话的其他选项：默认情况下，选择**如有可能，导入到原始池**选项。选择**导入副本作为原件**选项。
   e. 单击**完成**以开始导入，然后退出向导。

   有关详细信息，请参见《*Data Protector 帮助*》主题*"从 MCF 文件导入编目介质数据"*。
5. 在新 Cell Manager 上配置许可证。请参见 Data Protector 产品结构和许可证 (第 267 页)。
6. 如果存在以下情况，还需要执行一些额外步骤：
   - 单元是 MoM 环境的一部分。请参见 MoM 特别事项 (第 225 页)。
   - 单元跨防火墙工作。重新配置新 Cell Manager 上的所有防火墙相关设置。请参见 *Data Protector 帮助*索引："防火墙环境"。
   - 您希望在新 Cell Manager 上有 安装服务器。请参见 安装服务器 特别事项 (第 226 页)。

完成迁移后，可以升级 Data Protector。

MoM 特别事项

如果将在 MoM 中配置新 Cell Manager，那么在完成基本迁移过程后，还需要一些额外的步骤。需要的步骤取决于环境中新旧 Cell Manager 的 MoM 配置。支持的组合有：

- 旧 Cell Manager 过去为 MoM 客户机，新 Cell Manager 将成为同一 MoM Manager 的 MoM 客户机。

  执行以下步骤：

  1. 在 MoM Manager 上，从 MoM Manager 单元导出旧 Cell Manager，并导入新 Cell Manager。请参见 *Data Protector 帮助*索引："客户机系统导出"。
  2. 将 MoM 管理员添加到新 Cell Manager 上的用户列表。请参见 *Data Protector 帮助*索引："MoM 管理员, 添加"。
- 旧 Cell Manager 过去是 MoM Manager；新 Cell Manager 将成为 MoM Manager。

  如果旧 MoM 管理器是 MoM 中的唯一客户机，那么不需要任何操作。否则，请执行以下步骤：

1. 在旧 MoM Manager(旧 Cell Manager)上，导出所有 MoM 客户机。
2. 在新的 MoM Manager(新 Cell Manager)中，导入所有 MoM 客户机。
3. 将 MoM 管理员添加到所有 MoM 客户机上的用户列表。

安装服务器 特别事项

安装服务器 迁移并非作为 Cell Manager 迁移的一部分完成。如果 安装服务器 安装在旧 Cell Manager 上，它不会迁移到新 Cell Manager，并将依旧作为单元的 安装服务器。

要将新 Cell Manager 同时用作 安装服务器，请在迁移后在新 Cell Manager 上安装 安装服务器 组件，并将其导入单元中。请参见 *Data Protector 帮助*索引："安装服务器"。

将 Windows Cell Manager 内部数据库迁移到不同的服务器

以下场景举例说明如何在不同的 Windows Cell Manager 服务器之间迁移内部数据库 (IDB)。

术语

此场景中使用以下术语。

- **OLD_SERVER**。将从中删除 IDB 的源 Cell Manager。
- **NEW_SERVER**。IDB 要移动到的目标 Cell Manager。

先决条件

- 使用命令行参数时，用完全限定域名替换 OLD_SERVER 和 NEW_SERVER。
- 如果 OLD_SERVER 在 Windows 2008 上运行，则 NEW_SERVER 可运行 Windows 2008 或 Windows 2012。
- 如果 OLD_SERVER 在 Windows 2012 上运行，则 NEW_SERVER 必须在 Windows 2012 上运行。
- 这两台服务器必须在 Cell Manager 上安装相同版本的 Data Protector。
- 如果 NEW_SERVER 的 IP 地址与 OLD_SERVER 不同，则您必须联系 Password Center (https://software.microfocus.com/zh-cn/legal/software-licensing)，将许可证移至新的 IP 地址。
- 在 NEW_SERVER 上，必须能够从 OLD_SERVER 导入包含完整 IDB 备份的介质。
  - 如果 IDB 备份位于物理磁带中，则必须在 NEW_SERVER 上配置磁带驱动器或库，并确保磁带可访问。
  - 如果 IDB 备份位于文件库备份设备中，则可能需要从 OLD_SERVER 导出文件库，然后将其导入 NEW_SERVER。有关详细信息，请参见在 NEW_SERVER 上 (第 227 页)。
- 配置、日志和数据库文件存储在 *Data_Protector_program_data* 目录下，通常为 `C:\ProgramData\Omniback`.

如果已安装到其他位置，请记录该位置以供将来使用。

准备迁移

在开始迁移之前，必须先在 OLD_SERVER 和 NEW_SERVER 执行几项任务，将其做好 IDB 迁移的准备。

在 OLD_SERVER 上

- 迁移之前，在 OLD_SERVER 上对现有 IDB 运行扩展的数据库一致性检查，验证数据的一致性。
- 执行现有 IDB 的完整备份。

运行扩展的数据库一致性检查

1. 运行 `omnidbcheck -extended`。

   此命令将从以下方面验证数据一致性：

   - 数据库连接
   - 数据库和架构一致性
   - 数据文件和介质一致性

   如果检测到任何不一致，请确保先修复这些问题，然后再执行迁移。

在 OLD_SERVER 上执行 IDB 的完整备份

有关完整备份 IDB 的详细信息，请参见 *Data Protector 帮助*。

在 NEW_SERVER 上

- 保存在 *Data_Protector_program_data* 目录(通常为 `C:\ProgramData\Omniback\Config\Server\cell\cell_info`)中找到的 `cell_info` 文件的副本。稍后将使用此文件。

使用 omnidownload 和 omniupload 传输文件库的信息

1. 在 OLD_SERVER 上，使用 `omnidownload -library` *`Library`* 将文件库的信息从 Data Protector IDB 下载到 ASCII 文件。

   例如，对于名为 "FL1" 的文件库的 IDB 备份，请使用以下命令：

   ```
   omnidownload –library FL1 –file “C:\tmp\FL1.txt”
   ```

2. 将 `omnidownload` 输出文件复制到 NEW_SERVER。

   例如，复制到 `C:\tmp\FL1.txt`。

3. 在 NEW_SERVER 上，使用 omniupload -create_library <文件名>.txt 上载库文件，并在 NEW_SERVER 上创建新备份设备。

   ```
   omniupload -create_library “C:\tmp\FL1.txt”
   ```

4. 在 NEW_SERVER 上，从新备份设备导入介质。

有关命令的详细信息，请参见《*Data Protector 命令行界面参考*》。有关导入介质的详细信息，请参见 *Data Protector 帮助*。

迁移任务

Linux 的先决条件：

- 如果 IDB 恢复至新主机或 Cell Manager，user 和 group ID 必须与原始 Cell Manager 相同。使用以下命令，在新主机上更改 user 和 group ID，然后安装 Data Protector：
  - 要在原始主机上确定 hpdp user 和 group 的 ID，请使用 cat /etc/passwd。
  - 要在新主机上设置 user 和 group ID，请使用：

    ```
    usermod -u <NEWID> <LOGIN>
    groupmod -g <NEWID> <GROUP>
    usermod -g <GROUP> <LOGIN>
    ```

导入 IDB

在 NEW_SERVER 上导入 IDB

1. 介质导入后，确保可以在 Data Protector GUI 中看到 IDB 备份会话。
2. 创建恢复的 IDB 要使用的新目录。
   例如，在以下位置创建目录：

   ```
   C:\ProgramData\Omniback\server\db80_restore\idb
   ```

   > **注意：**不能将 IDB 从 OLD_SERVER 恢复到 NEW_SERVER 上的相同位置，因为该位置正在使用。

3. 在 Data Protector GUI“上下文列表”中，单击**恢复**。
4. 在“范围窗格”中，展开**恢复对象**，然后展开**内部数据库**。
5. 展开 OLD_SERVER 项，然后单击**内部数据库**。
   a. 在“内部数据库”属性页上，要恢复内部数据库的基本部分，请执行以下操作：
      i. 选择**恢复内部数据库**选项。
      ii. 指定要在恢复期间用于内部数据库服务的临时端口，并将恢复位置指定为 C:\ProgramData\Omniback\server\db80_restore\idb。
      iii. 选择**恢复目录二进制文件**以恢复 IDB 的 DCBF 部分，并选择**恢复到原始位置**。
   b. 在“配置文件”属性页上：
      在 Windows 系统中：
      i. 选择**恢复到原始位置**。

      > **注意：**
      > 确保已选中**恢复配置文件**选项。

      ii. 从**文件冲突处理**列表中选择“保留最新”。

在 UNIX 系统中：

请参见IDB 还原在还原进程结束时失败 (第 233 页)

c. 单击**恢复**以启动恢复 IDB。

在恢复过程中，您可能会看到以下错误消息及一些其他消息，这些消息可忽略：

```
[Major] From: OB2BAR_POSTGRES_BAR@mrou77.usa.hp.com "DPIDB" Time: 10/9/2014
10:35:29 PM The OS reported error while accessing
C:/ProgramData/OmniBack/config/server/certificates: [80] The file exists.
```

d. 恢复完成后，停止并启动 Data Protector 服务。

```
omnisrv -stop
```

```
omnisrv -start
```

注意：
如果在完成 IDB 恢复会话后遇到任何问题，请参见故障排除。

恢复后任务

执行以下恢复后任务。

1. 运行 `omnidbutil -show_db_files`，确保在导入 IDB (第 228 页)的步骤 3 中创建的目录中存在已恢复的文件。
2. 将 NEW_SERVER 添加为 Cell Manager。请参见将 NEW_SERVER 添加为 Cell Manager (第 229 页)
3. (可选)更改 IDB 中 Cell Manager 的名称。请参见更改 IDB 中 Cell Manager 的名称 (第 230 页)。
4. 运行 `omnidbcheck -extended`，验证已恢复 IDB 的一致性。请参见运行扩展的数据库一致性检查 (第 227 页)。

将 NEW_SERVER 添加为 Cell Manager

将 NEW_SERVER 添加为 Cell Manager

1. 在 Data Protector GUI“上下文列表”中，单击**客户机**。
2. 删除 OLD_SERVER 项。
3. 导入 NEW_SERVER，并确保它显示为 Cell Manager。

如果上述步骤不起作用

1. 在文本编辑器中，打开您在准备迁移 (第 227 页)中保存的 `cell_info` 文件。
2. 将包含 NEW_SERVER 的主机名的行复制到粘贴缓冲区。
3. 编辑 `cell_info` 文件。
   a. 从粘贴缓冲区为 NEW_SERVER 添加该条目。
   b. 为 OLD_SERVER 删除该条目，并保存 `cell_info` 文件。
4. 重新启动 GUI。

更改 IDB 中 Cell Manager 的名称

如果 NEW_SERVER 的主机名与 OLD_SERVER 不同，则必须更改 IDB 中 Cell Manager 的名称。

例如，OLD_SERVER 的名称是 oldcm.company.com，NEW_SERVER 的名称是 newcm.company.com。

在 NEW_SERVER 上

1. 运行 omnidbutil -show_cell_name，显示拥有 IDB 的 Cell Manager。
   例如

   ```
   > omnidbutil -show_cell_name
   Catalog database owner: "oldcm.company.com"
   ```

2. 运行 -change_cell_name *OldHost*，将 IDB 的所有权更改为 NEW_SERVER。
   例如

   ```
   > omnidbutil -change_cell_name oldcm.company.com
   This action will change ownership of libraries, devices, media pools and media.
   Are you sure [y/n]? y
   DONE!
   ```

下面的步骤

1. 通过运行 omnicc 命令，将客户机迁移到 NEW_SERVER。
   运行 omnicc -update_all -force_cs 命令，针对单元中的所有客户机，更新 NEW_SERVER cell_info 配置文件中的版本和安装组件信息。
   有关 omnicc 命令的说明，请参见《*Data Protector 命令行界面参考*》。
2. 为 NEW_SERVER 创建新的 IDB 备份规范，因为原始备份规范已配置为使用 OLD_SERVER。
   有关详细信息，请参见 *Data Protector 帮助*。
3. 导航至内部数据库，并检查是否有任何会话处于正在运行状态。如果有，运行 omnidbutil -clear 命令。
4. 停止并启动 Data Protector 服务。
   omnisrv -stop
   omnisrv -start

故障排除

问题

完成 IDB 恢复操作后，从 Data Protector GUI 连接到 Cell Manager 失败

完成恢复操作后，从 GUI 连接到 Cell Manager 失败并报错：

已发生服务器错误。Reported error message:
无法连接到主机。

hpdp-as 服务进程未在侦听端口 7116。

操作

1. 打开命令窗口并运行 netstat 命令，验证侦听端口是否为 7116。

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   ```

   如果 netstat 命令返回结果，表示侦听端口配置正确。
   如果 netstat 命令不返回任何结果，表示端口配置错误，例如：

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   c:\>
   ```

2. 对 /etc/opt/omni/server/AppServer/standalone.xml 文件进行备份。
3. 将 /etc/opt/omni/server/AppServer/standalone.xml 中的所有密钥库和信任库密码替换为 /etc/opt/omni/client/components/webservice.properties 中存储的密码。

   导航至 C:\ProgramData\Omniback\Config\client\components 目录，并在 webservice.properties 文件中，搜索以下代码行：

   ```
   keystorePassword=jones7XE7EJjHzZ
   ```

   ```
   truststorePassword=jones7XE7EJjHzZ
   ```

4. 记录密钥库密码以供将来使用。
5. 在文本编辑器中打开 standalone.xml 文件，搜索包含 keystore-password 的行，如：

   ```
   <jsse keystore-password="JypjEncO.9aG1"
   keystoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.k
   eystore"
   ```

   ```
   truststore-password="JypjEncO.9aG1"
   truststoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server
   .truststore"/>
   ```

6. 将 standalone.xml 文件中 keystore 和 truststore 密码的所有实例替换为步骤 4 的 webservice.properties 文件中的密钥库密码，并保存文件。
7. 在命令窗口中，导航到 C:\Program Files\OmniBack\bin。
8. 使用以下命令重新生成证书：

   ```
   perl omnigencert.pl -server_id NEW_SERVER -store_password <密钥库密码>
   ```

   其中，***<keystore-password>*** 是在步骤 4 中记录的密码。
9. 停止并启动 Data Protector 服务。

   ```
   omnisrv -stop
   ```

   ```
   omnisrv -start
   ```

10. 再次尝试连接到 Cell Manager.

问题

完成 **IDB** 恢复操作后，从 **Data Protector GUI** 连接到 **Cell Manager** 失败并出现 **SSL** 错误

完成恢复操作后，从 GUI 连接到 Cell Manager 失败并报错：

已发生服务器错误。Reported error message:
SSL 对等证书或 SSH 远程连接异常。

操作

1. 导航至 C:\ProgramData\Omniback\Config\client\components 目录并打开 webservice.properties 文件：

   ```
   # global property file for all components
   jce-serviceregistry.URL = https://newcm.company.com:7116/jce-
   serviceregistry/restws

   keystorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client.k
   eystore

   truststorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client
   .truststore
   keystorePassword=jones7XE7EJjHzZ
   truststorePassword=jones7XE7EJjHzZ
   ```

2. 记录 keystorePassword 和 truststorePassword。
3. 在命令窗口中，导航到 C:\Program Files\OmniBack\bin。
4. 使用以下命令重新生成证书：

   ```
   perl omnigencert.pl -server_id NEW_SERVER -store_password <密钥库密码>
   ```

   其中，***<keystore-password>*** 是在步骤 2 中记录的密码。
5. 停止并启动 Data Protector 服务。

   ```
   omnisrv -stop

   omnisrv -start
   ```

6. 再次尝试连接到 Cell Manager.

问题

在 **IDB** 备份期间，**IDB** 无法进入备份模式并失败

在 IDB 备份期间，会话消息显示错误：

[严重] 来自：OB2BAR_POSTGRES_BAR@oldcm.company.com "DPIDB" 时间：10/10/2014
12:19:51 PM

将内部数据库置于备份模式失败

操作

1. 导航至 C:\ProgramData\OmniBack\Config\Server\idb 并制作 idb.config 文件的副本，以作为备份。
2. 在文本编辑器中，打开 idb.config 文件并搜索 PGOSUSER。
   例如
   ```
   PGOSUSER='OLD_SERVER\Administrator';
   ```
3. 如果服务器名称错误，请将其编辑为 NEW_SERVER 名称。
   例如
   ```
   PGOSUSER='NEW_SERVER\Administrator';
   ```
4. 停止并启动 Data Protector 服务。
   ```
   omnisrv -stop
   ```
   ```
   omnisrv -start
   ```
5. 再次尝试 IDB 备份。

问题

IDB 还原在还原进程结束时失败

IDB 还原在还原进程结束时失败，并显示以下消息：

无法执行 omnidbutil -清除命令

操作

在以下情况下，可能会在 HP-UX Cell Manager 中出现此问题：在恢复到其他 Cell Manager 或同一个 Cell Manager 时，但是在备份会话恢复之后或者在全新安装 Cell Manager 之后 Postgres 密码发生了更改。

> **注意：**
> 在 Linux 环境中，还原将成功完成。这是由于 Linux 对于数据库主要使用操作系统身份验证，这与 HP-UX 不同，HP-UX 使用密码授权(在这种情况下，密码文件将不会正确恢复)。但是，解决方法也应该应用于 Linux 环境，以拥有正确的密码文件。

1. 在计划恢复整个 IDB 时，仅将配置文件恢复至其他位置 <restore-conf>。
2. 还原整个 IDB 但不选择还原 DCBF，或者将整个 DCBF 还原到原始位置。
3. 将 /etc/otp/omni/server/idb/idb.config 的备份保存到 idb.config.bkp
4. 将文件从 <restore-conf> 位置复制到原始位置：
   a. cp <restore-conf>/etc/opt/omni/server/idb/idb.config /etc/opt/omni/server/idb/idb.config
   b. cp <restore-conf>/etc/opt/omni/server/idb/ulist /etc/opt/omni/server/idb/ulist
   c. cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml /etc/opt/omni/server/AppServer/standalone.xml
5. 在 idb.config 中修改以下字段，以指向正确位置(正确位置存储在 idb.config.bkp)

a. PGDATA_PG='/space/restore1/pg';
b. PGDATA_IDB='/space/restore1/idb';
c. PGDATA_JCE='/space/restore1/jce';
d. PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;

6. 停止并启动 Data Protector 服务。
   a. 运行 omnisv stop(可能需要一段时间)
   b. 运行 omnisv start
   c. 运行 omnidbutil -clear

升级在 Serviceguard 中配置的 Cell Manager

在升级期间，只升级数据库，旧版本产品将被删除。最新版本的 Data Protector 将与默认选择的代理一起安装，其他代理将被删除。要获得相当于升级前状态的配置，必须在升级过程中手动选择任何其他代理，或者事后在每个物理节点上重新安装这些代理。

先决条件

- 不应在 Serviceguard 辅助节点上运行 Data Protector 服务。
  这将确保在升级主节点过程中使用导出的 IDB 进行升级，避免导出其他 IDB。

从以前版本的 Data Protector 升级到最新版本的 Data Protector 的过程包括升级主节点和辅助节点。请按照下节所述的说明按顺序执行操作。

主节点

登录到主节点，并执行以下步骤：

1. 运行 cmhaltpkg *PackageName* 命令(其中 *PackageName* 是群集包的名称)以停止旧的 Data Protector 包。例如：
   ```
   cmhaltpkg ob2cl
   ```
2. 以独占模式激活卷组：
   ```
   vgchange -a e -q y VGName
   ```
   例如：
   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```
3. 将逻辑卷装载为共享磁盘：
   ```
   mount LVPathSharedDisk
   ```
   *LVPath*参数是逻辑卷的路径名，*SharedDisk* 是装载点或共享目录。例如：
   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```
4. 启动 Data Protector 服务：
   ```
   omnisv -start
   ```
5. 按照本节中的说明升级 Cell Manager。某些步骤可能不同，具体取决于您升级哪个产品版本。

6. 停止 Data Protector 服务：

   ```
   omnisv -stop
   ```

7. 卸载共享磁盘：

   ```
   umount SharedDisk
   ```

   例如：

   ```
   umount /omni_shared
   ```

8. 停用卷组：

   ```
   vgchange -a n VGName
   ```

   例如：

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 以独占模式激活卷组：

   ```
   vgchange -a e -q y VGName
   ```

2. 将逻辑卷装载为共享磁盘：

   ```
   mount LVPathSharedDisk
   ```

3. 按照本节中的说明升级 Cell Manager。某些步骤可能不同，具体取决于您升级哪个产品版本。
4. 重命名 csfailover.sh 和 mafailover.ksh 启动脚本(在 /etc/opt/omni/server/sg 目录中)(例如，重命名为csfailover_DP70.sh 和 mafailover_DP70.ksh)，将新的 csfailover.sh 和 mafailover.ksh 脚本从 /opt/omni/newconfig/etc/opt/omni/server/sg 目录复制到 /etc/opt/omni/server/sg 目录。

   如果旧的启动脚本中有自定义内容，请在新启动脚本中重新实施这些更改。

5. 停止 Data Protector 服务：

   ```
   omnisv -stop
   ```

6. 卸载共享磁盘：

   ```
   umount SharedDisk
   ```

7. 停用卷组：

   ```
   vgchange -a n VGName
   ```

主节点

再次登录到主节点，并执行以下步骤：

1. 启动 Data Protector 包：

   ```
   cmrunpkg PackageName
   ```

2. 配置 Cell Manager。运行脚本时，确保当前位置不在 /etc/opt/omni 或 /var/opt/omni 目录或其子目录下。还要确保 /etc/opt/omni 或 /var/opt/omni 中没有装载的子目录。执行：

```
/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
```

3. 停止 Data Protector 包：

   ```
   cmhaltpkg PackageName
   ```

辅助节点

再次登录到辅助节点，并执行以下步骤：

1. 启动 Data Protector 包：

   ```
   cmrunpkg PackageName
   ```

2. 配置 Cell Manager。运行脚本时，确保当前位置不在 /etc/opt/omni 或 /var/opt/omni 目录或其子目录下。确保 /etc/opt/omni 或 /var/opt/omni 目录中未装载任何子目录。执行：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
   ```

   > **注意：**
   > /share 是群集节点之间的共享目录或存储。

3. 停止 Data Protector 包：

   ```
   cmhaltpkg PackageName
   ```

主节点

再次登录到主节点，并执行以下步骤：

1. 启动 Data Protector 包：

   ```
   cmrunpkg PackageName
   ```

   确保包切换和节点切换选项启用。

2. 重新导入虚拟主机：

   ```
   omnicc -import_host VirtualHostname -virtual
   ```

3. 更改 IDB 中 Cell Manager 的名称：

   ```
   omnidbutil -change_cell_name
   ```

4. 如果有安装服务器与 Cell Manager 同在一个包中，导入安装服务器虚拟主机名：

   ```
   omnicc -import_is VirtualHostname
   ```

> **注意：**
> 来自 Cell Manager 的所有请求将记入 Data Protector 客户机上的 /var/opt/omni/log/inet.log 文件。若要防止不必要的日志条目，请保护客户机。有关如何保护单元的信息，请参见 安全注意事项 (第 174 页)。

升级在 Symantec Veritas Cluster Server 中配置的 Cell Manager

在升级期间，只升级数据库，旧版本产品将被删除。Data Protector 将与默认选择的代理一起安装，其他代理将被删除。要获得相当于升级前状态的配置，必须在升级过程中手动选择任何其他代理，或者事后在每个物理节点上重新安装这些代理。

先决条件

不应在 Symantec Veritas Cluster Server 辅助节点上运行 Data Protector 服务。

从以前版本的 Data Protector 升级的过程包括升级主节点和辅助节点。请按照下节所述的说明按顺序执行操作。

主节点

登录到主节点，并执行以下步骤：

1. 使 Data Protector 应用程序资源脱机。
2. 禁用 Data Protector 应用程序资源。
3. 启动 Data Protector 服务：

   ```
   omnisv -start
   ```
4. 按照一节中的说明升级 Cell Manager。
5. 如果您自定义了 Data Protector 应用程序资源所使用的监控脚本，请在自定义脚本中重新实施由新安装的 /opt/omni/sbin/vcsfailover.ksh 脚本提供的更改。
6. 停止 Data Protector 服务：

   ```
   omnisv -stop
   ```

辅助节点

登录到辅助节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到辅助节点。
2. 按照一节中的说明升级 Cell Manager。
3. 如果您自定义了 Data Protector 应用程序资源所使用的监控脚本，请在自定义脚本中重新实施由新安装的 /opt/omni/sbin/vcsfailover.ksh 脚本提供的更改。
4. 停止 Data Protector 服务：

   ```
   omnisv -stop
   ```

主节点

再次登录到主节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到主节点。
2. 启用 Data Protector 应用程序资源。
3. 使 Data Protector 应用程序资源联机。
4. 配置 Cell Manager。确保不从 /etc/opt/omni 或 /var/opt/omni 目录或其子目录执行脚本。还要确保 /etc/opt/omni 或 /var/opt/omni 目录中未装载子目录。请执行以下命令：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
   ```

辅助节点

再次登录到辅助节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到辅助节点。
2. 配置 Cell Manager。确保不从 /etc/opt/omni 或 /var/opt/omni 目录或其子目录执行脚本。还要确保 /etc/opt/omni 或 /var/opt/omni 目录中未装载子目录。请执行以下命令：

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary dirname -upgrade
   ```

   其中 *dirname* 表示装载点或共享目录(例如 /omni_shared)。

主节点

再次登录到主节点，并执行以下步骤：

1. 将 Data Protector 服务组切换到主节点。
2. 如果安装服务器与 Cell Manager 位于同一个服务组中，请导入安装服务器虚拟主机名：

   ```
   omnicc -import_is VirtualHostname
   ```

> **注意：**
> 来自 Cell Manager 的所有请求将记入 /var/opt/omni/log/inet.logData Protector 客户机上的文件。若要防止不必要的日志条目，请保护客户机。有关如何保护单元的信息，请参见 安全注意事项 (第 174 页)。

升级在 Microsoft 群集服务器上配置的 Cell Manager

在 Microsoft 群集服务器 (MSCS) 上将 Cell Manager 升级的过程是通过 Windows 安装程序包在本地执行的。

先决条件

- 只有在以前安装的 Data Protector 软件是以群集感知模式安装的 Cell Manager 的情况下，才支持升级选项。如果群集中的某个系统有作为非群集感知安装的 Data Protector 软件，那么在开始安装之前，需要先将其卸载。

升级过程

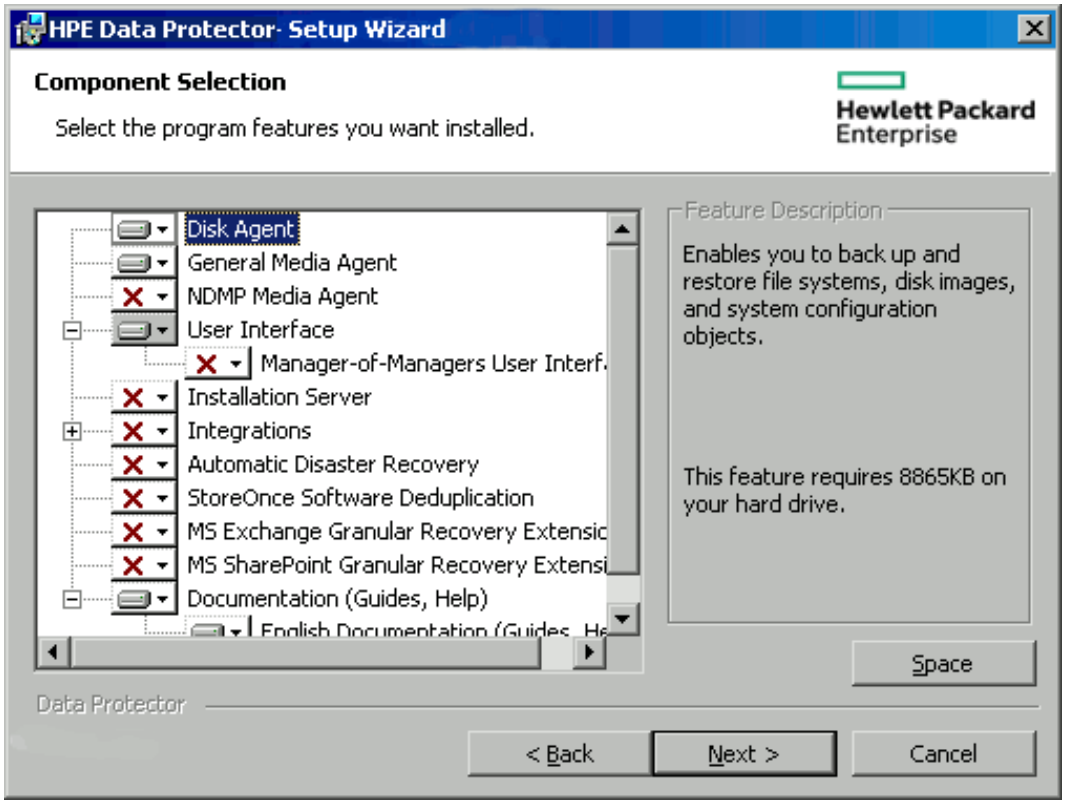
为了执行升级，请执行如下步骤：

1. 将下载的安装程序包复制到 Windows 系统上，然后将文件提取到临时目录。运行 \Windows_Other\x8664 位置中的 setup.exe 文件。建议在当前活动的虚拟服务器节点上启动安装。

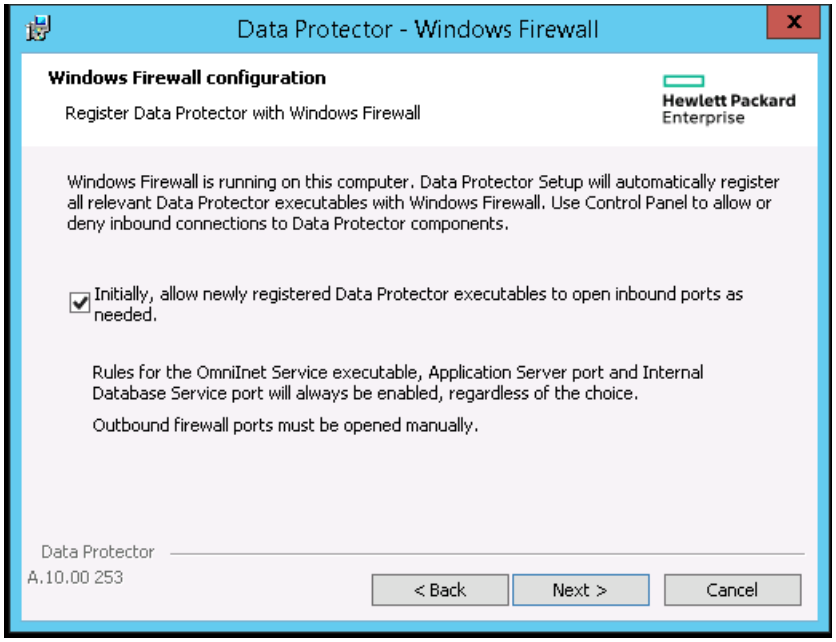
   安装程序将自动检测旧版本的产品，并提示将

   单击**下一步 (Next)** 继续。
2. Data Protector 自动选择已安装的组件。

   选择组件



   单击**下一步 (Next)**。
3. 如果 Data Protector 在系统上检测到 Windows 防火墙，则将显示“Windows 防火墙”配置页面。Data Protector 设置会注册所有必要的 Data Protector 可执行文件。默认情况下，**最初，允许新注册的 Data Protector 可执行文件按需打开入站端口**选项已选中。如果此时不想让 Data Protector 能打开端口，请取消选中此选项。为了正常运行具有先前版本的 10.00 客户机的 Data Protector，必须启用 Windows 防火墙中的 Data Protector 规则。无论哪种选择，必须始终启用 OmniInet Service 可执行文件、应用程序服务器端口和内部数据库服务端口的规则。



单击**下一步 (Next)**。

4. 或者，更改由 Data Protector IDB 和 HTTPS 应用程序服务器使用的用户帐户以及由这些服务使用的端口。

   单击**下一步 (Next)**。

5. 此时会显示组件选择摘要列表。单击**安装 (Install)**执行升级。

   此时将打开命令提示符窗口，然后软件开始通过导出较旧的 IDB 将 IDB 迁移到新的数据库格式。

   在导出较旧的 IDB 期间，此命令提示符窗口保持打开状态并显示状态消息。IDB 导出可能需要几分钟的时间才能完成。

   随着升级的进行，还会另外打开一个命令提示符窗口，用于显示将 IDB 配置信息和数据导入到 Data Protector 的状态。

   从 8.00 及更高版本升级：

   IDB 会自动更新；将不打开命令提示符窗口。

   注意在升级后，每个节点将有相同的组件集。

6. **安装状态**页随即显示。单击**下一步 (Next)**。

7. 若要在安装后立即开始使用 Data Protector GUI，选择**启动 Data Protector GUI**。

   如果English Documentation (Guides, Help)已经升级或者是新安装的，那么，要在设置后立即查看 Data Protector 产品声明、软件说明和参考，请选择**打开产品声明、软件说明和参考**。

   单击**完成**。

> **注意：**
> 如果要升级群集感知的客户机，应首先单独升级每个群集节点，然后重新导入虚拟服务器。不支持远程升级。

从以前的版本迁移计划

升级到 Data Protector 10.00 后，所有现有的计划将自动迁移到基于 Web 的新计划程序。 无需手动干预。

在升级到 Data Protector 10.00 期间，所有现有的计划文件都会附加 .migrate 后缀。

例如，在 10.00 之前的 Data Protector 版本中，如果您具有名称为 WeeklyBackup 的备份规范计划，则文件名将在升级过程中被修改为 WeeklyBackup.migrate。 如果迁移失败，则不会重命名文件。

如果计划未正确迁移，则可能会要求您将这些 .migrate 文件提供给客户支持以进行故障排除。

已迁移的计划文件可从以下位置获取：

规范类型	计划路径
备份计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\amoschedules Unix： /var/opt/omni/server/amoschedules
集成计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\Barschedules Unix： /var/opt/omni/server/Barschedules
复制操作计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\copylists\scheduled\schedules Unix： /var/opt/omni/server/copylists/scheduled/schedules
合并操作计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\consolidationlists\scheduled\schedules Unix： /var/opt/omni/server/consolidationlists/scheduled/schedules
验证操作计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\verificationlists\scheduled\schedules Unix： /var/opt/omni/server/verificationlists/scheduled/schedules
报告组计划	Windows： *Data Protector_program_data*\OmniBack\Config\Server\rptschedules Unix： /var/opt/omni/server/rptschedules

如果在升级过程中计划迁移失败，您可以手动运行以下命令，以便将现有计划成功迁移到新的计划程序：

```
omnidbutil -migrate_schedules
```

> **注意：**
> 以前版本的 Data Protector 中添加的计划没有与其关联的名称属性。 因此，迁移后，

> 迁移的计划的名称显示为 **...**。 您可以编辑这些计划并向计划提供名称。

第 8 章： Data Protector 许可

本章包含以下相关信息：

- 新引入的许可证密钥
- Data Protector 许可证检查和报告
- 获取和安装 Data Protector 密码
- Data Protector 产品结构和许可证

概述

您必须拥有许可证密钥才能使用 Data Protector 产品。

首次安装时，Data Protector 将获得一个即开即用(试用)许可证。

试用许可证的有效期为 60 天。在 60 天的试用期到期之前，您必须获取永久许可证才能继续使用 Data Protector。要获取永久许可证，请参见 获取许可证 (第 253 页)一节。

本章包含以下几节：

- 许可证类型 (第 243 页) - **基于功能的许可**基于功能和备份目标。**基于容量的许可**基于受 Data Protector 保护的原始源数据的数量。
- 选择许可证类型 (第 252 页) - 此节介绍基于功能的许可证和基于容量的许可证之间的区别。同一个客户可以利用功能模型和容量模型，但不能在同一个 Cell Manager 或 MoM 环境中将这两个模型结合使用。
- 获取许可证 (第 253 页) - 此节提供有关获取新的许可证密钥和请求密码的详细信息。
- 集中式许可 (centralized licensing) (第 260 页) - 通过 Data Protector，可为整个多单元环境配置中央许可，从而简化许可证管理。
- 许可证报告 (第 260 页) - 系统会检查 Data Protector 许可证，如果这些许可证缺失，则会在各项 Data Protector 操作期间报告。

许可证类型

Data Protector 支持两种许可模式：

- **基于功能的许可**：基于功能和备份目标。 基于功能的许可也称为传统许可。
- **基于容量的许可**：基于受 Data Protector 保护的原始源数据的数量。 容量以“前端千吉字节”或前端 TB 为单位。

基于功能的许可

Data Protector 产品结构和基于功能的许可模型包含三个主要类别：

与 Cell Manager 相关的许可证

- **Starter Pack：**

  Data Protector Starter Pack 包含：

- 指定的平台(Windows、UNIX 和 Linux)上一个 Cell Manager。
- 任何平台上无线数量的备份客户机(代理)(仅用于文件系统备份)。
- 一个驱动器许可证(一个驱动器，此案例中是一个磁带驱动器)
- 库(最多包含 60 个插槽)
- 系统灾难恢复选项
- 基本报告(通过 Data Protector GUI 和 Web 提供)

备份目标

- **驱动器扩展和库扩展：**
  - 备份驱动器扩展 - 包含用于在一个 Data Protector 单元中管理更多驱动器(加上 Starter Pack 中可管理的一个驱动器)的许可证
  - 库扩展 - 包含用于在一个 Data Protector 单元中管理磁带库(包含更多物理可用的插槽，加上 Starter Pack 中可用的插槽)的使用许可证 (LTU)。

如果在单元中配置的任何项目具有基于源的许可证的对象，则会检查是否有所需的基于实体的许可证及其数量。如果许可证数量少于配置的项目，则 Data Protector 会发出通知。

如果在 SAN 环境中为多个 Data Protector 客户机配置了一个备份设备，则必须使用多路径功能以便 Data Protector 将其识别为单备份设备。

以下备份目标按照容量进行许可：

- 适用于 1 TB 和 10 TB 的 UNIX 零宕机时间备份
- UNIX 零宕机时间备份非 HPE 阵列 1 TB
- 适用于 1 TB 和 10 TB 的 UNIX 即时恢复
- 适用于 1 TB 和 10 TB 的 Linux 零宕机时间备份
- Linux 零宕机时间备份非 HPE 阵列 1 TB
- 适用于 1 TB 和 10 TB 的 Linux 即时恢复
- 适用于 1 TB 和 10 TB 的 Windows 零宕机时间备份
- Windows 零宕机时间备份非 HPE 阵列 1 TB
- 适用于 1 TB 和 10 TB 的 Windows 即时恢复
- 使用 NDMP 直接备份，适用于 1 TB 和 10 TB
- 高级备份到磁盘，适用于 1 TB、10 TB 和 100 TB

检查基于容量的备份目标的许可证(除高级备份到磁盘许可证外)时，会将已备份的逻辑单元上的总磁盘空间量与安装的许可证的容量进行比较。有关到磁盘的高级备份许可证，请参见 到磁盘的高级备份许可证 (第 245 页)

以这种方式进行许可检查是为了即使在许可的容量用尽后也可执行即时恢复或备份。在这些情况下，会在备份会话期间显示警告消息，通知您已超出许可的容量。

已用磁盘的容量是基于在每次 ZDB 备份会话期间收集的历史信息进行计算的。计算的时间间隔是二十四小时。Data Protector 基于过去二十四小时内所有会话中使用的磁盘来计算已用磁盘容量，并将计算的容量与许可的容量相比较。

如果违反许可，则会在备份期间发出警告消息。此外，许可证报告工具每天运行，如果超出许可容量，则会向 Data Protector 事件日志写入通知。

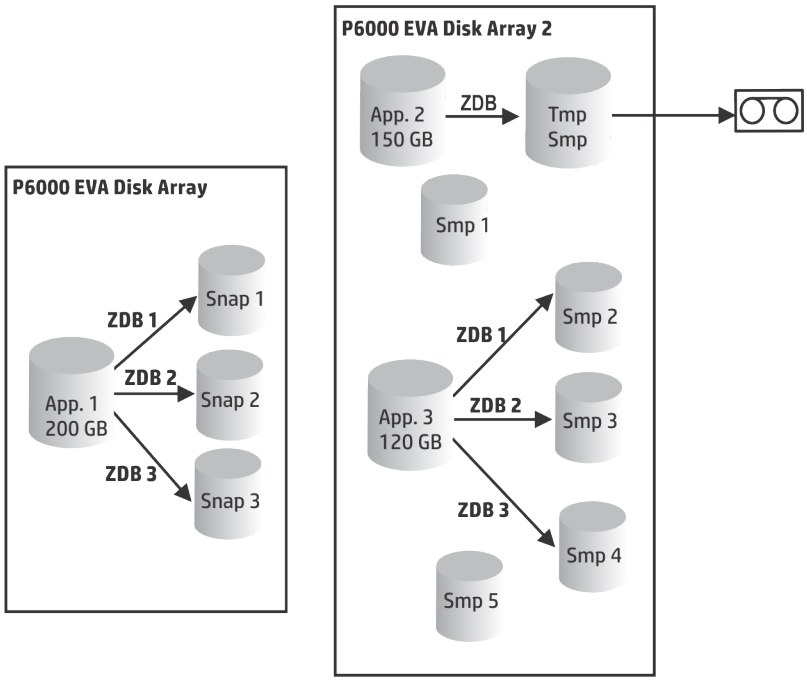
应用于备份目标的已用容量计算方法

已用容量计算会计算过去二十四小时内使用的每个磁盘阵列的许可容量。在指定时间间隔内使用过两次或多次的磁盘仅计为一次。磁盘阵列单元使用从每个阵列获取的标识号进行标识。阵列标识号的使用意味着可以知道某阵列已被计入。

如果已经运行包括即时恢复的 ZDB 备份，则将为每个磁盘阵列 ZDB 使用的容量以及每个磁盘阵列用于即时恢复的容量计算每个原始单元的总容量。

例如，假定有两个 P6000 EVA 磁盘阵列的情况。在一个阵列上有单个磁盘 (App.1)，它有 200 GB 的容量用于数据保护。一天触发三次的备份会话中，每个会话都附带了即时恢复选项。每次保留三个复本，这些复本轮流用于即时恢复用途。在另一个磁盘阵列上有两个磁盘(App.2 和 App.3)，分别有 150 GB 和 120 GB 的容量。在 App.2 磁盘上每天运行一次备份，数据移动到磁带后即删除快照。在 App.3 上，每天运行三次备份，并循环五个不同的复本以进行即时恢复。请参见 已用容量计算方法 (第 245 页)。

已用容量计算方法



ZDB 已用容量的计算包括过去二十四小时内用于备份会话的所有磁盘 200 GB (App.1) + 150 GB (App.2) + 120 GB (App.3) = 470 GB。

即时恢复已用容量的计算包括将数据用于即时恢复的 ZDB 会话的源容量。同一磁盘仅计算一次 200 GB (App.1) + 120 GB (App.3) = 320 GB。

到磁盘的高级备份许可证

到磁盘的高级备份许可证在备份到 Data Protector 文件库时不可获缺，并且可代替驱动器许可证用于虚拟磁带库 (VTL)。

- Data Protector 文件库的可用本机容量是磁盘上用于文件库的可用大小，如文件系统所报告。

- 虚拟完整备份以及要合并到合成或虚拟完整备份中的增量备份必须存储在 Data Protector 文件库中，这需要此许可证。

- 如果 Data Protector 独占使用 VTL，则建议许可与 VTL 的物理容量匹配的容量，也称为可用本机容量。
  - 虚拟磁带库 (VTL) 的可用本机容量是磁盘上所有受保护的 Data Protector 备份消耗的虚拟磁带库大小，如 VTL 所报告。
  - 对于每个 VTL，可以选择使用“备份到磁盘”还是“备份到磁带驱动器”许可模式。在一个 VTL 内，一定不能混合这两种概念。
  - 如果 VTL 具有将备份数据从磁盘缓存迁移到其他磁盘或磁带的内置功能，则需要完全许可迁移的存储容量。由 VTL 单独控制的磁带库不需要驱动器和库许可证，但是***物理磁带库中所有磁带的已用容量需要获得许可***。但是，如果 Data Protector 对象复制功能已用于将备份数据迁移到其他磁盘或磁带，则此方法不适用。
  - 默认情况下，Data Protector 将 VTL 设备视为普通库(例如 SCSI II 库)，不会利用基于容量的许可。要启用基于容量的许可，必须在设备配置期间将设备标记为 VTL。

    有关如何通过图形用户界面 (GUI) 配置 VTL 的详细信息，请参见 *Data Protector 帮助* 索引：“虚拟磁带库”。有关如何通过命令行界面 (CLI) 配置 VTL 的更多信息，请参见以下 示例 (第 246 页)。

- 对于使用 Manager-of-Manager (MoM) 的中央许可，需要使用“到磁盘的高级备份”功能为每个单元分配至少 1 TB 的空间。

> **注意：**
> 由于目前的虚拟磁带库以及某些托管 Data Protector文件库的文件服务器缺少工具和界面，Data Protector 无法报告所需要的许可证数量。您需要按照许可定义，进行一致的容量许可。

示例

如果使用 omniupload 命令通过命令行界面 (CLI) 配置一个名为“VTL_2011”的虚拟磁带库，则必须在配置文件中指定字符串 VTLCAPACITY 的估计带库容量。此估计值随后会在许可证检查程序报告中加总为“到磁盘的高级备份”的已用许可证容量。

> **注意：**
> 估计的虚拟带库容量消耗值 (VTLCAPACITY) (TB) 必须为整数，以避免出现错误消息“Invalid VTL capacity specified”。

在目录“C:\Temp”下名为“libVTL.txt”的配置文件中，键入估计的带库容量，例如 11，然后执行：

```
omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt
```

若要验证库配置，请执行：

```
omnidownload -library VTL_2011
```

```
#omnidownload -library VTL_2011
NAME "VTL2011"
DESCRIPTION ""
```

```
HOST computer.company.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 11
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

许可证检查程序会报告正在使用的许可证容量，即文件库 (FL) 的已用磁盘空间与虚拟磁带库中的估计磁盘空间大小之和。例如，用 2 TB 磁盘空间进行 FL 备份，VTL 上的磁盘容量为 10 TB，则所用总容量为 12 TB。如果仅安装了 5 TB 的许可证容量，则会收到通知，说明还需要 7 个“高级备份到磁盘，适用于 1 TB”许可证。

```
#omnicc -check_licenses -detail
-------------------------------------------------------------------
License Category               : Advanced Backup to disk for 1 TB
Licenses Capacity Installed    : 5 TB
Licenses Capacity In Use       : 12.0 TB
Add.Licenses Capacity Required: 7 TB

Summary
-------
Description                                        Licenses Needed
Advanced Backup to disk for 1 TB                                 7
Total protected data        1 TB
```

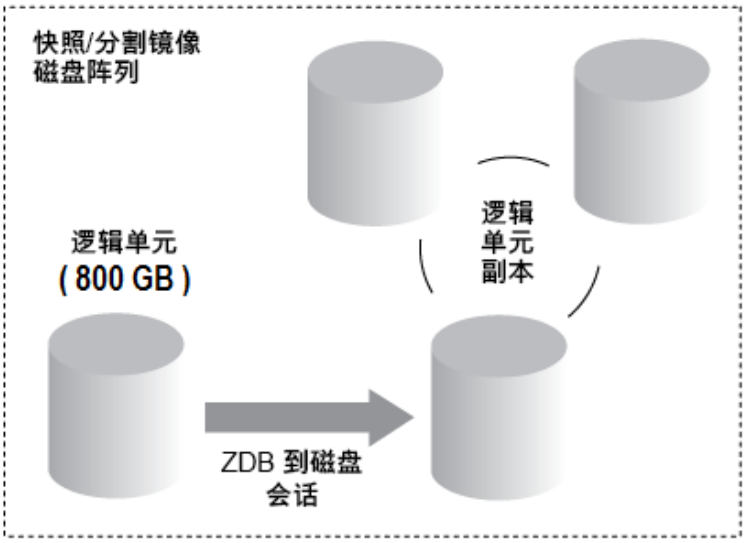
基于许可容量的备份目标示例

本节举例说明了基于容量的许可是如何计算的。

示例 1

ZDB 到磁盘会话 (第 248 页) 将显示在 ZDB 到磁盘会话中每天备份三次一个 800 GB 逻辑单元中的数据的情况。

ZDB 到磁盘会话



三个分割镜像或快照副本(复本)进行循环，并保留用于即时恢复。基于容量的许可的计算方法如下：

一个 800 GB 的逻辑单元用于“ZDB 到磁盘”会话：

1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。

为即时恢复保留同一 800 GB 逻辑单元的三个复本。请注意，这是源卷的容量，不是作为许可证主体的复本的容量：

1 x 800 GB = 0.8 TB，对于“即时恢复，用于 1 TB”许可证。

一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够。

示例 2

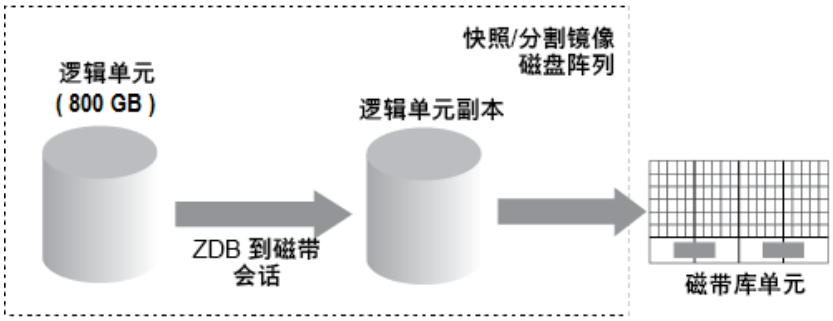
ZDB 到磁带会话 (第 249 页)显示如下情形：在 ZDB 到磁带会话中，一天对一个 800 GB 逻辑单元中的数据备份两次。因此，不必为即时恢复保留分割镜像或快照副本(复本)。基于容量的许可的计算方法如下：

一个 800 GB 的逻辑单元用于“ZDB 到磁盘”会话：

1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。

一个“零宕机时间备份，用于 1 TB”许可证已足够。

ZDB 到磁带会话



示例 3

ZDB 到磁盘 + 磁带会话 (第 249 页) 显示如下情形：在 ZDB 到磁盘会话中，一天对一个 800 GB 逻辑单元中的数据备份三次。五个分割镜像或快照副本(复本)进行循环，并保留用于即时恢复。基于容量的许可的计算方法如下：

一个 800 GB 逻辑单元用于“ZDB 到磁盘 + 磁带”会话：

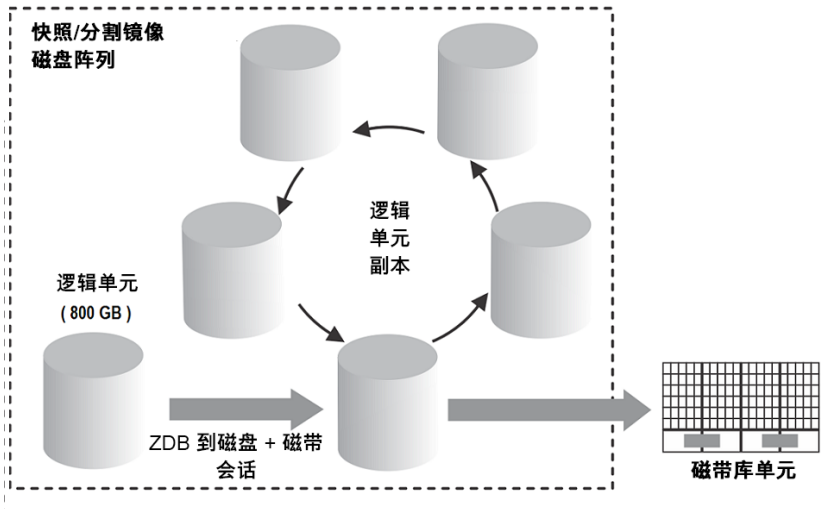
1 x 800 GB = 0.8 TB，对于“零宕机时间备份，用于 1 TB”许可证。

出于即时恢复目的，保留同一 800 GB 逻辑单元的五个复本。请注意，这是源卷的容量，不是作为许可证主体的复本的容量：

1 x 800 GB = 0.8 TB，对于“即时恢复，用于 1 TB”许可证。

一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够。

ZDB 到磁盘 + 磁带会话



示例 4

一个 200 GB 的逻辑单元、一个 500 GB 的逻辑单元、一个 120 GB 的逻辑单元和一个 300 GB 的逻辑单元用于 ZDB 会话：

1 x 200 GB + 1 x 500 GB + 1 x 120 GB + 1 x 300 GB = 1.12 TB 对于“零宕机时间备份，用于 1 TB 许可证”。

保留一个 200 GB 的逻辑单元、一个 120 GB 的逻辑单元和一个 300 GB 的逻辑单元的拆分镜像或快照副本用于即时恢复：

1 x 200 GB + 1 x 120 GB + 1 x 300 GB = 0.62 TB 对于“即时恢复，用于 1 TB”许可证。

一个“零宕机时间备份，用于 1 TB”许可证和一个“即时恢复，用于 1 TB”许可证已足够，前提是 ZDB 到磁盘会话 (第 248 页)到 ZDB 到磁盘 + 磁带会话 (第 249 页)中的三个示例在单元中配置。

功能扩展：

- 联机备份 – 能够在应用程序正在运行时备份应用程序服务器和虚拟环境。
- 用于一个 UNIX 系统的联机扩展和用于一个 Windows/Linux 系统的联机扩展
- Manager-of-Managers 功能。
- 具有超过 60 个介质插槽的带库。
- 适用于一个客户机系统的 Data Protector 加密扩展
- NDMP 备份。
- 用于一个数据库服务器的 Granular Recovery Extension。
- 零宕机时间备份 (ZDB) – 能够为 HP 存储系统备份基于阵列的快照。
- 即时恢复 (IR) - 能够从基于阵列的快照创建备份并从该备份恢复。
- 高级备份到磁盘 – 包含用于 1 TB 备份磁盘存储的许可证。每千兆字节 (TB) 备份磁盘存储的可用本机容量都需要一次该许可证。执行备份到 Data Protector 文件库以及备份到“Data Protector 备份到磁盘设备类型”操作时需要此许可证，而且您可以使用此许可证而非驱动器许可证来备份到虚拟磁带库。

基于容量的许可

基于容量的产品结构基于受 Data Protector 保护的主数据卷，且支持无限制地使用企业保护功能。容量以“前端千吉字节”或前端 TB 为单位。前端千吉字节的总量定义为 Cell Manager 中所有要备份的系统中的数据总量。对于每个系统，以最大完整数据量(即受保护的源数据量)进行度量。此许可证模型可应用到现有基础架构。新的基础架构会自动包含到同一个许可证中。

CBL 在计算费用时将所有受保护的数据包括在内，并且无法区分用于备份的当前许可证类型和原始许可证类型。可以将备份中不包含的系统(不再存在)复制到单独的介质，然后可以从 Cell Manager 系统导出该介质。

> **注意：**
> IDB 对象不包含在 CBL 计算中。

使用基于容量的许可时，以下模块是许可结构的一部分：

- Cell Managers 和 Manager of Managers
- 磁带驱动器和带库
- 联机备份和 Granular Recovery Extension
- 零宕机时间备份和即时恢复
- 高级备份到磁盘和 NDMP

不包含的产品以及与基于容量的许可分开销售的产品如下：

- 加密软件
- Backup Navigator
- Storage Optimizer
- DP Extended Online Backup
- 适用于非 HPE 阵列的 Data Protector 零宕机时间备份 (ZDB)
- Data Protector Management Pack，包含适用于 Operations Manager 和 Microsoft Systems Center 的 DP Smart 插件

有关容量层、说明和部件号，请参见 Data Protector QuickSpecs。

基于容量的许可证报告

在基于容量的许可模式下，Data Protector 仅会列出基于容量的许可证的数量(粒度为 1 TB)，以及未包括在基于容量的许可证范围内的许可证，即软件加密扩展。不会显示基于容量的许可所涵盖的基于功能的许可证。

```
#omnicc -check_license -detail

WARNING: Calculation of total protected data size may take some time.

Report generated            : 03/03/2016 1:48:27 AM
Licensing mode              : Server
License server              : host.domain.com
------------------------------------------------------------------------------
---
License Category               : Encryption Extension for one client system
Licenses Installed             : 0
Licenses Used                  : 0
Additional Licenses Required   : 0
------------------------------------------------------------------------------
---
License Category               : Data Protector - capacity based per TB SW
Licenses Capacity Installed    : 9 TB
Licenses Capacity In Use       : 0 TB
Add.Licenses Capacity Required : 0 TB
------------------------------------------------------------------------------
---
.
.
.

Summary
-------
Licensing is covered.
Total Protected Data        : 4,00 TB

------------------------------------------------------------------------------
---
Backup Type                                    |       Total Protected Data
------------------------------------------------------------------------------
---
```

```
MS Filesystem                                |       1 GB
MS SQL                                       |       1 GB
SAP                                          |       1 GB
UNIX Filesystem                              |       1 GB

--------------------------------------------------------------------------------
```

Total Protected Data(受保护的总数据)定义为正在从所有系统备份的聚合数据量。每个系统的 Total Protected Data(受保护的总数据)等于以下内容之和：

- 文件系统(包括合成备份)和虚拟环境备份的每个对象的最大完整备份之和。
- 每个应用程序集成备份的每个数据集的最大完整备份。

> **注意：**
> 每个文件系统和虚拟环境的唯一对象是在备份时创建的实际对象。实际对象可以是装载点、虚拟机或虚拟机磁盘。
>
> 每个应用程序集成的唯一数据集都按照不同的方式(通常为数据库实例或服务器名称)标识。

限制

- 在使用多个不同的代理备份相同数据时，会对备份进行多次计算。下面是双重计算的几个类似示例：
  - 使用 VSS 的数据库文件系统备份，同一个数据库的应用程序集成代理备份。
  - 虚拟主机的虚拟环境集成备份，以及在虚拟机(主机)内部运行的文件系统代理备份。

  > **注意：**
  > 建议备份唯一的对象，以避免进行双重计算。
- 当在外部重新配置 Oracle 备份对象名称格式时，这可能会导致不从新对象名称解析数据库名称。在计算受保护的总数据量时，类似的对象大小可能无法正确处理。

  > **注意：**
  > 对于重新配置的格式，仍必须包括定义为 `<DBID_*.dbf` 的 Oracle 数据库名称，以便在计算受保护的总数据大小时正确地添加 Oracle 对象。
- 当前，Data Protector 中没有任何方法可用于检测通过虚拟环境代理和已安装的磁带客户机(在 VM、VEPA 和磁带客户机中运行)备份的 VMware VM 是否正在使用相同数据运行。

选择许可证类型

同一个客户可以利用基于功能的模型和容量模型，但不能在同一个 Cell Manager 或 MoM 环境中将这两个模型结合使用。 列出的补充产品不受此限制约束，因为这些许可证可与 Data Protector 基于功能的许可方法和基于容量的许可方法结合使用。 支持从传统产品结构迁移到基于容量的产品结构：有关详细信息，请联系授权的 Hewlett Packard Enterprise 销售代表。 这两种许可模型对任何环境规模均有效。

基于功能的许可和基于容量的许可证之间的区别如下：

- 基于功能的许可提供更低的入门成本，但已启用的功能较少；而容量许可已启用大部分功能，它是一个“随增长付费”模型。
- 基于功能的许可要求每个 Cell Manager 和磁带驱动器等具有单独的许可证，并要求用户先记录现有环境再选择需要许可哪些备份软件功能来保护其环境。
- 灵活性更大 – 容量许可仅需一个许可证即可保护客户机上所有需要受保护的数据。
- 需要关注的另一个问题是：如果您计划将数据保留很长一段时间，并且数据将发生大量更改但容量不一定会增长，这也可能导致该备选的基于容量的模型随着时间的推移产生更多成本。

为什么要使用基于功能的许可？

- 提供更低的入门成本，但已启用的功能较少
- 如果组织内的数据持续以适当速度增长，则使用基于功能的许可方法可能更具有成本效益

为什么要使用基于容量的许可？

- 基于受 Data Protector 保护的生产数据量
- 可容纳多个备份副本，而不会增加许可证成本
- 允许无限制地使用企业保护功能
- 它是一个永久许可证，并且可转移到新的服务器、存储和应用程序等。
- 它是一个高度可扩展且成本不太高昂的“随增长付费”许可模型，可改善 OPEX 管理并简化规模估算

获取许可证

在本节，您将了解有关为 Data Protector 获取新许可证密钥并为现有许可证密钥请求新密码的信息。

获取新许可证密钥

在 Data Protector 8.00 和早期版本中生成的许可证密钥和密码必须升级，因为它们因许可技术的变化与 Data Protector 的最新版本不兼容。

在 Data Protector 10.00 之前生成的许可证密钥和现有密码与 Data Protector 10.00 和更高版本不兼容。要升级到 Data Protector 10.00，您需要新许可证。

> **注意：**
> Data Protector 10.00 不再显示已到期或无效的许可证。

对于新购买的许可证，在请求密码时您必须选择产品版本 Data Protector 10.00。为 Data Protector 10.00 生成的密码将无法与之前的任何 Data Protector 版本一起使用。

升级以后，将使用期限为 60 天的即开即用密码运行 Data Protector 10.00。该行为将与采用即开即用密码的全新安装相同。

> **重要：**
> 一旦安装 Data Protector 10.00 的*至少一个新许可证密钥*，将关闭即开即用密码，并且仅可识别已安装的有效密钥。

在升级后仅可激活即开即用密码一次。

> **提示：**
> 升级以后，现有许可证仍与新(即开即用)密码一起报告为无效。要避免出现此情况，请重命名(但不要删除)文件 `lic.dat`：
>
> ***Windows 系统***：转到目录 *Data_Protector_program_data*\Config\server\Cell 并重命名以下文件：
>
> ```
> ren lic.dat lic.bak
> ```
>
> ***UNIX 系统***：转到目录 /etc/opt/omni/server/cell 并重命名以下文件：
>
> ```
> mv lic.dat lic.bak
> ```

密码考虑事项

考虑以下事项以帮助确定合适的密码数量：

- 即开即用密码是内置的。每次在新安装和将现有 Data Protector 升级到 Data Protector 9.00 或更高版本后将提供为期 60 天的该密码，在这 60 天内您无需安装任何额外许可证密码，并且可为您提供完整的产品功能，以供您评估。

  在 60 天后，即开即用密码到期，除非安装永久许可证密钥，否则产品将停止工作。

  在安装首个常规许可证密钥之后，完整产品的评估期将终止。一旦已至少安装了一个许可证密钥后，仅可使用已安装许可证密钥对应的功能。
- 可将永久许可证移动到其他 Cell Manager。但是，需要使用“许可证移动表单”并将它们发送至 Password Delivery Center (PDC)。
- 密码安装在 Cell Manager 上且对整个单元有效。
- Manager-of-Managers (MoM) 功能中包含中央许可。如果您为多个单元购买了多个许可证，则可以将所有许可证都安装在 MoM 系统上。
- 您需要每个单元使用一个 Cell Manager 许可证。
- 执行 Data Protector 配置任务或启动备份会话时，软件会定期检查许可证密钥或密码。
- 即开即用密码可用于任何系统上，而评估密码和永久密码只能用于为其请求许可证的 Cell Manager 系统上。

Data Protector 许可需要以下某种密码：

- 即开即用密码

  首次安装时会在产品中创建即开即用密码。在 Data Protector 支持的任何系统上安装软件后，可以使用软件 60 天。在此期间内，您必须从 *Password Delivery Center (PDC)* 请求永久密码，然后安装该密码。

  对于现有的 Data Protector 安装，在升级到 Data Protector9.00 或更高版本后，您的安装将使用即开即用密码运行 60 天。在此期间内，您必须从有效支持协议中所指定的 Password Delivery Center 请求新的永久密码。无法升级未包括在支持协议中的旧许可证。
- 永久密码

  Data Protector 产品自带了一个*权利证书*许可证，它授权您获取永久密码。如果您已购买所有需要的许可证，则永久密码允许您根据备份策略配置 Data Protector 单元。在请求永久密码前，必须确定 Cell Manager 系统并了解单元配置要求。

- 紧急密码

  如果由于紧急情况，当前安装的密码与当前系统配置不匹配，则可使用紧急或后备密码。它们允许在任何系统上操作 120 天。

  紧急密码由支持组织发布。它们必须由您的客户支持代表请求，且仅发布给这些人员。请咨询支持联系人或查看许可站点：https://software.microfocus.com/zh-cn/legal/software-licensing。

  紧急密码的目的是当原始系统配置进行重构时，或移动到新的永久安装后启用备份操作。如果要移动许可证，则需要填写“许可证移动表单”并将其发送至 *Password Delivery Center (PDC)*，或访问网页 https://software.microfocus.com/zh-cn/legal/software-licensing，可在此执行生成密码、移动密码等操作。

有关如何获取和安装密码的相关说明，请参见 获取永久密码 (第 255 页)。

获取永久密码

以下是获取永久密码的步骤：

1. 收集永久密码*请求表单*所需的信息。请参见 Data Protector 许可表单 (第 256 页)，查找表单位置并获取关于如何填写表单的说明。
2. *Password Delivery Center* 将使用您发送请求的方式发送您的永久密码。例如，如果您通过电子邮件发送请求，那么您将通过电子邮件收到永久密码。
3. 执行以下某个操作：
   - 访问联机 *Password Delivery Center* 站点，地址为：https://software.microfocus.com/zh-cn/legal/software-licensing。
   - 填写*永久密码请求表单*并使用以下某种方式将其发送至 *Password Delivery Center*(请参见产品自带的权利证书以获取传真号码、电话号码、电子邮件地址和工作时间)：
     - 将表单传真至 *Password Delivery Center*
     - 发送电子邮件至 *Password Delivery Center*

       可以使用 Cell Manager 和安装介质上以下文件中包含的电子版许可表单：

       在 Windows Cell Manager 上： *Data_Protector_home*\Docs\license_forms.txt

       在 UNIX Cell Manager 上： /opt/omni/doc/C/license_forms_UNIX

       在 Windows 安装程序包上： \Docs\license_forms.txt

       将消息“复制”和“粘贴”到 *Password Delivery Center (PDC)*。

       您将在发送*永久密码请求表单*后 24 小时内收到永久密码。

安装永久密码

本节描述了安装 *Password Delivery Center (PDC)* 发送的永久密码的步骤。

先决条件：

您必须已收到 *Password Delivery Center* 发送的永久密码，并已在 Cell Manager 上安装 Data Protector 用户界面。密码安装在 Cell Manager 上且对整个单元有效。

使用 GUI：

要使用 Data Protector GUI 安装永久密码，请按以下步骤进行：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**Data Protector 单元**并单击**添加许可证**。
3. 按照*密码证书*上的显示输入或复制密码。

   一个密码由长度可变的 4 个字符组构成，以空格分隔，后面跟一个字符串。请确保此序列中没有换行符或回车符。以下是一个密码的示例：

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   键入密码后，请检查以下内容：

   - 确保在屏幕上正确显示密码。
   - 确保开头和结尾都没有空格，也没有多余字符。
   - 仔细检查 "1"(数字 1)字符和 "l"(字母 l)字符。
   - 仔细检查字符“O”(大写字母 O)和字符“0”(数字 0)。
   - 确保大小写使用正确。密码区分大小写。

   单击**确定**。

密码将写入 Cell Manager 上的以下文件：

Windows 系统：*Data_Protector_program_data*\Config\server\Cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

使用 CLI：

要使用 Data Protector CLI 安装永久密码，请按以下步骤进行：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -install_license password
   ```

   password 字符串必须按照*密码证书*上的显示准确输入。它必须是单行格式，不能包含任何嵌入的回车。密码必须在引号里。如果密码还包括在引号中的说明，则该说明的引号前必须有反斜杠。有关示例和详细信息，请参见 omnicc 手册页或《*Data Protector 命令行界面参考*》。

在 Cell Manager 上还可以将密码附加到以下文件：

Windows 系统：*Data_Protector_program_data*\config\server\cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

如果文件不存在，请使用编辑器(例如 vi 或 Notepad)创建文件。有关密码示例，请参见图形用户界面步骤中的按照密码证书上的显示输入或复制密码。 (第 256 页)。

Data Protector 许可表单

本节将讨论 Data Protector 许可表单。填写完成后可使用以下某种方法订购永久密码：

- 使用联机 *Password Delivery Center* 站点 https://software.microfocus.com/zh-cn/legal/software-licensing 订购永久密码。
- 打印在 Cell Manager 系统和安装介质上的以下文件中包含的许可表单的电子版：

  HP-UX 和 Linux 系统： `/opt/omni/doc/C/license_forms_UNIX`

  Windows 安装程序包： `Docs\license_forms.txt`

  或使用电子文件将您的消息“复制”并“粘贴”到 *Password Delivery Center (PDC)*。

> **重要：**
> 请确保清楚地输入信息且记住必需字段。

下面简单描述一下许可表单中必须填写的常规字段：

个人数据	该字段包含客户信息，包括新密码的发送对象。
许可数据	提供有关 Data Protector 单元的许可信息。
当前 Cell Manager	输入有关当前 Cell Manager 的必要信息。
新 Cell Manager	输入有关新 Cell Manager 的必要信息。
订单号	输入打印在*权利证书*上的*订单号*。需要*订单号*以验证您有权请求永久密码。
IP 地址	该字段定义 *Password Delivery Center* 将为哪些系统生成密码。如果要使用中央许可(仅限 MoM 环境)，那么该系统必须是 MoM 管理器系统。 如果 Cell Manager 具有多个 LAN 卡，则可以输入任何一个 IP 地址。Micro Focus 建议输入主 IP 地址。 如果您的 Data Protector 在 Serviceguard 或 Microsoft Cluster 环境中，则输入虚拟服务器的 IP 地址。有关群集的详细信息，请参见《*Data Protector 帮助*》。
Password Delivery Center 传真号码	有关联系信息，请参见产品随附的*权利证书*。
产品许可证类型	在*产品号*旁边的字段中，输入要在该 Cell Manager 上安装的许可证数量。该数量可以是随*订单号*购买的许可证的全部或一部分。

验证密码

使用 GUI

要验证安装的许可证密码是否正确，请在 Data Protector GUI 中执行如下步骤：

1. 在“帮助”菜单中，单击**许可证...**。
2. 单击**许可证**选项卡。所有安装的许可证都会显示出来。单击**密码信息**选项卡以查看已

安装的有效密码的详细信息。无效的密码将被标记为已过期或已删除。

整个弹出窗口及各个列可调整大小。

使用 CLI

要验证安装的许可证密码是否正确，请使用以下命令：

```
omnicc -password_info
```

此命令显示所有安装的许可证。如果输入的密码错误，会将其列出并标注 `Password could not be decoded.`

查找安装的许可证数量

使用 GUI

安装永久密码后，可以检查当前在 Cell Manager 上安装的许可证数量：

1. 启动 Data Protector 管理器。
2. 在菜单栏中，单击**帮助**，然后单击**许可证...**。此时将打开“关于管理器”窗口，显示安装的许可证。

使用 CLI

如果使用命令行，请执行如下步骤：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -query
   ```

此时将显示一个列出了当前安装的许可证的表。

升级现有许可证

如果您已经是 Data Protector 的用户，为了将您的旧许可证密码升级到 Data Protector 的最新版本，您必须具有有效的支持协议，其中涵盖了您正在使用的许可证数量和类型。

在收到新许可证密钥之后，应将其与已安装在 Data Protector 环境中的许可证密钥的数量和类型进行比较。只有在确认拥有足够有效的基于 许可证密钥之后，才可升级软件。

如果收到的新许可证密钥少于或不同于实际安装在 Data Protector 环境中的密钥，则不应升级到 Data Protector 的最新版本。否则，由于缺少许可证密钥，将存在 Data Protector 环境不再能运行的风险。

首先，联系您的销售代表或合作伙伴，以确定需执行哪些步骤来消除支持合同所涵盖的功能许可证与当前使用的实际许可证(在早于 Data Protector10.00 的 Data Protector 版本中使用的许可证)之间的差异。

安装 Data Protector 产品后，可以使用 60 天。60 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

将许可证移动到其他 Cell Manager 系统

在以下某种情况下，您必须联系 *Password Delivery Center*：

- 如果希望将 Cell Manager 移动到其他系统。
- 如果打算将安装在 Cell Manager 上但当前并未在单元中使用的许可证移动到其他 Data Protector 单元。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。
>
> 可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。
>
> 所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

在不同的 Cell Manager 之间移动许可证：

1. 为每个新的 Cell Manager 填写一份*许可证移动表单*，并将其发送至 *Password Delivery Center*。如果要移动无法再购买的产品的许可证，请使用以前版本的产品自带的*许可证移动表单*。请参见 Data Protector 许可表单 (第 266 页)。

   在表单上，必须指定要从现有 Cell Manager 移动的许可证的数量。

   或者，访问密码交付中心网站 (https://software.microfocus.com/zh-cn/legal/software-licensing) 并使许可证联机移动。
2. 删除以下文件：

   Windows 系统：

   Data_Protector_program_data\config\server\cell\lic.dat

   UNIX 系统：

   /etc/opt/omni/server/cell/lic.dat
3. 填写*许可证移动表单*并将其发送至 *Password Delivery Center (PDC)* 后，即可就从法律上迫使您从当前 Cell Manager 中删除所有 Data Protector。
4. 安装新密码。对于每个新的 Cell Manager，您都将收到一个密码。如果许可证仍留在当前 Cell Manager 上，则您还将收到一个新密码用于当前 Cell Manager。这个新密码将替换当前 Cell Manager 上的当前密码项。

> **注意：**
> Data Protector 也作为 Adaptive Backup and Recovery (ABR) 套件的一部分提供。ABR 套件将非结构化文件分析和自动存储分层 (Storage Optimizer) 与核心保护引擎 (Data Protector) 及报告和操作分析软件工具 (Backup Navigator) 相结合，以根据实时分析和优化，提供创新的数据保护方法。

集中式许可 (centralized licensing)

所有许可证都保留在 Manager-of-Managers (MoM) Manager 系统上。 虽然许可证仍然是在 MoM 管理器配置的，但是它们会被分配到特定单元。

有关如何配置许可证的详细信息，请参见《*Data Protector 帮助*》。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。
>
> 可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。 适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。
>
> 所有其他许可证可以无限制地移动到任何 Cell Manager 平台。 Cell Manager 平台类型对许可证没有任何限制。 例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

MoM 功能允许在 MoM 单元间移动(重分配)许可证。 有关详细信息，请参见《*Data Protector 帮助*》的索引："MoM 环境"。

如果是安装新的 Data Protector 许可证，请确保先检查 MoM 功能再请求许可证。 如果您决定以后使用中央许可，则必须完成移动许可证的步骤。

作为 100 TB 许可证的一部分，您将收到单个许可证密钥。 您无法从 Webware 或 Micro Focus 许可获取多个密钥。 要使用此单个许可证密钥，您必须在 MoM 环境中使用集中式许可。 您不需要额外购买 1 TB LTU，相反，即使需要 100 GB，也会为每个 Cell Manager 分配 1 TB LTU。

> **注意：**
> MoM 功能允许中央许可。 这意味着您可以在 MoM Manager 上安装所有许可证，然后将它们分配到属于 MoM 单元的各个 Cell Manager。 以后可以在 MoM 单元间移动(重分配)许可证。 有关详细信息，请参见《*Data Protector 帮助*》的索引："MoM 环境"。

许可证报告

Data Protector 许可证会被检查，如果丢失，则会在各种 Data Protector 操作期间进行报告，例如：

- 作为 Data Protector 检查和维护机制的一部分，许可证会得到检查，如果丢失，则会在 Data Protector 事件日志中进行报告。 Data Protector 事件日志位于 Cell Manager 上的 *Data_Protector_program_data*\log\server\Ob2EventLog.txt(Windows 系统)或 /var/opt/omni/server/log/Ob2EventLog.txt(UNIX 系统)。 有关 Data Protector 检查和维护机制的详细信息，请参见《*Data Protector 帮助*》的索引："事件日志, Data Protector"。
- 启动 Data Protector GUI 后，如果 Data Protector 事件日志中报告了任何缺少的许可证，则显示事件日志通知。 有关 Data Protector 事件日志的详细信息，请参见《*Data Protector 帮助*》的索引："事件日志, Data Protector"。
- 启动 Data Protector 会话后，将检查许可证，如果缺少，则报告。

按需生成许可证报告

要从单元生成有关许可信息的报告，请执行：

```
omnicc -check_licenses [-detail]
```

如果指定了 `-detail` 选项，则生成详细的报告。 许可证检查程序会为单元中的每个许可证返回以下信息：许可证名称、安装的许可证、使用的许可证、受保护的总数据 (TB) 和需要的其他许可证(容量)。

如果未指定 `-detail` 选项，则命令返回关于是否涵盖 Data Protector 许可的信息。 命令将返回信息：生成报告的时间、许可模式、许可证服务器以及受保护的总数据 (TB)。

请注意，对于驱动器扩展所用许可证，许可证检查程序返回有关配置的驱动器和建议的其他许可证的相关信息。 在任何时候，您需要的许可证数量与所使用的驱动器数量一样。此数量通常是已配置的驱动器的总数，以允许同时使用所有驱动器。

请注意，命令不会列出许可证的失效日期。 报告的生成可能需要一些时间，具体取决于环境和安装的许可证数量。 要获取有关许可证失效日期的信息，请执行：

```
omnicc -password_info
```

> **重要：**
> 在配置有 CMMDB 的 MoM 环境中，当为属于库和驱动器的项目生成许可证报告时，必须在安装有 CMMDB 的 Cell Manager 上运行 `omnicc` 命令。
>
> 有关详细信息，请参见 `omnicc` 手册页或《*Data Protector 命令行界面参考*》。

Data Protector 密码

安装 Data Protector产品后，可以使用 60 天。60 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

Data Protector 许可需要以下某种密码：

- 即开即用密码

  首次安装时会在产品中创建即开即用密码。在 Data Protector 支持的任何系统上安装软件后，可以使用软件 60 天。在此期间内，您必须从 *Password Delivery Center (PDC)* 请求永久密码，然后安装该密码。

  对于现有的 Data Protector 安装，在升级到 Data Protector 10.00 或更高版本后，您的安装将使用有效期为 60 天的即开即用密码运行。在此期间内，您必须从有效支持协议中所指定的 Password Delivery Center 请求新的永久密码。无法升级未包括在支持协议中的旧许可证。

- 永久密码

  Data Protector产品自带了一个*权利证书*许可证，它授权您获取永久密码。如果您已购买所有需要的许可证，则永久密码允许您根据备份策略配置 Data Protector 单元。在请求永久密码前，必须确定 Cell Manager 系统并了解单元配置要求。

- 紧急密码

  如果由于紧急情况，当前安装的密码与当前系统配置不匹配，则可使用紧急或后备密码。它们允许在任何系统上操作 120 天。

紧急密码由支持组织发布。它们必须由您的客户支持代表请求，且仅发布给这些人员。请咨询支持联系人或查看许可站点：https://software.microfocus.com/zh-cn/legal/software-licensing。

紧急密码的目的是当原始系统配置进行重构时，或移动到新的永久安装后启用备份操作。如果要移动许可证，则需要填写“许可证移动表单”并将其发送至 *Password Delivery Center (PDC)*，或访问网页 https://software.microfocus.com/zh-cn/legal/software-licensing，可在此执行生成密码、移动密码等操作。

有关如何获取和安装密码的相关说明，请参见获取和安装永久密码 (第 262 页)。

获取和安装永久密码

获取

以下是获取永久密码的步骤：

1. 收集永久密码*请求表单*所需的信息。请参见Data Protector 许可表单 (第 266 页)，查找表单位置并获取关于如何填写表单的说明。
2. 有关产品结构的详细信息，请参见Data Protector 产品结构和许可证 (第 267 页)。*Password Delivery Center* 将使用您发送请求的方式发送您的永久密码。例如，如果您通过电子邮件发送请求，那么您将通过电子邮件收到永久密码。
3. 执行以下某个操作：
   - 访问联机 *Password Delivery Center* 站点，地址为：https://software.microfocus.com/zh-cn/legal/software-licensing。
   - 填写*永久密码请求表单*并使用以下某种方式将其发送至 *Password Delivery Center*(请参见产品自带的权利证书以获取传真号码、电话号码、电子邮件地址和工作时间)：
     - 将表单传真至 *Password Delivery Center*
     - 发送电子邮件至 *Password Delivery Center*

       可以使用 Cell Manager 和安装介质上以下文件中包含的电子版许可表单：

       在 Windows Cell Manager 上： *Data_Protector_home*\Docs\license_forms.txt

       在 UNIX Cell Manager 上： /opt/omni/doc/C/license_forms_UNIX

       将消息“复制”和“粘贴”到 *Password Delivery Center (PDC)*。

       您将在发送*永久密码请求表单*后 24 小时内收到永久密码。

本节描述了安装 *Password Delivery Center (PDC)* 发送的永久密码的步骤。

先决条件

您必须已收到 *Password Delivery Center* 发送的永久密码，并已在 Cell Manager 上安装 Data Protector 用户界面。密码安装在 Cell Manager 上且对整个单元有效。

使用 GUI

要使用 Data Protector GUI 安装永久密码，请按以下步骤进行：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击 **Data Protector 单元**并单击**添加许可证**。
3. 严格按照*密码证书*上的显示输入或复制密码。

   一个密码由长度可变的 4 个字符组构成，以空格分隔，后面跟一个字符串。请确保此序列中没有换行符或回车符。以下是一个密码的示例：

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   键入密码后，请检查以下内容：

   - 确保在屏幕上正确显示密码。
   - 确保开头和结尾都没有空格，也没有多余字符。
   - 仔细检查 "1"(数字 1)字符和 "l"(字母 l)字符。
   - 仔细检查字符“O”(大写字母 O)和字符“0”(数字 0)。
   - 确保大小写使用正确。密码区分大小写。

   单击**确定**。

密码将写入 Cell Manager 上的以下文件：

Windows 系统：*Data_Protector_program_data*\Config\server\Cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

使用 CLI

要使用 Data Protector CLI 安装永久密码，请按以下步骤进行：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -install_license password
   ```

   password 字符串必须严格按照*密码证书*上的显示准确输入。它必须是单行格式，不能包含任何嵌入的回车。密码必须在引号里。如果密码还包括在引号中的说明，则该说明的引号前必须有反斜杠。有关示例和详细信息，请参见 omnicc 手册页或《***Data Protector** 命令行界面参考***》**。

在 Cell Manager 上还可以将密码附加到以下文件：

Windows 系统：*Data_Protector_program_data*\config\server\cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

如果文件不存在，请使用编辑器(例如 vi 或记事本)创建文件。有关密码示例，请参见图形用户界面步骤前一页中的严格按照密码证书上的显示输入或复制密码。 (第 274 页)。

验证密码

使用 GUI

要验证安装的许可证密码是否正确，请在 Data Protector GUI 中执行如下步骤：

1. 在“帮助”菜单中，单击**许可证...**。
2. 单击**许可证**选项卡。所有安装的许可证都会显示出来。单击**密码信息**选项卡以查看已安装的有效密码的详细信息。无效的密码将被标记为已过期或已删除。

   整个弹出窗口及各个列可调整大小。

使用 CLI

要验证安装的许可证密码是否正确，请使用以下命令：

```
omnicc -password_info
```

此命令显示所有安装的许可证。如果输入的密码错误，会将其列出并标注`Password could not be decoded.`。

查找安装的许可证数量

使用 GUI

安装永久密码后，可以检查当前在 Cell Manager 上安装的许可证数量：

1. 启动 Data Protector 管理器。
2. 在菜单栏中，单击**帮助**，然后单击**许可证...**。此时将打开“关于管理器”窗口，显示安装的许可证。

使用 CLI

如果使用命令行，请执行如下步骤：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -query
   ```

此时将显示一个列出了当前安装的许可证的表。

将许可证移动到其他 Cell Manager 系统

在以下某种情况下，您必须联系 *Password Delivery Center*：

- 如果希望将 Cell Manager 移动到其他系统。
- 如果打算将安装在 Cell Manager 上但当前并未在单元中使用的许可证移动到其他 Data Protector 单元。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台

无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。

可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。

所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

在不同的 **Cell Manager** 之间移动许可证

1. 为每个新的 Cell Manager 填写一份*许可证移动表单*，并将其发送至 *Password Delivery Center*。如果要移动无法再购买的产品的许可证，请使用以前版本的产品自带的*许可证移动表单*。请参见Data Protector 许可表单 (第 266 页)。

   在表单上，必须指定要从现有 Cell Manager 移动的许可证的数量。

   或者，访问密码交付中心网站 (https://software.microfocus.com/zh-cn/legal/software-licensing) 并使许可证联机移动。
2. 删除以下文件：

   Windows 系统：

   Data_Protector_program_data\config\server\cell\lic.dat

   UNIX 系统：

   /etc/opt/omni/server/cell/lic.dat
3. 填写*许可证移动表单*并将其发送至 *Password Delivery Center (PDC)* 后，即可就从法律上迫使您从当前 Cell Manager 中删除所有 Data Protector 密码。
4. 安装新密码。对于每个新的 Cell Manager，您都将收到一个密码。如果许可证仍留在当前 Cell Manager 上，则您还将收到一个新密码用于当前 Cell Manager。这个新密码将替换当前 Cell Manager 上的当前密码项。

集中式许可

通过 Data Protector，可为整个多单元环境配置中央许可，从而简化许可证管理。所有许可证都保留在 Manager-of-Managers (MoM) Manager 系统上。虽然许可证仍然是在 MoM 管理器配置的，但是它们会被分配到特定单元。

有关如何配置许可证的详细信息，请参见《*Data Protector 帮助*》。

注意：
UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。

可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。

所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

MoM 功能允许在 MoM 单元间移动(重分配)许可证。有关详细信息，请参见 *Data Protector 帮助*索引："MoM 环境"。

如果是安装新的 Data Protector 许可证，请确保先检查 MoM 功能再请求许可证。如果您决定以后使用中央许可，则必须完成移动许可证的步骤。

> **注意：**
> MoM 功能允许中央许可。这意味着您可以在 MoM Manager 上安装所有许可证，然后将它们分配到属于 MoM 单元的各个 Cell Manager。以后可以在 MoM 单元间移动(重分配)许可证。有关详细信息，请参见 *Data Protector 帮助*索引："MoM 环境"。

许可证迁移到 Data Protector 10.00

支持合同中的 Data Protector 8.1 及更高版本的客户可免费收到 Data Protector 10.00，其中包括支持合同中所有许可证的新许可证密钥。

Data Protector 10.00 不会显示已过期的或未用于同一个产品版本的许可证。

可以访问 Software Support Online (SSO) 上的 MyUpdates 门户，网址为 https://softwaresupport.softwaregrp.com/。

在此处，可以根据有效支持合同 (SAID) 下载您有权访问的软件和许可证密钥。

可以查看与 SAID 关联的所有软件，选中 Data Protector 10.00 或更高版本前面的复选框并单击**获取更新**。

将显示以下三个选项卡：

- **获取软件**：用于下载软件。
- **获取许可证**：用于获取映射到 Data Protector 9.00 或更高版本的 LTU 的许可证。
- **获取文档**：用于下载产品文档。

当您单击**获取许可证**链接时，会直接将您指向更新订单软件许可证门户 (https://software.microfocus.com/zh-cn/legal/software-licensing)，在这里您可以获取与服务协议标识符 (SAID) 上数量一致的 LTU 许可证密钥。

Data Protector 许可表单

本节将讨论 Data Protector 许可表单。填写完成后可使用以下某种方法订购永久密码：

- 使用联机 *Password Delivery Center* 站点 https://software.microfocus.com/zh-cn/legal/software-licensing 订购永久密码。
- 打印在 Cell Manager 系统和安装介质上的以下文件中包含的许可表单的电子版：

  HP-UX 和 Linux 系统： `/opt/omni/doc/C/license_forms_UNIX`

  Windows 安装程序包： *`DriveLetter`*`:Docs\license_forms.txt`

  或使用电子文件将您的消息"复制"并"粘贴"到 *Password Delivery Center (PDC)*。

> **重要：**
> 请确保清楚地输入信息且记住必需字段。

下面简单描述一下许可表单中必须填写的常规字段：

个人数据	该字段包含客户信息，包括新密码的发送对象。
许可数据	提供有关 Data Protector 单元的许可信息。
当前 Cell Manager	输入有关当前 Cell Manager 的必要信息。
新 Cell Manager	输入有关新 Cell Manager 的必要信息。
订单号	输入打印在*权利证书*上的*订单号*。需要*订单号*以验证您有权请求永久密码。
IP 地址	该字段定义 *Password Delivery Center* 将为哪些系统生成密码。如果要使用中央许可(仅限 MoM 环境)，那么该系统必须是 MoM 管理器系统。 如果 Cell Manager 具有多个 LAN 卡，则可以输入任何一个 IP 地址。Micro Focus 建议输入主 IP 地址。 如果您的 Data Protector 在 Serviceguard 或 Microsoft Cluster 环境中，则输入虚拟服务器的 IP 地址。有关群集的详细信息，请参见《*Data Protector 帮助*》。
Password Delivery Center 传真号码	有关联系信息，请参见产品随附的*权利证书*。
产品许可证类型	在*产品号*旁边的字段中，输入要在该 Cell Manager 上安装的许可证数量。该数量可以是随*订单号*购买的许可证的全部或一部分。

Data Protector 产品结构和许可证

密码考虑事项

考虑以下事项以帮助确定合适的密码数量。

- 即开即用密码是内置的。每次在新安装和将现有 Data Protector 升级到 Data Protector 10.00 版本或更高版本后将提供为期 60 天的该密码，在这 60 天内您无需安装任何额外许可证密码，并且可为您提供完整的产品功能，以供您评估。

  在 60 天后，即开即用密码到期，除非安装永久许可证密钥，否则产品将停止工作。

  > **重要：**
  > 在安装首个常规许可证密钥之后，完整产品的评估期将终止。一旦已至少安装了一个许可证密钥后，仅可使用已安装许可证密钥对应的功能。

- 可将永久许可证移动到其他 Cell Manager。但是，需要使用“许可证移动表单”并将它们发送至 *Password Delivery Center (PDC)*。
- 密码安装在 Cell Manager 上且对整个单元有效。
- Manager-of-Managers (MoM) 功能中包含中央许可。如果您为多个单元购买了多个许可证，则可以将所有许可证都安装在 MoM 系统上。

- 您需要每个单元使用一个 Cell Manager 许可证。
- 执行 Data Protector 配置任务或启动备份会话时，软件会定期检查许可证密钥或密码。
- 即开即用密码可用于任何系统上，而评估密码和永久密码只能用于为其请求许可证的 Cell Manager 系统上。

> **注意：**
> 要更改 Cell Manager 的 IP 地址，要移动 Cell Manager 到另一个系统或者将许可证从一个单元移动到另一个单元(而不使用 MoM 功能)，应联系 *Password Delivery Center (PDC)* 以便更新许可证。有关联系 Password Delivery Center 的信息，请参见*获取和安装永久密码*部分。

Data Protector 密码

安装 Data Protector产品后，可以使用 60 天。60 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

Data Protector 许可需要以下某种密码：

- 即开即用密码

  首次安装时会在产品中创建即开即用密码。在 Data Protector 支持的任何系统上安装软件后，可以使用软件 60 天。在此期间内，您必须从 *Password Delivery Center (PDC)* 请求永久密码，然后安装该密码。

  对于现有的 Data Protector 安装，在升级到 Data Protector 10.00 或更高版本后，您的安装将使用有效期为 60 天的即开即用密码运行。在此期间内，您必须从有效支持协议中所指定的 Password Delivery Center 请求新的永久密码。无法升级未包括在支持协议中的旧许可证。

- 永久密码

  Data Protector产品自带了一个*权利证书*许可证，它授权您获取永久密码。如果您已购买所有需要的许可证，则永久密码允许您根据备份策略配置 Data Protector 单元。在请求永久密码前，必须确定 Cell Manager 系统并了解单元配置要求。

- 紧急密码

  如果由于紧急情况，当前安装的密码与当前系统配置不匹配，则可使用紧急或后备密码。它们允许在任何系统上操作 120 天。

  紧急密码由支持组织发布。它们必须由您的客户支持代表请求，且仅发布给这些人员。请咨询支持联系人或查看许可站点：https://software.microfocus.com/zh-cn/legal/software-licensing。

  紧急密码的目的是当原始系统配置进行重构时，或移动到新的永久安装后启用备份操作。如果要移动许可证，则需要填写“许可证移动表单”并将其发送至 *Password Delivery Center (PDC)*，或访问网页 https://software.microfocus.com/zh-cn/legal/software-licensing，可在此执行生成密码、移动密码等操作。

有关如何获取和安装密码的相关说明，请参见获取和安装永久密码 (第 269 页)。

获取和安装永久密码

获取

以下是获取永久密码的步骤：

1. 收集永久密码*请求表单*所需的信息。请参见Data Protector 许可表单 (第 266 页)，查找表单位置并获取关于如何填写表单的说明。
2. 有关产品结构的详细信息，请参见 Data Protector 产品结构和许可证 (第 267 页)。*Password Delivery Center* 将使用您发送请求的方式发送您的永久密码。例如，如果您通过电子邮件发送请求，那么您将通过电子邮件收到永久密码。
3. 执行以下某个操作：
   - 访问联机 *Password Delivery Center* 站点，地址为：https://software.microfocus.com/zh-cn/legal/software-licensing。
   - 填写*永久密码请求表单*并使用以下某种方式将其发送至 *Password Delivery Center*(请参见产品自带的权利证书以获取传真号码、电话号码、电子邮件地址和工作时间)：
     - 将表单传真至 *Password Delivery Center*
     - 发送电子邮件至 *Password Delivery Center*

     可以使用 Cell Manager 和安装介质上以下文件中包含的电子版许可表单：

     在 Windows Cell Manager 上： *Data_Protector_home*\Docs\license_forms.txt

     在 UNIX Cell Manager 上： /opt/omni/doc/C/license_forms_UNIX

     将消息“复制”和“粘贴”到 *Password Delivery Center (PDC)*。

     您将在发送*永久密码请求表单*后 24 小时内收到永久密码。

本节描述了安装 *Password Delivery Center (PDC)* 发送的永久密码的步骤。

先决条件

您必须已收到 *Password Delivery Center* 发送的永久密码，并已在 Cell Manager 上安装 Data Protector 用户界面。密码安装在 Cell Manager 上且对整个单元有效。

使用 GUI

要使用 Data Protector GUI 安装永久密码，请按以下步骤进行：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击 **Data Protector 单元**并单击**添加许可证**。
3. 严格按照*密码证书*上的显示输入或复制密码。

   一个密码由长度可变的 4 个字符组构成，以空格分隔，后面跟一个字符串。请确保此序列中没有换行符或回车符。以下是一个密码的示例：

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

键入密码后，请检查以下内容：

- 确保在屏幕上正确显示密码。
- 确保开头和结尾都没有空格，也没有多余字符。
- 仔细检查 "1"(数字 1)字符和 "l"(字母 l)字符。
- 仔细检查字符“O”(大写字母 O)和字符“0”(数字 0)。
- 确保大小写使用正确。密码区分大小写。

单击**确定**。

密码将写入 Cell Manager 上的以下文件：

Windows 系统：*Data_Protector_program_data*\Config\server\Cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

使用 CLI

要使用 Data Protector CLI 安装永久密码，请按以下步骤进行：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   omnicc -install_license *password*

   password 字符串必须严格按照*密码证书*上的显示准确输入。它必须是单行格式，不能包含任何嵌入的回车。密码必须在引号里。如果密码还包括在引号中的说明，则该说明的引号前必须有反斜杠。有关示例和详细信息，请参见 omnicc 手册页或《*Data Protector 命令行界面参考*》。

在 Cell Manager 上还可以将密码附加到以下文件：

Windows 系统：*Data_Protector_program_data*\config\server\cell\lic.dat

UNIX 系统：/etc/opt/omni/server/cell/lic.dat

如果文件不存在，请使用编辑器(例如 vi 或记事本)创建文件。有关密码示例，请参见图形用户界面步骤前一页中的严格按照密码证书上的显示输入或复制密码。 (第 274 页)。

验证密码

使用 GUI

要验证安装的许可证密码是否正确，请在 Data Protector GUI 中执行如下步骤：

1. 在“帮助”菜单中，单击**许可证...**。
2. 单击**许可证**选项卡。所有安装的许可证都会显示出来。单击**密码信息**选项卡以查看已安装的有效密码的详细信息。无效的密码将被标记为已过期或已删除。

   整个弹出窗口及各个列可调整大小。

使用 CLI

要验证安装的许可证密码是否正确，请使用以下命令：

```
omnicc -password_info
```

此命令显示所有安装的许可证。如果输入的密码错误，会将其列出并标注`Password could not be decoded.`。

查找安装的许可证数量

使用 **GUI**

安装永久密码后，可以检查当前在 Cell Manager 上安装的许可证数量：

1. 启动 Data Protector 管理器。
2. 在菜单栏中，单击**帮助**，然后单击**许可证...**。此时将打开"关于管理器"窗口，显示安装的许可证。

使用 **CLI**

如果使用命令行，请执行如下步骤：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -query
   ```

此时将显示一个列出了当前安装的许可证的表。

将许可证移动到其他 **Cell Manager** 系统

在以下某种情况下，您必须联系 *Password Delivery Center*：

- 如果希望将 Cell Manager 移动到其他系统。
- 如果打算将安装在 Cell Manager 上但当前并未在单元中使用的许可证移动到其他 Data Protector 单元。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。
>
> 可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。
>
> 所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

在不同的 **Cell Manager** 之间移动许可证

1. 为每个新的 Cell Manager 填写一份*许可证移动表单*，并将其发送至 *Password Delivery Center*。如果要移动无法再购买的产品的许可证，请使用以前版本的产品自带的*许可证移动表单*。请参见Data Protector 许可表单 (第 266 页)。

   在表单上，必须指定要从现有 Cell Manager 移动的许可证的数量。

或者，访问密码交付中心网站 (https://software.microfocus.com/zh-cn/legal/software-licensing) 并使许可证联机移动。

2. 删除以下文件：

   Windows 系统：

   Data_Protector_program_data\config\server\cell\lic.dat

   UNIX 系统：

   /etc/opt/omni/server/cell/lic.dat

3. 填写*许可证移动表单*并将其发送至 *Password Delivery Center (PDC)* 后，即可就从法律上迫使您从当前 Cell Manager 中删除所有 Data Protector 密码。
4. 安装新密码。对于每个新的 Cell Manager，您都将收到一个密码。如果许可证仍留在当前 Cell Manager 上，则您还将收到一个新密码用于当前 Cell Manager。这个新密码将替换当前 Cell Manager 上的当前密码项。

集中式许可

通过 Data Protector，可为整个多单元环境配置中央许可，从而简化许可证管理。所有许可证都保留在 Manager-of-Managers (MoM) Manager 系统上。虽然许可证仍然是在 MoM 管理器配置的，但是它们会被分配到特定单元。

有关如何配置许可证的详细信息，请参见《*Data Protector 帮助*》。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。
>
> 可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。
>
> 所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

MoM 功能允许在 MoM 单元间移动(重分配)许可证。有关详细信息，请参见 *Data Protector 帮助*索引：“MoM 环境”。

如果是安装新的 Data Protector 许可证，请确保先检查 MoM 功能再请求许可证。如果您决定以后使用中央许可，则必须完成移动许可证的步骤。

> **注意：**
> MoM 功能允许中央许可。这意味着您可以在 MoM Manager 上安装所有许可证，然后将它们分配到属于 MoM 单元的各个 Cell Manager。以后可以在 MoM 单元间移动(重分配)许可证。有关详细信息，请参见 *Data Protector 帮助*索引：“MoM 环境”。

许可证密码

安装 Data Protector产品后，可以使用 60 天。60 天后，必须在 Cell Manager 上安装永久密码以启用软件。您可以在 Data Protector Cell Manager 上加载软件，但是没有永久密码就无法

执行配置任务，因为特定 Data Protector 功能所需的许可证需要密码。

密码考虑事项

考虑以下事项以帮助确定合适的密码数量：

- 即开即用密码是内置的。每次在新安装和将现有 Data Protector 升级到 Data Protector 9.00 或更高版本后将提供为期 60 天的该密码，在这 60 天内您无需安装任何额外许可证密码，并且可为您提供完整的产品功能，以供您评估。

  在 60 天后，即开即用密码到期，除非安装永久许可证密钥，否则产品将停止工作。

  在安装首个常规许可证密钥之后，完整产品的评估期将终止。一旦已至少安装了一个许可证密钥后，仅可使用已安装许可证密钥对应的功能。
- 可将永久许可证移动到其他 Cell Manager。但是，需要使用“许可证移动表单”并将它们发送至 Password Delivery Center (PDC)。
- 密码安装在 Cell Manager 上且对整个单元有效。
- Manager-of-Managers (MoM) 功能中包含中央许可。如果您为多个单元购买了多个许可证，则可以将所有许可证都安装在 MoM 系统上。
- 您需要每个单元使用一个 Cell Manager 许可证。
- 执行 Data Protector 配置任务或启动备份会话时，软件会定期检查许可证密钥或密码。
- 即开即用密码可用于任何系统上，而评估密码和永久密码只能用于为其请求许可证的 Cell Manager 系统上。

Data Protector 许可需要以下某种密码：

- 即开即用密码

  首次安装时会在产品中创建即开即用密码。在 Data Protector 支持的任何系统上安装软件后，可以使用软件 60 天。在此期间内，您必须从 *Password Delivery Center (PDC)* 请求永久密码，然后安装该密码。

  对于现有的 Data Protector 安装，在升级到 Data Protector 9.00 或更高版本后，您的安装将使用即开即用密码运行 60 天。在此期间内，您必须从有效支持协议中所指定的 Password Delivery Center 请求新的永久密码。无法升级未包括在支持协议中的旧许可证。
- 永久密码

  Data Protector产品自带了一个*权利证书*许可证，它授权您获取永久密码。如果您已购买所有需要的许可证，则永久密码允许您根据备份策略配置 Data Protector 单元。在请求永久密码前，必须确定 Cell Manager 系统并了解单元配置要求。
- 紧急密码

  如果由于紧急情况，当前安装的密码与当前系统配置不匹配，则可使用紧急或后备密码。它们允许在任何系统上操作 120 天。

  紧急密码由支持组织发布。它们必须由人员请求，且仅发布给这些人员。请咨询支持联系人或查看许可站点：https://software.microfocus.com/zh-cn/legal/software-licensing。

  紧急密码的目的是当原始系统配置进行重构时，或移动到新的永久安装后启用备份操作。如果要移动许可证，则需要填写“许可证移动表单”并将其发送至 *Password Delivery Center (PDC)*，或访问网页 https://software.microfocus.com/zh-cn/legal/software-licensing，可在此执行生成密码、移动密码等操作。

有关如何获取和安装密码的相关说明，请参见获取永久密码 (第 274 页)。

获取永久密码

以下是获取永久密码的步骤：

1. 收集永久密码*请求表单*所需的信息。请参见Data Protector 许可表单 (第 275 页)，查找表单位置并获取关于如何填写表单的说明。
2. *Password Delivery Center* 将使用您发送请求的方式发送您的永久密码。例如，如果您通过电子邮件发送请求，那么您将通过电子邮件收到永久密码。
3. 执行以下某个操作：
   - 访问联机 *Password Delivery Center* 站点，地址为：https://software.microfocus.com/zh-cn/legal/software-licensing。
   - 填写*永久密码请求表单*并使用以下某种方式将其发送至 *Password Delivery Center*(请参见产品自带的权利证书以获取传真号码、电话号码、电子邮件地址和工作时间)：
     - 将表单传真至 *Password Delivery Center*
     - 发送电子邮件至 *Password Delivery Center*

       可以使用 Cell Manager 和安装介质上以下文件中包含的电子版许可表单：

       在 Windows Cell Manager 上： *Data_Protector_home*\Docs\license_forms.txt

       在 UNIX Cell Manager 上： /opt/omni/doc/C/license_forms_UNIX

       在 Windows 安装程序包上： *Disk_Label*:\Docs\license_forms.txt

       将消息“复制”和“粘贴”到 *Password Delivery Center (PDC)*。

       您将在发送*永久密码请求表单*后 24 小时内收到永久密码。

安装永久密码

本节描述了安装 *Password Delivery Center (PDC)* 发送的永久密码的步骤。

先决条件：

您必须已收到 *Password Delivery Center* 发送的永久密码，并已在 Cell Manager 上安装 Data Protector 用户界面。密码安装在 Cell Manager 上且对整个单元有效。

使用 GUI：

要使用 Data Protector GUI 安装永久密码，请按以下步骤进行：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击 **Data Protector 单元**并单击**添加许可证**。
3. 严格按照*密码证书*上的显示输入或复制密码。

   一个密码由长度可变的 4 个字符组构成，以空格分隔，后面跟一个字符串。请确保此序列中没有换行符或回车符。以下是一个密码的示例：

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ```

```
ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
```

键入密码后，请检查以下内容：

- 确保在屏幕上正确显示密码。
- 确保开头和结尾都没有空格，也没有多余字符。
- 仔细检查 "1"(数字 1)字符和 "l"(字母 l)字符。
- 仔细检查字符“O”(大写字母 O)和字符“0”(数字 0)。
- 确保大小写使用正确。密码区分大小写。

单击**确定**。

密码将写入 Cell Manager 上的以下文件：

Windows 系统： *Data_Protector_program_data*\Config\server\Cell\lic.dat

UNIX 系统： /etc/opt/omni/server/cell/lic.dat

使用 CLI：

要使用 Data Protector CLI 安装永久密码，请按以下步骤进行：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -install_license password
   ```

   password 字符串必须严格按照*密码证书*上的显示准确输入。它必须是单行格式，不能包含任何嵌入的回车。密码必须在引号里。如果密码还包括在引号中的说明，则该说明的引号前必须有反斜杠。有关示例和详细信息，请参见 omnicc 手册页或《*Data Protector 命令行界面参考*》。

在 Cell Manager 上还可以将密码附加到以下文件：

Windows 系统： *Data_Protector_program_data*\config\server\cell\lic.dat

UNIX 系统： /etc/opt/omni/server/cell/lic.dat

如果文件不存在，请使用编辑器(例如 vi 或 Notepad)创建文件。有关密码示例，请参见图形用户界面步骤中的严格按照密码证书上的显示输入或复制密码。 (第 274 页)。

Data Protector 许可表单

本节将讨论 Data Protector 许可表单。填写完成后可使用以下某种方法订购永久密码：

- 使用联机 *Password Delivery Center* 站点 https://software.microfocus.com/zh-cn/legal/software-licensing 订购永久密码。
- 打印在 Cell Manager 系统和安装介质上的以下文件中包含的许可表单的电子版：

  HP-UX 和 Linux 系统： /opt/omni/doc/C/license_forms_UNIX

  Windows 安装程序包： Docs\license_forms.txt

  或使用电子文件将您的消息“复制”并“粘贴”到 *Password Delivery Center (PDC)*。

> **重要：**
> 请确保清楚地输入信息且记住必需字段。

下面简单描述一下许可表单中必须填写的常规字段：

个人数据	该字段包含客户信息，包括新密码的发送对象。
许可数据	提供有关 Data Protector 单元的许可信息。
当前 Cell Manager	输入有关当前 Cell Manager 的必要信息。
新 Cell Manager	输入有关新 Cell Manager 的必要信息。
订单号	输入打印在*权利证书*上的*订单号*。需要*订单号*以验证您有权请求永久密码。
IP 地址	该字段定义 *Password Delivery Center* 将为哪些系统生成密码。如果要使用中央许可(仅限 MoM 环境)，那么该系统必须是 MoM 管理器系统。 如果 Cell Manager 具有多个 LAN 卡，则可以输入任何一个 IP 地址。Micro Focus 建议输入主 IP 地址。 如果您的 Data Protector 在 Serviceguard 或 Microsoft Cluster 环境中，则输入虚拟服务器的 IP 地址。有关群集的详细信息，请参见《*Data Protector 帮助*》。
Password Delivery Center 传真号码	有关联系信息，请参见产品随附的*权利证书*。
产品许可证类型	在*产品号*旁边的字段中，输入要在该 Cell Manager 上安装的许可证数量。该数量可以是随*订单号*购买的许可证的全部或一部分。

验证密码

使用 GUI

要验证安装的许可证密码是否正确，请在 Data Protector GUI 中执行如下步骤：

1. 在“帮助”菜单中，单击**许可证...**。
2. 单击**许可证**选项卡。所有安装的许可证都会显示出来。单击**密码信息**选项卡以查看已安装的有效密码的详细信息。无效的密码将被标记为已过期或已删除。

   整个弹出窗口及各个列可调整大小。

使用 CLI

要验证安装的许可证密码是否正确，请使用以下命令：

```
omnicc -password_info
```

此命令显示所有安装的许可证。如果输入的密码错误，会将其列出并标注`Password could not be decoded.`。

查找安装的许可证数量

使用 GUI

安装永久密码后，可以检查当前在 Cell Manager 上安装的许可证数量：

1. 启动 Data Protector 管理器。
2. 在菜单栏中，单击**帮助**，然后单击**许可证...**。此时将打开"关于管理器"窗口，显示安装的许可证。

使用 CLI

如果使用命令行，请执行如下步骤：

1. 登录到 Cell Manager。
2. 请执行以下命令：

   ```
   omnicc -query
   ```

此时将显示一个列出了当前安装的许可证的表。

将许可证移动到其他 Cell Manager 系统

在以下某种情况下，您必须联系 *Password Delivery Center*：

- 如果希望将 Cell Manager 移动到其他系统。
- 如果打算将安装在 Cell Manager 上但当前并未在单元中使用的许可证移动到其他 Data Protector 单元。

> **注意：**
> UNIX 产品许可证适用于 UNIX、Windows 和 Novell NetWare 平台且提供的功能与平台无关，而 Windows 产品许可证只适用于 Windows、Novell NetWare 和 Linux 平台。
>
> 可以将适用于 HP-UX 的 Cell Manager 许可证移动到任何 Cell Manager 平台，并且可以在这些平台上进行使用。适用于 Windows 或 Linux 的 Cell Manager 许可证无法移动到 HP-UX Cell Manager 平台，也无法在这些平台上进行使用。
>
> 所有其他许可证可以无限制地移动到任何 Cell Manager 平台。Cell Manager 平台类型对许可证没有任何限制。例如，Windows 驱动器许可证可安装在 HP-UX Cell Manager 上，但是无法用于连接到 UNIX 系统的驱动器。

在不同的 **Cell Manager** 之间移动许可证：

1. 为每个新的 Cell Manager 填写一份*许可证移动表单*，并将其发送至 *Password Delivery Center*。如果要移动无法再购买的产品的许可证，请使用以前版本的产品自带的*许可证移动表单*。请参见Data Protector 许可表单 (第 266 页)。

   在表单上，必须指定要从现有 Cell Manager 移动的许可证的数量。

   或者，访问密码交付中心网站 (https://software.microfocus.com/zh-cn/legal/software-licensing) 并使许可证联机移动。
2. 删除以下文件：

   Windows 系统：

Data_Protector_program_data\config\server\cell\lic.dat

UNIX 系统：

/etc/opt/omni/server/cell/lic.dat

3. 填写*许可证移动表单*并将其发送至 *Password Delivery Center (PDC)* 后，即可就从法律上迫使您从当前 Cell Manager 中删除所有 Data Protector 密码。
4. 安装新密码。对于每个新的 Cell Manager，您都将收到一个密码。如果许可证仍留在当前 Cell Manager 上，则您还将收到一个新密码用于当前 Cell Manager。这个新密码将替换当前 Cell Manager 上的当前密码项。

第 9 章： 安装和升级故障诊断

本章包含与安装问题相关的信息。 有关常规故障排除的信息，请参见《*Data Protector 故障诊断指南*》。

安装 Windows Cell Manager 时的名称解析问题

在 Windows 上安装 Data Protector Cell Manager期间， Data Protector 将检测 DNS 或 LMHOSTS 文件是否未按要求设置正确，并发出相应警告。 此外， Data Protector 还会通知您，系统上是否未安装 TCP/IP 协议。

问题

使用 DNS 或 LMHOSTS 时名称解析失败

如果名称解析失败，将显示“error expanding hostname”消息，并中止安装。

- 如果在使用 DNS 时遇到解析问题，您将获得有关当前 DNS 配置的警告消息。
- 如果在使用 LMHOSTS 文件时遇到解析问题，您将获得要求检查 LMHOSTS 文件配置的警告消息。
- 如果尚未配置 DNS 或 LMHOSTS，您将获得警告消息，提示在 TCP/IP 属性对话框中启用 DNS 或 LMHOSTS 解析。

操作

检查 DNS 或 LMHOSTS 文件配置或将其激活。 请参见验证 Data Protector 单元中的 DNS 连接 (第 279 页)。

问题

系统上未安装和配置 TCP/IP 协议

Data Protector 使用 TCP/IP 协议进行网络通信；必须在单元中的每台客户机上安装并配置该协议。 否则，安装将中止。

操作

检查 TCP/IP 设置。 有关信息，请参见更改默认的 Data Protector Inet 端口 (第 306 页)。

验证 Data Protector 单元中的 DNS 连接

DNS(域名系统)是 TCP/IP 主机的名称服务。 DNS 配置了主机名和 IP 地址的列表，使用户能够按主机名而不是按 IP 地址指定远程系统。 DNS 确保 Data Protector 单元的成员之间正确通信。

如果 DNS 配置不正确， Data Protector 单元中可能会发生名称解析问题，并且其成员将无法相互通信。

Data Protector 提供了 `omnicheck` 命令用于验证 Data Protector 单元各成员间的 DNS 连接。 虽然可以用此命令检查单元中所有可能的连接，但是只需验证以下连接即可，这些连接在 Data Protector 单元中非常重要：

- Cell Manager 与单元其他成员的双向连接
- 介质代理与单元其他成员的双向连接

使用 omnicheck 命令

限制

- 该命令只验证单元成员之间的连接；一般不验证 DNS 连接。

omnicheck 命令的语法为：

```
omnicheck -dns [-host Client | -full] [-verbose]
```

可以使用不同的选项在 Data Protector 单元中验证以下 DNS 连接：

- 若要检查 Cell Manager 和单元中的每个介质代理是否可正确解析与单元中每个 Data Protector 客户机之间的 DNS 双向连接，则执行：

  ```
  omnicheck -dns [-verbose]
  ```

- 若要检查某个特定的 Data Protector 客户机是否可以正确解析与单元中每个 Data Protector 客户机的双向 DNS 连接，则执行：

  ```
  omnicheck -dns -host client [-verbose]
  ```

  其中 *client* 是接受检查的 Data Protector 客户机名称。

- 若要检查单元中所有可能存在的 DNS 连接，则执行：

  ```
  omnicheck -dns -full [-verbose]
  ```

如果指定 [-verbose] 选项，命令将返回所有消息。 如果不设置此选项(默认)，那么将只返回检查失败的结果的消息。

有关详细信息，请参见 omnicheck 手册页。

返回消息 (第 280 页)列出了 omnicheck 命令的返回消息。 如果返回消息指出 DNS 解析出现问题，请参见《*Data Protector 故障诊断指南*》的“网络和通信故障排除”一章。

返回消息

返回消息	含义
client_1 cannot connect to *client_2*	连接 *client_2* 超时。
client_1 connects to *client_2*, but connected system presents itself as *client_3*	*client_1* 上的 *%SystemRoot%*\System32\drivers\etc\hosts/etc/hosts (UNIX 系统)文件配置不正确，或者 *client_2* 的主机名与其 DNS 名称不匹配。
client_1 failed to connect to *client_2*	*client_2* 不可访问(例如，断开连接)，或者 *client_1* 上的 *%SystemRoot%*

返回消息	含义
	\System32\drivers\etc\hosts(Windows 系统)或 /etc/hosts(UNIX 系统)文件配置不正确。
checking connection between *client_1* and *client_2*	
all checks completed successfully.	
number_of_failed_checks checks failed.	
client is not a member of the cell.	
client contacted, but is apparently an older version. Hostname is not checked.	

故障诊断常见问题

问题

系统报告以下某条错误消息

- The Windows Installer Service could not be accessed.
- This application must be installed to run.
- This patch package could not be opened.
- The system cannot open the device or file specified.

安装或升级 Data Protector 后，Windows 可能报告某些应用程序未安装，或者需要重新安装。

原因是 Microsoft Installer 升级过程中出现错误。 Microsoft Installer 1.x 版数据信息未迁移到 Data Protector 在计算机上安装的 Microsoft Installer 2.x 版。

操作

有关如何解决该问题的信息，请参见 Microsoft 知识库文章 Q324906。

问题

如果Cell Manager 在未加入任何 Windows 域的 Windows 系统上安装失败，

系统报告以下消息：

Setup is unable to match the password with the given account name.

操作

有两种解决方案：

- 将要安装 Cell Manager 的 Windows 系统加入域。
- 对 CRS 服务使用本地管理员帐户。

问题

系统报告以下错误消息

`msvcr90.dll file is not found`

找不到 `MSVCR90.dll` 库(大写)，因为网络共享上只有 `msvcr90.dll`(小写)。 由于 `MSVCR90.dll` 和 `msvcr90.dll` 未被视作同一个文件，因此 `setup.exe` 未能找到相应的 `dll`。

操作

将 `msvcr90.dll`(小写)文件重命名为 `MSCVCR90.dll`(大写)，或者将网络共享重新配置为不区分大小写。

问题

取消安装未卸载已经安装的组件

如果取消 Data Protector 安装，但是某些组件已经安装，那么 Data Protector 不会卸载已经安装的组件。 安装将完成，并带有错误。

操作

取消安装后，手动卸载已经安装的组件。

问题

报告了以下错误：

`"too many open files" error`

单元请求服务器 (CRS) 会调整其 `ulimit` 以支持大量打开的文件和套接字，但当前值通常足以满足需求。 如果遇到“打开的文件过多”错误，则您需要调整操作系统参数。

操作

操作系统参数涵盖两个方面：

- 它们更改针对打开的文件和套接字的限制。
- 它们影响存在大量套接字连接时的性能。

以下列表不是确切的。 有关详细信息，请参见 OS 文档。

HP-UX

打开文件的最大数量由内核变量设置。

要配置变量，请使用 `kctune variable=value`。

要查看变量，请使用 `kctune -v variable` 或 `kcusage`。

变量	默认	有限制	注意
maxfiles	2048	32 … 1,048,576 <= maxfiles_lim	每个进程的初始(软)最大文件描述符数量 ulimit –Sn

变量	默认	有限制	注意
maxfiles_lim	4096	32 … 1,048,576 >= maxfiles <= nfile/2	每个进程的硬最大文件描述符数量 ulimit -Hn
nfile	65,536	2048 … 2,147,483,647 >= 2*maxfiles_lim	系统范围的最大文件描述符数量**注意：** 即使 nnn > nfile/2，“ulimit –Hn nnn”也能成功

此外，如果存在大量套接字，请使用 ndd 调整网络参数，如下所述：

```
ndd -h tcp_time_wait_interval
ndd -h tcp_fin_wait_2_timeout
ndd -h /dev/tcp tcp_smallest_anon_port
vi /etc/rc.config.d/nddconf
```

Linux

内核参数保存在以下位置：

```
/etc/sysctl.conf
```

可以编辑 sysctl.conf 文件或调用 sysctl –w name=value。 您还可以使用 sysctl –p 加载正在运行的内核或修改其相应的 procfs 文件。 例如，变量 fs.file-max 与 /proc/sys/fs/file-max 对应。

> **注意：**
> 默认值取决于可用内存。

变量	注意
fs.file-max	系统范围的最大文件描述符数量。
net.core.somaxconn	侦听套接字的挂起连接队列可增长到的最大长度。
net.ipv4.tcp_max_syn_backlog	尚未从连接客户机收到确认的已记录连接请求的最大数量。

此外，每进程限制的默认值存储在以下位置：

```
/etc/limits.conf
```

(或)

```
/etc/security/limits.conf
```

UNIX 系统上的安装故障诊断

问题

UNIX 客户机远程安装失败

远程安装或升级 UNIX 客户机失败，并出现以下错误消息：

```
Installation/Upgrade session finished with errors.
```

远程安装或升级 UNIX 客户机时，客户机系统上 /tmp 文件夹下的可用磁盘空间应至少为要用于安装的最大包的大小。 在 Solaris 客户机系统上，/var/tmp 文件夹下也应该有相同的磁盘空间量。

操作

检查上面提到的目录中是否有足够的磁盘空间，然后重新启动安装或升级过程。

有关磁盘空间要求，请参见安装 Data Protector 客户机 (第 49 页)。

问题

安装 HP-UX 客户机时出现问题

在将新的 HP-UX 客户机添加到 Data Protector单元时，出现以下错误消息：

```
/tmp/omni_tmp/packet: you do not have the required permissions to perform this SD function.....

Access denied to root at to start agent on registered depot /tmp/omni_tmp/packet.
No insert permission on host.
```

操作

按如下方式先停止再重新启动 swagent 后台程序：终止该进程，然后通过运行 /opt/omni/sbin/swagentd 命令重新启动该进程；或者运行 /opt/omni/sbin/swagentd -r 命令。

确保 hosts 文件 (/etc/hosts) 中有 local host, loopback 条目。

问题

安装 Mac OS X 客户机时存在的问题

将 Mac OS X 客户机添加到 Data Protector 单元时，不会启动 com.hp.omni 进程。

操作

在 Mac OS X 上，launchd 用于启动 com.hp.omni 进程。

若要启动服务，请转到：

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

执行：

```
launchctl load com.hp.omni
```

问题

安装 UNIX Cell Manager 后无法启动 Inet 进程 the UNIX Cell Manager

启动 Cell Manager 时，出现以下错误：

```
ERROR: Cannot start "omniinet" service, system error: [1053] Unknown error 1053.
```

操作

检查 inetd 或 xinetd 服务是否正在运行：

HP-UX 系统： ps -ef | grep inetd

Linux 系统： ps -ef | grep xinetd

要启动该服务，请执行：

HP-UX 系统： /usr/sbin/inetd

Linux 系统： rcxinetd start

问题

具有有效凭据的 Linux 客户机上的推送安装失败，并显示以下错误消息：

[严重] <iwf1114165.hpeswlab.net> SSH 配置失败。 输入的凭据不正确或者发生了某个错误。

<iwf1114165.hpeswlab.net>：已跳过 0%

[严重] <iwf1114165.hpeswlab.net> 连接到客户机 iwf1114165.hpeswlab.net 时出错

正在跳过客户机！

[正常] 安装会话已于 Mon 14 Nov 2016 03:13:52 PM IST 完成。

已完成安装。

操作

确保为 Linux 客户机上的 ssh 服务启用了密码身份验证。 否则，请执行以下步骤：

1. 通过将以下行添加到 ssh config 文件中来启用身份验证：
   PasswordAuthentication yes
2. 重新启动 ssh 服务。

Windows 系统上的安装故障诊断

问题

Windows 客户机远程安装失败

将 Data Protector 客户机远程安装到 Windows 系统失败，系统报告以下错误消息：

[Normal] Connecting to client computer.company.com...

[Normal] Done.

[Normal] Installing the Data Protector bootstrap service on client computer.company.com...

[Critical] Cannot connect to the SCM (Service Control Manager) on client computer.company.com: [5] Access is denied.

操作

1. 在安装服务器系统上，执行下面的命令将本地操作系统 Administrators 用户组中的某个用户帐户标记为在远程安装期间将由安装服务器使用：

   ```
   omniinetpasswd -inst_srv_user User@Domain
   ```

   请注意，该用户帐户必须已经添加到本地 Inet 配置中。有关详细信息，请参见《*Data Protector 命令行界面参考*》中的 omniinetpasswd 命令说明。
2. 再次启动 Data Protector 客户机的远程安装。

问题

Windows 客户机远程安装失败 (Windows XP)

如果 Windows XP 系统是工作组成员，并且“简单文件共享”安全策略设置已启用，那么将强制尝试通过网络访问此系统的用户使用来宾帐户。远程安装 Data Protector 客户机期间，Data Protector 反复要求提供有效的用户名和密码，因为远程安装需要管理员权限。

操作

关闭“简单文件共享”：在 Windows XP 上，打开 **Windows 资源管理器**或**我的电脑**，依次单击**工具**菜单、**文件夹选项**、**查看**选项卡，然后取消选中**使用简单文件共享(推荐)**复选框。

以下情况下，“简单文件共享”策略将被忽略：

- 计算机是域成员
- 如果 Network access: Sharing and security model for local accounts 安全策略设置配置为 Classic: Local users authenticate as themselves

问题

如果 Windows 7 或 Windows 2008 R2 系统断开连接，数字签名验证可能会失败。

数字签名验证失败，并显示以下错误消息：

```
[Critical] <computer.company.com> [70:32] Digital Signature verification of the
install kit failed.
```

操作

执行以下操作之一：

- 启用 Internet 连接，并等待直至正确的证书自动导入到受信任的根证书颁发机构和中间证书颁发机构。

  (或)
- 要了解如何在断开连接的系统上更新受信任的根证书，请参见以下文章：

  https://support.microsoft.com/en-us/kb/3004394

  https://support.microsoft.com/en-us/kb/2813430

问题

安装 Cell Manager 时，应用程序服务器服务无法启动

应用程序服务器服务无法启动，并显示以下消息

```
Timeout reached before Data Protector Application Server started.
```

安装摘要日志文件中记录了以下错误：

```
Caused by: org.jboss.as.cli.
CommandLineException: The controller is not available at localhost:9999
```

由于 PATH 系统环境变量不包含 %SystemRoot%\system32 目录，因此安装进程无法访问各种实用程序。

操作

将 %SystemRoot%\system32 目录添加到 PATH 变量。

> **注意：**
> 以下文件放置在 Windows 系统上的 %SystemRoot%\system32 文件夹(取决于所选组件)中：

BrandChgUni.dll	这是资源库。它仅供内部使用；但是，它还包含注册表设置的路径，因此必须位于众所周知的位置，以便集成库能在那里访问它。
ob2informix.dll	该库用于与 Informix Server 数据库集成。
snmpOB2.dll	该库用于实现系统 SNMP 陷阱。

验证 Data Protector 客户机安装

验证 Data Protector 客户机安装包含以下步骤：

- 检查 Cell Manager 和客户机系统上的 DNS 配置，并确保 Cell Manager 和客户机系统上 omnicheck -dns 命令的结果与指定的系统匹配。
- 检查客户机上安装的软件组件。
- 将要安装的某个软件组件所需要的文件列表与客户机上已安装的文件进行比较。
- 验证某个软件组件所需要的每个只读文件的校验和。

先决条件

安装服务器必须可用于您所选类型的客户机系统(UNIX、Windows)。

限制

若要使用 Data Protector GUI 验证 Data Protector 安装：

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，展开**客户机**，右键单击 Cell Manager 系统，然后单击**检查安装**以启动向导。
3. 遵循向导以验证单元中系统的安装。“检查安装”窗口随即打开，其中显示了安装结果。

   有关详细信息，请参见《*Data Protector 帮助*》。

如果安装未成功，请参见使用日志文件 (第 294 页)。

有关如何使用 Data Protector CLI 在 UNIX 系统上验证安装的信息，请参见 ob2install 手册页。

升级故障诊断

问题

如果将以前版本的产品安装在长路径中，则升级将失败

Data Protector 不支持将 Cell Manager 安装到长于 80 个字符的路径中。结果是升级失败。

操作

1. 将 omnimigrate.pl 脚本从安装程序包的目录 x8664\tools\Upgrade 复制到一个临时目录 (例如 c:\temp)。
2. 使用 omnimigrate 命令导出 IDB：

   ```
   perl c:\temp\omnimigrate.pl -export -shared_dir c:\output
   ```

   使用在 Data Protector 安装中提供的 Perl 版本，并驻留在默认命令目录中。
3. 删除以前版本的 Data Protector，但保留其配置和数据库数据。不要删除 *Data_Protector_program_data*\db40 目录。
4. 安装 Data Protector 10.00。确保您要安装的路径短于 80 个字符。
5. 停止所有 Data Protector 服务：

   ```
   omnisv –stop
   ```
6. 将文件从旧的 *Data_Protector_program_data*\db40 目录(在删除以前版本的 Data Protector 之后保留的目录)复制到新的 *Data_Protector_program_data*\db40 文件夹。确保不移动 DCBF 目录。
7. 将配置从旧的 *Data_Protector_program_data*\Config\Server 文件夹复制到新的文件夹：
   a. 将旧的配置目录复制到新的目录，但保留旧的文件。不要复制 *Data_Protector_program_data*\Config\Server\install 目录中的文件。
   b. 如果要保留单元配置(客户机、安装服务器)，请复制和覆盖 *Data_Protector_program_data*\Config\Server\cell\cell_info 与 *Data_Protector_program_data*\Config\Server\cell\installation_servers 文件。
8. 合并新的通知和全局选项文件：
   a. 要合并通知，请执行 omninotifupg.exe 工具：

      ```
      omninotifupg.exe -quiet
      ```
   b. 要合并全局选项文件，请执行：

      ```
      mrgcfg.exe –global -except BackupDeviceIdle -rename
      DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
      =SessSuccessfulWhenNoObjectsBackedUp
      ```

      或者，可以从旧的安装手动合并全局选项文件。
9. 启动 Data Protector 服务：

   ```
   omnisv -start
   ```
10. 将 IDB 导入到新的安装。执行：

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

问题

如果将以前版本的产品安装在不受支持的字符的路径中，则升级将失败

Data Protector 不支持将 Cell Manager 安装在以下路径：

- 包含非 ASCII 字符
- 包含“@”或“#”字符
- 包含以“!”字符结尾的目录

结果是升级失败。

操作

1. 将 omnimigrate.pl 脚本从安装程序包的目录 x8664\tools\Upgrade 复制到一个临时目录(例如 c:\temp)。
2. 创建两个使用 ASCII 名称的目录，例如：

   ```
   c:\output\cdb
   ```

   ```
   c:\output\mmdb
   ```
3. 导出 MMDB 和 CDB：

   ```
   omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb
   ```

   此过程将需要一段时间。当开始导出文件名时，可以使用 **Ctrl+C** 停止 omnidbutil 进程，因为升级不需要此数据。
4. 使用 omnimigrate 命令导出 IDB：

   ```
   perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output
   ```

   使用在 Data Protector 安装中提供的 Perl 版本，并驻留在默认命令目录中。
5. 创建一个 ANSI 字符集文件，c:\output\old_cm。此文件应包含以下两行：

   ```
   OLDCM_SHORTNAME=OldCmName
   OLDCM_ENDIANNESS=LITTLE_ENDIAN
   ```

   使用 Cell Manager 的短名称替代 *OldCmName*。
6. 删除以前版本的 Data Protector，但保留其配置和数据库数据。不要删除 *Data_Protector_program_data*\db40 目录。
7. 安装 Data Protector。确保您要安装的路径不包含任何非 ASCII 字符。
8. 停止所有 Data Protector 服务：

   ```
   omnisv –stop
   ```
9. 将文件从旧的 *Data_Protector_program_data*\db40 目录(在删除以前版本的 Data Protector 之后保留的目录)复制到新的 *Data_Protector_program_data*\db40 文件夹。确保不移动 DCBF 目录。
10. 将配置从旧的 *Data_Protector_program_data*\Config\Server 文件夹复制到新的文件夹：
    a. 将旧的配置目录复制到新的目录，但保留旧的文件。不要复制 *Data_Protector_program_data*\Config\Server\install 目录中的文件。
    b. 如果要保留单元配置(客户机、安装服务器)，请复制和覆盖 *Data_Protector_program_data*\Config\Server\cell\cell_info 与 *Data_Protector_program_data*\Config\Server\cell\installation_servers 文件。

11. 合并新的通知和全局选项文件：
    a. 要合并通知，请执行 omninotifupg.exe 工具：
       ```
       omninotifupg.exe -quiet
       ```
    b. 要合并全局选项文件，请执行：
       ```
       mrgcfg.exe –global -except BackupDeviceIdle -rename
       DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
       =SessSuccessfulWhenNoObjectsBackedUp
       ```
       或者，可以从旧的安装手动合并全局选项文件。
12. 启动 Data Protector 服务：
    ```
    omnisv -start
    ```
13. 将 IDB 导入到新的安装。执行：
    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

问题

如果旧的(基于 Raima DB)IDB 损坏，升级过程将中止

在升级期间，将检测并更正 IDB 中的以下损坏字段：

- 介质 blocks_used 设置为 0
- 介质 blocks_total 设置为 blocks_used
- 池 media_age_limit 设置为默认值(相同介质类的默认池的 media_age_limit)
- 池 media_overwrite_limit 设置为默认值(相同介质类的默认池的 media_overwrite_limit)

但是，如果 IDB 中的其他任何字段损坏，升级就会中止。

操作

将 Data Protector 安装还原到旧版本：

1. 删除当前版本的 Data Protector。
2. 重新安装以前版本的 Data Protector。
3. 还原旧的 IDB。

尝试安装其他升级时，需要修复旧的 IDB。要获得进一步协助，请与客户支持人员联系。

问题

升级后，omnidbcheck -bf 失败并显示错误

在先前版本的 Data Protector 中，由于 DC 进制文件中介质的实际大小和头大小不一致，因此 omnidbcheck -bf 无法正确报告错误。

omnidbcheck -bf 可以正确报告升级之前 IDB 中可能存在的所有一致性错误。

操作

如果 DC 二进制文件损坏，可以删除 DC 二进制文件并通过导入具有正确日志记录级别的介质来重新创建它们。删除文件所产生的唯一影响是某些介质位置将指向不存在的二进制文件，因此在浏览相关的文件系统时将显示错误消息。

1. 从 omnidbcheck -dc 输出中，找出损坏的 DC 二进制文件的介质 ID。
2. 运行 omnimm -media_info *medium-id* 命令以获取介质的其他属性，如介质标签和介质池。
3. 找出受影响介质的 DC 二进制文件。DC 二进制文件的名称为：*MediumID_TimeStamp*.dat(在 MediumID 中)，冒号":"替换为"_")。
4. 删除损坏的 DC 二进制文件。
5. 运行 omnidbutil -fixmpos 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
6. 从介质导入编目，以重新创建二进制文件。

   有关详细信息，请参见 *Data Protector 帮助*和 *Data Protector 故障诊断指南*中的"处理 DCBF 部分中的细微 IDB 损坏"。要获得进一步协助，请与客户支持人员联系。

问题

如果 Velois IDB 损坏，升级过程将中止

在升级期间，将检测并更正 IDB 中的以下损坏字段：

- 介质 blocks_used 设置为 99
- 介质 blocks_total 设置为 blocks_used
- 池 media_age_limit 设置为默认值(相同介质类的默认池的 media_age_limit)
- 池 media_overwrite_limit 设置为默认值(相同介质类的默认池的 media_overwrite_limit)

但是，如果 IDB 中的以下任何字段损坏，升级将会中止。

介质：LAST_SEGMENT

位置：

SEQUENCE_NR

START_SEGMENT

START_OFFSET

LOG_LEVEL

DCBF_OFFSET

DCBF_NUMOFDIRS

DCBF_NUMOFITEMS

DCBF_SIZE

操作

将 Data Protector 安装还原到旧版本：

1. 删除当前版本的 Data Protector。
2. 重新安装以前版本的 Data Protector。
3. 还原旧的 IDB。

尝试安装其他升级时，需要修复旧的 IDB。要获得进一步协助，请与客户支持人员联系。

问题

IDB 和配置文件在升级后不可用

从以前的版本升级 Cell Manager 后，IDB 和所有配置文件不可用。如果升级过程出于任何原因而中断，则会出现此问题。

操作

从升级前生成的备份还原 Data Protector，消除造成中断的原因，然后再次开始升级。

问题

升级后，旧的 Data Protector 补丁没有删除

如果在 Data Protector 升级完成后运行 `swlist` 命令，那么旧的 Data Protector 补丁会作为已安装的程序列出。这些补丁在升级期间已从系统中删除，但是它们仍保留在 sw 数据库中。

要检查已安装的 Data Protector 补丁，使用 GUI 验证 Data Protector 补丁 (第 197 页)。

操作

若要从 sw 数据库中移除旧补丁，请运行下面的命令：

`swmodify -u`*`patch`*`.\*`*`patch`*

例如，要从 sw 数据库中删除补丁“PHSS_30143”，则运行下面的命令：

```
swmodify -u PHSS_30143.\* PHSS_30143
```

问题

升级使用 StorageTek 库的“介质代理”客户机会导致连接问题

在使用 StorageTek 库的系统上升级 Data Protector 介质代理组件后，与库的连接会丢失，涉及该库的 Data Protector 会话可能会停止响应或异常终止。

操作

重启 StorageTek 库支持服务或守护程序可以解决此问题：

Windows 系统：使用管理工具服务重新启动 `LibAttach` 服务。

HP-UX 和 Solaris 系统：运行命令 `/opt/omni/acs/ssi.sh stop` 和 `/opt/omni/acs/ssi.sh start` *`ACSLS_hostname`*，其中 *ACSLS_hostname* 是安装自动磁带盒系统库软件的系统的名称。

AIX 系统：运行命令 `/usr/omni/acs/ssi.sh stop` 和 `/usr/omni/acs/ssi.sh start` *`ACSLS_hostname`*，其中 *ACSLS_hostname* 是安装自动磁带盒系统库软件的系统的名称。

问题

升级到 Data Protector 10.00 或更高版本之后，如果您执行还原操作，系统将显示一条 DCBF 错误消息。在 Data Protector GUI 的“还原”上下文中，当您选择某个对象并尝试浏览文件时，系统将显示以下消息：

`[12:10907] Invalid format of detail catalog binary file`。

但是，由于 DCBF 文件并未真正损坏，因此 `omnidbcheck -dc` 不会报告任何错误。发生这种情况的原因是系统读取了两个不同版本的文件，从而导致版本不匹配。

操作

选项 1：转至“恢复会话”上下文并尝试恢复单个文件。

选项 2：导出/导入介质，此时，系统将创建 DCBF 编目。有关详细信息，请参见 *Data Protector 帮助*的“*导入介质*”和“*导出介质*”部分。

选项 3：编目迁移。`perl omnimigrate.pl –start_catalog_migration`

> **注意：**
> 完整编目迁移完成后(没有旧编目之后)，将全局变量 `SupportOldDCBF` 更改为 `0`。

问题

升级到 Data Protector 10.00 或更高版本后，如果您选择使用 Data Protector 7.03 进行备份的单个磁盘进行还原，那么 Data Protector GUI 会显示以下错误消息：

对象 `scsi0:<disk number>` 没有版本信息。此对象的备份很可能未完成 - 将无法进行还原。

还原对象 `'<VCenter host> Virtual Environment [<Data center>]'` 有问题。它可能没有版本信息或存在一些冲突。还原已中止。

操作

选择完整的虚拟机进行还原。

问题

计划迁移在升级期间失败

操作

如果在升级过程中计划迁移失败，您可以手动运行以下命令，以便将现有计划成功迁移到新的计划程序：

```
omnidbutil -migrate_schedules
```

Windows 系统上的远程升级故障诊断

问题

启动安装过程时出错

当使用 Data Protector 远程安装功能升级 Windows 客户机时，您收到以下错误：

```
Error starting setup process, err=[1326] Logon failure: unknown user name or bad password.
```

该问题的原因是远程计算机上的 `Data Protector Inet` 服务在运行时所用的用户帐户无权访问 安装服务器 计算机上的 OmniBack 共享。该帐户极有可能是本地用户。

操作

将 `Data Protector Inet` 服务的用户更改为可访问 Data Protector 共享的用户。

问题

Data Protector Cell Request Server (CRS) 在升级后无法启动

手动启动 CRS 时，显示以下错误消息：

```
Windows could not start the Data Protector CRS on Local Computer.
```

```
For more information, review the System Event Log. If this is a non-Microsoft
service, contact the service vendor, and refer to service-specific error code 1007.
```

安装后显示以下错误消息：

```
Timeout reached before Data Protector CRS started.
```

操作

- 使用 omnisv stop 命令，停止 Data Protector 服务。
- 打开任务管理器并结束剩余的 Data Protector 进程。
- 使用 omnisv start 命令，启动 Data Protector 服务。

UNIX 系统上的手动本地升级过程

通常，您执行 omnisetup.sh 命令来升级 UNIX Cell Manager 和 安装服务器 上的.Data Protector 8.1 及更高版本，该命令执行自动升级过程。但是，也可以手动执行升级。请参见在 HP-UX 和 Linux 系统上使用本机工具进行升级 (第 302 页)。

手动升级客户机后，在 Cell Manager 中运行以下 omnicc 命令来更新客户机信息：

```
omnicc -update_host [hostname] -accept_host
```

要更新单元中的所有客户机信息，请运行以下命令：

```
omnicc -update_all -accept_host
```

有关 omnicc 命令的详细信息，请参见 *Data Protector 命令行界面参考* 指南。

使用日志文件

如果在安装 Data Protector 时遇到问题，可以检查以下日志文件来确定问题：

- 安装日志文件 (Windows)
- 系统日志文件 (UNIX)
- Data Protector 日志文件

出现安装问题时应检查哪些日志文件取决于安装类型(本地或远程)以及操作系统。

本地安装

本地安装出现问题时，请检查以下日志文件：

HP-UX Cell Manager:

- /var/adm/sw/swinstall.log
- /var/adm/sw/swagent.log(有关更多详细信息)

Linux Cell Manager:

```
/var/opt/omni/log/debug.log
```

Windows 客户机(运行安装程序的系统)：

- *Temp*\SetupLog.log
- *Temp*\OB2DBG_*did*__setup_*HostName*_*DebugNo*_setup.txt(有关更多详细信息)
  其中：
  - *did*(调试 ID)是接受调试参数的第一个进程的进程 ID。此 ID 用作调试会话的 ID。所有后续进程将使用此 ID。
  - *HostName* 是创建跟踪文件的主机的名称。
  - *DebugNo* 是 Data Protector 生成的编号。
- *Temp*\CLUS_DBG_*DebugNo*.TXT(在群集环境中)

Temp 目录的位置由 TEMP 环境变量指定。要检查此变量的值，请运行 set 命令。

远程安装

远程安装出现问题时，请检查以下日志文件：

UNIX 安装服务器：

/var/opt/omni/log/IS_install.log

Windows 客户机(组件将要安装到的远程系统)：

- *SystemRoot*\TEMP\OB2DBG_*did*_INSTALL_SERVICE_*DebugNo*_debug.txt
- *SystemRoot*\TEMP\CLUS_DBG_*DebugNo*.TXT

Temp 目录的位置由 TEMP 环境变量指定，并且 *SystemRoot* 是在 SystemRoot 环境变量中指定的路径。

如果没有创建安装日志文件，请带调试选项运行远程安装。请参见创建安装执行跟踪 (第 296 页)。

Data Protector 日志文件

下面列出的 Data Protector 日志文件位于：

Windows Server 2008 和 Windows Server 2012： *Data_Protector_program_data*\log

其他 Windows 系统： *Data_Protector_home*\log

HP-UX、Solaris 和 Linux 系统： /var/opt/omni/log 和 /var/opt/omni/server/log

其他 UNIX 系统和 Mac OS X 系统： /usr/omni/log

下面的日志文件对于安装故障诊断非常重要：

debug.log	包含意外情况。虽然其中的某些内容可能对您有意义，但是这些信息主要供支持人员或支持部门使用。
inet.log	包含向 Data Protector inet 服务发送的请求。它对于检查客户机上 Data Protector 的近期活动很有用。
IS_	包含远程安装的跟踪，并且位于 安装服务器 上。

install.log	
omnisv.log	包含有关 Data Protector 服务停止和启动时间的信息。
upgrade.log	此日志是在升级期间创建的，并包含升级核心部分 (UCP) 和升级详细信息部分 (UDP) 消息。
OB2_ Upgrade.log	此日志是在升级期间创建的，并包含升级过程的跟踪。

有关更多日志文件，请参见《*Data Protector 故障诊断指南*》。

创建安装执行跟踪

如果客户支持服务要求，请使用 debug 选项运行安装。 有关调试的详细信息，包括下面的调试选项，以及如何准备要发送给客户支持服务的数据，请参见《*Data Protector 故障诊断指南*》。

要调试远程安装，请运行带调试选项的 Data Protector GUI：

```
Manager -debug 1-200 DebugPostfix
```

会话完成/终止后，从以下位置收集调试输出：

- 在安装服务器系统上：

  Data_Protector_program_data\tmp\OB2DBG_*did*__BM_ *Hostname_DebugNo_DebugPostfix*
- 在远程系统上：

  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hostname_DebugNo_DebugPostfix*

附录 A： 使用 UNIX 系统本机工具安装和升级

本附录介绍如何使用本机安装工具(适用于 HP-UX 系统的 swinstall 和适用于 Linux 系统的 rpm)在 UNIX 系统上对 Data Protector 进行安装与升级。

在 HP-UX 和 Linux 系统上使用本机工具安装

注意：
建议使用 omnisetup.sh 安装 Data Protector。有关详细信息，请参见在 HP-UX 和 Linux 系统上使用本机工具安装 (第 297 页)。

HP-UX 和 Linux 上的本机安装步骤仅适用于使用有限的一组远程安装包安装 安装服务器。

在 HP-UX 系统上使用 swinstall 安装 Cell Manager

在 HP-UX 系统上安装 UNIX Cell Manager

1. 复制 HP-UX 上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 运行 /usr/sbin/swinstall 实用程序。
3. 在“指定源”窗口中，选择**网络目录/CDROM**，然后在**源仓库路径**中输入 hpux/DP_DEPOT。单击**确定**打开“SD 安装 - 软件选择”窗口。
4. 在可用于安装的包列表中，Data Protector 产品显示在名称 B6960MA 下。
5. 右键单击 **DATA-PROTECTOR**，然后单击**标记以安装 (Mark for Install)** 安装整个软件。

   如果不需要所有子产品，请双击 **DATA-PROTECTOR**，然后右键单击列表中的项目。单击**不标记安装**可排除包，单击**标记以安装**可选择进行安装。

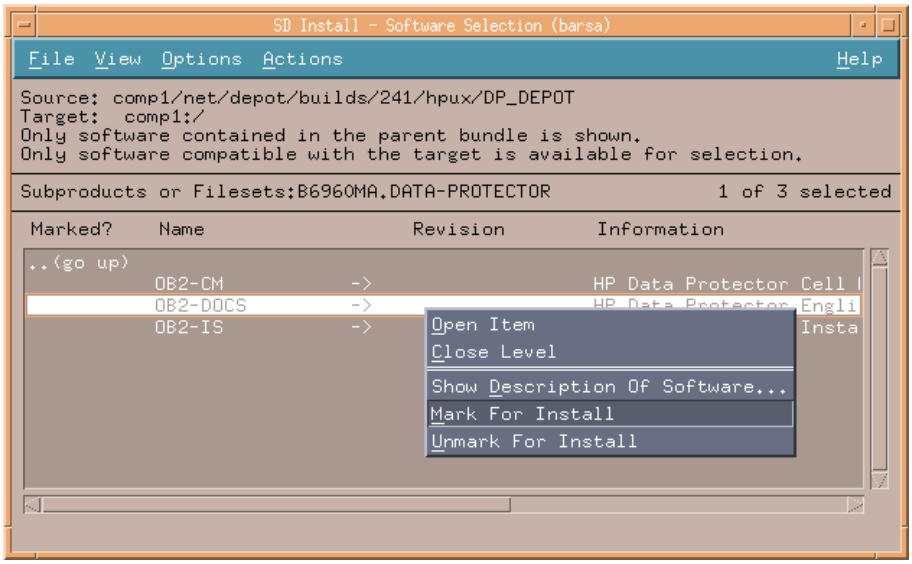
   产品中包含以下子产品：

OB2-CM	Cell Manager 软件
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 指南和 WebHelp 格式的 *Data Protector 帮助*。
OB2-IS	Data Protector 安装服务器

   如果在系统上为 UNIX 安装 Cell Manager，请确保 OB2-CM 包旁边的 Marked? 状态值设置为是 (Yes)。请参见 “SD 安装 - 软件选择 (SD install - software selection)”窗口 (第 297 页)。

   注意：
   如果使用长于 32 位的用户 ID，则必须在安装核心 Cell Manager 软件组件后在 Cell Manager 上远程安装用户界面组件 (OMNI-CS)。

“SD 安装 - 软件选择 (SD install - software selection)”窗口



6. 在"操作"列表中，单击**安装(分析)**，然后单击**确定**继续。如果 Install (analysis) 失败并显示错误消息，请单击**日志文件**查看文件。

注意：
要跨越网络从某个磁带设备安装软件，首先需要在计算机上装载源目录。

在 Linux 系统上使用 rpm 安装 Cell Manager

在 Linux 系统上安装 Cell Manager

1. 复制 Linux 上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到 linux_x86_64/DP_DEPOT 目录。
3. 要安装组件，请执行：

   rpm -i *package_name*-A.10.00-1.x86_64.rpm

   其中 *package_name* 是相应的子产品包的名称。

   必须安装以下组件：

OB2-CORE	Data Protector 核心软件。
OB2-TS-CORE	Data Protector 核心技术堆栈库
OB2-CC	单元控制台软件。它包含命令行界面。
OB2-TS-CS	Cell Manager 技术堆栈库。
OB2-TS-JRE	与 Data Protector 一起使用的 Java 运行时环境。
OB2-TS-AS	Data Protector 应用程序服务器
OB2-WS	Data Protector Web 服务
OB2-JCE-	作业控制引擎调度程序

DISPATCHER	
OB2-JCE-SERVICEREGISTRY	作业控制引擎服务注册表
OB2-CS	Cell Manager 软件。
OB2-DA	磁盘代理软件。它是必需的，否则无法备份 IDB。
OB2-MA	常规介质代理软件。如果要将备份设备连接到 Cell Manager，则该软件是必需的。
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 指南和 WebHelp 格式的 *Data Protector 帮助*。

重要：
Linux 上的组件相互依赖。应以上面列出的顺序安装这些组件。

4. 重新启动 Data Protector 服务：

```
omnisv stop
omnisv start
```

在 HP-UX 系统上使用 swinstall 安装 安装服务器

1. 复制 HP-UX 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 运行 `/usr/sbin/swinstall` 实用程序。
3. 在“指定源”窗口中，选择**网络目录/CDROM**，然后在**源仓库路径**中输入 `hpux/DP_DEPOT`。单击**确定**打开“SD 安装 - 软件选择”窗口。
4. 在可用于安装的组件列表中，Data Protector 产品显示在名称 B6960MA 下。双击它显示用于 UNIX 系统的 DATA-PROTECTOR 产品。双击它显示内容。

   产品中包含以下子产品组件：

OB2-CM	Cell Manager 软件
OB2-DOCS	Data Protector 文档子产品，包括 PDF 格式的 Data Protector 指南和 WebHelp 格式的 *Data Protector 帮助*。
OB2-IS	Data Protector 安装服务器

5. 在“SD 安装 - 软件选择”窗口中，双击**DATA-PROTECTOR**会列出用于安装的软件。右键单击 **OB2-IS**，然后单击**标记以安装**。
6. 在“操作”菜单中，单击**安装(分析)**。单击**确定**继续。

安装完成时，UNIX 的软件仓库位于 `/opt/omni/databases/vendor` 目录中。

重要：
如果不在网络中为 UNIX 安装 安装服务器，则必须从 HP-UX 安装程序包 (tar) 本地安装每个 UNIX 客户机。此外，也无法为 Data Protector 客户机上的组件打补丁。

在 Linux 系统上使用 rpm 安装 安装服务器

在 Linux 本地安装

在 Linux 系统上安装 UNIX 的安装服务器

1. 复制 Linux 系统上下载的 Data Protector 安装程序包 (tar)，然后将文件提取到本地目录。
2. 转到包含安装存档的目录(在此例中是 `linux_x86_64/DP_DEPOT`)。
3. 对于每个组件，请执行：

   `rpm -i package_name-A.10.00-1.x86_64.rpm`

   产品中包括以下与 安装服务器 安装相关的组件 *package_name*：

OB2-CORE	Data Protector 核心软件。请注意，如果是在 Cell Manager 系统上安装 安装服务器，则已安装该子产品包。
OB2-TS-CORE	Data Protector 核心技术堆栈库。
OB2-CORE-IS	安装服务器 核心软件。
OB2-CFP	适用于所有 UNIX 平台的公用 安装服务器 核心软件。
OB2-TS-CFP	适用于所有 UNIX 平台的公用 安装服务器 技术堆栈软件
OB2-DAP	适用于所有 UNIX 系统的磁盘代理远程安装包。
OB2-MAP	适用于所有 UNIX 系统的介质代理远程安装包。
OB2-NDMPP	NDMP 介质代理组件。
OB2-CCP	适用于所有 UNIX 系统的单元控制台远程安装包。

   如果是安装独立的 安装服务器(即不在 Cell Manager 上)且要使用用户界面：

OB2-CC	单元控制台软件。它包含命令行界面。

4. 安装完这些组件后，使用 `rpm` 为所有将远程安装的组件安装远程安装包。例如：

OB2-INTGP	Data Protector 集成核心软件。该组件为安装集成所必需。
OB2-TS-PEGP	PEGASUS 技术堆栈组件。
OB2-OR8P	Oracle Integration 组件。
OB2-MYSQLP	MySQL 集成组件。
OB2-POSTGRESQLP	PostgreSQL 集成组件。
OB2-SAPP	SAP Integration 组件。
OB2-SAPDBP	SAP MaxDB 集成组件。

OB2-SAPHANAP	SAP HANA 集成组件。
OB2-INFP	Informix Integration 组件。
OB2-LOTP	Lotus Notes/Domino Integration 组件。
OB2-SYBP	Sybase Integration 组件。
OB2-DB2P	DB2 Integration 组件。
OB2-EMCP	EMC Symmetrix Integration 组件。
OB2-EMCVNXP	EMC VNX 集成组件。
OB2-EMCVMAXP	EMC VMAX 集成组件。
OB2-SMISAP	P6000/ 3PAR SMI-S 代理组件。
OB2-SSEAP	P9000 XP 代理组件。
OB2-NETAPPP	NetApp Storage Provider 组件。
OB2-VEPAP	虚拟环境保护代理组件。
OB2-SODAP	StoreOnce Software 重复数据删除组件。
OB2-AUTODRP	自动灾难恢复组件。
OB2-VMWAREGRE-AGENTP	VMware Granular Recovery Extension 组件。
OB2-DOCSP	英语文档 (指南、帮助) (English Documentation (Guides, Help)) 组件。
OB2-FRAP	法语文档 (指南、帮助) (French Documentation (Guides, Help)) 组件。
OB2-JPNP	日语文档 (指南、帮助) (Japanese Documentation (Guides, Help)) 组件。
OB2-CHSP	简体中文文档(指南和帮助)组件。

有关组件和依赖关系的完整列表，请参见安装 UNIX Cell Manager (第 26 页)。

安装完成时，UNIX 的软件仓库位于 `/opt/omni/databases/vendor` 目录中。

重要：
如果不在网络中为 UNIX 安装 安装服务器，则必须从 Linux 安装程序包 (tar) 本地安装每个 UNIX 客户机。

重要：
将 Data Protector 安装到链接目录中，例如：

`/opt/omni/ -> /prefix/opt/omni/`

/etc/opt/omni/ -> /*prefix*/etc/opt/omni/

/var/opt/omni/ -> /*prefix*/var/opt/omni/

则必须在安装前创建链接并确保目标目录存在。

下面的步骤

至此，您应该已在网络中安装了 UNIX 的安装服务器。现在应执行以下任务：

1. 如果已安装独立的安装服务器(即不在 Cell Manager 上)，则必须手动将系统添加(导入)到 Data Protector 单元中。请参见在 UNIX 系统上安装 安装服务器 (第 39 页)。

   注意：
   导入安装服务器后，Cell Manager 上的 /etc/opt/omni/server/cell/installation_servers 文件将更新以列出已安装的远程安装包。该文件可用于在 CLI 中检查可用的远程安装包。为保持该文件最新，每当安装或删除远程安装包后应导出再导入安装服务器。即使安装服务器安装在与 Cell Manager 相同的系统上，此方法也适用。

2. 如果 Data Protector 单元中有任何 Windows 系统，请安装 Windows 的安装服务器。请参见在 HP-UX 和 Linux 系统上使用本机工具安装 (第 297 页)。
3. 将软件分发到客户机上。请参见安装 Data Protector 客户机 (第 49 页)。

安装客户机

Cell Manager 或安装服务器安装期间没有安装客户机。必须使用 omnisetup.sh 或从 Data Protector GUI 远程安装组件来安装客户机。有关如何安装客户机的详细信息，请参见安装 Data Protector 客户机 (第 49 页)。

在 HP-UX 和 Linux 系统上使用本机工具进行升级

在 HP-UX 系统上使用 swinstall 升级 Data Protector

Cell Manager 的升级必须从 HP-UX 安装程序包执行。

如果在安装有安装服务器的情况下升级 Cell Manager，则必须首先升级 Cell Manager，然后升级安装服务器。

在 Cell Manager 升级期间不升级 Cell Manager 系统上安装的客户机组件，必须使用 omnisetup.sh 或从安装服务器中远程安装组件来升级这些组件。有关详细信息，请参见在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)或远程安装 (第 83 页)。

升级过程

使用下列方式升级到 **Data Protector 10.00** swinstall

1. 导出现有 IDB:
   a. 将 omnimigrate.pl 脚本从安装程序包复制到临时目录:

      ```
      cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omnimigrate.pl /tmp
      ```

   b. 使用 omnimigrate.pl 命令导出 IDB:

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir /var/opt/omni/server/exported-export
      ```

2. 以 root 身份登录，然后通过执行 omnisv -stop 命令停止 Data Protector 服务。

   输入 ps -ef | grep omni 以验证是否已关闭所有服务。 执行 ps -ef | grep omni 命令后必须没有 Data Protector 服务列出。

3. 要升级 Cell Manager 和/或 安装服务器，请遵循在 HP-UX 系统上使用 swinstall 安装 Cell Manager (第 297 页)和/或在 HP-UX 系统上使用 swinstall 安装 安装服务器 (第 299 页)中所述的步骤。

   安装步骤将自动检测以前的版本并*仅升级选定的*组件。 如果没有选定以前版本的 Data Protector 中已安装的组件，则*不会*升级该组件。 因此，必须确保选定了所有必须升级的组件。

   > **注意:**
   > 如果同时在同一系统上升级 Cell Manager 和 安装服务器，则 Match what target has 选项不受支持。

在 **Linux** 系统上使用 **rpm** 升级 **Data Protector**

要升级 Linux Cell Manager 或 安装服务器，请卸载产品的旧版本并安装新版本。

在 Cell Manager 升级期间不升级 Cell Manager 系统上安装的客户机组件，必须使用 omnisetup.sh 或从 安装服务器 中远程安装组件来升级这些组件。 有关详细信息，请参见在 UNIX 和 Mac OS X 系统上进行本地安装 (第 90 页)或远程安装 (第 83 页)。

升级过程

使用下列方式升级到 **Data Protector 10.00** rpm

1. a. 将 omnimigrate.pl 脚本从安装程序包复制到临时目录:

      ```
      cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omnimigrate.pl /tmp
      ```

   b. 使用 omnimigrate.pl 命令导出 IDB:

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir /var/opt/omni/server/exported-export
      ```

2. 以 root 身份登录，然后通过执行 omnisv -stop 命令停止 Data Protector 服务。

输入 ps -ef | grep omni 以验证是否已关闭所有服务。 执行 ps -ef | grep omni 命令后必须没有 Data Protector 服务列出。

3. 使用 rpm 卸载 Data Protector。

   在此步骤中会保留配置文件和数据库。

4. 运行 rpm –q 命令以验证是否已卸载旧版本的 Data Protector。 旧版本的 Data Protector 不应被列出。

   验证数据库和配置文件是否还在。 以下目录应还在且包含二进制文件：

   - /opt/omni
   - /var/opt/omni
   - /etc/opt/omni

5. 如果升级 Cell Manager，请使用 rpm 安装 Cell Manager。 有关详细步骤，请参见在 Linux 系统上使用 rpm 安装 Cell Manager (第 298 页)。

   如果升级 安装服务器，请使用 Linux 安装程序包。 有关详细步骤，请参见在 Linux 系统上使用 rpm 安装 安装服务器 (第 300 页)。

附录 B： 系统准备和维护任务

本附录介绍不属于本指南的范畴、但对安装过程有很大影响的任务的一些附加信息。 这些任务包括系统准备和维护任务。

UNIX 系统上的网络配置

在 UNIX 系统上安装 Data Protector 时， Data Protector Inet 注册为网络服务。 这通常需要执行以下步骤：

- 修改 /etc/services 文件，以注册 Data Protector Inet 将侦听的端口。
- 在系统的 inetd 后台程序或其等效后台程序(xinetd、launchd)中注册 Data Protector Inet。

修改网络配置时，初始 Data Protector Inet 配置可能会变成未完成或处于无效状态。 由于将 IPv6 支持添加到网络服务的系统特定设置，每当您添加或移除 Internet 协议版本 6 (IPv6) 网络接口时就会发生此问题。 其他情况下也可能会发生此问题。

要更新 Data Protector Inet 配置，可以使用 dpsvcsetup.sh 实用程序。 此实用程序(也可用于安装，收集所需信息并相应地更新系统配置)位于目录 /opt/omni/sbin(HP-UX、Solaris 和 Linux 系统)或 /usr/omni/bin(其他 UNIX 系统)中。

- 要更新 Data Protector Inet 配置，请执行：

  dpsvcsetup.sh -update.
- 要将 Data Protector Inet 注册为网络服务，请执行：

  dpsvcsetup.sh -install.
- 要将 Data Protector Inet 取消注册为网络服务，请执行：

  dpsvcsetup.sh -uninstall.

检查 TCP/IP 设置

TCP/IP 配置过程的一个重要方面是设置主机名解析机制。 网络中的每个系统必须能够解析 Cell Manager 的地址以及连接了介质代理和物理媒体设备的所有客户机。 Cell Manager 必须能够解析单元中所有客户机的名称。

安装 TCP/IP 协议后，可以使用 ping 和 ipconfig/ifconfig 命令来验证 TCP/IP 配置。

请注意，在某些系统上，不能对 IPv6 地址使用 ping 命令，而应使用 ping6 命令。

检查 TCP/IP 设置

1. 在命令行处运行：

   Windows 系统： ipconfig /all

   UNIX 系统： ifconfig*接口* 或者 ifconfig -a 或 nestat -i，具体取决于系统

   为网络适配器设置的 TCP/IP 配置和地址的精确信息。 检查 IP 地址和子网掩码是否设置正确。
2. 键入 ping *your_IP_address* 以确认软件的安装和配置。 默认情况下，应该收到四个响应包。

3. 键入 ping *default_gateway*。

   网关应处于您所在的子网中。 如果未能 ping 到网关，请检查网关 IP 地址是否正确，并且网关是否正在运行。

4. 如果前面的步骤都成功，那么就可以测试名称解析。 运行 ping 命令时输入系统名称，以测试 hosts 文件和/或 DNS。 如果计算机名称为 computer，域名为 company.com，则应输入： ping computer.company.com.

   如果此命令不起作用，则确认“TCP/IP 属性”窗口中的域名正确。 还应该检查主机文件和 DNS。 确保要成为 Cell Manager 的系统和要成为客户机的系统的名称解析双向有效：

   - 在 Cell Manager 上可以 ping 到每个客户机。
   - 在客户机上可以 ping 到 Cell Manager 和装有介质代理的每个客户机。

   注意：
   使用 hosts 文件进行名称解析时，上述测试不保证名称解析工作正确。 在此情况下，可能要在安装 Data Protector 后使用 **DNS 检查工具**。

   重要：
   如果上方指定的名称解析不起作用，则无法正确安装 Data Protector。

   另请注意，Windows 计算机名必须与主机名相同。 否则，Data Protector 安装程序将报告警告。

5. 安装 Data Protector 并且创建 Data Protector 单元之后，可以使用 DNS 检查工具确认 Cell Manager 和装有介质代理的每个客户机正确解析与单元中所有其他客户机的 DNS 连接，反之亦然。 可以通过执行 omnicheck -dns 来执行此操作。 失败的检查以及失败检查的数量将列出。

   有关 omnicheck 命令的详细信息，请参见*Data Protector 命令行界面参考*。

更改默认的 Data Protector 端口

更改默认的 Data Protector Inet 端口

Data Protector Inet 服务(进程)(该进程启动备份和还原所需的其他进程)应在 Data Protector 单元中的每个系统上使用相同的端口号。

默认情况下，Inet 使用端口号 5555/5565。 要验证此特定端口没有被其他程序使用，请检查本地 /etc/services 文件(UNIX 系统)或在本地调用的 netstat -a 命令的输出(Windows 系统)。 如果端口已被其他程序使用，您必须重新配置 Inet 以使用未使用的端口。 必须在单元的*每个*系统上完成此重新配置，以便单元中的*所有*系统均使用相同的端口。

一旦在充当安装服务器的 Cell Manager 上或在独立安装服务器上进行了更改，则使用此安装服务器远程安装的所有客户机都将自动使用新端口。 因此，在建立单元时更改 Inet 端口是最容易的。

警告：
不要更改为灾难恢复准备的系统上的默认 Inet 侦听端口。 反之，如果此类系统受

到灾难打击，灾难恢复进程可能会失败。

UNIX 系统

要在将成为 Cell Manager、安装服务器或 Data Protector 客户机的 UNIX 系统上更改 Inet 端口，请遵循以下步骤：

- 创建指明了所需端口号的 /tmp/omni_tmp/socket.dat。

要在已成为 Cell Manager、安装服务器或 Data Protector 客户机的 UNIX 系统上更改 Inet 端口，请遵循以下步骤：

1. 编辑 /etc/services 文件。 默认情况下，此文件应包含以下条目：

   ```
   omni 5565/tcp # DATA-PROTECTOR
   ```

   使用未使用的端口号替换端口号 5565。
2. 如果系统上存在文件 /etc/opt/omni/client/customize/socket 和 /opt/omni/newconfig/etc/opt/omni/client/customize/socket，则将所需的端口号更新到其内容中。
3. 通过使用 kill -HUP *inetd_pid* 命令终止相关进程，重新启动 Inet 服务。 要确定进程 ID (*inetd_pid*)，请运行 ps -ef 命令。
4. 如果要在 Cell Manager 上重新配置 Inet，请为 Port 全局选项设置新值。
5. 如果要在 Cell Manager 上重新配置 Inet，请重新启动 Data Protector 服务：

   ```
   - omnisv stop
   - omnisv start
   ```

Windows 系统

在将成为 Cell Manager、安装服务器或 Data Protector 客户机的 Windows 系统上更改 Inet 端口

1. 在命令行上，运行 regedit 以打开注册表编辑器。
2. 在键 HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Common 下，创建注册表项 InetPort：

   注册表项名称： InetPort

   注册表项类型： REG_SZ (string)

   注册表项的值： *PortNumber*

在已成为 Cell Manager、安装服务器或 Data Protector 客户机的 Windows 系统上更改 Inet 端口

1. 在命令行上，运行 regedit 以打开注册表编辑器。
2. 依次展开 **HKEY_LOCAL_MACHINE**、**SOFTWARE**、**Hewlett-Packard**、**OpenView** 和 **OmniBack**，然后选择**通用**。
3. 单击 **InetPort** 打开“编辑字符串”对话框。 在“数值数据”文本框中，输入未用的端口号。 必须在 Common 文件夹的 Parameters 子文件夹中完成相同操作。

4. 在 Windows 控制面板中，打开**管理工具**、**服务**，选择 **Data Protector Inet** 服务，然后通过单击工具栏上的**重新启动**图标重新启动该服务。

在 UNIX 系统中更改默认的 Data Protector IDB 端口和用户帐户

在 UNIX 系统上，安装由 omnisetup.sh 脚本执行且不是交互式的。 在启动安装之前必须先更改文件 /tmp/omni_tmp/DP.dat 中的端口值。

以下端口条目与 IDB 服务相对应：

- Data Protector IDB (hpdp-idb) 服务端口： PGPORT
- Data Protector IDB 连接池程序 (hpdp-idb-cp) 端口： PGCPORT
- Data Protector 应用程序服务器 (hpdp-as) 服务端口： APPSSPORT
- Data Protector 应用程序服务器 (hpdp-as) 管理端口： APPSNATIVEMGTPORT

通过设置变量 PGOSUSER，可以更改运行 IDB 所使用的默认用户帐户。

DP.dat 文件示例：

```
PGPORT=7112
PGCPPORT=7113
PGOSUSER=hpdp
APPSSPORT=7116
APPSNATIVEMGTPORT=7119
```

准备在运行 Windows Server 2008 或 Windows Server 2012 的 Microsoft 服务器群集上安装 Data Protector

要在带 Microsoft 群集服务 (MSCS) 的、运行于 Windows Server 2008 或 Windows Server 2012 操作系统的服务器群集上执行 Data Protector 的群集感知安装，需提前准备该群集。 如果未准备，可能会导致备份本地的 CONFIGURATION 对象(该对象必须在准备期间予以备份，以便进行灾难恢复)会话失败，甚至有可能导致数据丢失。 有关支持的 Data Protector 单元角色与 Windows 操作系统版本群集感知的组合的信息，请参见 https://softwaresupport.softwaregrp.com/ 上的最新支持列表。

先决条件

- 请确保您已使用域用户帐户登录到系统。 域用户帐户必须是本地 Administrators 组的成员。

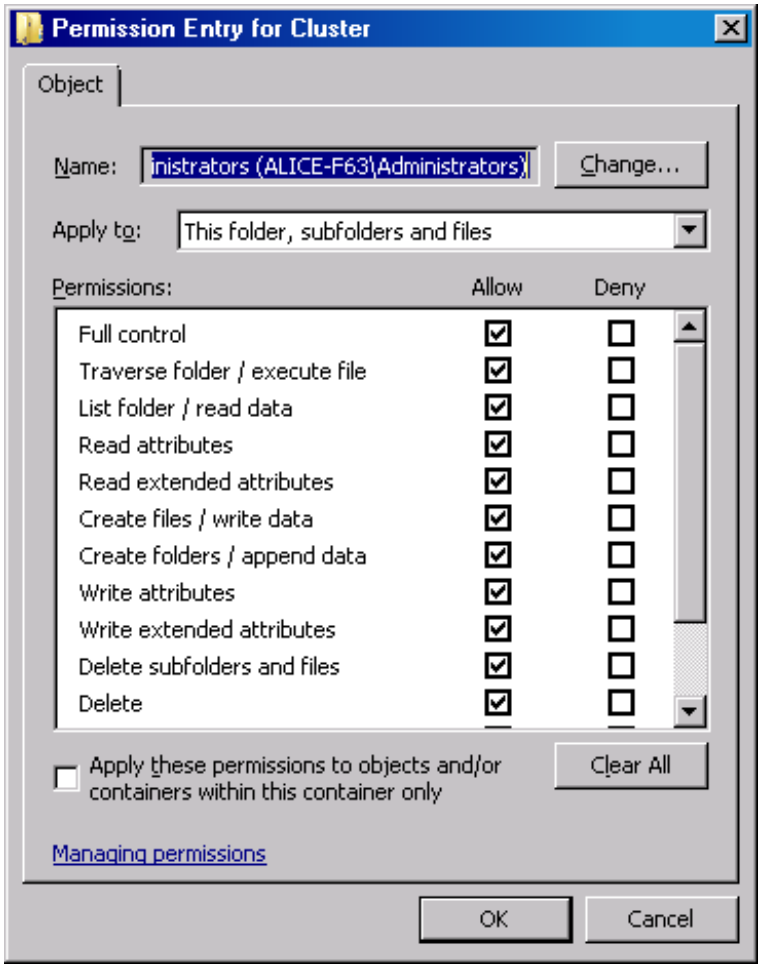
准备过程

若要正确准备群集以安装 Data Protector，请执行以下操作：

1. 在两个群集节点上，启动 Windows 防火墙，并为File and Printer Sharing程序启用例外。
2. 在活动的群集节点中，启动“故障转移群集管理 (Failover Cluster Management)”，并验证 quorum 资源中的见证磁盘是否已联机。 如果该资源已脱机，请将它联机。

   仅在活动的群集节点中执行以下步骤。
3. 如果正在准备尚未配置多数节点集 (MNS) 的群集，请启动 Windows 资源管理器，并将 *WitnessDiskLetter*:\Cluster 文件夹的所有权更改为本地 Administrators 组。 在“群集的高级安全性设置 (Advanced Security Settings for Cluster)”窗口中更改所有权时，请确保已选中**替换子容器及对象的所有者 (Replace owner on subcontainers and objects)** 选项。 在“Windows 安全性 (Windows Security)”对话框中，通过单击**是 (Yes)** 确认建议操作，然后再通过单击**是 (Yes)** 来确认通知。
4. 如果正在准备尚未配置 MNS 的群集，请在 Windows 资源管理器中将 SYSTEM 和本地 Administrators 组对 *WitnessDiskLetter*:\Cluster 文件夹的权限更改为允许完全控制。 验证这两个组的权限设置是否与 适用于 Cluster 文件夹和本地用户组 Administrators 的适当权限 (第 309 页)中显示的设置匹配。

   适用于 Cluster 文件夹和本地用户组 Administrators 的适当权限



5. 如果要准备将承担 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理”中添加 Cluster Access Point 资源。 选择**添加资源 (Add a resource)**，然后单击**1- 客户机**

访问点 (1- Client Access Point) 以启动“新建资源 (New Resource)”向导。

a. 在“客户机访问点 (Client Access Point)”窗格中，在“名称 (Name)”文本框中输入虚拟服务器的网络名称。

b. 在“地址 (Address)”文本框中，输入虚拟服务器的 IP 地址。

6. 如果在准备一个将执行 Data Protector Cell Manager 角色的群集，请在“故障转移群集管理 (Failover Cluster Management)”中，将一个共享文件夹添加到群集。单击**添加共享文件夹 (Add a shared folder)** 以启动“置备共享文件夹 (Provision a Shared Folder)”向导：

a. 在“共享文件夹位置 (Shared Folder Location)”窗格上的“位置 (Location)”文本框中，输入目录路径。请确保所选目录具有足够的可用空间，可以存储在 Data Protector 安装过程中创建的数据。单击**下一步 (Next)**。

b. 在“NTFS 权限 (NTFS Permissions)”、“共享协议 (Share Protocols)”和“SMB 设置 (SMB Settings)”窗格中，保留默认选项值不变。单击**下一步 (Next)**，移到下一个窗格。

c. 在“SMB 权限 (SMB Permissions)”窗格上，选中**管理员具有完全控制权限；所有其他用户和组仅具有读访问和写访问权限 (Administrators have Full Control; all other users and groups have only Read Access and Write Access)** 选项。单击**下一步 (Next)**。

d. 在“DFS 名称空间发布 (DFS Namespace Publishing)”中，保留默认选项值。单击**下一步 (Next)**。

e. 在“检查设置 (Review Settings)”和“创建共享 (Create Share)”窗格中，单击**创建 (Create)**。

在带 Veritas Volume Manager 的 Microsoft 群集服务器上安装 Data Protector

若要在带 Veritas Volume Manager 的 Microsoft Cluster Server (MSCS) 上安装 Data Protector，先遵循在 MSCS 上安装 Data Protector的常规过程。请参见在 Microsoft 群集服务器上安装 Data Protector (第 157 页)。

安装完成后，还需要一些额外的步骤，以使 Data Protector Inet 服务能区别本地磁盘资源，以及使用自己的资源驱动程序，而不是使用 Microsoft 资源驱动程序的群集磁盘资源：

1. 通过在 Cell Manager 上执行 omnisv -maintenance 命令以启动维护模式。
2. 按如下所示定义新的环境变量 OB2CLUSTERDISKTYPES 并使用 Volume Manager Disk Group 作为其值，或者在两个群集节点上设置 omnirc 选项：

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

   要指定更多专有磁盘资源(如 NetRAID4 磁盘)，只需将资源类型名称附加到 OB2CLUSTERDISKTYPES 环境变量值即可：

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
   ```

   有关使用 omnirc 文件选项的详细信息，请参见 *Data Protector 故障诊断指南*。
3. 通过执行 omnisv -maintenance –stop 命令退出维护模式。

准备 NIS 服务器

此过程将使 NIS 服务器能识别 Data ProtectorCell Manager。

将 Data Protector 信息添加到 NIS 服务器

1. 以 root 身份登录到 NIS 服务器。
2. 如果通过 /etc/services 管理 NIS 文件，将下面的行附加到 /etc/services 文件：

   ```
   omni 5565/tcp # Data Protector for Data Protector inet server
   ```

   如果端口 5565 不可用，将其替换成其他端口。 请参见更改默认的 Data Protector Inet 端口 (第 306 页)。

   如果通过 /etc/inetd.conf 管理 NIS 文件，将下面的行附加到 /etc/inetd.conf 文件：

   ```
   #Data Protector
   omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log
   ```
3. 运行下面的命令，使 NIS 服务器读取文件并更新配置。

   ```
   cd /var/yp; make
   ```

> **注意：**
> 在 NIS 环境中，nsswitch.conf 文件定义了各个配置文件的使用顺序。 例如，可以定义是在本地计算机上还是从 NIS 服务器上使用 /etc/inetd.conf 文件。 还可以在该文件中插入语句，声明由 nsswitch.conf 文件来控制保留名称的位置。 请参见手册页获得详细信息。
>
> 如果已经安装了 Data Protector，则您必须准备 NIS 服务器，然后在同时作为 Data Protector 客户机的每台 NIS 客户机上使用 kill -HUP *pid* 命令终止相关进程，以重新启动 inet 服务。

故障排除

- 如果在 NIS 环境中安装 Data Protector 后，Data Protector Inet 服务未启动，请检查 /etc/nsswitch.conf 文件。

  如果找到下面一行：

  ```
  services: nis [NOTFOUND=RETURN] files
  ```

  将该行替换为：

  ```
  services: nis [NOTFOUND=CONTINUE] files
  ```

更改 Cell Manager 名称

安装 Data Protector后，它将使用当前主机名作为 Cell Manager名称。 如果要更改 Cell Manager 的主机名，需要手动更新 Data Protector 文件。

> **重要：**
> 必须更新有关 Cell Manager 名称的客户机信息。 更改 Cell Manager 主机名之前，从单

元中导出客户机。有关相应的过程，请参见从单元导出客户机 (第 172 页)。更改主机名后，将客户机重新导入单元中。

注意：
必须修改使用旧 Cell Manager 名称配置的任何设备和备份规范，以反映正确的名称。

在 UNIX 系统上

在 UNIX Cell Manager 上，执行以下操作：

1. 更改计算机名称或域名。

   注意：
   确保新主机名能够由 DNS、所有成员在两个方向上解析。如果名称解析不起作用，请不要继续此过程。

2. 请执行以下命令：

   ```
   omnisv stop
   ```

   注意：
   确保以下文件中不存在旧主机名的实例：

   ```
   /etc/opt/omni/client/components
   ```

   可以执行以下命令：

   ```
   "grep -rn /etc/opt/omni/client/components -e "<OLD_HOSTNAME_FQDN>""
   ```

3. 更改下列文件中的 Cell Manager 主机名条目：

   ```
   /etc/opt/omni/client/cell_server
   /etc/opt/omni/server/cell/cell_info
   /etc/opt/omni/server/config
   /etc/opt/omni/server/cell/installation_servers
   /etc/opt/omni/server/users/UserList
   ```

4. 通过执行以下命令重新生成证书：

   ```
   # perl -CA /opt/omni/sbin/omnigencert.pl -server_id <NEW_HOSTNAME_FQDN> -
   server_san dns:<short_hostname>,dns:< NEW_HOSTNAME_FQDN > -user_id hpdp -store_
   password <STORE_PASSWORD>
   ```

   注意：
   可以通过执行以下命令来查找密钥库密码：

   ```
   # grep keystorePassword
   /etc/opt/omni/client/components/webservice.properties
   ```

5. 请执行以下命令：

   ```
   omnisv start
   ```

6. 通过执行以下命令更改 IDB 中的 Cell Manager 名称：

   ```
   omnidbutil -change_cell_name
   ```

7. 使用 Data Protector GUI 连接到 Cell Manger，并接受新证书
8. 如果磁带设备连接到 Cell Manager，请导航到**设备和介质**，然后在磁带设备的属性中更改主机名。
9. 对于所配置的文件设备：
   a. 要查看所配置的设备，使用以下命令：

      "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"

   b. 要修改“库”中的主机名，导航到 # omnidownload -library <LIBRARY_NAME> >/tmp/file_lib.txt 并按如下方式编辑 file_lib.txt 文件：

      # omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt

   c. 要修改“设备”中的主机名，导航到 # omnidownload -device <DRIVE_NAME> >/tmp/writer_0.txt 并按如下方式编辑 writer_0.txt 文件：

      # omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt

10. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
11. 更改受到主机名更改影响的其他备份规范。
12. 根据以下目录中的 Cell Server 主机名更改更新 UNIX 或 LINUX 客户机：

    /etc/opt/omni/client/cell_server

13. 根据注册表中的 Cell Server 主机名更改更新 Windows 客户机：

    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer

14. 检查以下配置文件中是否存在旧主机名：

    # grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"

    > **注意：**
    > 可以在以下位置查看旧主机名：
    >
    > /etc/opt/omni/server/dr/p1s -> If the system recovery data has been stored in the past.
    >
    > /etc/opt/omni/server/certificates -> old certificate
    >
    > /etc/opt/omni/client/certificates -> old certificate

15. 检查 IDB 内容并将其导出到以下文件：

    /opt/omni/sbin/omnidbutil -writedb /tmp

    <ENTER>

    > **注意：**
    > dpidb.dat 文件包含内部数据库的主要部分。旧主机名仍保留在如下表格中：
    >
    > dp_frontend_application
    >
    > dp_catalog_object
    >
    > dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)
    >
    > dp_management_session
    >
    > dp_medmng_library (in case the current device name(s) contain the old hostname)

> dp_medmng_media_pool (in case the old pool name(s) contain the old hostname)
>
> dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

而且，dpjce.dat 文件包含作业控制引擎 (JCE) 数据库。 它包含几个对于计划程序至关重要的 URL 条目。 此文件中不得存在旧主机名

如果您在 jce_service_description 表中找到了旧主机名，请按如下方式继续操作：

a. 登录到 hpjce 数据库。

> **注意：**
> 可以在以下文件中查找数据库凭据：
>
> /etc/opt/omni/server/idb/idb.config 文件

```
# grep PGSUPERPASSWORD /etc/opt/omni/server/idb/idb.config
PGSUPERPASSWORD='a2ZudGV4cjBpdTZnMg==';
# export PGPASSWORD=`echo 'a2ZudGV4cjBpdTZnMg==' | base64 -d`
# echo $PGPASSWORD
kfntexr0iu6g2
```

b. 创建连接。 请执行以下操作：

i. 在命令提示符下，导航到 bin 位置 (/opt/omni/idb/bin/)。

ii. 执行以下命令，以使用 hpdp 用户登录 hpjce 数据库：

```
# /opt/omni/idb/bin/psql -h localhost -p 7112 -U hpdp hpdpidb
psql (9.1.9)
Type "help" for help.
```

iii. 通过在 hpjce 数据库中执行以下命令来检查当前内容：

```
hpjce=# select url from jce_service_description;
```

> **注意：**
> 如果您需要更改主机名，请执行以下命令：
>
> ```
> hpjce=# update jce_service_description
> hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
> hpjce=# \q
> ```

在 **Windows** 系统上

在 Windows Cell Manager 上，执行以下操作：

1. 更改计算机名称或域名。

> **注意：**
> 确保新主机名能够由 DNS、所有成员在两个方向上解析。 如果名称解析不起作用，请不要继续此过程。

2. 请执行以下命令：

```
omnisv stop
```

3. 更改以下注册表项中的 Cell Manager 名称：

   ```
   HKEY_LOCAL_
   MACHINE\SOFTWARE\HewlettPackard\OpenView\OmniBackII\Site\CellServer\newnameHKE
   Y_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Packages\newname
   ```

4. 导航到以下文件，以确保不存在旧主机名的任何实例：

   ```
   Data_Protector_program_data\Config\client\components
   ```

   > **注意：**
   > 使用 Windows `find in file` 功能。

5. 更改下列文件中的 Cell Manager 主机名条目：

   Data_Protector_program_data\Config\Server\users\UserList

   Data_Protector_program_data\Config\Server\config

   Data_Protector_program_data\Config\Server\cell\cell_info

   Data_Protector_program_data\Config\Server\cell\installation_servers

6. 从 C:\Program Files\OmniBack\bin 文件夹执行以下命令以重新生成证书：

   ```
   perl omnigencert.pl -server_id <NEW_HOSTNAME> -server_san
   dns:<hostname>,dns:<FQDN> -user_id hpdp -store_password <PASSWORD>
   ```

   > **注意：**
   > 可从以下位置查找密钥库密码：
   >
   > *Data_Protector_program_*
   > *data*\Config\client\components\webservice.properties

7. 请执行以下命令：

   ```
   omnisv start
   ```

8. 通过执行下面的命令以更改 IDB 中的 Cell Manager 名称：

   ```
   omnidbutil -change_cell_name
   ```

9. 使用 Data Protector GUI 连接到 Cell Manger，并接受新证书。
10. 如果磁带设备连接到 Cell Manager，请导航到**设备和介质**，然后在磁带设备的属性中更改主机名。
11. 对于所配置的文件设备：
    a. 要查看所配置的设备，使用以下命令：

       ```
       "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"
       ```

    b. 要修改“库”中的主机名，导航到 "omnidownload -library <LIBRARY_NAME> > c:\temp\file_lib.txt" 并按如下方式编辑 file_lib.txt 文件：

       ```
       omniupload -modify_library <LIBRARY_NAME> -file c:\temp\file_lib.txt
       ```

    c. 要修改“设备”中的主机名，导航到 "omnidownload -device <Device Name> > c:\temp\device.txt" 并按如下方式编辑 device.txt 文件：

       ```
       omniupload -modify_device <Device Name> -file c:\temp\device.txt
       ```

12. 删除 Data Protector IDB 中的备份规范并重新创建一个新规范。
13. 更改受到主机名更改影响的其他备份规范。

14. 根据以下目录中的 Cell Server 主机名更改更新 UNIX 或 LINUX 客户机：

    `/etc/opt/omni/client/cell_server`

15. 根据注册表中的 Cell Server 主机名更改更新 Windows 客户机：

    `HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer`

16. 使用 Windows "find in file" 功能检查以下配置文件，以搜索旧主机名：

    Data_Protector_program_data\Config

    > **注意：**
    > 可以在以下位置查看旧主机名：
    >
    > *Data_Protector_program_data*\Config\Server\dr -> 如果过去存储了系统恢复数据。
    >
    > *Data_Protector_program_data*\Config\Server\certificates -> old certificate
    >
    > *Data_Protector_program_data*\Config\client\certificates -> old certificate

17. 检查 IDB 内容并将其导出到以下文件：

    ```
    omnidbutil -writedb e:\idb_export
    <ENTER>
    ```

    > **注意：**
    > dpidb.dat 文件包含内部数据库的主要部分。 旧主机名仍保留在如下表格中：
    >
    > dp_frontend_application
    >
    > dp_catalog_object
    >
    > dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)
    >
    > dp_management_session
    >
    > dp_medmng_library (in case the current device name(s) contain the old hostname)
    >
    > dp_medmng_media_pool (in case the old pool name(s) contain the old hostname)
    >
    > dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)

    而且，dpjce.dat 文件包含作业控制引擎 (JCE) 数据库。 它包含几个对于计划程序至关重要的 URL 条目。 此文件中不得存在旧主机名。

    如果您在 jce_service_description 表中找到了旧主机名，请按如下方式继续操作：

    a. 登录到 hpjce 数据库。

       > **注意：**
       > 可以在 *Data_Protector_program_data*\Config\Server\idb\idb.config 文件中查找数据库凭据。 可以使用以下链接解码 PGSUPERPASSWORD：
       >
       > https://www.base64decode.org

    b. 创建连接。 请执行以下操作：

i. 在命令提示符下，导航到 bin 位置 (C:\Program Files\OmniBack\idb\bin)。
ii. 执行以下命令，以使用 hpdp 用户登录 hpjce 数据库：

```
.\psql -h localhost -p 7112 -d hpjce -U hpdp <Enter the decoded password>
```

iii. 通过在 hpjce 数据库中执行以下命令来检查当前内容：

```
hpjce=# select url from jce_service_description;
```

> **注意：**
> 如果您需要更改主机名，请执行以下命令：
>
> ```
> hpjce=# update jce_service_description
> hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
> hpjce=# \q
> ```

更改作业控制引擎 (JCE) 数据库中的主机名

在 UNIX 系统中

要使用 PGADMIN3 更改 JCE 数据库中的主机名，请执行以下步骤：

1. 导航到 /var/opt/omni/server/db80/pg/pg_hba.conf 文件。
2. 将 host all all 127..0.0.1/32 md5 更改为 host all all 10.17.0.0/16 md5。
   (或)
   将 host all all 127..0.0.1/32 md5 更改为仅连接到特定主机 (host all all 10.17.16.121/32 md5)。
3. 重新加载 pg config 文件并执行以下命令：

   ```
   su hpdp
   /opt/omni/idb/bin/pg_ctl reload -D /var/opt/omni/server/db80/pg
   ```
4. 连接到 pgAdmin3。

在 Windows 系统中

要使用 PGADMIN3 通过命令行更改 JCE 数据库中的主机名，请执行以下步骤：

1. 请执行以下命令：

   ```
   omnidbutil –set_passwd hpdp
   ```
2. 设置密码。
3. 导航到 C:\Program Files\OmniBack\idb\bin 文件夹并运行 **pgadmin3.exe**。
   pgAdmin3 程序将启动。
4. 单击  插件以添加服务器。
   此时将显示“注册新服务器”窗口。

5. 在“注册新服务器”窗口中，执行以下操作：
   a. 在“名称”字段中，输入 local 或按照自己的要求输入。
      例如，输入 jce_service_description。
   b. 在“主机”字段中，输入 localhost。
   c. 在“端口”字段中，输入 7112。
   d. 将“服务”字段留空。
   e. 在“维护数据库”字段中，选择 hpdpidb。
   f. 在“用户名”字段中，输入 hpdp。
   g. 在“密码”字段中，输入在步骤 1 中使用 omnidbutil –set_passwd hpdp 命令设置的密码。
6. 单击**确定**。
7. 在对象浏览器区域中，展开“数据库 > hpjce > 架构 > hpjce_app > 表”以展开已添加的服务器。
   例如：您可能会看到 jce_service_description 表名称。 单击 jce_service_description。
8. 选择工具栏中的 SQL 按钮。
   使用以下命令可显示 SQL 编辑器：
   ```
   UPDATE jce_service_description
   SET url=replace (url, ‘old_hostname’, ‘new_hostname’);
   ```
   例如，可以将 testHostname.1 用作 old_hostname 并将 testHostname 用作 new_hostname。 然后单击“播放”按钮执行此命令。
   在“数据输出”选项卡中，您会看到一条消息，指明已更改的行的数量。

使用 CLI

要在不使用 PGADMIN3 的情况下更改 JCE 数据库中的主机名，请执行以下步骤：

1. 执行以下命令：
   在 Windows 系统中：
   ```
   C:\Program Files\OmniBack\idb\psql --port=7112 -U hpdp -d hpjce -h localhost
   ```
   在 UNIX 系统中：
   ```
   /opt/omni/idb/bin/psql --port=7112 -U hpdp -d hpjce -h localhost
   ```
2. 执行以下命令：
   ```
   hpjce=# select url from jce_service_description;
   hpjce=# update jce_service_description
   hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
   hpjce=# \q
   ```

在 Windows Cell Manager 上运行大型备份会话

要在 Windows Cell Manager 上运行大量备份会话，您应在 Windows 注册表中调整桌面堆限制。 桌面堆由以下注册表项控制：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows

此注册表项的默认值如下所示：

%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

Data Protector 受 SharedSection 参数影响，该参数包括以下值：

- 1024：所有桌面通用的共享堆大小。要避免出现与桌面堆耗尽相关的问题，不得更改此值。
- 20480：与交互式窗口站关联的每个桌面的桌面堆大小。
- 768：与非交互式窗口站关联的每个桌面的桌面堆大小。

应将 SharedSection 参数的第三个值 (768) 设置为 20480。修改的 Windows 注册表项值将如下所示：

%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,20480 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

> **注意：**
> 请勿设置非常高的值，因为值以千字节为单位。

设置新值后，必须重新启动系统。

附录 C： 设备和介质相关的任务

本附录提供有关超出本指南范围的任务的一些附加 Data Protector 特定信息。 这些任务包括设备驱动程序配置、管理 SCSI 机械手和维护 SCSI 环境等。

在 Windows 系统上使用磁带和机械手驱动程序

Data Protector 支持默认情况下为连接到 Windows 系统的已启用磁带驱动器加载的本机磁带驱动程序。 Data Protector 不支持为介质更换器(机械手)设备加载的 Windows 本机驱动程序。

在下面的示例中，4mm DDS 磁带设备连接到 Windows 系统。 如果 4mm DDS 磁带设备连接到 Windows 系统并配置用于 Data Protector，则需要禁用为介质更换器设备加载的本机驱动程序。本节将介绍相关步骤。

磁带驱动程序

如果设备列在硬件兼容性列表 (HCL) 中，则 Windows 中通常带有驱动程序。 HCL 是 Windows 支持的设备列表，可在以下站点找到：

http://www.microsoft.com/whdc/hcl/default.mspx

计算机一启动，设备驱动程序就会自动为所有启用的设备加载。 您不需要单独加载本机磁带驱动程序，但可以更新它。

更新或更换 Windows 系统上的本机磁带驱动程序

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在**管理工具**窗口中，双击**计算机管理**。 单击**设备管理器 (Device Manager)**。
3. 展开磁带驱动器。 要检查当前为设备加载了哪个驱动程序，请右键单击磁带驱动器，然后单击**属性 (Properties)**。
4. 选择**驱动程序**选项卡并单击**更新驱动程序**。 然后在向导中可以指定是要更新当前安装的本机磁带驱动程序还是要将其替换为其他驱动程序。
5. 重新启动系统以应用更改。

> **重要：**
> 如果已为 Data Protector 配置了不使用本机磁带驱动程序的设备，则必须对引用此特定磁带驱动器的所有已配置的 Data Protector 备份设备重命名设备文件(例如，从 `scsi1:0:4:0` 重命名为 tape3:0:4:0)。 `tape3:0:4:0)`.
>
> 有关详细信息，请参见在 Windows 系统上创建设备文件(SCSI 地址) (第 322 页)。

机械手驱动程序

在 Windows 中，将为启用的磁带库自动加载机械手驱动程序。 要在 Data Protector 中使用带库机械手，必须禁用各个驱动程序。

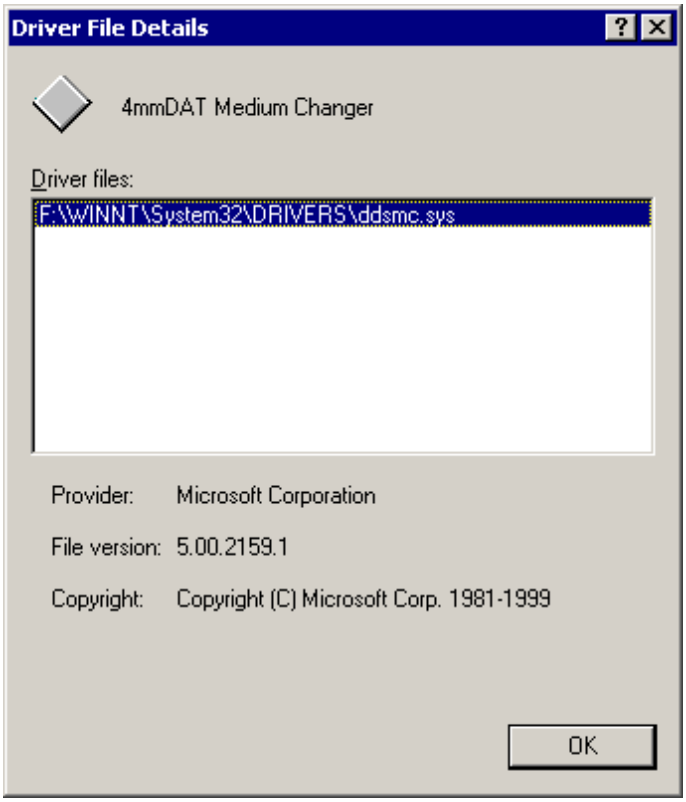
下面的示例中是使用 4mm DDS 磁带的 1557A 磁带库。

在 **Windows** 系统上禁用自动加载的机械手驱动程序 (ddsmc.sys)

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在“管理工具”窗口中，双击**计算机管理**。单击**设备管理器 (Device Manager)**。
3. 在“设备管理器 (Device Manager)”窗口的“结果区域 (Results Area)”中，展开介质更换器。
4. 要检查当前加载了哪个驱动程序，请右键单击 **4mm DDS 介质更换器 (4mm DDS Medium Changer)**，然后单击**属性 (Properties)**。

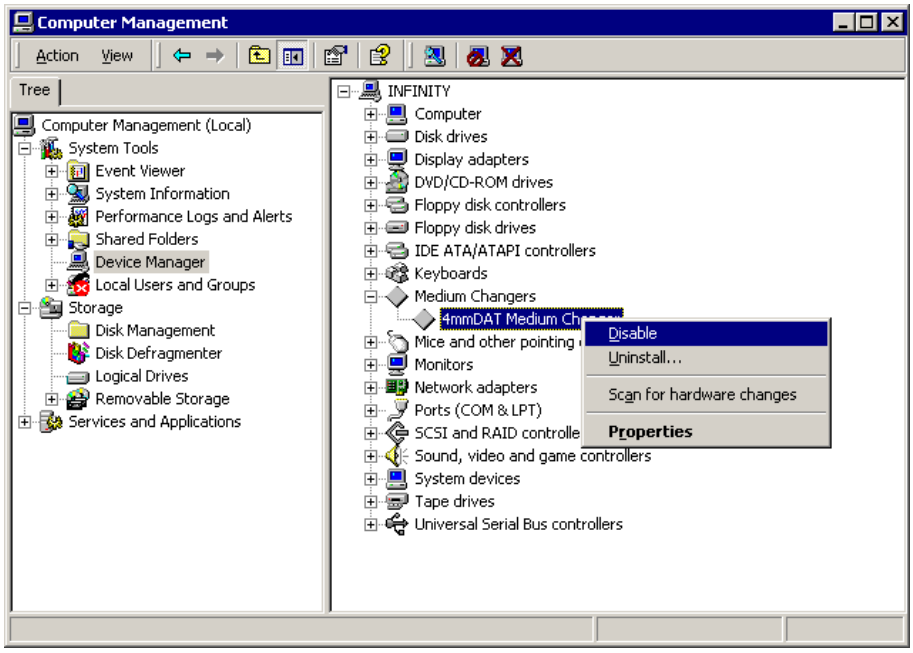
   选择**驱动程序 (Driver)** 选项卡并单击**驱动程序详细信息 (Driver details)**。此时，将显示以下窗口：

   介质更换器属性



   要禁用本机机械手驱动程序，请右键单击 **4mm DDS 介质更换器**，然后选择**禁用**。

   禁用机械手驱动程序



5. 重新启动系统以应用更改。 现在可以使用 Data Protector 配置机械手了。

在 Windows 系统上创建设备文件(SCSI 地址)

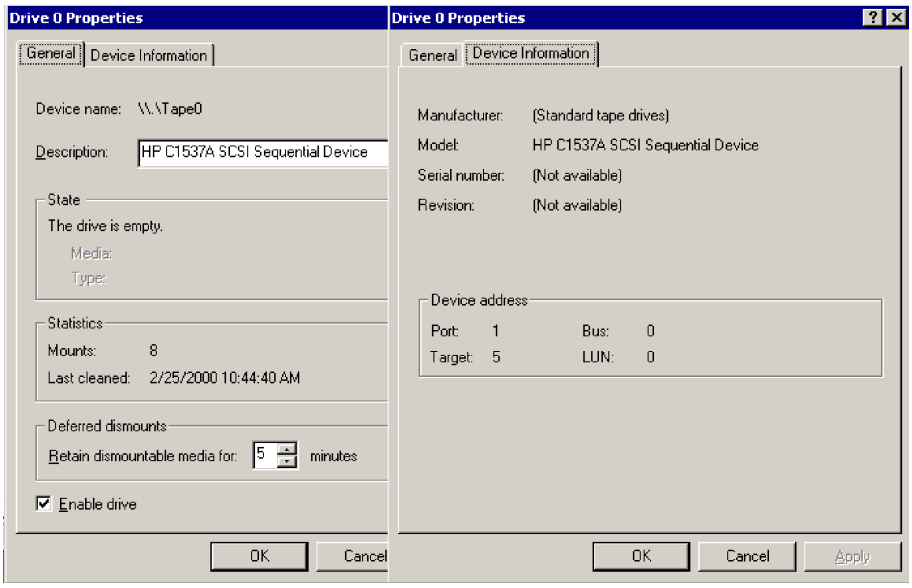
磁带设备文件名语法取决于为磁带驱动器加载 (tapeN:B:T:L) 还是卸载 (scsiP:B:T:L) 了本机磁带驱动程序。

使用本机磁带驱动程序的 Windows

要为连接到使用本机磁带驱动程序的 Windows 系统的磁带驱动器创建设备文件，请执行以下步骤：

1. 在 Windows 控制面板中，双击**管理工具 (Administrative Tools)**。
2. 在“管理工具”窗口中，双击**计算机管理**。 展开可移动存储，然后展开物理位置。 右键单击磁带驱动器并选择**属性 (Properties)**。
3. 如果加载了本机磁带驱动程序，则设备文件名会显示在“常规”属性页中。 否则，可在“设备信息 (Device Information)”属性页中找到相关信息。 请参见 磁带驱动器属性 (第 322 页)。

磁带驱动器属性



磁带驱动器属性 (第 322 页)中为磁带驱动器创建的文件名如下所示：

使用了本机磁带驱动程序	`Tape0 or Tape0:0:5:0`
未使用本机磁带驱动程序	`scsii1:0:5:0`

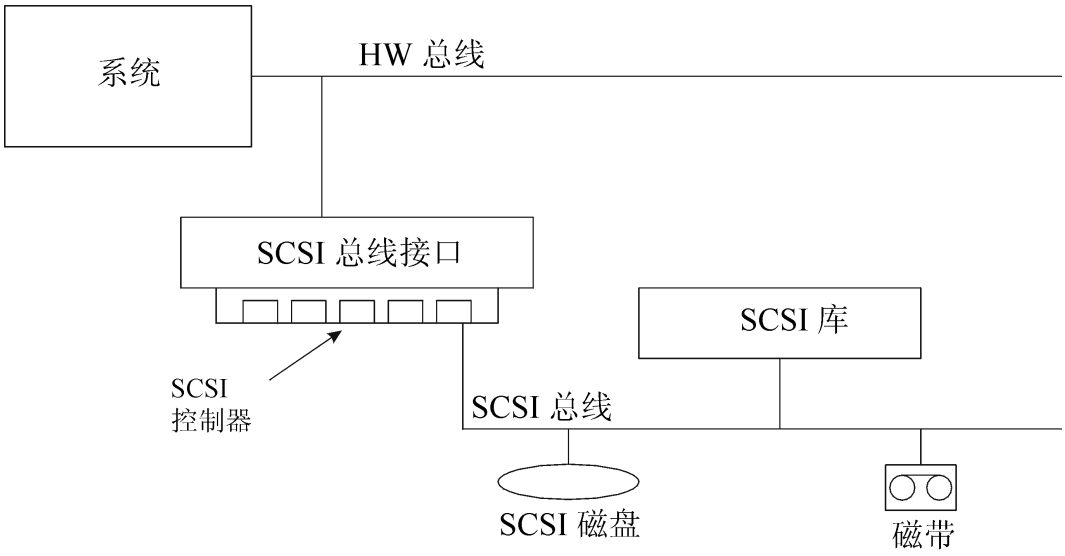
磁光设备

如果将磁光设备连接到 Windows 系统，则在重新启动系统后会给设备分配一个驱动器字母。稍后会在创建设备文件时使用该驱动器字母。例如，`E:` 是为分配了驱动器盘符 `E` 的磁光盘驱动器创建的设备文件。

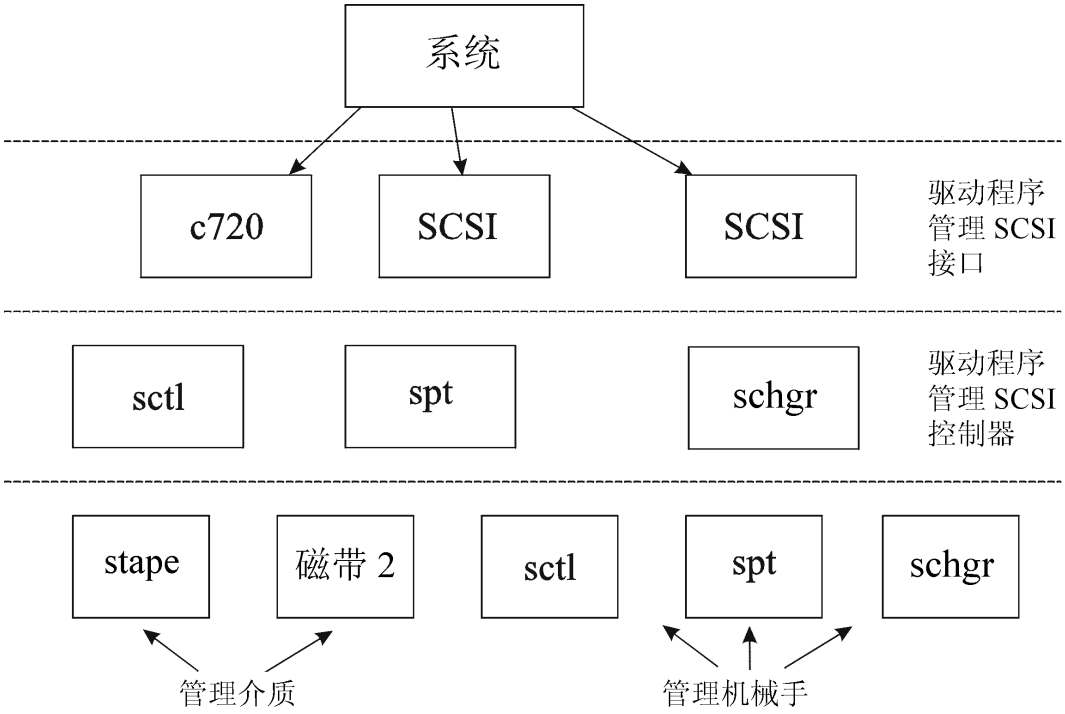
在 HP-UX 系统上配置 SCSI 机械手

在 HP-UX 系统上，SCSI Pass-Through 驱动程序用于管理磁带库设备(例如 12000e)的 SCSI 控制器*和*控制设备(也称为机械手或选择器)。带库中的控制设备负责将介质装入驱动器/从驱动器中取出介质以及将介质导入这种设备/从这种设备导出介质。

SCSI 控制的设备



管理设备



使用的 SCSI 机械手驱动程序的类型取决于硬件。配备 GSC/HSC 或 PCI 总线的系统具有名为 schgr 的 SCSI 自动更换器驱动程序，配备 EISA 总线的系统具有名为 sctl 的 SCSI Pass-Through 驱动程序，它已置于内核中。但是，用于配备 NIO 总线的服务器的 SCSI Pass-Through 驱动程序名为 spt。默认情况下，它安装在系统上而不置于内核中。

如果 SCSI 机械手驱动程序尚未链接到当前内核，则必须手动添加并将其分配给连接的磁带库的机械手。

下面的步骤说明了如何*手动*将 SCSI 机械手驱动程序添加到内核以及如何手动重建一个新的内核。

> **提示：**
> 在 HP-UX 平台上，还可以使用 *System Administration Manager (SAM)* 实用程序构建内核。 请参见安装 HP-UX 客户机 (第 64 页)。

使用 `/opt/omni/sbin/ioscan -f` 命令，检查是否已将 SCSI 机械手驱动程序分配给要配置的库。

SCSI Pass-Through 驱动程序 (sctl) 的状态

```
root@superhik$ ioscan -f
Class       I  H/W Path    Driver      S/W State H/W Type  Description
=============================================================================
bc          0               root        CLAIMED   BUS_NEXUS
bc          1  8            ccio        CLAIMED   BUS_NEXUS I/O Adapter
unknown    -1  8/0                      CLAIMED   DEVICE    GSC-to-PCI Bus Bridge
ext_bus     0  8/12          c720        CLAIMED   INTERFACE GSC Fast/Wide SCSI Interfac
e
target      0  8/12.0        tgt         CLAIMED   DEVICE
disk        0  8/12.0.0      sdisk       CLAIMED   DEVICE    SEAGATE ST19171W
target      1  8/12.1        tgt         CLAIMED   DEVICE
tape        5  8/12.1.0      stape       CLAIMED   DEVICE    QUANTUM DLT7000
target      2  8/12.2        tgt         CLAIMED   DEVICE
ctl         0  8/12.2.0      sctl        CLAIMED   DEVICE    EXABYTE EXB-210
target      3  8/12.7        tgt         CLAIMED   DEVICE
ctl         0  8/12.7.0      sctl        CLAIMED   DEVICE    Initiator
ba          0  8/16          bus_adapter CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus     2  8/16/0        CentIf      CLAIMED   INTERFACE Built-in Parallel Interface
audio       0  8/16/1        audio       CLAIMED   INTERFACE Built-in Audio
tty         0  8/16/4        asio0       CLAIMED   INTERFACE Built-in RS-232C
ext_bus     1  8/16/5        c720        CLAIMED   INTERFACE Built-in SCSI
target      4  8/16/5.2      tgt         CLAIMED   DEVICE
disk        2  8/16/5.2.0    sdisk       CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5401TA
target      7  8/16/5.3      tgt         NO_HW     DEVICE
tape        3  8/16/5.3.0    stape       NO_HW     DEVICE    SONY     SDX-300C
target      6  8/16/5.5      tgt         NO_HW     DEVICE
tape        0  8/16/5.5.0    stape       NO_HW     DEVICE    SONY     SDX-300C
target      5  8/16/5.7      tgt         CLAIMED   DEVICE
```

在 SCSI Pass-Through 驱动程序 (sctl) 的状态 (第 325 页)中，可以看到分配给 Exabyte 磁带设备的控制设备的 `sctl` SCSI Pass-Through 驱动程序。 相应的硬件路径 (H/W Path) 是 `8/12.2.0`。 (SCSI=2，LUN=0)

此外，还有一个磁带驱动器连接到同一 SCSI 总线，但是控制该磁带驱动器的驱动程序是 `stape`。 相应的硬件路径 (H/W Path) 是 `8/12.1.0`。 (SCSI=0，LUN=0)

> **重要：**
> SCSI 地址 7 始终由 SCSI 控制器使用，虽然相应的行可能不显示在 `ioscan -f` 命令的输出中。 在本示例中，控制器由 `sctl` 管理。

SCSI Pass-Through 驱动程序 (spt) 的状态

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
#
```

在 SCSI Pass-Through 驱动程序 (spt) 的状态 (第 325 页) 中，可以看到一个已连接的磁带设备，其机械手由 spt SCSI Pass-Through 驱动程序控制。该特定设备是 12000e 带库设备，使用 SCSI 地址 4 并通过 H/W Path 52 连接到 SCSI 总线。相应的硬件路径是 52.4.1。机械手正确分配给 spt SCSI Pass-Through 驱动程序。

如果 sctl、spt 或 schgr 驱动程序没有分配给机械手，则必须将机械手的 H/W Path 添加到 system 文件的驱动程序声明中并重建内核。请执行以下步骤。

以下步骤说明如何*手动*将 SCSI 机械手驱动程序添加到内核，将其分配给机械手，然后手动重建新的内核：

1. 以 *root* 用户身份登录并切换到 build 目录：

   ```
   cd /stand/build
   ```

2. 从现有内核创建新系统文件：

   ```
   /usr/lbin/sysadm/system_prep -s system
   ```

3. 检查哪个 SCSI 机械手驱动程序已置于当前内核中。在 /stand 目录中，执行以下命令：

   ```
   grep SCSIRoboticDriver system
   ```

   其中 *SCSIRoboticDriver* 可以是 spt、sctl 或 schgr。如果该驱动程序已置于当前内核中，则系统将显示相应的行。

4. 使用编辑器将驱动程序声明：

   ```
   driver H/W Path spt
   ```

   附加到 /stand/build/system 文件，其中 *H/W Path* 是设备的完整硬件路径。

   对于上例中的 12000e 磁带库，请输入：

   ```
   driver 52.4.1 spt
   ```

   对于连接到同一系统的多个带库，必须使用相应的硬件路径为每个带库机械手添加一个驱动程序行。

   配置 schgr 驱动程序时，请将以下行附加到驱动程序声明中：

   ```
   schgr
   ```

5. 输入 mk_kernel -s./system 命令以构建新内核。

6. 使用其他名称保存原始的旧系统文件，并将新系统文件改为原始名称，这样它便成为当前系统文件：

   ```
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
   ```

7. 使用其他名称保存旧内核，并将新内核改为原始名称，这样它便成为当前内核：

   ```
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
   ```

8. 输入以下命令从新内核重新启动系统：

   ```
   shutdown -r 0
   ```

9. 重新启动系统后，使用 /usr/sbin/ioscan -f 命令验证已作的更改。

在 HP-UX 系统上创建设备文件

先决条件

创建设备文件前，备份设备应已连接到系统。 使用 /usr/sbin/ioscan -f 命令，检查设备是否正常连接。 使用 /usr/sbin/infs -e 命令，自动为某些备份设备创建设备文件。

如果在系统初始化(启动进程)期间或运行 infs -e 命令后没有创建对应于特定备份设备的设备文件，则必须手动创建这些设备文件。 管理带库控制设备(带库机械手)所需的设备文件就需要手动创建。

我们来看一个为连接到 HP-UX 系统的 12000e 带库设备的机械手创建设备文件的示例。 磁带驱动器的设备文件已在系统重新启动后自动创建，而控制设备的设备文件必须手动创建。

在 SCSI Pass-Through 驱动程序 (spt) 的状态 (第 325 页) 中，您可以查看选定 HP-UX 系统上 ioscan -f 命令的输出。

已连接设备的列表

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
# 
```

SCSI 总线接口由 scsi1 系统驱动程序控制。 这是 SCSI NIO 接口。 要访问 SCSI NIO 总线上的带库机械手，必须使用已安装并分配给使用硬件路径 52.4.1 的 12000e 磁带设备的机械手的 spt SCSI Pass-Through 驱动程序。

> **注意：**
> 如果不使用基于 SCSI NIO 的总线接口，则不需要 spt 驱动程序而使用 sctl 驱动程序。

要创建设备文件，需要知道 SCSI Pass-Through 驱动程序的*主号字符*和*次号字符*，它与使用的 SCSI Pass-Through 驱动程序无关。

要获取属于 spt, 的*主号字符*，请运行系统命令：

```
lsdev -d spt
```

在本示例中(请参见已连接设备的列表 (第 327 页))，命令报告*主号字符* 75.

要获取属于 sctl 的*主号字符*，请运行系统命令：

```
lsdev -d sctl
```

在本示例中，命令报告*主号字符* 203.

无论使用哪种 SCSI Pass-Through 驱动程序，*次号字符*都具有以下格式：

```
0xIITL00
```

II -> ioscan -f 输出报告的 SCSI 总线接口(不是设备)的*实例号*位于第二列中，标签为 I。在本示例中，实例号是 0，所以必须输入两位十六进制数 00。

T -> 库机械手的 SCSI 地址。 在本示例中，SCSI 地址是 4，所以必须输入 4。

L -> 库机械手的 LUN 号。 在本示例中，LUN 号是 1，所以必须输入 1。

00 -> 两位十六进制的零。

创建设备文件

以下命令用于创建设备文件：

```
mknod /dev/spt/devfile_name c Major # Minor #
```

通常 spt 的设备文件位于 /dev/spt 或 /dev/scsi 目录中。 在这种情况下，我们将控制设备文件命名为 /dev/spt/SS12000e。

因此，在 /dev/spt 目录中创建名为 SS12000e 的设备文件的完整命令是：

```
mknod /dev/spt/SS12000e c 75 0x004100
```

如果为 sctl 创建名为 SS12000e 且位于 /dev/scsi 目录的设备文件，则完整命令是：

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

设置 SCSI 控制器的参数

通过 Data Protector 可更改设备的块大小，这可能需要在某些 SCSI 控制器上进行附加配置。

在 Windows 系统上，通过编辑 Adaptec SCSI 控制器及某些使用 Adaptec 芯片组的控制器的注册表值来设置 SCSI 控制器的参数：

1. 设置以下注册表值：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aic78xx\Parameters\Device0\MaximumSGList
2. 输入包含 4 kB 块数量的 DWORD 值再加一。

   MaximumSGList = (OBBlockSize in kB / 4) + 1

   例如，要启用 260 kB 的块大小，MaximumSGList 至少必须为 (260 / 4) + 1 = 66。
3. 重新启动系统。

> **注意：**
> 该注册表值设置块大小的上限。 设备的实际块大小必须使用设备配置的 Data Protector GUI 进行配置。

在 HP-UX 系统上查找未使用的 SCSI 地址

连接到 HP-UX 系统的备份设备是通过必须对每个物理设备都存在的设备文件来访问和控制的。 必须先找出仍未使用、对新设备可用的 SCSI 地址(端口)，才能创建设备文件。

在 HP-UX 系统上，/usr/sbin/ioscan -f 系统命令用于显示已占用的 SCSI 地址的列表。 因此，/usr/sbin/ioscan -f 命令的输出中未列出的地址就是仍未使用的地址。

HP-UX 系统上 ioscan -f 命令的输出 (第 329 页)中显示了在 HP-UX 11.x 系统上运行 /usr/sbin/ioscan -f 命令后的输出。

HP-UX 系统上 ioscan -f 命令的输出

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
============================================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
#
```

只有第三列 (H/W Path) 和第五列 (S/W State) 与确定可用的 SCSI 地址相关。 (H/W Path) 分解后的格式如下所示：

SCSI_bus_H/W_Path. SCSI_address. LUN_number

在本示例中，只有一个 SCSI 总线，使用 H/W Path 52。 在该总线上，可以使用 SCSI 地址 0 和 3，因为它们没有显示在列表中。

在 HP-UX 系统上 ioscan -f 命令的输出 (第 329 页)中，可以看到选定 SCSI 总线上已被占用的 SCSI 地址：

- SCSI 地址 1 被 SCSI 磁盘占用
- SCSI 地址 2 被 CD-ROM 占用
- SCSI 地址 4，LUN 0，被磁带驱动器占用
- SCSI 地址 4，LUN 1，被磁带库机械手占用
- SCSI 地址 5 被 SCSI 磁盘占用
- SCSI 地址 6 被 SCSI 磁盘占用
- SCSI 地址 7 被 SCSI 控制器占用

> **注意：**
> 虽然默认情况下 SCSI 地址 7 被 SCSI 控制器占用，但是它*没有*列出。

所有设备的 S/W State 值都设置为 CLAIMED ，且 H/W Type 值都设置为 H/W DEVICE，这说明设备当前已连接。 如果 S/W State 列中有 UNCLAIMED 值或 H/W Type 列中有 NO-HW 值，则说明系统无法访问该设备。

SCSI 地址 4 被磁带库占用，其中磁带驱动器在 LUN 0，机械手在 LUN 1。 驱动器由 tape2 驱动程序控制，机械手由 spt SCSI 直通驱动程序控制。 通过描述可以看到，该设备是 12000e 带库；很容易就在 SCSI 带库中认出它，因为它对磁带驱动器和机械手使用相同的 SCSI 地址，但是使用不同的 LUN。

整个 SCSI 总线由 scsi1 接口模块控制。

在 Solaris 系统上查找未使用的 SCSI 目标 ID

连接到 Solaris 系统的备份设备是通过设备文件访问和控制的。 该设备文件是当备份设备已连接且客户机系统和备份设备通电时，由 Solaris 操作系统在目录 /dev/rmt 中自动创建的。

但是，在连接备份设备前，必须检查可用的 SCSI 地址并将备份设备的地址设置为尚未分配的地址。

在 Solaris 系统上列出可用的 SCSI 地址：

1. 按**停止**和 **A** 停止系统。
2. 在 ok 提示符中运行 probe-scsi-all 命令：

   ```
   probe-scsi-all
   ```

   系统可能会要求您在执行 probe-scsi-all 命令之前启动 reset-all 命令。
3. 要恢复正常操作，请在 ok 提示符中输入 go：

   ```
   go
   ```

在列出可用地址并选择一个用于备份设备后，必须先更新相关的配置文件，然后再连接和启动设备。 请参见下一节获取更新配置文件的相关说明。

在 Solaris 系统上更新设备和驱动程序配置

更新配置文件

以下配置文件用于设备和驱动程序配置。必须先检查(必要时编辑)它们，然后才能使用连接的设备：

- st.conf
- sst.conf

st.conf: 所有设备

在每个连接了磁带设备的 Data Protector Solaris 客户机上，都需要此文件。对于连接到该客户机的每个备份设备，它必须包含相应的设备信息和一个或多个 SCSI 地址。对于单驱动器设备，需要单个 SCSI 条目；对于多驱动器库设备，需要多个 SCSI 条目。

1. 在客户机上检查未使用的 SCSI 地址(如上一节所述)，并为要连接的设备选择一个地址。
2. 在备份设备上设置选择的 SCSI 地址。
3. 关闭客户机系统。
4. 连接备份设备。
5. 首先打开设备，然后再打开客户机系统。
6. 按 Stop 和 A 停止系统。
7. 在 ok 提示符中输入 probe-scsi-all 命令：

   probe-scsi-all

   这会提供连接的 SCSI 设备的相关信息，包括新连接的备份设备的正确设备 ID 字符串。
8. 返回到正常运行：

   go
9. 编辑 /kernel/drv/st.conf 文件。Solaris st(SCSI 磁带)驱动程序使用该文件。它包含 Solaris 正式支持的设备列表以及适用于第三方设备的配置条目集。如果使用支持的设备，则应该可以连接和使用设备而无需进一步配置。否则，应将以下类型的条目添加到 st.conf 中：
   - 磁带配置列表条目(和磁带数据变量定义)。文件中有带注释的示例条目。如果适用，您可以使用其中一个条目，或进行修改以满足您的需要。

     该条目必须位于文件中第一个 name= 条目之前，且格式要求如下：

     tape-config-list= "*Tape unit*", "*Tape reference name*", "*Tape data*";

     其中：

Tape unit	磁带设备的供应商和产品 ID 字符串。必须按照设备制造商文档所述正确指定该条目。
Tape	您选择的名称，系统将通过该名称识别磁带设备。您提供的名称不

reference name	会更改磁带产品 ID，但是系统启动后，该参考名称将显示在系统识别的外围设备列表中。
Tape data	参考一系列其他磁带设备配置项目的变量。 也必须按照设备制造商文档所述指定该变量定义。

例如：

```
tape-config-list= “Quantum DLT4000”, “Quantum DLT4000”, “DLT-data”;
DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

第二个参数 0x38 将 DLTtape 磁带类型指定为“其他 SCSI 驱动器”。 此处指定的值应在 /usr/include/sys/mtio.h 中定义。

> **注意：**
> 请确保 tape-config-list 中的最后一个条目以分号(;)结尾。

- 对于多驱动器设备，目标条目如下：

  ```
  name="st" class="scsi"
  target=X lun=Y;
  ```

  其中：

X	是分配给数据驱动器(或机械手装置)的 SCSI 端口。
Y	是逻辑单元值。

  例如：

  ```
  name="st" class="scsi"
   target=1 lun=0;
  name="st" class="scsi"
   target=2 lun=0
  ```

  通常在 st.conf 中仅对驱动器要求目标条目，对机械手装置不要求，它在其他目标上。 这些设备的条目通常在 sst.conf 文件中提供(请参见下文)。 但是，某些设备(例如 24x6)将机械手装置视为与其他驱动器类似。 在这种情况下，需要具有相同目标的两个条目(一个用于驱动器，一个用于机械手)，但是这两个条目必须具有不同的 LUN。

  例如：

  ```
  name="st" class="scsi"
   target=1 lun=0;
  name="st" class="scsi"
  target=1 lun=1
  ```

sst.conf: 库设备

在每个连接了多驱动器库设备的 Data Protector Solaris 客户机上，都需要此文件。 一般来说，它需要每个连接到客户机的带库设备机械手装置的 SCSI 地址条目(也有例外，例如上一节中提到的 24x6)。

1. 将 sst 驱动程序(模块)和配置文件 sst.conf 复制到要求的目录：
   - 对于 32 位操作系统：

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

   - 对于 64 位操作系统：

     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

2. 编辑 sst.conf 文件并添加以下条目：

   ```
   name="sst" class="scsi" target=X lun=Y;
   ```

   其中：

X	是机械手装置的 SCSI 地址。
Y	是逻辑单元。

   例如：

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

3. 将驱动程序添加到 Solaris 内核：

   ```
   add_drv sst
   ```

创建和检查设备文件

设置配置文件和安装驱动程序后，可按以下步骤创建新的设备文件：

1. 从 /dev/rmt 目录中删除所有现有的设备文件：

   ```
   cd /dev/rmt rm *
   ```

2. 输入以下命令以关闭系统：

   ```
   shutdown -i0 -g0
   ```

3. 重新启动系统：

   ```
   boot -rv
   ```

   boot 命令中的 r 开关启用内核编译并包括创建用于与磁带设备通信的设备特殊文件。 v 开关启用系统启动文件的详细模式显示。 启用详细模式后，系统应通过显示您在 /devices 目录配置引导阶段选择的 *Tape reference name* 字符串来表明设备已连接。

4. 请输入以下命令以验证安装：

   ```
   mt -t /dev/rmt/0 status
   ```

   该命令的输出取决于配置的驱动器。 它与以下内容类似：

   ```
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention residual= 0 retries=
   0 file no= 0 block no= 0
   ```

5. 系统重新启动完成后，可以使用命令 ls -all. 检查已创建的设备文件。对于带库设备，该命令的输出可能是：

/dev/rmt/0hb	适用于第一个磁带驱动器
/dev/rmt/1hb	适用于第二个磁带驱动器
/dev/rsst6	适用于机械手驱动器

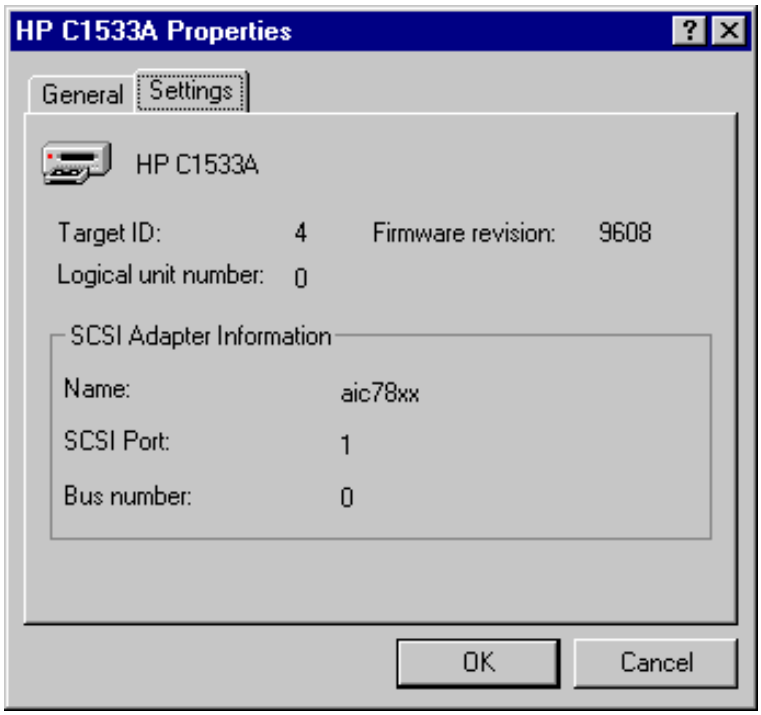
在 Windows 系统上查找未使用的 SCSI 目标 ID

在 Windows 系统上确定未使用的 SCSI 目标 ID(SCSI 地址)

1. 在 Windows 控制面板中，单击 **SCSI 适配器 (SCSI Adapters)**。
2. 对于列表中每个连接到 SCSI 适配器的设备，检查其属性。双击设备名称，然后单击 **设置 (Settings)** 打开属性页。请参见 设备设置 (第 334 页)。

   记住分配给设备的 SCSI Target IDs 和 LUNs(Logical Unit Numbers)。这样可以找出哪些 SCSI Target ID 和 LUNs 已被占用。

设备设置



在 330fx 带库上设置 SCSI ID

为机械手和驱动器选择未使用的 SCSI ID 后，可以使用带库设备的控制面板对它们进行检查和配置。

示例

如果有带库模型 330fx，则可以按如下步骤找到配置的 SCSI ID：

1. 从 READY 状态中，按**下一步**，随后将显示 ADMIN*。
2. 按 **Enter**，此时将提示您输入密码。请输入密码。
3. TEST* 将出现，按**下一步**，直至显示 SCSI IDs * 为止。
4. 按 **Enter**。此时会出现 VIEW IDs*。
5. 按 **Enter**。此时会出现 JKBX ID 6 LUN 0。
6. 按**下一步**。此时会出现 DRV 1 ID 5 LUN 0。
7. 按**下一步**。将显示 DRV 2 ID 4 LUN 0 等。

按几次“取消”可返回到 READY 状态。

连接备份设备

以下是将备份设备连接到 HP-UX、Solaris、Linux 或 Windows 系统的常规步骤。

1. 选择将连接备份设备的客户机。
2. 在选定系统上安装介质代理。请参见远程安装 (第 83 页)。
3. 确定可供设备使用的未使用的 SCSI 地址。对于 HP-UX 系统，请参见在 HP-UX 系统上查找未使用的 SCSI 地址 (第 329 页)。对于 Solaris 系统，请参见在 Solaris 系统上查找未使用的 SCSI 目标 ID (第 330 页)。对于 Windows 系统，请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
   - 如果连接到 HP-UX 系统，请检查所需驱动程序是否已安装并置入当前内核中。请参见检查 HP-UX 上的内核配置 (第 65 页)。

     如果需要配置 SCSI Pass-Through 驱动程序，请参见在 HP-UX 系统上配置 SCSI 机械手 (第 323 页)。
   - 如果连接到 Solaris 系统，请检查是否已为要安装的设备安装所需驱动程序和更新配置文件。请参见在 Solaris 系统上更新设备和驱动程序配置 (第 331 页)。如果需要配置 SCSI Pass-Through 驱动程序，它还描述了如何更新 sst.conf 文件。
   - 如果连接到 Windows 客户机，则可以加载或禁用本机磁带驱动程序，这取决于 Windows 系统版本。请参见在 Windows 系统上使用磁带和机械手驱动程序 (第 320 页)。

     如果为已在 Data Protector 中配置的设备加载了本机磁带驱动程序且未使用本机磁带驱动程序，请确保为引用此特定设备的所有已配置的 Data Protector 逻辑设备重命名设备文件名(例如，从 scsi1:0:4:0 重命名为 tape3:0:4:0)。

     有关相应设备文件名的详细信息，请参见在 Windows 系统上创建设备文件(SCSI 地址) (第 322 页)。
4. 在设备上设置 SCSI 地址 (ID)。根据设备类型，此操作通常可使用设备上的开关完成。有关详细信息，请参见设备自带的文档。

   有关相应的示例，请参见在 330fx 带库上设置 SCSI ID (第 334 页)。

   有关受支持的设备的详细信息，请参见 https://softwaresupport.softwaregrp.com/。

   > **注意：**
   > 在安装有 Adaptec SCSI 适配器并连接到 SCSI 设备的 Windows 系统上，必须启

> 用 Host Adapter BIOS 选项，这样系统发出 SCSI 命令时才不会出现问题。
>
> 要设置 Host Adapter BIOS 选项，请在系统启动期间按 **Ctrl+A** 进入“SCSI 适配器”菜单，然后选择**配置/查看 Host Adapter 设置 > 高级配置选项**并启用 Host Adapter BIOS。

5. 首先，打开设备和计算机，等待启动过程完成。 验证系统是否正确识别新的备份设备。

   Windows 系统：如果使用 devbra 实用程序，则可以验证系统是否正确识别新的备份设备。 在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。

   在 devbra 命令的输出中，您将发现对于每个已连接且正确识别的设备都有以下行：

   backup device specification

   hardware_path

   media_type

   .....

   例如，以下输出：

   ```
   HP:C1533A
   tape3:0:4:0
   DDS
   ...
   ...
   ```

   意味着 DDS 磁带设备(已加载本机磁带驱动程序)具有驱动器实例号 3，已连接到 SCSI 总线 0、SCSI 目标 ID 4 和 LUN 号 0。

   或者，以下输出：

   ```
   HP:C1533A
   scsi1:0:4:0
   DDS
   ...
   ...
   ```

   意味着 DDS 磁带设备(未加载本机磁带驱动程序)已连接到 SCSI 端口 1、SCSI 总线 0，磁带驱动器具有 SCSI 目标 ID 4 和 LUN 号 0。

   HP-UX 系统：运行命令 /usr/sbin/ioscan -fn 显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含新连接的设备及其正确的 SCSI 地址。

   如果在系统启动过程中没有自动创建设备文件，则应当手动创建。 请参见在 HP-UX 系统上创建设备文件 (第 327 页)。

   Solaris 系统：在 /dev/rmt 目录中运行 ls -all 命令显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含使用正确的 SCSI 地址新连接的设备。

   Linux 系统：在 /dev/rmt 目录中运行 ls -all 命令显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含使用正确的 SCSI 地址新连接的设备。

   AIX 系统：运行命令 lsdev -C 显示连接的设备列表(包括相应的设备文件)。

硬件压缩

多数现代的备份设备都提供内置的硬件压缩功能，它可在设备配置过程中创建设备文件或 SCSI 地址时启用。 有关详细步骤，请参见 *Data Protector 帮助*。

硬件压缩由从介质代理客户机收到原始数据并以压缩模式将其写入磁带的设备来完成。 硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数据较少。

使用软件压缩而禁用硬件压缩时，数据由磁带客户机压缩并以压缩的形式发送到介质代理。 如果使用软件压缩，则压缩算法可能会占用磁带客户机系统中大量的资源，但是这减小了网络负载。

要在 Windows 系统上启用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加“C”，例如：scsi:0:3:0C(如果加载磁带驱动程序，则为 tape2:0:1:0C)。 如果设备支持硬件压缩，则会使用硬件压缩，否则将忽略 C 选项。

要在 Windows 系统上禁用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加 “N”，例如：scsi:0:3:0:N。

要在 UNIX 系统上启用/禁用硬件压缩，请选择正确的设备文件。 有关详细信息，请参见设备和操作系统文档。

下面的步骤

至此，您应该已连接备份设备，这使您能够配置备份设备和介质池。 有关进一步的配置任务的详细信息，请参见《*Data Protector 帮助*》索引：“配置，备份设备”。

系统上必须安装有介质代理。 请参见远程安装 (第 83 页)。

以下章节将介绍如何将 Standalone 24 磁带设备、 12000e 带库和 DLT 带库 28/48 插槽连接到 HP-UX 和 Windows 系统。

连接 24 独立设备

24 DDS 备份设备是一种基于 DDS3 技术的独立磁带驱动器。

连接到 HP-UX 系统

将 HPE 24 独立设备连接到 HP-UX 系统

1. 检查所需驱动程序((stape 或 tape2))是否已安装并置入当前内核中。 请参见检查 HP-UX 上的内核配置 (第 65 页)。
2. 确定可供磁带驱动器使用的未使用的 SCSI 地址。 请参见在 HP-UX 系统上查找未使用的 SCSI 地址 (第 329 页)。
3. 在设备上设置 SCSI 地址 (ID)。 使用设备背面的开关。

   有关详细信息，请参见设备自带的文档。
4. 首先，打开设备和计算机，等待启动过程完成。
5. 验证系统是否正确识别新连接的磁带驱动器。 使用 ioscan 实用程序：

`/usr/sbin/ioscan -fn`

显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。驱动器的设备文件已在启动过程中创建。

下面的步骤

在正确连接设备之后，请参见《*Data Protector 帮助*》的索引："配置，备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接到 Windows 系统

将 HPE 24 独立设备连接到 Windows 系统

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址(目标 ID)。请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
2. 在设备上设置 SCSI 地址 (ID)。使用设备背面的开关。有关详细信息，请参见设备自带的文档。
3. 首先，打开设备和计算机，等待启动过程完成。
4. 验证系统是否正确识别新连接的磁带驱动器。在 Data Protector 命令目录中，执行 `devbra -dev` 命令。

   在 `devbra` 命令的输出中，应包含 HPE 24 独立设备新连接的磁带驱动器。

下一步？

在正确连接设备之后，请参见《*Data Protector 帮助*》的索引："配置，备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接 DAT 自动加载器

12000e 和 DAT24x6 库都有一个存储库(带六个磁带盒)、一个驱动器和一个用于将磁带盒移入/移出驱动器的机械手臂。这两个带库还具有内置的脏磁带检测功能。

连接到 HP-UX 系统

将 12000e 库设备连接到 HP-UX 系统

1. 在自动加载器背面，将模式开关设置为 6.
2. 检查所需驱动程序(`stape` 或 `tape2`)是否已*安装并置入*当前内核中。请参见检查 HP-UX 上的内核配置 (第 65 页)。
3. 检查所需的 SCSI Pass-Through 驱动程序(`sctl` 或 `spt`)是否已*安装并置入*当前内核中。请参见在 HP-UX 系统上配置 SCSI 机械手 (第 323 页)。
4. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。请参见在 HP-UX 系统上查找未使用的 SCSI 地址 (第 329 页)。

> **注意：**
> 12000e 库使用与磁带驱动器和机械手相同的 SCSI 地址，但是使用不同的 LUN 号。

5. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。
6. 首先，打开设备和计算机，等待启动过程完成。
7. 验证系统是否正确识别新连接的磁带驱动器。使用 ioscan 实用程序

   ```
   /usr/sbin/ioscan -fn
   ```

   显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。
8. 驱动器的设备文件已在启动过程中创建，而机械手的设备文件必须手动创建。请参见在 HP-UX 系统上创建设备文件 (第 327 页)。
9. 验证系统是否正确识别为带库机械手新创建的设备文件。运行 ioscan 实用程序：

   ```
   /usr/sbin/ioscan -fn
   ```

   在该命令的输出中应包含新创建的设备文件。

下面的步骤

在正确连接带库设备之后，请参见《*Data Protector 帮助*》的索引："配置，备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接到 Windows 系统

将 12000e 库设备连接到 Windows 系统

1. 在自动加载器背面，将模式开关设置为 6.
2. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
3. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。

   > **注意：**
   > 12000e 库使用与磁带驱动器和机械手相同的 SCSI 地址，但是使用不同的 LUN 号。

4. 首先，打开设备和计算机，等待启动过程完成。
5. 验证系统是否正确识别新连接的磁带驱动器和机械手。在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。

   在 devbra 命令的输出中，应包含 12000e 库设备的新连接磁带驱动器和机械手。

下面的步骤

在正确连接带库设备之后，请参见《*Data Protector 帮助*》的索引："配置，备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接DLT 带库 28/48 插槽

DLT 库 28/48 插槽是用于要备份 80-600 GB 的企业环境的多驱动器库。它具有四个 DLT 4000 或 DLT 7000 驱动器、多个数据通道、一个邮件插槽和一个条形码读取器。

连接到 HP-UX 系统

将 DLT 库 28/48 插槽库设备连接到 HP-UX 系统

1. 检查所需的驱动程序((stape 或 tape2) 驱动程序)是否已安装并置入当前内核中。请参见检查 HP-UX 上的内核配置 (第 65 页)。
2. 检查所需的 SCSI Pass-Through 驱动程序((sctl 或 spt))是否已安装并置入当前内核中。请参见在 HP-UX 系统上配置 SCSI 机械手 (第 323 页)。
3. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址。请参见在 HP-UX 系统上查找未使用的 SCSI 地址 (第 329 页)。

   > **注意：**
   > DLT 带库 28/48 插槽具有四个磁带驱动器和机械手，因此需要五个未使用的 SCSI 地址以防同时使用所有磁带驱动器。磁带驱动器和机械手必须使用不同的 SCSI 地址。

4. 在设备上设置 SCSI 地址 (ID)。有关详细信息，请参见设备自带的文档。
5. 打开设备和计算机，等待启动过程完成。
6. 验证系统是否正确识别新连接的磁带驱动器。使用 ioscan 实用程序

   ```
   /usr/sbin/ioscan -fn
   ```

   显示连接的设备列表(包括相应的硬件路径和设备文件)，其中应包含新连接的磁带驱动器及其正确的 SCSI 地址。
7. 驱动器的设备文件已在启动过程中创建,而机械手的设备文件必须手动创建。请参见在 HP-UX 系统上创建设备文件 (第 327 页)。
8. 验证系统是否正确识别为带库机械手新创建的设备文件。使用 ioscan 实用程序：

   ```
   /usr/sbin/ioscan -fn
   ```

   在该命令的输出中应包含新创建的设备文件。

下面的步骤

在正确连接 DLT 带库 28/48 插槽的带库设备之后，请参见《*Data Protector 帮助*》的索引："配置, 备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接到 Solaris 系统

对于此示例，假定两个驱动器将分配给 Data Protector。

在 Solaris 系统上配置 C5173-7000 库设备

1. 将 sst 驱动程序(模块)和配置文件 sst.conf 复制到要求的目录：
   - 对于 32 位操作系统：

     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```

   - 对于 64 位操作系统：

     ```
     $cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv /sparcv9/sst.conf
     ```

2. 将驱动程序添加到 Solaris 内核：

   ```
   add_drv sst
   ```

3. 从 /dev/rmt 目录中删除所有现有的设备文件：

   ```
   cd /dev/rmt rm *
   ```

4. 按**停止**和停止系统。 **A.**
5. 在出现“ok”提示时运行 probe-scsi-all 命令以检查哪些 SCSI 地址可用。

   ```
   ok probe-scsi-all
   ```

   系统可能会要求您先启动 reset-all 命令，再执行 probe-scsi-all 命令。

   在此例中，端口 6 用于 SCSI 控制设备，端口 2 用于第一个驱动器，端口 1 用于第二个驱动器，LUN 是 0。
6. 返回到正常运行：

   ```
   ok go
   ```

7. 将 st.conf 配置文件复制到要求的目录：

   ```
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   ```

   st.conf 文件存在于每个 Solaris Data Protector 客户机上并包含每个连接到客户机的备份设备的 SCSI 地址。
8. 编辑 /kernel/drv/st.conf 文件并添加以下各行：

   ```
   tape-config-list= "QUANTUM DLT7000", "Digital DLT7000", "DLT-data3";
    DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;
   name="st" class="scsi"
    target=1 lun=0;
   name="st" class="scsi"
    target=2 lun=0;
    name="st" class="scsi"
    target=6 lun=0;
   ```

   这些条目分别为驱动器 1、驱动器 2 和机械手驱动器提供 SCSI 地址。
9. 编辑在将 sst 驱动程序(模块)和配置文件 sst.conf 复制到要求的目录： (第 341 页)中复制的 sst.conf 文件并添加以下行：

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

> **注意：**
> 该条目必须与 st.conf 文件中的机械手驱动器的条目匹配。 请参见以上编辑 /kernel/drv/st.conf 文件并添加以下各行： (第 341 页)。

10. 关闭客户机系统，并连接库设备。
11. 首先打开库设备，然后打开客户机系统。

    现在系统将启动并自动为机械手驱动器和磁带驱动器创建设备文件。 使用命令 ls -all. 可以列出这些设备文件。在此例中：

/dev/rmt/0hb	适用于第一个磁带驱动器
/dev/rmt/1hb	适用于第二个磁带驱动器
/dev/rsst6	适用于机械手驱动器

下一步？

在正确连接 DLT 带库 28/48 插槽的带库设备之后，请参见《*Data Protector 帮助*》的索引："配置, 备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接到 Windows 系统

将 DLT 28/48 插槽库设备连接到 Windows 系统

1. 确定可供磁带驱动器和机械手使用的未使用的 SCSI 地址(目标 ID)。 请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
2. 在设备上设置 SCSI 地址(目标 ID)。 有关详细信息，请参见设备自带的文档。

   > **注意：**
   > DLT 带库 28/48 插槽具有四个磁带驱动器和机械手，因此需要五个未使用的 SCSI 地址以防同时使用所有磁带驱动器。 磁带驱动器和机械手必须使用不同的 SCSI 目标 ID。

3. 首先，打开设备和计算机，等待启动过程完成。
4. 验证系统是否正确识别新连接的磁带驱动器和机械手。 在默认的 Data Protector 命令目录中，执行 devbra -dev 命令。

   在 devbra 命令的输出中，应包含 DLT 库 28/48 插槽库设备新连接的磁带驱动器和机械手。

下面的步骤

在正确连接 DLT 库 28/48 插槽的库设备之后，请参见《*Data Protector 帮助*》的索引："配置, 备份设备"，了解有关为新连接的库设备配置 Data Protector 备份设备的说明。

连接 Seagate Viper 200 LTO Ultrium 磁带驱动器

Seagate Viper 200 LTO Ultrium 磁带驱动器是一种用于要备份 100-200 GB 的企业环境的独立设备。

连接到 **Solaris** 系统

在 **Solaris** 系统上配置 **Seagate Viper 200 LTO Ultrium** 磁带驱动器

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址。运行 `modinfo` 或 `dmesg` 命令查找使用中的 SCSI 控制器和已安装的 SCSI 目标设备：

   ```
   dmesg | egrep “target” | sort | uniq
   ```

   应得到以下输出：

   ```
   sd32 at ithps0: target 2 lun 0
    sd34 at ithps0: target 4 lun 0
    st21 at ithps1: target 0 lun 0
    st22 at ithps1: target 1 lun 0
   ```

   > **注意：**
   > 在将 Viper 200 LTO 设备连接到 Solaris 系统时，建议使用 `glm` 或 `isp` SCSI 控制器。另建议使用 Ultra2 SCSI 或 Ultra3 SCSI 控制器。

2. 编辑 `/kernel/drv/st.conf` 文件并添加以下各行：

   ```
   tape-config-list=
    “SEAGATE ULTRIUM06242-XXX” , “SEAGATE LTO” , \
    “SEAGATE_LTO”;
    SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
    0x00, 1;
   ```

3. 关闭客户机系统，并连接设备。
4. 依次打开设备和客户机系统。

   现在系统将启动并自动为磁带驱动器创建设备文件。使用以下命令可以列出这些设备文件 `ls -all`.

下一步？

在正确连接 Seagate Viper 200 LTO Ultrium 磁带机之后，请参见《*Data Protector 帮助*》的索引：“配置, 备份设备”，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

连接到 **Windows** 系统

在 **Windows** 系统上连接 **Seagate Viper 200 LTO Ultrium** 磁带驱动器

1. 确定可供磁带驱动器使用的未使用的 SCSI 地址(目标 ID)。请参见在 Windows 系统上查找未使用的 SCSI 目标 ID (第 334 页)。
2. 在设备上设置 SCSI 地址(目标 ID)。有关详细信息，请参见设备自带的文档。
1. 首先，打开设备和计算机，等待启动过程完成。
2. 验证系统是否正确识别新连接的磁带驱动器和机械手。在默认的 Data Protector 命令目

录中，执行 devbra -dev 命令。

在 devbra 命令的输出中，应包含 Seagate Viper 200 LTO Ultrium 磁带驱动器新连接的磁带驱动器。

下面的步骤

在正确连接 Seagate Viper 200 LTO Ultrium 磁带机之后，请参见《*Data Protector 帮助*》的索引："配置, 备份设备"，了解有关为新连接的设备配置 Data Protector 备份设备的说明。

> **注意：**
> 在 Data Protector 中配置 Seagate Viper 200 LTO Ultrium 磁带驱动器时，请确保设置了压缩模式。方法是在驱动器的 SCSI 地址后指定 C 参数，例如：
>
> ```
> scsi2:0:0:0C
> ```

附录 D： 详细信息

> **注意：**
> 客户支持网站(网址为： https://softwaresupport.softwaregrp.com/)中可用的文档集包含最新更新和更正。

您可从以下位置访问 Data Protector 文档集：

- Data Protector 安装目录。

  Windows 系统： *Data_Protector_home*\docs

  UNIX 系统： /opt/omni/doc/C
- Data Protector GUI 的**帮助**菜单。
- 支持网站(网址为： https://softwaresupport.softwaregrp.com/)

Data Protector 文档的查看要求

要查看 Data Protector 指南 Data Protector 帮助，必须安装支持的 PDF 文档查看器和 Web 浏览器。以下是支持的应用程序和版本的列表。Micro Focus 建议使用适合您的操作系统的最新版本：

- 要查看指南，您需要 Adobe Reader。支持的版本如下：

  Windows、Solaris 和 Linux 系统：

  - Adobe Reader 9 或更高版本

    可以从 http://get.adobe.com/reader/ 下载该软件。

  HP-UX 系统：

  - Adobe Reader 7 或更高版本

    可以从 ftp://ftp.adobe.com/pub/adobe/reader/unis/7x/7.0.9/enu/ 下载该软件。

  其他 PDF 文档查看器也可以满足此条件，但尚未经过测试。
- 要查看“帮助”，需要在 Data Protector GUI 过程中能在相同帐户下运行的 Web 浏览器。必须在 Web 浏览器中启用 JavaScript。支持下列 Web 浏览器：

  Windows 系统：

  - Windows Internet Explorer 8.0 或更高版本 [1]

    对于本地存储的网站，应禁用兼容性视图。

    可以从 http://windows.microsoft.com/en-us/internet-explorer/download-ie 下载 Windows Internet Explorer。
  - Mozilla Firefox 17.0.5(扩展的支持版本)或更高版本

[1] 您还需要此浏览器以查看 Microsoft Exchange Server 帮助中的 Data Protector Granular Recovery Extension。

可以从 http://www.mozilla.org/en-US/firefox/organizations/all.html 下载该软件。

其他 Web 浏览器也可以满足此条件，但尚未经过测试。

帮助

未安装 Data Protector 时，可以从安装程序包 (zip/tar) 的顶级目录访问“帮助”：

Windows 系统： 打开 `DP_help.chm`

UNIX 系统： 解压缩经过压缩的 tar 文件 `DP_help.tar.gz`，并打开 `DP_help.htm`。

文档映射图

下表显示了可以从何处查找不同类型的信息。带灰色阴影的方框代表首选查找位置。

											集成指南					ZDB 指南		GRE 指南		
	Admin	帮助	入门	概念	安装	故障排除	DR	CLI	PA	集成 VSS	MSFT	Oracle/SAP	IBM	Sybase/NDMP	虚拟环境	ZDB 管理	ZDB IG	Exchange	SharePoint	VMware
管理任务	X	X																		
备份		X	X	X						X	X	X	X	X	X	X	X			
CLI								X												
概念、技术		X		X						X	X	X	X	X	X	X	X	X	X	X
灾难恢复				X			X													
安装、升级			X		X				X											
即时恢复				X	X											X	X			
许可					X				X											
限制		X			X	X			X	X	X	X	X	X	X		X			
新功能		X							X											
计划策略		X		X																
过程、任务	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
建议				X					X											
要求					X				X	X	X	X	X	X	X					
还原	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
支持的配置				X																
故障排除		X			X	X				X	X	X	X	X	X	X	X	X	X	X

缩写

以下对文档映射图中的缩写进行了说明。文档项标题前面均带有单词“Data Protector”。

缩写	文档项	
管理员	管理员指南	本指南介绍 Data Protector 中的管理任务。

缩写	文档项	
CLI	命令行界面参考	本指南描述了 Data Protector 命令行界面、命令选项和它们的用途，并提供一些基本命令行示例。
概念	概念指南	本指南介绍 Data Protector 概念、零宕机时间备份 (ZDB) 概念，并提供有关 Data Protector 工作原理的背景信息。它应与面向任务的帮助配合使用。
DR	灾难恢复指南	本指南介绍如何规划、准备、测试和执行灾难恢复。
入门	入门指南	本指南包含使用 Data Protector 的入门信息。本指南列出安装先决条件，提供有关为执行备份和还原而安装和配置基本备份环境和过程的说明，还列出了可供了解进一步信息的资源。
GRE 指南	适用于 Microsoft SharePoint Server、Exchange 和 VMware 的 Granular Recovery Extension 用户指南	本指南介绍如何配置和使用适用于以下组件的 Data Protector Granular Recovery Extension： • Microsoft SharePoint Server • Exchange Server • VMware vSphere
帮助	帮助	
安装	安装指南	本指南介绍如何针对您所用环境的操作系统和体系结构来安装 Data Protector 软件。本指南还详细介绍了如何升级 Data Protector，以及如何获取适用于您所用环境的正确许可证。
集成指南	集成指南	本指南介绍 Data Protector 与以下应用程序的集成： • **MSFT**：Microsoft SQL Server、Microsoft SharePoint Server 和 Microsoft Exchange Server。 • **IBM**：Informix Server、IBM DB2 UDB 和 Lotus Notes/Domino Server。

缩写	文档项	
		• **Oracle/SAP**：Oracle Server、SAP R3、SAP MaxDB 和 SAP HANA Appliance。 • **Sybase/NDMP**：Sybase 和 Network Data Management Protocol Server、 • **虚拟环境**：与 VMware vSphere、VMware vCloud Director、Microsoft Hyper-V 和 Citrix XenServer 进行虚拟环境集成。
集成 VSS	Microsoft Volume Shadow Copy Service 的集成指南	本指南介绍 Data Protector 与 Microsoft 卷影复制服务 (VSS) 的集成。
PA	产品声明、软件说明和参考	本指南介绍最新版本的新功能。此外，它还提供有关安装要求、必需补丁、限制以及已知问题和变通方法的信息。
故障排除	故障诊断指南	本指南介绍如何对在使用 Data Protector 时遇到的问题进行故障诊断。
ZDB 管理	ZDB 管理员指南	本指南介绍如何配置和使用 Data Protector 与 P4000 SAN 解决方案、P6000 EVA 磁盘阵列系列、P9000 XP 磁盘阵列系列、3PAR StoreServ Storage、NetApp Storage 和 EMC Symmetrix Remote Data Facility 以及 TimeFinder 的集成。适用于备份管理员或操作员。它涵盖了零宕机时间备份、即时恢复以及文件系统和磁盘映像的还原。
ZDB IG	ZDB 集成指南	本指南介绍如何配置和使用 Data Protector 来执行零宕机时间备份、即时恢复，以及 Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server 数据库和适用于 VMware 的虚拟环境的标准还原。

集成

软件应用程序集成

软件应用程序	指南
IBM DB2 UDB	集成指南
Informix Server	集成指南
Lotus Notes/Domino Server	集成指南
Microsoft Exchange Server	集成指南、ZDB IG、GRE 指南
Microsoft Hyper-V	集成指南
Microsoft SharePoint Server	集成指南、ZDB IG、GRE 指南
Microsoft SQL Server	集成指南、ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	集成 VSS
Network Data Management Protocol (NDMP) Server	集成指南
Oracle Server	集成指南、ZDB IG
SAP HANA Appliance	集成指南
SAP MaxDB	集成指南
SAP R/3	集成指南、ZDB IG
Sybase Server	集成指南
VMware vCloud Director	集成指南
VMware vSphere	集成指南、ZDB IG、GRE 指南

磁盘阵列系统集成

查看以下指南了解与以下系列的磁盘阵列系统的集成有关的详细信息:

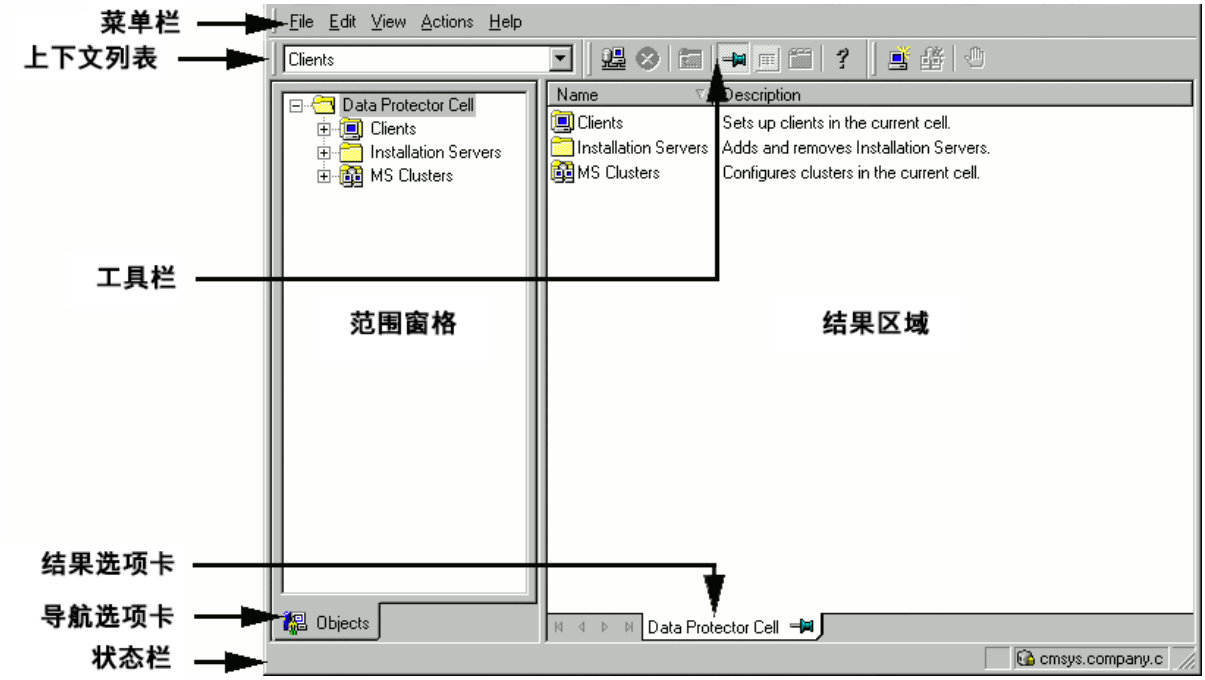
磁盘阵列系列	指南
EMC Symmetrix	所有 ZDB
P4000 SAN 解决方案	概念、ZDB 管理、集成指南
P6000 EVA 磁盘阵列系列	所有 ZDB、集成指南

磁盘阵列系列	指南
P9000 XP 磁盘阵列系列	所有 ZDB、集成指南
3PAR StoreServ Storage	概念、ZDB 管理、集成指南
NetApp Storage	所有 ZDB

Data Protector 图形用户界面

Data Protector 提供了在 Microsoft Windows 操作系统上使用的图形用户界面。 有关信息，请参见《 *Data Protector 帮助*》。

Data Protector 图形用户界面



发送文档反馈

如果对此文档有任何评论，可以通过电子邮件联系文档团队。如果该系统配置了电子邮件客户机，请单击上面的链接，此时会打开一个电子邮件窗口，其主题行中将显示以下信息：

有关安装指南 (Data Protector 10.00) 的反馈

将反馈添加到电子邮件中并单击**发送**。

如果无可用的电子邮件客户机，请将以上信息复制到 Web 邮件客户机中的新邮件，并将反馈发送至 docs.feedback@microfocus.com 。

期待您的反馈！