HP Data Protector 7.00
Installation and Licensing Guide

HP Part Number: N/A
Published: October 2013
Edition: Fifth

Contents

Publication history

Guide updates may be issued between editions to correct errors or document product changes. To ensure that you receive updated or new editions, subscribe to the appropriate product support service. See your HP sales representative for details.

Table 1 Edition history

Part number	Guide edition	Product
N/A	March 2012	Data Protector Release 7.00
N/A	April 2012	Data Protector Release 7.00
N/A	July 2012	Data Protector Release 7.00 with any of the following patch bundles: DPWINBDL_00701, DPUXBDL_00701, DPLNXBDL_00701
N/A	March 2013	Data Protector Release 7.00 with any of the following patches: DPWIN_00631, PHSS_43339, DPLNX_00241
N/A	October 2013	Data Protector Release 7.00 with any of the following patch bundles: DPWINBDL_00703, DPUXBDL_00703, DPLNXBDL_00703

About this guide

This guide provides information about:

- installing the Data Protector network product
- prerequisites that must be met before starting the installation procedure
- upgrading and licensing

Intended audience

This guide is intended for administrators responsible for installing and maintaining the environment and backup administrators responsible for planning, installing, and managing the backup environment.

Conceptual information can be found in the *HP Data Protector Concepts Guide*, which is recommended to fully understand the fundamentals and the model of Data Protector.

Documentation set

Other guides and Help provide related information.

Guides

Data Protector guides are available in the electronic PDF format. Install the PDF files during the Data Protector setup procedure by selecting the installation component `English Documentation (Guides, Help)` on Windows systems and the installation component `OB2-DOCS` on UNIX systems. Once installed, the guides reside in the directory *`Data_Protector_home`*`\docs` on Windows systems and in the directory `/opt/omni/doc/C` on UNIX systems.

You can find these documents from the Manuals page of the HP support website:

http://support.openview.hp.com/selfsolve/manuals

In the Storage section, click **Storage Software** and then select your product.

- *HP Data Protector Concepts Guide*

  This guide describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented Help.

- *HP Data Protector Installation and Licensing Guide*

  This guide describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This guide also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.

- *HP Data Protector Troubleshooting Guide*

  This guide describes how to troubleshoot problems you may encounter when using Data Protector.

- *HP Data Protector Disaster Recovery Guide*

  This guide describes how to plan, prepare for, test, and perform a disaster recovery.

- *HP Data Protector Integration Guides*

  These guides describe how to configure and use Data Protector to back up and restore various databases and applications. They are intended for backup administrators or operators. There are six guides:

  - *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*

    This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server.

  - *HP Data Protector Integration Guide for Oracle and SAP*

    This guide describes the integrations of Data Protector with Oracle Server, SAP R/3, SAP MaxDB, and SAP HANA Appliance.

  - *HP Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino*

    This guide describes the integrations of Data Protector with the following IBM applications: Informix Server, IBM DB2 UDB, and Lotus Notes/Domino Server.

  - *HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*

    This guide describes the integrations of Data Protector with Sybase Server, HP Network Node Manager, and Network Data Management Protocol Server.

  - *HP Data Protector Integration Guide for Virtualization Environments*

    This guide describes the integrations of Data Protector with virtualization environments: VMware Virtual Infrastructure, VMware vSphere, VMware vCloud Director, Microsoft Hyper-V, and Citrix XenServer.

  - *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

    This guide describes the integration of Data Protector with the Microsoft Volume Shadow Copy Service. This guide also documents application writer specifics.

- *HP Data Protector Integration Guide for HP Operations Manager for UNIX*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX systems.

- *HP Data Protector Integration Guide for HP Operations Manager for Windows*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager on Windows systems.

- *HP Data Protector Zero Downtime Backup Concepts Guide*

  This guide describes Data Protector zero downtime backup and instant recovery concepts and provides background information on how Data Protector works in a zero downtime backup environment. It is intended to be used with the task-oriented *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Zero Downtime Backup Integration Guide*.

- *HP Data Protector Zero Downtime Backup Administrator's Guide*

  This guide describes how to configure and use the integration of Data Protector with HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, HP P10000 Storage Systems, and EMC Symmetrix Remote Data Facility and TimeFinder. It is

intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

- *HP Data Protector Zero Downtime Backup Integration Guide*

  This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle Server, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases.

- *HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server*

  This guide describes how to configure and use the Granular Recovery Extension for Microsoft Exchange Server 2010 environments. Graphical user interface of the Data Protector Granular Recovery Extension for Microsoft Exchange Server is integrated into the Microsoft Management Console. This guide is intended for Microsoft Exchange Server administrators and Data Protector backup administrators.

- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for Microsoft SharePoint Server. The Data Protector Granular Recovery Extension is integrated into Microsoft SharePoint Server Central Administration and enables you to recover individual items. This guide is intended for Microsoft SharePoint Server administrators and Data Protector backup administrators.

- *HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for VMware vSphere. The Data Protector Granular Recovery Extension is integrated into VMware vCenter Server and enables you to recover individual items. This guide is intended for VMware vCenter Server users and Data Protector backup administrators.

- *HP Data Protector Media Operations User Guide*

  This guide provides information for network administrators responsible for maintaining and backing up systems on the tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.

- *HP Data Protector Product Announcements, Software Notes, and References*

  This guide gives a description of new features of HP Data Protector 7.00. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.

- *HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager*

  This guide fulfills a similar function for the HP Operations Manager integration.

- *HP Data Protector Media Operations Product Announcements, Software Notes, and References*

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector Command Line Interface Reference*

  This guide describes the Data Protector command-line interface, command options, and their usage as well as provides some basic command-line examples. It is located in the following directory:

  Windows systems: `Data_Protector_home\docs\MAN`

  UNIX systems: `/opt/omni/doc/C/`

  On UNIX systems, you can use the `omniintro` man page to display a list of the available Data Protector commands. You can then execute the `man CommandName` command to retrieve information about a specific Data Protector command.

Help

Data Protector provides Help topics and context-sensitive (F1) Help for Windows and UNIX platforms. Install the Help during the Data Protector setup procedure by selecting the installation component `English Documentation (Guides, Help)` on Windows systems and the installation component `OB2-DOCS` on UNIX systems. Once installed, the Help resides in the directory *`Data_Protector_home`*`\help\enu` on Windows systems and in the directory `/opt/omni/help/C/help_topics` on UNIX systems.

You can access the Help from the top-level directory of any installation DVD-ROM without installing Data Protector:

Windows systems: Open `DP_help.chm`.

UNIX systems: Unpack the zipped tar file `DP_help.tar.gz`, and access the Help system through `DP_help.htm`.

Documentation map

Abbreviations

Abbreviations in the documentation map that follows are explained below. The documentation item titles are all preceded by the words "HP Data Protector".

Abbreviation	Documentation item
CLI	Command Line Interface Reference
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
GRE-Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE-SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	Help
IG-IBM	Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server
IG-O/S	Integration Guide for Oracle and SAP
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server
IG-VirtEnv	Integration Guide for Virtualization Environments
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	Installation and Licensing Guide
MO-GS	Media Operations Getting Started Guide
MO-PA	Media Operations Product Announcements, Software Notes, and References
MO-UG	Media Operations User Guide
PA	Product Announcements, Software Notes, and References

Abbreviation	Documentation item
Trouble	Troubleshooting Guide
ZDB-Admin	ZDB Administrator's Guide
ZDB-Concept	ZDB Concepts Guide
ZDB-IG	ZDB Integration Guide

Map

The following table shows where to find information of different kinds. Shaded squares are a good place to look first.

								Integration Guides								ZDB			GRE			MO			
	Help	GS	Concepts	Install	Trouble	DR	PA	MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	Exchange	SPS	VMware	GS	UG	PA	CLI
Backup	X	X	X					X	X	X	X	X	X			X	X	X							
CLI																									X
Concepts/ techniques	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Disaster recovery	X		X			X																			
Installation/ upgrade	X	X		X			X							X	X							X	X		
Instant recovery	X		X													X	X	X							
Licensing	X			X			X																X		
Limitations	X				X		X	X	X	X	X	X	X					X						X	
New features	X						X																	X	
Planning strategy	X		X													X									
Procedures/ tasks	X			X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X		X		
Recommendations			X				X									X								X	
Requirements				X			X	X	X	X	X	X	X	X	X							X	X	X	
Restore	X	X	X					X	X	X	X	X	X				X	X	X	X	X				
Supported configurations																X									
Troubleshooting	X			X	X			X	X	X	X	X	X	X	X		X	X	X	X	X				

Integrations

Look in these guides for details of the integrations with the following software applications:

Software application	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO-UG
Microsoft Exchange Server	IG-MS, ZDB IG, GRE-Exchange

Software application	Guides
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB-IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB-IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Network Data Management Protocol (NDMP) Server	IG-Var
Oracle Server	IG-O/S, ZDB-IG
SAP HANA Appliance	IG-O/S
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB-IG
Sybase Server	IG-Var
VMware vCloud Director	IG-VirtEnv
VMware vSphere	IG-VirtEnv, GRE-VMware

Look in these guides for details of the integrations with the following families of disk array systems:

Disk array family	Guides
EMC Symmetrix	all ZDB
HP P4000 SAN Solutions	ZDB-Concept, ZDB-Admin, IG-VSS
HP P6000 EVA Disk Array Family	all ZDB, IG-VSS
HP P9000 XP Disk Array Family	all ZDB, IG-VSS
HP P10000 Storage Systems	ZDB-Concept, ZDB-Admin, IG-VSS

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 16)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

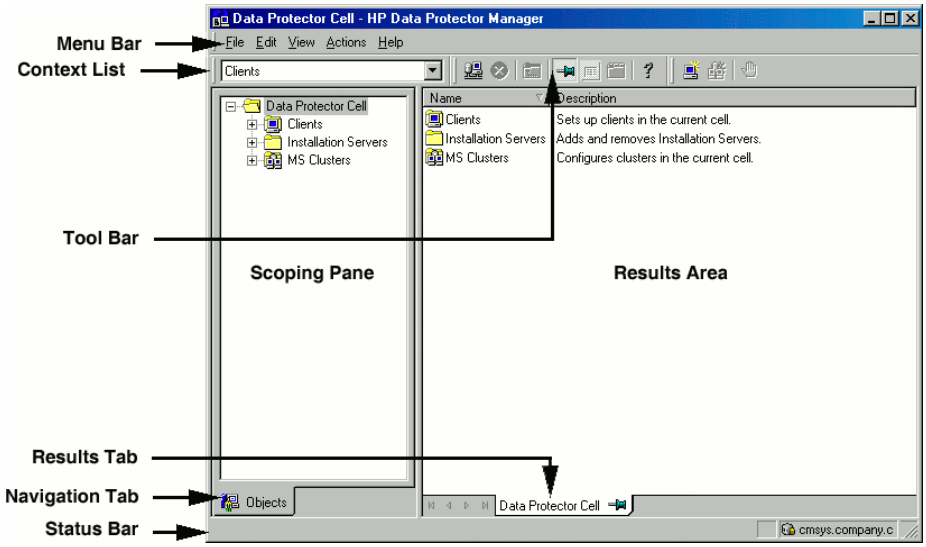
NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Data Protector graphical user interface

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface. You can use the original Data Protector GUI (Windows only) or the Data Protector Java GUI. For information about the Data Protector graphical user interface, see the *HP Data Protector Help*.

Figure 1 Data Protector graphical user interface



General information

General information about Data Protector can be found at http://www.hp.com/go/dataprotector.

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/software
- http://support.openview.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

1 Overview of the installation procedure

In this chapter

This chapter provides an overview of the Data Protector installation procedure and introduces concepts that apply to the installation. The chapter also introduces Data Protector Cell Manager and Data Protector.

Overview of the installation procedure

A Data Protector backup environment is a set of systems with a common backup policy located in the same time zone and existing on the same LAN/SAN. This network environment is referred to as a Data Protector **cell**. A typical cell consists of a Cell Manager, Installation Servers, clients, and backup devices.

The **Cell Manager** is the main system that manages the cell from a central point. It contains the Data Protector internal database (IDB) and runs core Data Protector software and session managers.

The IDB keeps track of backed up files and the cell configuration.

The **Installation Server** is a separate system or a Cell Manager component that contains the Data Protector software repository used for remote client installations. This Data Protector feature greatly facilitates the software installation process, particularly for remote clients.

A cell typically consists of one Cell Manager and several clients. A computer system becomes a Data Protector **client** as soon as one of the Data Protector software components is installed on the system. The client components installed on a system depend on the role of that system in your backup environment. Data Protector components can be installed either locally on a single system, or onto several systems from Installation Servers.

The **User Interface** component is needed to access the Data Protector functionality and is used to perform all configuration and administration tasks. It must be installed on systems used for backup administration. Data Protector provides a graphical user interface (GUI) and command-line interface (CLI).

Client systems with disks that need to be backed up must have an appropriate Data Protector **Disk Agent** components installed. The Disk Agent enables you to back up data from the client disk or restore it.

Client systems that are connected to a backup device must have a **Media Agent** component installed. This software manages backup devices and media. Data Protector features two Media Agents: the **General Media Agent** and the **NDMP Media Agent**. The NDMP Media Agent is only needed on client systems that control the backup of an NDMP server (on client systems controlling NDMP dedicated drives). In all other cases the two Media Agents are interchangeable.

Before installing Data Protector on your network, define the following:

- The system on which the Cell Manager will be installed. For supported operating systems and versions, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

  There can only be one Cell Manager per cell. Data Protector cannot be run without a Cell Manager installed.

- Systems that will be used to access the Data Protector functionality through the user interface. These systems must have the User Interface component installed.
- Systems that will be backed up. These must have the Disk Agent component installed for filesystem backup and the relevant Application Agent component for online database integrations.

- Systems to which the backup devices will be connected. These must have a Media Agent component installed.
- The system(s) on which the Data Protector Installation Server(s) will be installed. Two types of Installation Servers are available for remote software installation: one for UNIX clients and one for Windows clients.

  The choice of computer for the Installation Server is independent of the Cell Manager and the system(s) on which the User Interface is installed. The Cell Manager and Installation Server can be installed on the same system (if they run on the same platform) or on different systems.

  An Installation Server can be shared between multiple Data Protector cells.

NOTE: The Installation Server for Windows must be installed on a Windows system. The Installation Server for UNIX must be installed on an HP-UX or Linux system. For supported operating system versions, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

IMPORTANT: When installing a Data Protector client on Solaris systems, make sure to save all your files from the `/usr/omni` directory to some other directory. The Data Protector installation deletes all the files from the `/usr/omni` directory.

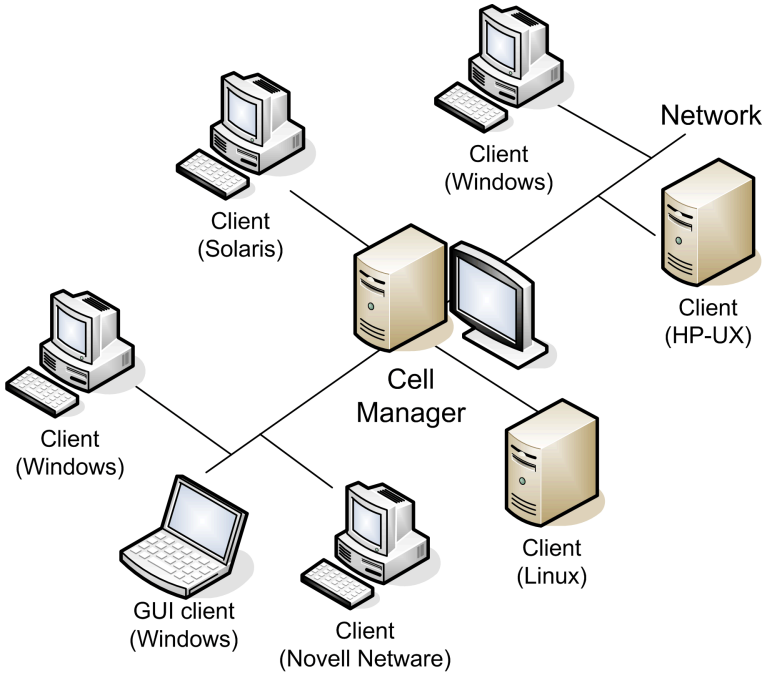
After you have defined the roles of the systems in your future Data Protector cell, the installation procedure comprises the following general steps:

1. Checking the prerequisites for installation.
2. Installing the Data Protector Cell Manager.
3. Installing the Installation Server(s) and the User Interface.
4. Installing client systems either remotely (recommended option, where possible), or locally from the installation DVD-ROM.

NOTE: You cannot remotely install a Data Protector client on a Windows system if an Installation Server has already been installed on this system. To install an Installation Server and client component(s) on the same system, you must perform a local client installation from the Data Protector Windows installation DVD-ROM. In the Custom Setup window, select all desired client components and the Installation Server component.

Remote installation is also not possible for Windows XP Home Edition, Novell NetWare, and HP OpenVMS clients. These have to be installed locally.

Figure 2 Data Protector Cell



The remote installation concept

Once you have installed the Data Protector Cell Manager, User Interface, and Installation Server(s) (at least one Installation Server is needed for each platform, UNIX and Windows), you can distribute Data Protector software to clients using operating systems on which remote installation is supported. See "Data Protector installation concept" (page 22).

Every time you perform a remote installation, you access the Installation Server through the GUI. The User Interface component may be installed on the Cell Manager, although this is not a requirement. It would be prudent to install the User Interface on several systems so that you can access the Cell Manager from different locations.

Client software can be distributed to any Windows system, except Windows XP Home Edition, from an Installation Server for Windows.

Windows XP Home Edition client systems must be installed locally from the Data Protector Windows installation DVD-ROM.

Data Protector also supports Novell NetWare clients, although there is no remote client installation. Installation is performed through a Windows system connected to the Novell network.

Client software can be installed remotely on HP-UX, Solaris, Linux, AIX, and other supported UNIX operating systems from an Installation Server for UNIX. For a list of supported platforms, see the *HP Data Protector Product Announcements, Software Notes, and References*. Even though Installation Server is not required for local installation of clients, it is required to keep the clients up to date with patches.

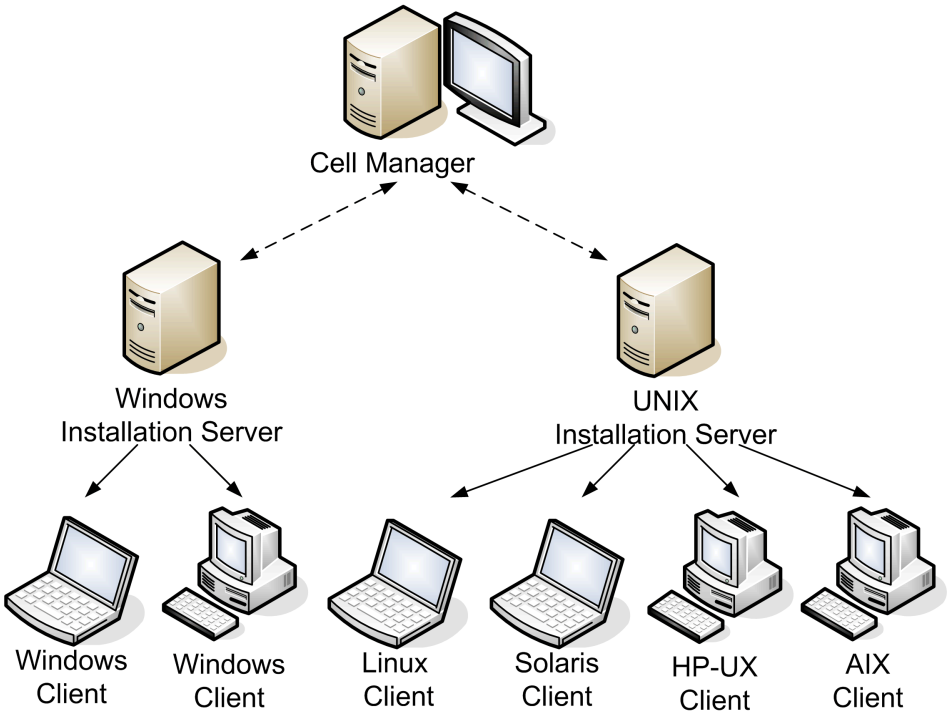
For UNIX operating systems on which remote installation is not supported, or if you do not install an Installation Server for UNIX, you can install UNIX clients locally, from the Data Protector UNIX installation DVD-ROM.

Note that there are some exceptions that require remote installation only.

For further information on available installation methods for the various Data Protector clients, see "Installing Data Protector clients" (page 43).

For the procedure for deinstalling UNIX clients locally, see "Local installation on UNIX and Mac OS X systems" (page 81).

Figure 3 Data Protector installation concept



Data Protector installation DVD-ROMs

Data Protector supports various operating systems and several processor architectures. Consequently, three DVD-ROMs are required to cover all platforms. "Data Protector DVD-ROM list" (page 23) lists the components found on the DVD-ROMs.

NOTE: Data Protector installation files for Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 systems are digitally signed by HP.

Table 3 Data Protector DVD-ROM list

DVD num.	DVD-ROM title	Contents
1	Data Protector Starter Pack for Windows Includes agents for Novell Netware and HP OpenVMS clients	• Cell Manager and Installation Server for Windows 32-bit and Windows 64-bit (AMD64/Intel EM64T) systems • HP AutoPass[1] • The complete set of English guides in the electronic PDF format (in the DOCS directory) • Windows IA-64 clients • Novell NetWare clients • HP OpenVMS clients (Alpha and IA-64 systems) • Product information • HP software integration packages
2	Data Protector Starter Pack for HP-UX Includes agents for HP-UX, Solaris, and Linux clients	• Cell Manager, Installation Server, and clients for HP-UX systems • Clients for other UNIX systems • Clients for Mac OS X systems • HP AutoPass[2] • The complete set of English guides in the electronic PDF format (in the DOCS directory) • HP software integration packages
3	Data Protector Starter Pack for Linux Includes agents for HP-UX, Solaris, and Linux clients	• Cell Manager, Installation Server, and clients for Linux systems • Clients for Solaris systems • Clients for other UNIX systems • Clients for Mac OS X systems • HP AutoPass[2] • The complete set of English guides in the electronic PDF format (in the DOCS directory) • HP software integration packages

[1] HP AutoPass is not available for Windows Server 2003 x64, Windows Vista x64, Windows Server 2008 x64, and Windows Server 2012 x64.

[2] HP AutoPass is not available for Linux.

Choosing the Cell Manager system

The Cell Manager is the main system in the Data Protector cell. The Cell Manager does the following:

- Manages the cell from one central point.
- Contains the IDB (files with information about backup, restore and media management sessions).
- Runs the core Data Protector software.
- Runs the Session Manager that starts and stops backup and restore sessions and writes session information to the IDB.

Before deciding on which system in your environment to install the Cell Manager, be aware of the following:

- Supported platforms

  The Cell Manager can be installed on either the Windows, HP-UX or Linux platform. For details on supported versions or releases of these platforms, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

- Reliability of the Cell Manager system

  Since the Cell Manager contains the IDB and since backup and restore cannot be performed if the Cell Manager is not functioning properly, it is important to choose a very reliable system in your environment for the installation.

- Database growth and required disk space

  The Cell Manager holds the Data Protector Internal Database (IDB). The IDB contains information regarding the backed up data and its media, session messages and devices. The IDB can grow to a significant size, depending on your environment. For example, if the majority of backups are filesystem backups, then a typical IDB size would be 2% of the disk space used by the backed up data. You can use the `IDB_capacity_planning.xls` table (located on any Data Protector installation DVD-ROM) to estimate the size of the IDB.

  For information on planning and managing the size and growth of the database, see the *HP Data Protector Help* index: "growth and performance of the IDB".

  For minimum disk space requirements for the IDB, see the *HP Data Protector Product Announcements, Software Notes, and References*.

NOTE: You do not have to use the Cell Manager as the graphical user interface system. For example, you may have a UNIX Cell Manager, but a user interface component installed on a Windows client.

What's next?

To determine the minimum requirements for your future Cell Manager system, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Choosing the Data Protector user interface system

Data Protector provides a GUI and CLI for Windows, HP-UX, Solaris, and Linux platforms. The user interface is installed as a Data Protector software component.

The system selected to control the cell will be used by a network administrator or a backup operator.

However, in a large computer environment, it may be desirable to run the user interface on several systems, and if the environment is a mixed one, on various platforms.

For instance, if you have a mixed UNIX network, and the user interface installed on at least one Solaris or HP-UX system, you can export the display of that user interface to any other UNIX system running an X server. However, for purposes of performance, it is recommended to install the Data Protector GUI interface on all systems that will be used to control the Data Protector cell.

If you have an office area with many Windows systems to back up, you might, as a matter of convenience, want to control local backup and restore operations from a local Windows system. In this case, install the user interface component on a Windows system. In addition, the Data Protector GUI on Windows systems is simpler to handle in heterogeneous environments, because changing the locale is not necessary.

On UNIX Cell Manager platforms, you can use the Data Protector Java GUI.

For details on supported operating system versions/releases for the user interface, see http://support.openview.hp.com/selfsolve/manuals. For more information on local language support

and usage of non-ASCII characters in file names, see the *HP Data Protector Help* index: “language settings, customizing”.

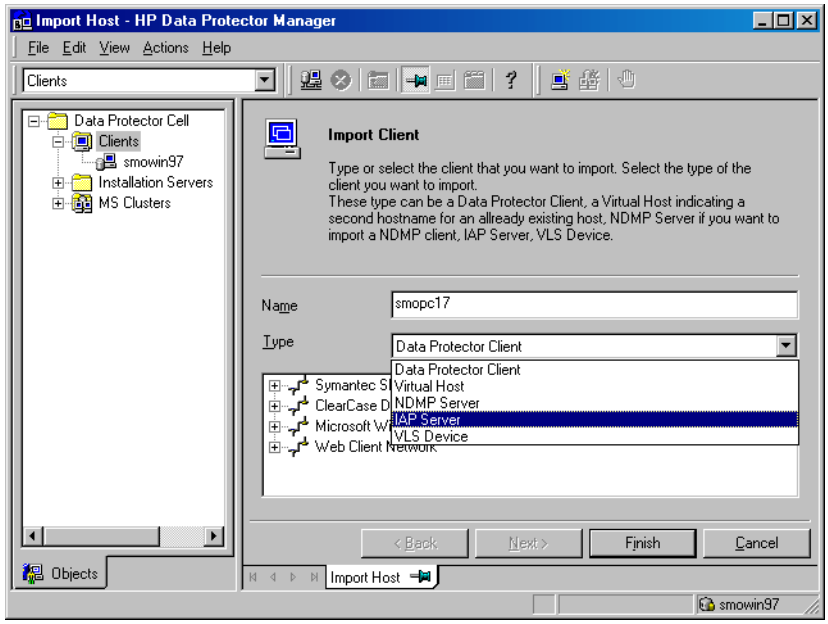
Once you have installed the user interface on a system in the cell, you can remotely access the Cell Manager from that system. You do not have to use the graphical user interface system on the Cell Manager.

The Data Protector graphical user interface

The Data Protector GUI is a powerful user interface that provides easy access to the Data Protector functionality. The main window contains several views, such as **Clients**, **Users**, **Devices & Media**, **Backup**, **Restore**, **Object Operations**, **Reporting**, **Monitor**, **Instant Recovery**, and **Internal Database**, allowing you to perform all related tasks.

For example, in the **Clients** view, you can remotely install (add) clients by specifying all the target systems and defining the installation paths and options which are sent to the specified Installation Server. When the setup on the client is running, only installation specific messages are displayed in the monitor window.

Figure 4 Data Protector graphical user interface



See also “Data Protector graphical user interface” (page 17), which defines the most important areas of the Data Protector GUI.

NOTE: On UNIX systems, locale settings must be adjusted on the system on which the Data Protector GUI is running, before starting the GUI. This will enable you to switch character encoding in GUI and thus choose the right encoding to correctly display non-ASCII characters in filenames and session messages. For details, see the *HP Data Protector Help* index: “setting, locale for GUI on UNIX”.

2 Installing Data Protector on your network

In this chapter

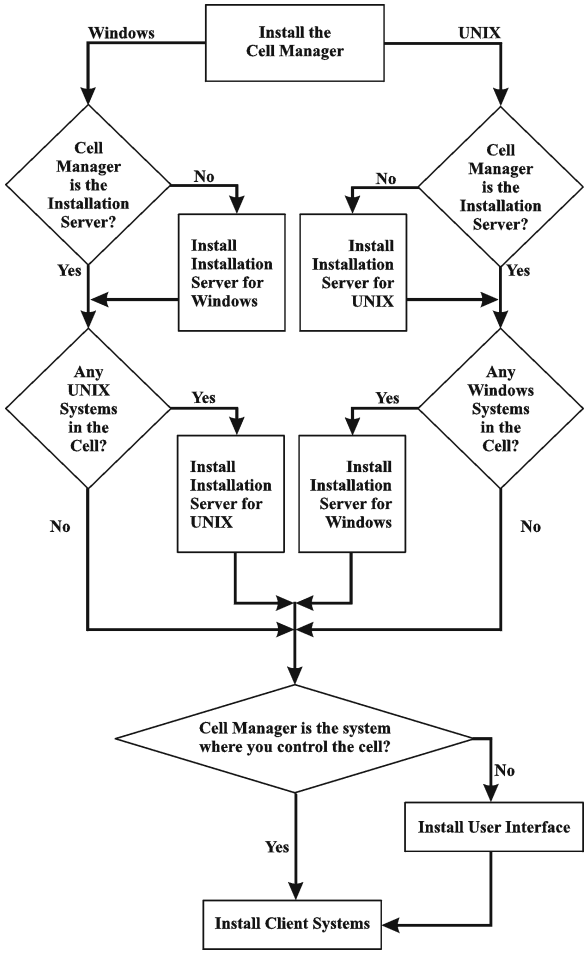
This chapter contains detailed instructions about:

- Installing the Data Protector Cell Manager (CM) and Installation Servers (IS). See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
- Installing the Data Protector clients. See "Installing Data Protector clients" (page 43).
- Installing the Data Protector integration clients. See "Installing the Data Protector integration clients" (page 89).
- Installing the localized Data Protector user interface. See "Installing localized Data Protector user interface" (page 115).
- Installing the Data Protector Single Server Edition. See "Installing the Data Protector Single Server Edition" (page 118).
- Installing Data Protector Web Reporting. See "Installing Data Protector web reporting" (page 119).
- Installing Data Protector on MC/ServiceGuard. See "Installing Data Protector on MC/ServiceGuard" (page 119).
- Installing Data Protector on a Microsoft Cluster Server. See "Installing Data Protector on Microsoft Cluster Server" (page 120).
- Installing Data Protector Clients on a Veritas Cluster. See "Installing Data Protector clients on a Veritas Cluster" (page 129).
- Installing Data Protector Clients on a Novell NetWare Cluster. See "Installing Data Protector clients on a Novell NetWare Cluster" (page 129).

Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)

For the flow of installation procedure, see "Installation procedure" (page 27).

Figure 5 Installation procedure



If you install the Cell Manager and the Installation Server on the same system, you can perform this task in one step.

IMPORTANT: All configuration and session information files in a Data Protector cell are stored on the Cell Manager. It is difficult to transfer this information to another system. Therefore, ensure that the Cell Manager is a reliable system in a stable, controlled environment.

Installing a UNIX Cell Manager

This section provides step-by-step instructions on how to install a UNIX Cell Manager. To install the Windows Cell Manager only, see "Installing a Windows Cell Manager" (page 32).

Prerequisites

- The HP-UX or Linux system that will become the Cell Manager must:
  - Have sufficient disk space for the Data Protector software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*. You can overcome a shortage of space by installing to linked directories, but you should first see "The installed directory structure on HP-UX and Linux systems" (page 29) and "Allocating more disk space for the Cell Manager installation" (page 32).
  - Have sufficient disk space (about 2% of the planned data to be backed up) for the IDB. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*. Note that the current IDB design allows the database binary files to be relocated if growth in database size makes it necessary. See the *HP Data Protector Help* index: "IDB, calculating the size of".

- Support long filenames. To find out if your filesystem supports long filenames use the `getconf NAME_MAX directory` command.
- Have the `inetd` or `xinetd` daemon up and running.
- Have the port number 5555 (default) free. If this is not the case, see "Changing the default Data Protector Inet port" (page 226).
- Have the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames.
- Have access to a DVD-ROM drive.
- Recognize the Cell Manager, if using a NIS server. See "Preparing a NIS server" (page 230).
- Have the port number 5556 free to install Java GUI Server or Java GUI Client.
- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

- You need `root` permissions on the target system.

Cluster-aware Cell Manager

Additional prerequisites and steps are required for installing a cluster-aware Cell Manager. See "Installing a cluster-aware Cell Manager" (page 120).

NOTE: In a multiple-cell environment (MoM), all Cell Managers must have the same Data Protector version installed.

Recommendation

- ***UNIX systems:*** It is recommended to use Large file support (LFS). The recommendation applies to the file systems which hold an internal database, including DC binary files that are expected to grow larger than 2 GB.

Setting kernel parameters

HP-UX systems: It is recommended to set the kernel parameter `maxdsiz` (Max Data Segment Size) or `maxdsiz_64` (for 64bit systems) to at least 134217728 bytes (128 MB), and the kernel parameter `semmnu` (Number of Semaphore Undo Structures) to at least 256. After committing these changes, recompile the kernel and restart the system.

Installation procedure

TIP: If you install the Cell Manager and Installation Server on the same system, you can perform the installation in one step by executing `omnisetup.sh -CM -IS`.

For a description of the `omnisetup.sh` command, see the `README` file located in the *`Mount_point`*`/LOCAL_INSTALL` directory on the DVD-ROM or the *HP Data Protector Command Line Interface Reference* located in the *`Mount_point`*`/DOCS/C/MAN` directory on the DVD-ROM.

Follow the procedure below to install the Cell Manager on an HP-UX or Linux system:

1. Insert and mount the appropriate UNIX installation DVD-ROM (for HP-UX or Linux) to a mount point, for example to `/dvdrom`.

   Note that the DVD-ROM filesystem uses the Rock Ridge extensions.

   Optionally, you can install Data Protector from a depot on the disk:

   - To copy the directory, where the installation files are stored, to your local disk, execute:

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     Where *platform_dir* is:

`hpux`	HP-UX systems
`linux_x86_64`	Linux systems on AMD64/Intel EM64T

   - To copy the whole DVD-ROM to your local disk, execute:

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. Execute the `omnisetup.sh` command from the DVD-ROM:

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh -CM
   ```

   To start the installation from disk:

   - If you have copied the installation directories to your local disk into *directory*, execute the commands:

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

   - If you have copied entire DVD-ROM content to *dvd_image_dir*, execute the commands:

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

3. **On HP-UX systems** `omnisetup.sh` prompts you to install or upgrade the HP AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, see "Obtaining and installing permanent passwords using the HP AutoPass utility" (page 199) and the *AutoPass License Management Online Help*. It is recommended to install AutoPass.

   If AutoPass is installed on MC/ServiceGuard, it must be installed on all nodes.

   When prompted, press **Return** to install or upgrade AutoPass. If you do not want to install or upgrade AutoPass, enter **n**.

   On Linux systems, HP AutoPass is not installed.

If you want to install an Installation Server for UNIX on your Cell Manager, you can do it at this point. For the required steps, see "Installing Installation Servers for UNIX systems" (page 38).

The installed directory structure on HP-UX and Linux systems

When the installation completes, the core Data Protector software is located in the `/opt/omni/bin` directory and the Installation Server for UNIX in the `/opt/omni/databases/vendor` directory. The following list shows the Data Protector subdirectories and their contents:

IMPORTANT: To install Data Protector to linked directories, for instance:

`/opt/omni/ -> /prefix/opt/omni/`

`/var/opt/omni/ -> /prefix/var/opt/omni/`

`/etc/opt/omni/ -> /prefix/etc/opt/omni/`

you should create the links before the installation and ensure that the destination directories exist. For more information, see "Allocating more disk space for the Cell Manager installation" (page 32).

`/opt/omni/bin`	All commands
`/opt/omni/help/C`	Data Protector Help files
`/opt/omni/lbin`	Data Protector internal commands
`/opt/omni/sbin`	Superuser commands
`/opt/omni/sbin/install`	Installation scripts
`/etc/opt/omni`	Configuration information
`/opt/omni/lib`	Shared libraries for compression, data encoding, and device handling
`/opt/omni/doc/C`	Guides in the electronic PDF format (optional)
`/var/opt/omni/log` `/var/opt/omni/server/log`	Log files
`/opt/omni/lib/nls/C`	Message catalog files
`/opt/omni/lib/man`	Man pages
`/var/opt/omni/tmp`	Temporary files
`/var/opt/omni/server/db40`	IDB files. For details, see the *HP Data Protector Help* index: "IDB, location of directories".
`/opt/omni/java/server`	Directory containing Java GUI Server executables
`/opt/omni/java/client`	Directory containing Java GUI Client executables

Configuring automatic startup and shutdown

The Data Protector installation procedure configures an automatic startup and shutdown of all Data Protector processes whenever a system is restarted. Some of this configuration is operating system dependent.

The following files are automatically configured:

HP-UX systems:

`/sbin/init.d/omni`

A script with startup and shutdown procedures.

`/sbin/rc1.d/K162omni`

A link to the `/sbin/init.d/omni` script that shuts down Data Protector.

`/sbin/rc2.d/S838omni`

A link to the `/sbin/init.d/omni` script that starts up Data Protector.

`/etc/rc.config.d/omni`

Contains an `omni` parameter defining:

`omni=1` Data Protector is automatically stopped and started at system restart. This is the default option.

`omni=0` Data Protector is not automatically stopped and started at system restart.

Linux systems:

`/etc/init.d/omni`
A script with startup and shutdown procedures.

`/etc/rc`*`init_level`*`.d/K10omni`
A link to the `/etc/init.d/omni` script that shuts down Data Protector.
Where *`init_level`* is 1 and 6.

`/etc/rc`*`init_level`*`.d/S90omni`
A link to the `/etc/init.d/omni` script that starts up Data Protector.
Where *`init_level`* is 2,3,4, and 5.

During the installation, the following system files on the Cell Manager system are modified:

HP-UX systems:

`/etc/services`
The Data Protector port number for the service is added to the file.

`/opt/omni/lbin/crs`
The Data Protector CRS service is added.

When the installation is finished, the following processes are running on the Cell Manager:

`/opt/omni/lbin/crs`
The Data Protector `Cell Request Server (CRS)` service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The CRS starts and controls backup and restore sessions in the cell.

`/opt/omni/lbin/rds`
The Data Protector `Raima Database Server (RDS)` service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The RDS manages the IDB.

`/opt/omni/lbin/mmd`
The Data Protector `Media Management Daemon (MMD)` service runs on the Cell Manager and is started when the Cell Manager software is installed on the system. The MMD manages the device and media management operations.

`/opt/omni/lbin/inetd`
The Data Protector resident service that allows communication with Data Protector services on other systems on the network. The Inet service must run on all systems in the Data Protector cell.

`/opt/omni/lbin/kms`
The Data Protector `Key Management Server (KMS)` service runs on the Cell Manager and is started when the Cell Manager software is installed on the system. The KMS provides key management for the Data Protector encryption functionality.

`/opt/omni/java/server/bin/uiproxyd`
The Data Protector Java GUI Server (`UIProxy` service) runs on the Cell Manager and is started when the Cell Manager software is installed on the system. The `UIProxy` service is responsible for communication between the Java GUI Client and the Cell Manager.

Setting environment variables

Before using Data Protector, HP recommends that you extend the values of specific environment variables in your operating system configuration:

- To enable the Data Protector man pages to be viewed from any location, add the `/opt/omni/lib/man` to the `MANPATH` variable.
- To enable the Data Protector commands to be invoked from any directory, add the command locations to the `PATH` variable. Procedures in the Data Protector documentation assume the variable value has been extended. The command locations are listed in the `omniintro`

reference page in the *HP Data Protector Command Line Interface Reference* and the `omniintro` man page.

Before launching the graphical user interface, also ensure that the `DISPLAY` variable and locale are set correctly.

NOTE: To use the Data Protector user interface for performing backups or restores across platforms, see the *HP Data Protector Product Announcements, Software Notes, and References* for the limitations incurred. For information on how to customize language settings in the Data Protector GUI, see the *HP Data Protector Help* index: "customizing language settings".

Allocating more disk space for the Cell Manager installation

You need a considerable amount of disk space to install the UNIX Cell Manager, in particular on the `/opt` directory and later on the `/var` directory where the database is stored (about 2% of the planned backup data). For details on the required disk space, see the *HP Data Protector Product Announcements, Software Notes, and References*. If you do not have enough disk space, you can use linked directories, but you must create the links before the installation and ensure that the destination directories exist.

What's next?

At this stage, the Cell Manager is installed and – if it was selected – also the Installation Server for UNIX. Your next tasks are:

1. If you have not installed an Installation Server for UNIX on the same system, see "Installing Installation Servers for UNIX systems" (page 38).
2. Install an Installation Server for Windows, if you wish to remotely install software to Windows clients. See "Installing an Installation Server for Windows" (page 40).
3. Distribute the software to clients. See "Installing Data Protector clients" (page 43).

Installing a Windows Cell Manager

Prerequisites

To install a Windows Cell Manager, you must have `Administrator` rights. The Windows system that will become your Cell Manager must meet the following requirements:

- Have a supported Windows operating system installed. For details on supported operating systems for the Cell Manager, see http://support.openview.hp.com/selfsolve/manuals.
- Have sufficient disk space for the Data Protector Cell Manager software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have sufficient disk space (about 2% of the backed up data) for the IDB. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have the port number 5555 (default) free. If this is not the case, see "Changing the default Data Protector Inet port" (page 226).
- Have a static IP address for the system on which the Cell Manager will be installed. If the system is configured as a DHCP client, its IP address changes; therefore, it is required to either assign a permanent DNS entry for the system (and reconfigure it), or to configure a DHCP server to reserve a static IP address for the system (IP address is bound to the system's MAC address).
- Have the Microsoft implementation of the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames. The computer name and the hostname must be the same.
- Have access to a DVD-ROM drive.
- Have the port number 5556 free to install Java GUI Server or Java GUI Client.

- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
- Ensure that network access user rights are set under the Windows local security policy for the account performing the installation.

Microsoft Terminal Services Client

- To install Data Protector on Windows through Microsoft Terminal Services Client, ensure that the system you want to install Data Protector on has the **Terminal Server Mode** specified as **Remote Administration**:
  1. In the Windows Control Panel, click **Administrative Tools** and then **Terminal Services Configuration**.
  2. In the Terminal Services Configuration dialog box, click **Server Settings**. Ensure that the Terminal Services server is running in the Remote Administration mode.

Recommendations

- If you expect DC binary files to grow larger than 2 GB (they are limited only by the file system settings), it is recommended to use the NTFS file system.

Cluster-aware Cell Manager

Additional prerequisites and steps are required for installing a cluster-aware Cell Manager. See "Installing a cluster-aware Cell Manager" (page 121).

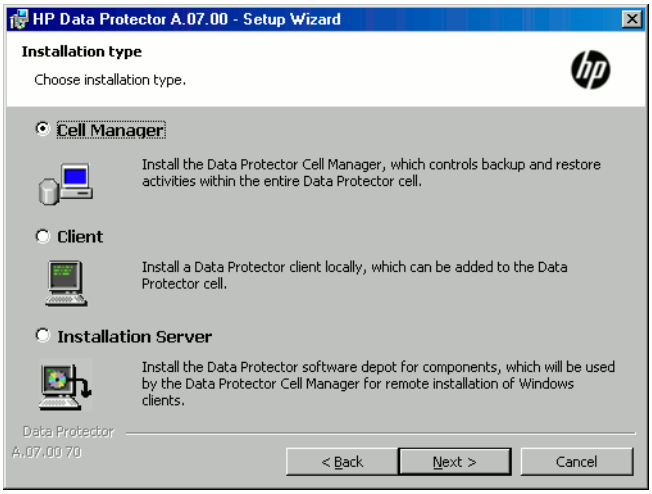
Installation procedure

To perform a new installation on a Windows system, follow these steps:

1. Insert the Windows installation DVD-ROM.

   On Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, the User Account Control dialog is displayed. Click **Continue** to proceed with the installation.
2. In the HP Data Protector window, select **Install Data Protector** to start the Data Protector Setup Wizard.
3. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
4. In the Installation Type page, select **Cell Manager** and then click **Next** to install Data Protector Cell Manager software.

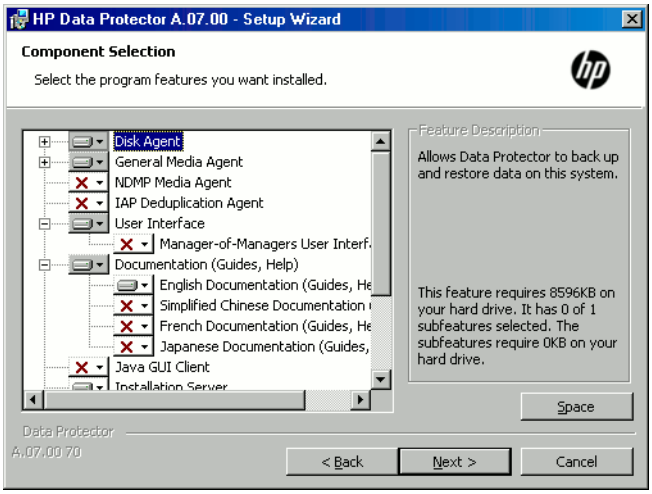
Figure 6 Selecting the installation type



5. Provide the username and password for the account under which the Data Protector services will run. Click **Next** to continue.
6. Click **Next** to install Data Protector in the default folder.

   Otherwise, click **Change** to open the Change Current Destination Folder window and enter a new path.
7. In the Component Selection page, select the components you want to install. For a list and descriptions of the Data Protector components, see "Data Protector components" (page 45).

Figure 7 Selecting software components



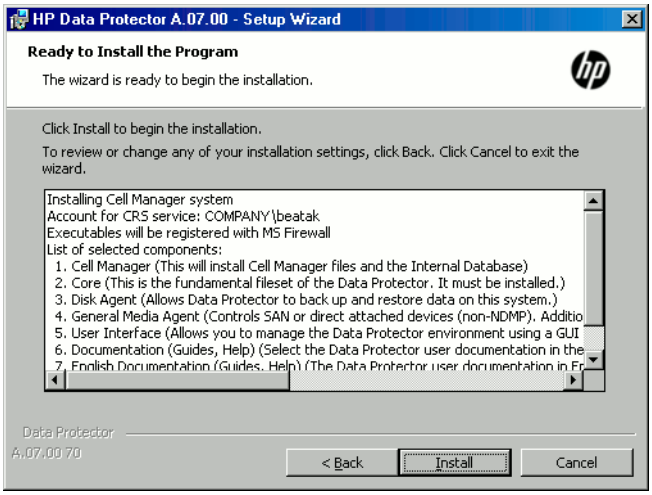
Disk Agent, **General Media Agent**, **User Interface**, and **Installation Server** are selected by default. Click **Next**.

8. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

   Note that only inbound firewall rules are automatically created and you must manually create any outbound firewall rules. For the required port ranges, see the *HP Data Protector Help* index: "firewall support".

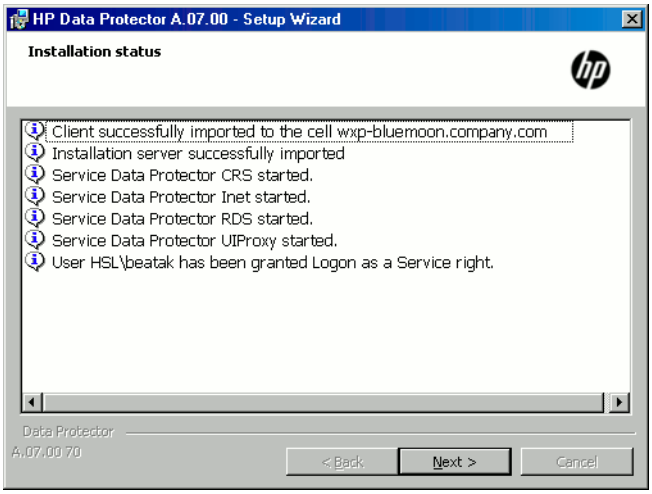
   Click **Next**.
9. The component summary list is displayed. Click **Install** to start installing the selected components. This may take several minutes.

Figure 8 Component summary list



10. The **Installation status** page is displayed. Click **Next**.

Figure 9 Installation status page



11. The Setup Wizard enables you to install or upgrade the HP AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, see "Obtaining and installing permanent passwords using the HP AutoPass utility" (page 199) and the *AutoPass License Management Online Help*.

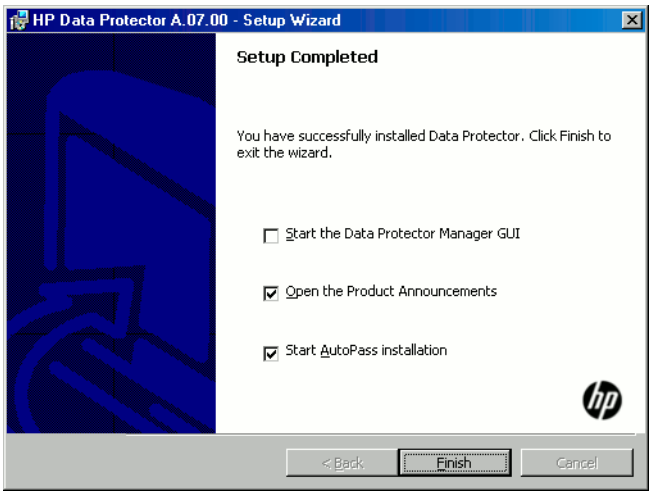
    By default, the **Start AutoPass installation** or the **Upgrade AutoPass installation** option is selected. It is recommended to install the HP AutoPass utility. If you do not want to install or upgrade AutoPass, deselect the option.

    On Windows Server 2003 x64, Windows Vista x64, Windows Server 2008 x64, and Windows Server 2012 x64 systems, HP AutoPass is not installed.

    To start using Data Protector immediately after setup, select **Start the Data Protector Manager GUI**.

    To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

Figure 10 Selecting AutoPass for installation



Click **Finish**.

After the installation

The Cell Manager files are located in the *Data_Protector_home* directory, on Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, also in *Data_Protector_program_data*.

The software depot is located in *Data_Protector_home*\Depot, except for Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, where it is located in the *Data_Protector_program_data*\Depot directory.

The Data Protector commands are located in the directories, listed in the omniintro reference page in the *HP Data Protector Command Line Interface Reference* and the omniintro man page.

IMPORTANT: HP recommends that you enable invocations of the Data Protector commands from any directory by extending the value of the appropriate environment variable in your operating system configuration with the command locations. Procedures in the Data Protector documentation assume the value has been extended.

The following processes are running on the Cell Manager system:

crs.exe	The Data Protector Cell Request Server (CRS) service runs on the Cell Manager system and is started when the Cell Manager software is installed

	on the system. The CRS starts and controls backup and restore sessions in the cell. It runs in the *Data_Protector_home*\bin directory.
rds.exe	The Data Protector Raima Database Server (RDS) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The RDS manages the IDB. It runs in the *Data_Protector_home*\bin directory.
mmd.exe	The Data Protector Media Management Daemon (MMD) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The MMD manages the device and media management operations. It runs in the *Data_Protector_home*\bin directory.
omniinet.exe	The Data Protector client service that enables the Cell Manager to start agents on other systems. The Data Protector Inet service must run on all systems in the Data Protector cell. It runs in the *Data_Protector_home*\bin directory.
kms.exe	The Data Protector Key Management Server (KMS) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The KMS provides key management for the Data Protector encryption functionality. It runs in the *Data_Protector_home*\bin directory.
uiproxy.exe	The Data Protector Java GUI Server (UIProxy service) runs on the Cell Manager system in the *Data_Protector_home*\java\server\bin directory. The UIProxy service is responsible for communication between the Java GUI Client and the Cell Manager.

NOTE: If you intend to use the Data Protector user interface to perform backups or restores across platforms, see the *HP Data Protector Product Announcements, Software Notes, and References* for the limitations incurred.

TIP: You can install additional code page conversion tables to correctly display filenames, if the appropriate encoding is not available from the Data Protector GUI. For detailed steps, see the operating system documentation.

Troubleshooting

In case of an unsuccessful setup, try to verify the requirements that are checked by Setup itself and what could have caused the failure if they had not been fulfilled. See "Prerequisites" (page 32).

This is the list of the requirements checked by Setup:

- Service Pack version
- nslookup, so that Data Protector is able to expand hostnames
- disk space
- administrative rights

What's next?

At this stage, the Cell Manager is installed and – if it was selected – also the Installation Server for Windows. Your next tasks are:

1. Install the Installation Server for UNIX, if you have a mixed backup environment. See "Installing Installation Servers" (page 38). Skip this step if you do not need the Installation Server for UNIX.
2. Distribute the software to clients. See "Installing Data Protector clients" (page 43).

Installing Installation Servers

Installation Servers can be installed on the Cell Manager system or any supported system that is connected to the Cell Manager by a LAN. For details on supported operating systems for the Installation Server, see http://support.openview.hp.com/selfsolve/manuals.

To keep the Installation Servers on systems separate from the Cell Manager, install the corresponding software depot locally. The detailed procedure is described in this section.

Installing Installation Servers for UNIX systems

Prerequisites

The system that will become your Installation Server must meet the following requirements:

- Have the HP-UX or Linux operating system installed. For details on supported operating systems for the Installation Server, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have the `inetd` or `xinetd` daemon up and running.
- Have the port number 5555 (default) free. If this is not the case, see "Changing the default Data Protector Inet port" (page 226).
- Have the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames.
- Have enough disk space for the complete Data Protector software depot. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have a DVD-ROM drive.
- The Cell Manager in the Data Protector cell must be of the 7.00 version.

IMPORTANT: To install Data Protector to linked directories, for instance:

`/opt/omni/ -> /prefix/opt/omni/`

`/etc/opt/omni/ -> /prefix/etc/opt/omni/`

`/var/opt/omni/ -> /prefix/var/opt/omni/`

Create the links before the installation and ensure that the destination directories exist.

NOTE: To install software from a device across the network, first mount the source directory on your computer.

Installation procedure

Follow these steps to install the Installation Server for UNIX systems on an HP-UX or Linux system:

1. Insert and mount the appropriate UNIX installation DVD-ROM (for HP-UX or Linux) to a mount point, for example to `/dvdrom`.

   Note that the DVD-ROM filesystem uses the Rock Ridge extensions.

   Optionally, you can install Data Protector from a depot on the disk:

   - To copy the directory, where the installation files are stored, to your local disk, execute:

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     Where *platform_dir* is:

`hpux`	HP-UX systems
`linux_x86_64`	Linux systems on AMD64/Intel EM64T

   - To copy the whole DVD-ROM to your local disk, execute:

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. Execute the `omnisetup.sh` command from the DVD-ROM:

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh -IS
   ```

   To start the installation from disk:

   - If you have copied the installation directories to your local disk into *directory*, execute the commands:

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh -IS
     ```

   - If you have copied entire DVD-ROM content to *dvd_image_dir*, execute the commands:

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ./omnisetup.sh -IS
     ```

   For a description of the `omnisetup.sh` command, see the `README` file located in the *Mount_point/* directory on the DVD-ROM or to the *HP Data Protector Command Line Interface Reference* located in the *Mount_point*`/DOCS/C/MAN` directory on the DVD-ROM.

When the installation is finished, the software depot for UNIX is located in the `/opt/omni/databases/vendor` directory.

The `omnisetup.sh` command installs the Installation Server with all packages. To install only a subset of the packages, use `swinstall` (for HP-UX) or `rpm` (for Linux). See "Installing on HP-UX and Linux systems using native tools" (page 219).

IMPORTANT: If you do not install the Installation Server for UNIX on your network, you will have to install every UNIX client locally from the UNIX installation DVD-ROM (for HP-UX or Linux). Furthermore, patching of components on Data Protector clients will not be possible.

NOTE: If you install the User Interface component (either the graphical user interface or the command-line interface), update your environment variables before using it. For more information, see "Setting environment variables" (page 31).

If you intend to use the Data Protector user interface to perform backups or restores across platforms, see the *HP Data Protector Product Announcements, Software Notes, and References* for the limitations incurred.

What's next?

At this point, you should have the Installation Servers for UNIX installed on your network. Your next tasks are:

1. If you installed the Installation Server on a different system than the Cell Manager, you must manually add (import) the system to the Data Protector cell. See "Importing an installation server to a cell" (page 133).

   NOTE: When an Installation Server is imported, the file `/etc/opt/omni/server/cell/installation_servers` on the Cell Manager is updated to list the installed remote installation packages. This can be used from the CLI to check the available remote installation packages. For this file to be kept up to date, you should export and re-import an Installation Server whenever remote installation packages are installed or deleted. This applies even if an Installation Server is installed on the same system as the Cell Manager.

2. If you have any Windows systems in your Data Protector cell, install the Installation Server for Windows. See "Installing an Installation Server for Windows" (page 40).
3. Distribute the software to clients. See "Installing Data Protector clients" (page 43).

Installing an Installation Server for Windows

Prerequisites

A Windows system that will become your future Installation Server must meet the following requirements:

- Have one of the supported Windows operating systems installed. For details on supported operating systems for the Installation Server, see http://support.openview.hp.com/selfsolve/manuals.
- Have enough disk space for the complete Data Protector software depot. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have access to a DVD-ROM drive.
- Have the Microsoft implementation of the TCP/IP protocol up and running. The protocol must be able to resolve hostnames. The computer name and the hostname must be the same.

Limitations

- Due to the security restrictions imposed by the Windows operating system, Installation Server can be used to remotely install clients only in the same domain.

IMPORTANT: If you do not install the Installation Server for Windows on your network, you will have to install every Windows client locally from the DVD-ROM.

NOTE: You cannot remotely install a Data Protector client on the Windows system after an Installation Server has been installed on this system. To install an Installation Server and client component(s) on the same system, you must perform a local client installation. During the installation procedure, select all desired client components and the Installation Server component. See "Installing Windows clients" (page 48).

Installation procedure

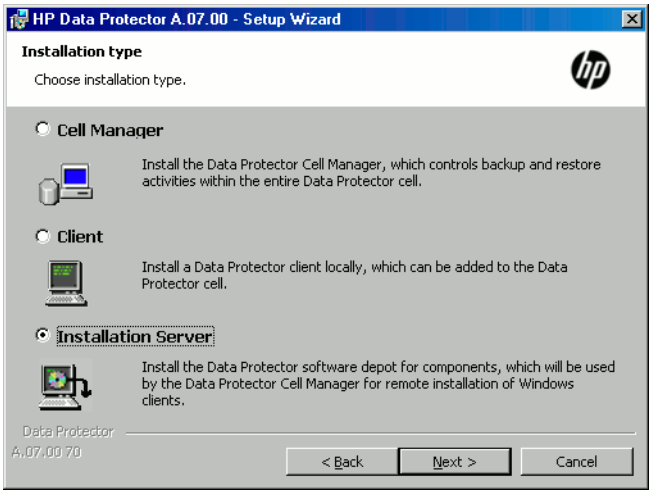
Follow these steps to install the Installation Server for Windows systems:

1. Insert the Windows installation DVD-ROM.

   On Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, the User Account Control dialog is displayed. Click **Continue** to proceed with the installation.

2. In the HP Data Protector window, select **Install Data Protector** to start the Data Protector Setup Wizard.
3. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
4. In the **Installation Type** page, select **Installation Server** and then click **Next** to install Data Protector software depot.

Figure 11 Selecting the installation type



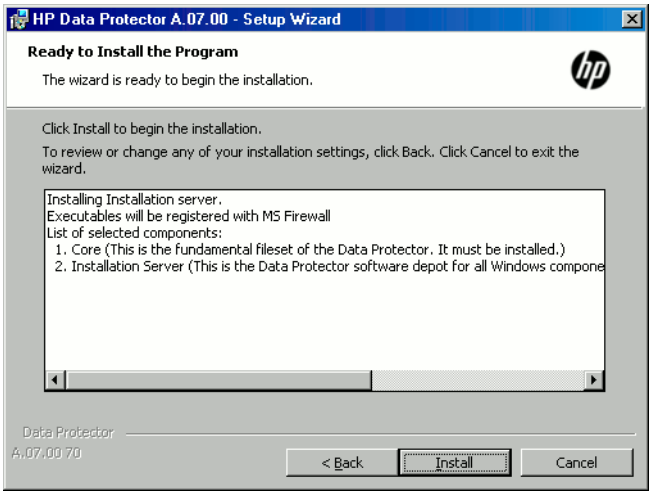
5. Click **Next** to install Data Protector on the default folder.

   Otherwise, click **Change** to open the Change Current Destination Folder window and enter a new path.
6. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

   Note that only inbound firewall rules are automatically created and you must manually create any outbound firewall rules. For the required port ranges, see the *HP Data Protector Help* index: “firewall support”.

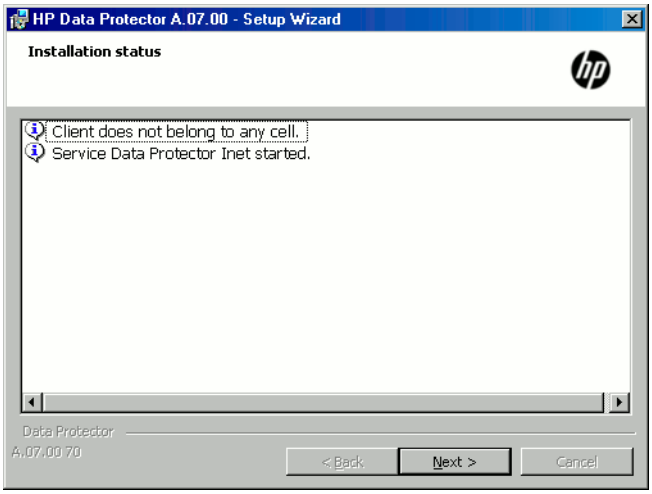
   Click **Next**.
7. The component summary list is displayed. Click **Install** to start installing the selected components. This may take several minutes.

Figure 12 Component selection summary page



8. The Installation status page is displayed. Click **Next**.

Figure 13 Installation status page



9. To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

   Click **Finish**.

As soon as the installation is finished, the software is, by default, installed in the directory `Data_Protector_program_data\Depot` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012) or `Data_Protector_home\Depot` (other Windows systems). The software is shared so that it can be accessed from the network.

What's next?

At this point, you should have Installation Server for Windows installed on your network. Now you should perform the following tasks:

1. If you have set up an independent Installation Server (for example, not on the Cell Manager) you must manually add (import) the system to the Data Protector cell. See "Importing an installation server to a cell" (page 133).
2. Install an Installation Server for UNIX on HP-UX or Linux if you have a mixed backup environment. See "Installing Installation Servers for UNIX systems" (page 38).
3. Distribute the software to clients. See "Installing Data Protector clients" (page 43).

Installing Data Protector clients

You can install the Data Protector clients *remotely*, by distributing them using the Installation Server, or *locally*, from the appropriate installation DVD-ROM.

For the list of Data Protector installation DVD-ROMs, see "Data Protector installation DVD-ROMs" (page 22).

After you have installed the clients, HP recommends that you enable invocations of the Data Protector commands from any directory by adding the command locations to the appropriate environment variable on each client. Procedures in the Data Protector documentation assume the variable value has been extended. Command locations are listed in the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* and the `omniintro` man page.

After installing and importing the Data Protector clients into the cell, it is also highly recommended to verify the installation and to protect clients from unwarranted access. For procedure on verifying the client installation, see "Verifying Data Protector client installation" (page 213). For more information on security protection, see "Security considerations" (page 137).

"Installing Data Protector clients" (page 43) lists Data Protector client systems with references to detailed descriptions.

Table 4 Installing Data Protector client systems

Client system	Installation type and reference
Windows	Remote and local installation; see "Installing Windows clients" (page 48).
HP-UX	Remote and local installation; see "Installing HP-UX clients" (page 51).
Solaris	Remote and local installation; see "Installing Solaris clients" (page 54).
Linux	Remote and local installation; see "Installing Linux clients" (page 59).
ESX Server	Remote and local installation; see "Installing ESX Server clients" (page 62).
Mac OS X	Remote and local installation; see "Installing Mac OS X clients" (page 62).
IBM AIX	Remote and local installation; see "Installing IBM AIX clients" (page 63).
Tru64	Remote and local installation; see "Installing Tru64 clients" (page 64).
SCO	Remote and local installation; see "Installing SCO clients" (page 66).
HP OpenVMS	Local installation; see "Installing HP OpenVMS clients" (page 67).
Novell NetWare	Local installation; see "Installing Novell NetWare clients" (page 72).
other UNIX system	Local installation; see "Local installation on UNIX and Mac OS X systems" (page 81).
DAS Media Agent client	Remote and local installation; see "Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library" (page 84).
ACS Media Agent client	Remote and local installation; see "Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library" (page 84).

Integrations

Data Protector integrations are software components that allow you to back up database applications with Data Protector. The systems running database applications are installed the same way as any Windows or UNIX client systems, provided that the appropriate software component has been selected (for example, the `MS Exchange Integration` component for backing up the Microsoft Exchange Server database, `Oracle Integration` component for backing up an Oracle database, and so on). For the references, see "Installing integrations" (page 44).

Table 5 Installing integrations

Software application or disk array family	Reference
Microsoft Exchange Server	See "Microsoft Exchange Server clients" (page 92).
Microsoft SQL Server	See "Microsoft SQL Server clients" (page 94).
Microsoft SharePoint Server	See "Microsoft SharePoint Server clients" (page 94).
Microsoft Volume Shadow Copy Service (VSS)	See "Microsoft Volume Shadow Copy Service clients" (page 96).
Sybase Server	See "Sybase Server clients" (page 96).
Informix Server	See "Informix Server clients" (page 96).
SAP R/3	See "SAP R/3 clients" (page 97).
SAP MaxDB	See "SAP MaxDB clients" (page 97).
SAP HANA Appliance	See "SAP HANA Appliance clients" (page 97).
Oracle Server	See "Oracle Server clients" (page 97).
IBM DB2 UDB	See "IBM DB2 UDB clients" (page 98).
Lotus Notes/Domino Server	See "Lotus Notes/Domino Server clients" (page 98).
VMware	See "VMware clients" (page 98).
Microsoft Hyper-V	See "Microsoft Hyper-V clients" (page 100).
HP Network Node Manager (NNM)	See "HP NNM clients" (page 101).
Network Data Management Protocol (NDMP) Server	See "NDMP Server clients" (page 101).
HP P4000 SAN Solutions	See "HP P4000 SAN Solutions clients" (page 101).
HP P6000 EVA Disk Array Family	See "HP P6000 EVA Disk Array Family clients" (page 102).
HP P9000 XP Disk Array Family	See "HP P9000 XP Disk Array Family clients" (page 106).
HP P10000 Storage Systems	See "HP P10000 Storage Systems clients" (page 111).
EMC Symmetrix	See "EMC Symmetrix clients" (page 111).

Table 6 Other installations

Installation	Reference
Virtual Library System (VLS) automigration	See "VLS automigration clients" (page 114).
Localized user interface	See "Installing localized Data Protector user interface" (page 115).
Web reporting	See "Installing Data Protector web reporting" (page 119).
MC/ServiceGuard	See "Installing Data Protector on MC/ServiceGuard" (page 119).
Microsoft Cluster Server	See "Installing Data Protector on Microsoft Cluster Server" (page 120).
Microsoft Hyper-V cluster	See "Installing Data Protector on a Microsoft Hyper-V cluster" (page 128).

Table 6 Other installations *(continued)*

Installation	Reference
Veritas Cluster Server	See "Installing Data Protector clients on a Veritas Cluster" (page 129).
Novell NetWare Cluster	See "Installing Data Protector clients on a Novell NetWare Cluster" (page 129).
IBM HACMP Cluster	See "Installing Data Protector on IBM HACMP Cluster" (page 130).

Data Protector components

For the latest information on the supported platforms, visit the HP Data Protector home page at http://support.openview.hp.com/selfsolve/manuals.

These are the Data Protector components you can select and their descriptions:

User Interface

The User Interface component includes the Data Protector graphical user interface on Windows systems and part of the command-line interface on Windows and UNIX systems. The software is needed to access the Data Protector Cell Manager and must be installed at least to the system that is used for managing the cell.

NOTE: Specific commands of the Data Protector command-line interface are included in other Data Protector components. For details, see the *HP Data Protector Command Line Interface Reference*.

Before using the Data Protector User Interface in heterogeneous environments, see the *HP Data Protector Product Announcements, Software Notes, and References* for the limitations incurred.

Java GUI Client

The Data Protector Java GUI is a Java-based graphical user interface with a client-server architecture. It contains the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface. The Java GUI Client will not be selected for installation by default; you have to select it manually. To install the command-line interface to a client with Java GUI installed, also install the User Interface or another appropriate Data Protector component to that system.

English Documentation (Guides, Help)

This is the Data Protector English language documentation file set.

French Documentation (Guides, Help)

This is the Data Protector French language documentation file set.

Japanese Documentation (Guides, Help)

This is the Data Protector Japanese language documentation file set.

Simplified Chinese Documentation (Guides, Help)

This is the Data Protector Simplified Chinese language documentation file set.

Manager-of-Managers User Interface

The Manager-of-Managers User Interface includes the Data Protector graphical user interface. The software is needed to access the Data Protector Manager-of-Managers functionality and control the multi-cell environment. The Manager-of-Managers User Interface and the Manager User Interface are available as a common application.

Disk Agent

The Disk Agent component must be installed on systems that have disks that will be backed up with Data Protector.

General Media Agent	The General Media Agent component must be installed on systems that have backup devices connected or have access to a library robotics and will be managed by Data Protector.
VLS Automigration	The VLS Automigration component must be installed on clients that will perform Virtual Library System (VLS) smart media copying using Data Protector.
Automatic Disaster Recovery	The Automatic Disaster Recovery component must be installed on systems for which you want to enable recovery using any of the automatic disaster recovery methods and on systems where the DR CD ISO image for Enhanced Automated Disaster Recovery (EADR) or One Button Disaster Recovery (OBDR) will be prepared to provide automatic preparation for the disaster recovery.
SAP R/3 Integration	The SAP R/3 Integration component must be installed on systems that have an SAP R/3 database that will be backed up with Data Protector.
SAP DB Integration	The SAP DB Integration component must be installed on systems that have an SAP MaxDB database that will be backed up using Data Protector.
SAP HANA Integration	The SAP HANA Integration component must be installed on systems that represent or constitute an SAP HANA Appliance that you want to protect using Data Protector.
Oracle Integration	The Oracle Integration component must be installed on systems that have an Oracle database that will be backed up with Data Protector.
VMware Integration (Legacy)	The VMware Integration (Legacy) component must be installed on VirtualCenter systems (if they exist) and all the ESX Server systems that you plan to back up with Data Protector. If you plan to use the VCBfile or VCBimage backup methods, the integration component must also be installed on the backup proxy systems.
Virtual Environment Integration	The Virtual Environment Integration component must be installed on the systems which you will use as backup hosts to control the backup and restore of virtual machines using the Data Protector Virtual Environment integration.
DB2 Integration	The DB2 Integration component must be installed on all systems that have a DB2 Server that will be backed up with Data Protector.
Sybase Integration	The Sybase Integration component must be installed on systems that have a Sybase database that will be backed up with Data Protector.
Informix Integration	The Informix Integration component must be installed on systems that have an Informix Server database that will be backed up with Data Protector.
MS Exchange Integration	The MS Exchange Integration component must be installed on Microsoft Exchange Server 2003/2007 systems that you intend to back up using the Data Protector Microsoft Exchange Server 2003/2007 integration or the Data Protector Microsoft Exchange Single Mailbox integration. It must also be installed on Microsoft Exchange Server 2010 systems that you intend to back up using the Data Protector Microsoft Exchange Single Mailbox integration.
MS Exchange Server 2010 Integration	The MS Exchange Server Integration component must be installed on Microsoft Exchange Server 2010 systems that you intend to back up using the Data Protector Microsoft Exchange Server 2010 integration.
MS SQL Integration	The SQL Integration component must be installed on the systems that have an Microsoft SQL Server database which will be backed up with Data Protector.

MS SharePoint Portal Server Integration	The MS SharePoint Portal Server Integration component must be installed on Microsoft SharePoint Portal Server systems that will be backed up with Data Protector.
MS SharePoint 2007/2010/2013 Integration	The MS SharePoint 2007/2010/2013 Integration component must be installed on Microsoft SharePoint Server 2007/2010/2013 systems that will be backed up with Data Protector.
MS Volume Shadow Copy Integration	The MS Volume Shadow Copy Integration component must be installed on the Windows Server systems where you want to run backups coordinated by Volume Shadow Copy Service.
HP P4000 Agent	The HP P4000 Agent component must be installed on the application and the backup system to integrate HP P4000 SAN Solutions with Data Protector.
HP P6000 EVA SMI-S Agent	The HP P6000 EVA SMI-S Agent component must be installed on the application and the backup system to integrate HP P6000 EVA Disk Array Family with Data Protector.
HP P9000 XP Agent	The HP P9000 XP Agent component must be installed on the application and the backup system to integrate HP P9000 XP Disk Array Family with Data Protector.
HP P10000 Agent	The HP P10000 Agent component must be installed on the application and the backup system to integrate HP P10000 Storage Systems with Data Protector.
EMC Symmetrix Agent	The EMC Symmetrix Agent component must be installed on the application and backup system to integrate EMC Symmetrix with Data Protector.
HP Network Node Manager Integration	The NNM Integration component must be installed on all systems in the cell that have an NNM database that will be backed up with Data Protector.
NDMP Media Agent	The NDMP Media Agent component must be installed on all systems that will be backing up data to NDMP dedicated drives through an NDMP server.
Lotus Integration	The Lotus Integration component must be installed on all systems in the Data Protector cell that have Lotus Notes/Domino Server databases that you plan to back up with Data Protector.
MS Exchange Granular Recovery Extension	The Data Protector Granular Recovery Extension for Microsoft Exchange Server must be installed on each Microsoft Exchange Server system to enable the granular recovery feature. In a Microsoft Exchange Server Database Availability Group (DAG) environment, it must be installed on any of the Exchange Server systems in DAG. Only remote installation is supported.
MS SharePoint Granular Recovery Extension	The Data Protector Granular Recovery Extension for Microsoft SharePoint Server must be installed on the Microsoft SharePoint Server Central Administration system.
VMware Granular Recovery Extension Web Plug-In	The Data Protector VMware Granular Recovery Extension Web Plug-In component must be installed on the VMware Virtual Server system to enable the granular recovery feature of the VMware virtual machines. Only remote installation is supported.
VMware Granular Recovery Extension Agent	The Data Protector VMware Granular Recovery Extension Agent component must be installed on the mount proxy system to enable restore and granular recovery of the VMware virtual machines. Only remote installation is supported.

NOTE: You cannot install the General Media Agent and the NDMP Media Agent on the same system.

Installing Windows clients

For details on supported platforms and components for a particular Windows operating system, see http://support.openview.hp.com/selfsolve/manuals.

Prerequisites

To install a Windows client, you must have the Administrator rights. The Windows system that will become your future Data Protector client system must meet the following requirements:

- Have sufficient disk space for the Data Protector client software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have port number 5555 (default) free.
- Have the Microsoft implementation of the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames. The computer name and the hostname must be the same.
- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
- Ensure that network access user rights are set under the Windows local security policy for the account performing the installation.

Limitations

- Due to the security restrictions imposed by the Windows operating system, Installation Server can be used to remotely install clients only in the same domain.
- On Windows XP Home Edition, Data Protector clients can only be installed locally.
- When installing clients remotely to Windows Vista, Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012, use one of the following accounts:
  - A built-in administrator account on the remote system. The account must be enabled and with disabled *Admin Approval Mode*.
  - A domain user account, which is a member of the local Administrators user group on the remote system.

Automatic disaster recovery

The `Automatic Disaster Recovery` component must be installed on systems for which you want to enable recovery using Enhanced Automated Disaster Recovery (EADR), One Button Disaster Recovery (OBDR), or Automated System Recovery (ASR), and on systems where the DR CD ISO image for EADR or OBDR will be prepared.

Cluster-aware clients

Additional prerequisites are required for installing cluster-aware clients. For more details, see "Installing cluster-aware clients" (page 126).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Local installation

Windows clients can be installed locally, from the Windows installation DVD-ROM:

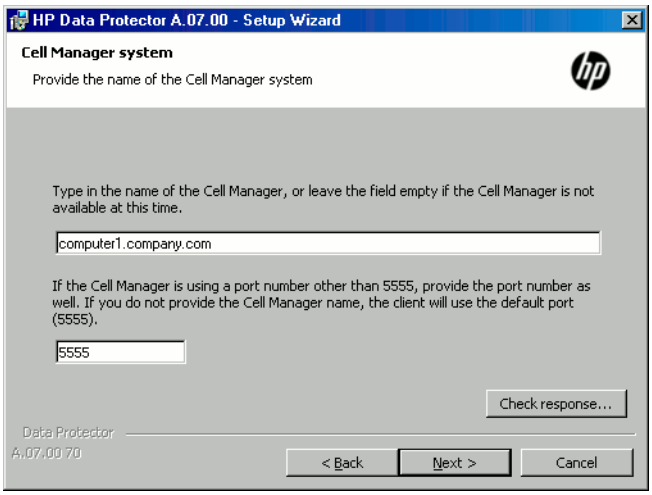
1. Insert the DVD-ROM.

   On Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, the User Account Control dialog box is displayed. Click **Continue** to proceed with the installation.
2. In the HP Data Protector window, select **Install Data Protector** to start the Data Protector Setup Wizard.
3. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
4. In the **Installation Type** page, select **Client**. For Itanium clients, the type is selected automatically.
5. Enter the name of the Cell Manager. See "Choosing the Cell Manager" (page 49).

   If your Cell Manager uses a different port then the default 5555, change the port number. You can test if the Cell Manager is active and uses the selected port by clicking **Check response**.

   Click **Next**.

Figure 14 Choosing the Cell Manager



6. Click **Next** to install Data Protector on the default folder.

   Otherwise, click **Change** to open the Change Current Destination Folder page and enter the path.
7. Select the Data Protector components that you want to install.

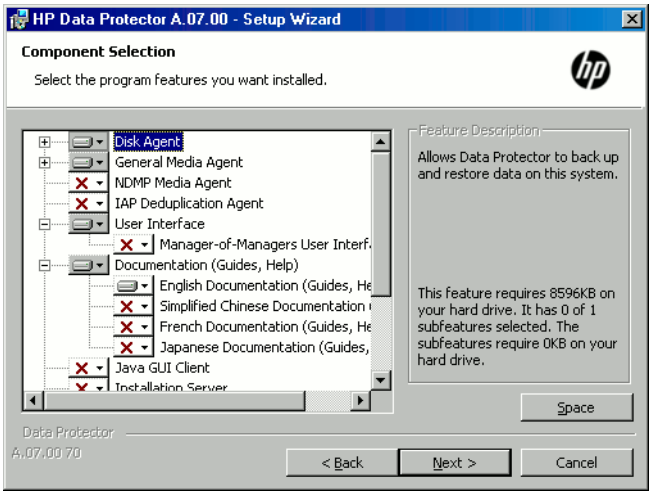
   For information on other Data Protector components, see "Data Protector components" (page 45).

   Click **Next**.
8. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

   Note that only inbound firewall rules are automatically created and you must manually create any outbound firewall rules. For the required port ranges, see the *HP Data Protector Help* index: "firewall support".

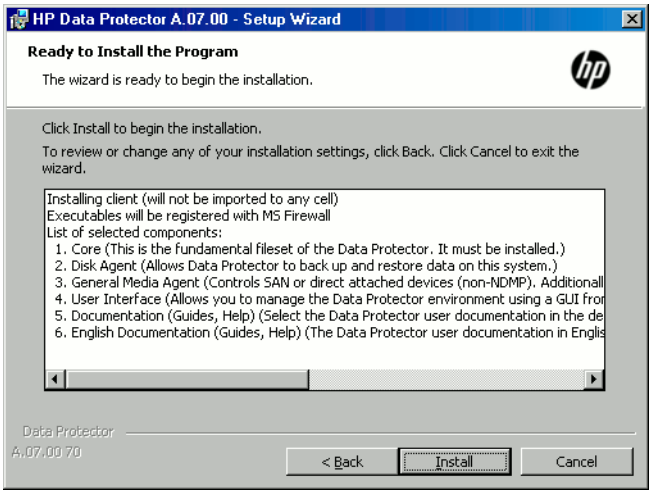
   Click **Next**.
9. The component selection summary page is displayed. Click **Install** to install the selected components.

Figure 15 Component selection summary page



10. The Installation status page is displayed. Click **Next**.

Figure 16 Installation summary page



11. To start using Data Protector immediately after setup, select **Start the Data Protector Manager GUI**.

    To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

    Click **Finish**.

Connecting a backup device to Windows systems

Once you have installed a Media Agent component, you can attach a backup device to a Windows system by performing the following steps:

1. Find the available SCSI addresses (referred to as *SCSI Target IDs* on Windows) for the drives and control device (robotics) of the backup device you want to connect. See "Finding unused SCSI target IDs on Windows systems" (page 243).
2. Set unused `SCSI Target IDs` for the drives and control device (robotics). Depending on the device type, this can usually be done with switches on the device. For details, see the documentation that comes with the device.

   For information about supported devices, see http://support.openview.hp.com/selfsolve/manuals.

3. Switch off your computer and connect your backup device to the system.
4. Switch on the device, then the computer, and wait until the boot process completes.
5. To verify that the system correctly recognizes your new backup device, in the *Data_Protector_home*\bin directory, run the `devbra -dev` command.

   See a new device listed in the output of the command. For example, you might get the following output from the `devbra -dev` command:

   - If the tape driver for your device is loaded:

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

     The first line represents the device specification, the second one is the device filename.

     The path format says that an HP DDS tape device has Drive instance number 3 and is connected to SCSI bus 0, SCSI Target ID 4, and LUN number 0.

   - If the tape driver for your device is unloaded:

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

     The first line represents the device specification, the second one provides the device filename.

     The path format says that an HP DDS tape device is connected to SCSI port 1, SCSI bus 0, and the tape drive has the SCSI Target ID 4, and LUN number 0.

For loading or unloading the native tape driver for your device, see "Using tape and robotics drivers on Windows systems" (page 232). For more information on creating a device filename, see "Creating device files (SCSI Addresses) on Windows systems" (page 233).

What's next?

At this stage, you should have client components installed and backup devices connected, so that you are able to configure backup devices and media pools. For information on configuration tasks, see the *HP Data Protector Help* index: "configuring, backup devices".

Installing HP-UX clients

HP-UX clients can be installed remotely using the Installation Server for UNIX, or locally from the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX installed on your network. If not, for instructions see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

- You will need either *root* access or an account with *root* capabilities.
- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Remote installation

You install the client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

After the remote installation, the client system automatically becomes a member of the Data Protector cell.

If you have installed a Media Agent on your client, you must physically connect the backup device to the system. To see if the device drivers, appropriate for the type of your device, are already build in the kernel, check your kernel configuration before running a backup.

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

After the local installation, the client system has to be manually imported into the cell. See "Importing clients to a cell" (page 132).

Cluster-aware clients

Additional prerequisites and steps are required for installing cluster-aware clients. For more details, see "Installing cluster-aware clients" (page 120).

Checking the kernel configuration on HP-UX

The following procedure explains how to check and build your kernel configuration on the HP-UX 11.x, using the *HP System Administration Manager (SAM)* utility. For instructions on how to build the kernel manually, see "SCSI robotics configuration on HP-UX systems" (page 234).

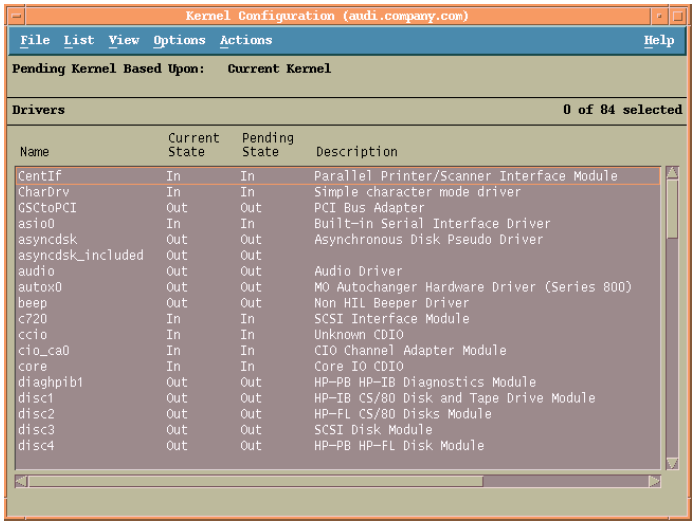
Follow this procedure to build the kernel configuration using the *HP System Administration Manager (SAM)* utility:

1. Log in as a `root` user, open the terminal and type `sam`.
2. In the **System Administration Manager** window, double-click **Kernel Configuration**, and then **Drivers**.

3. In the **Kernel Configuration** window, verify the following:
   - The drivers for the devices you will be using must be listed among the installed drivers. See "Kernel configuration Window" (page 53). If the driver you are looking for is not listed, you have to install it using the `/usr/sbin/swinstall` utility. For example:
     - A Tape Device Driver is required for tape devices and must be installed if you have connected a tape device to the system. For example, for generic SCSI tape drives, like DLT or LTO, the `stape` driver is used, and for DDS devices the `tape2` driver.
     - A SCSI Pass-Through driver named `sctl` or `spt`, or an autochanger robotics driver named `schgr` (depending on the hardware) is required to control robotics in Tape library devices.

       For details, see "SCSI robotics configuration on HP-UX systems" (page 234).

Figure 17 Kernel configuration Window



   - The status of a driver that is displayed in the **Current State** column must be set to **In**. If the status value is set to **Out**, proceed as follows:
     1. Select the driver in the list. Click **Actions** and select **Add Driver to Kernel**. In the **Pending State** column, the status will be set to `In`.

        Repeat this for each driver for which the **Current State** is **In**.
     2. Click **Actions** and select **Create a New Kernel** to apply the changes, that is to build a **Pending Kernel** into the **Current Kernel**. The action requires a restart of the system.

Once you have all the required drivers built in the kernel, you can continue by connecting a backup device to your system.

Connecting a backup device to HP-UX systems

1. Determine the available SCSI addresses for the drives and control device (robotics). Use the `/usr/sbin/ioscan -f` system command.

   For more information, see "Finding the unused SCSI addresses on HP-UX systems" (page 239).
2. Set the SCSI address on the device. Depending on the device type, this can be usually done with switches on the device. For details, see the documentation that comes with the device.

   For details about supported devices, see http://support.openview.hp.com/selfsolve/manuals.
3. Connect the device to the system, switch on the device, and then the computer, and wait until the boot process completes. The device files are usually created during the boot process.

4. Verify that the system correctly recognizes your new backup device. Use the `ioscan` utility:

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

   so that you can see the device files listed for each connected backup device. If the device file has not been created automatically during the boot process you must create it manually. See "Creating device files on HP-UX systems" (page 237).

Once the installation procedure has been completed and the backup devices have been properly connected to the system, see the *HP Data Protector Help* index: "configuring, backup devices" for detailed information about configuring devices and media pools or other Data Protector configuration tasks.

Installing Solaris clients

Solaris clients can be installed remotely using the Installation Server for UNIX, or locally from the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
- To install a Solaris client, you will need either *root* access or an account with *root* capabilities.
- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Remote installation

You install the client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

NOTE: If you install the `User Interface` component (which includes the graphical user interface and the command-line interface), you should update your environment variables before using it. For more information, see "Setting environment variables" (page 31).

If you install the User Interface on a Solaris 2.6 client, only the command-line interface is available.

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

IMPORTANT: To install Data Protector to linked directories, for instance:

```
/opt/omni/ -> /prefix/opt/omni/
/etc/opt/omni/ -> /prefix/etc/opt/omni/
/var/opt/omni/ -> /prefix/var/opt/omni/
```

you should create the links before the installation and ensure that the destination directories exist.

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

Cluster-aware clients

Additional prerequisites are required for installing cluster-aware clients. For more details, see "Installing cluster-aware clients" (page 129).

Post-installation configuration

Configuration files

Once you have a Media Agent component installed on the client system, you have to check your configuration to determine the required changes, depending on the platform and the device type you will be using.

- If your Solaris system is a patched Solaris 9 or Solaris 10 system, the tape device driver may already support your device by default. To check this, use the `strings` command.

  For example, to check whether your HP DAT-72 device can be used without additional configuration steps, execute:

  Solaris (SPARC) systems:

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

  Solaris (x86, x64) systems:

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

  Inspect the command output. If your device is present in it, no additional steps are necessary. In the opposite case, follow the instructions below.

- For an HP DAT (4 mm) device, add the following lines to your `/kernel/drv/st.conf` file:

  ```
  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;
  ```

IMPORTANT: These HP data entries differ from the default entries that are usually suggested by HP Support. Specify these lines exactly, or Data Protector will not be able to use your drive.

- For DLT, DLT1, SuperDLT, LTO1, LTO2 and STK9840 devices, add the following lines to the `/kernel/drv/st.conf` file:

  ```
  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;
```

- For an HP StorageWorks 12000e (48AL) autoloader (HP C1553A), add the following entries in addition to HP data entries in your `/kernel/drv/st.conf` file:

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

  Replace the *ID* symbol with the autoloader's SCSI address and set the autoloader option number to `5` (the switch is located on the device's rear panel) and the drive's DIP switch setting to `11111001` (the switches are accessible from the bottom side of the autoloader).

NOTE: The HP StorageWorks 12000e library does not have a dedicated SCSI ID for the picker device but accepts both data drive access commands and picker commands through the same SCSI ID. However, the data drive access commands must be directed to SCSI lun=0 and the picker commands to SCSI lun=1.

For all other devices, check the `st.conf.templ` template (located in `/opt/omni/spt`) for required entries in the `st.conf` file. This is only a template file and is not meant as a replacement for the `st.conf` file.

- For each tape device you want to use, check if the following line is present in the file `/kernel/drv/st.conf` and add it if necessary. Replace the *ID* placeholder with the address of the device:

  SCSI devices:

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

  Fibre channel devices:

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

  Note that the value for the `parent` parameter may differ for your tape device. For more information, see your tape device documentation.

- To enable controlling the SCSI Exchanger devices on Solaris 9 and earlier Solaris versions, you have to install the SCSI Pass-Through driver first, and then install the SCSI device.

  Install the SCSI Pass-Through driver using the following steps:

  1. Copy the `sst` module into the `/usr/kernel/drv/sparcv9` directory and the `sst.conf` configuration file into the `/usr/kernel/drv` directory:

     32-bit Solaris systems:

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

     64-bit Solaris systems:

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

  2. Add the following line to the `/etc/devlink.tab` file:

IMPORTANT: When editing the `/etc/devlink.tab` file, do not use [space] characters. Use only [TAB] characters.

"type=ddi_pseudo;name=sst;minor=character rsst\A1"

This will cause devlinks (1M) to create link(s) to devices with names of the /dev/rsstX form, where X is the SCSI target number.

3. For each SCSI Exchanger device that you want to control, check if the following line is present in the file /kernel/drv/sst.conf and add it if necessary. Replace the *ID* placeholder with the address of the device:

   SCSI devices:

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

   Fibre channel devices:

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

   Note that the value for the parent parameter may differ for your tape device. For more information, see your tape device documentation.

4. Install the driver on the system by entering the following command:

   ```
   add_drv sst
   ```

5. At this stage, you are ready to install the SCSI device. Before the installation, you must assign the correct SCSI address to each drive and the robotics (picker) of the exchanger device. The chosen addresses must not be used by any other device of the system.

   To check the SCSI configuration, shut down the system by running the following command (Solaris (SPARC)-specific step):

   ```
   shutdown -i0
   ```

   then run the probe-scsi-all command at the ok prompt to check the assigned addresses:

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

   When you have finished, restart the system with:

   ```
   ok boot -r
   ```

   To prepare your system for using a SCSI device, follow the steps as shown in the example below:

   a. Edit /kernel/drv/st.conf to set up the device parameters for using the assigned SCSI ports. For details, see the device documentation. Modify the tape-config-list parameter only if the tape device driver does not already support your device by default.

   b. Edit /usr/kernel/drv/sgen.conf to set up the ADIC SCSI control device in order to use the assigned SCSI port 4. Add the following data for the ADIC SCSI Exchanger drive to the /usr/kernel/drv/sst.conf file:

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

- To enable controlling the SCSI Exchanger devices on Solaris 10 (SPARC, x86, x64), configure the in-built sgen driver and then install the SCSI device. Follow the steps:

  1. Open the file /kernel/drv/sgen.conf.

     If the parameter device-type-config-list is present in the file, add a reference for the changer device to the already existing line, for example:

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

     If the parameter is not defined yet, add the following line to the file:

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

2. For each SCSI Exchanger device that you want to control, check if the following line is present in the file `/kernel/drv/sgen.conf` and add it if necessary. Replace the *ID* placeholder with the address of the device:

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

3. At this stage, you are ready to install the SCSI device. Before the installation, you must assign the correct SCSI address to each drive and the robotics (picker) of the exchanger device. The chosen addresses must not be used by any other device of the system.

   To check the SCSI configuration, shut down the system by the following command (SPARC system-specific step):

   ```
   shutdown -i0
   ```

   then run the `probe-scsi-all` command at the `ok` prompt to check the assigned addresses:

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

   When you have finished, restart the system with:

   ```
   ok boot -r
   ```

   To prepare your system for using a SCSI device, follow the steps as shown in the example below:

   a. Edit `/kernel/drv/st.conf` to set up the device parameters for using the assigned SCSI ports. For details, see the device documentation. Modify the `tape-config-list` parameter only if the tape device driver does not already support your device by default.

   b. Edit `/kernel/drv/sgen.conf` to set up the ADIC SCSI control device in order to use the assigned SCSI port 4. Add the following data for the ADIC SCSI Exchanger drive to the `/kernel/drv/sgen.conf` file:

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

When you have modified the `/kernel/drv/st.conf` file and the `/usr/kernel/drv/sst.conf` file (Solaris 9 and earlier Solaris versions) or the `/kernel/drv/sgen.conf` file (Solaris 10), you are ready to physically connect a backup device to your system.

Connecting a backup device to a Solaris system

Follow the procedure below to connect a backup device to a Solaris system:

1. Create a `reconfigure` file:

   ```
   touch /reconfigure
   ```

2. Shut down the system by entering the `$shutdown -i0` command, and then switch off your computer and physically connect the device to the SCSI bus. Check that no other device is using the same SCSI address you have selected for the device.

   See http://www.hp.com/support/manuals for details about supported devices.

   NOTE: Data Protector does not automatically recognize cleaning tapes on a Solaris system. If Data Protector detects and inserts a cleaning tape in the StorageWorks 12000e (48AL) device, the tape driver enters an undefined state and may require you to restart your system. Load a cleaning tape manually, when Data Protector issues a request for it.

3. If your system is a Solaris (SPARC) system, switch the system back on and interrupt the startup process by pressing the `Stop-A` key.

4. Verify that the new device is recognized correctly by entering the `probe-scsi-all` command at the `ok` prompt:

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

   Then, enter:

   ```
   ok > go
   ```

   to continue.

5. The device should work properly at this stage. The device files must be located in the `/dev/rmt` directory for the drives and in the `/dev` directory for the SCSI control device (picker).

   NOTE: On Solaris 9 and earlier Solaris versions (especially in case of 64-bit Solaris), links to the SCSI control device (picker) are not always created automatically. On Solaris 10, such links are never created. Under such circumstances, create symbolic links to join suitable device files to `/dev/rsst`*`Num`* where *`Num`* is a number of your choice. For example:

   When sst is used:

   ```
   ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4
   ```

   When sgen is used:

   ```
   ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /dev/rsst4
   ```

   You can use the Data Protector `uma` utility to verify the device. To check the picker of the SCSI Exchanger device from the previous example (using the SCSI port 4), enter:

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

   The picker must identify itself as a SCSI-2 device library. The library can be checked by forcing it to initialize itself. The command is:

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

Make sure you use Berkeley-style device files, in this case, `/dev/rmt/0cbn` (not `/dev/rmt/0h`) for the tape drive and `/dev/rsst4` for the SCSI control device (picker).

What's next?

Once the installation procedure has been completed and the backup devices are properly connected to the Solaris client, for additional information about configuring backup devices, media pools, and other configuration tasks, see the *HP Data Protector Help* index: "configuring, backup devices".

Installing Linux clients

Linux client systems can be installed remotely using the Installation Server for UNIX, or locally by using the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
- The `rpm` utility must be installed and set up. Other packaging systems, for example `deb`, are not supported.

- For the Java GUI Client, a supported version of Java runtime environment is required. See the *HP Data Protector Product Announcements, Software Notes, and References* or the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
- To install Data Protector components on a *remote system*, the following prerequisites must be met on the remote system:
  - The `inetd` or `xinetd` service must be running or set up so that Data Protector is able to start it.
  - Either the `ssh` or, if `ssh` is not installed, the `rexec` service must be enabled.
- Ensure that the kernel supports SCSI devices (modules `SCSI support`, `SCSI tape support`, `SCSI generic support`). The parameter `Probe all LUNa on each SCSI device` is optional.

  For more details on SCSI support in the Linux kernel, see the documentation of your Linux distribution or the Linux kernel documentation.

NOTE: Data Protector uses the default port number 5555. Therefore, this particular port number should not be used by another program. Some Linux operating system distributions use this number for other purposes.

If the port number 5555 is already in use, you should make it available for Data Protector or you can change the default port number to an unused port number. See "Changing the default Data Protector Inet port" (page 226).

Automatic disaster recovery

The `Automatic Disaster Recovery` component must be installed on systems for which you want to enable recovery using Enhanced Automated Disaster Recovery (EADR) or One Button Disaster Recovery (OBDR), and on systems where the DR CD ISO image for EADR or OBDR will be prepared.

MC/ServiceGuard cluster

With MC/ServiceGuard clusters, the Data Protector agents (Disk agent, Media Agent) must be installed separately *on each cluster node* (local disk) and not on the shared disk.

After the installation, you need to import the *virtual host* (application package) to the cell as a client. Therefore the application package (for example Oracle) must run on the cluster with its *virtual IP*. Use the command `cmviewcl -v` to check this before importing the client.

You can use the passive node to install an Installation Server.

Novell Open Enterprise Server (OES)

On Novell OES systems, Data Protector automatically installs the OES aware Disk Agent. However, there are some Novell OES specific aspects:

- If you install Novell OES on 32-bit SUSE Linux Enterprise Server 9.0 (SLES), after installing a Data Protector Linux client on a system, you have to upgrade the Data Protector client as well.

  Note that the new Novell OES aware Disk Agent will be remotely installed to the client system during the upgrade.
- If you remove the Novell OES component from SLES, you have to reinstall the Data Protector client.

Remote installation

You remotely install a Linux client system by distributing the Data Protector components from the Installation Server for UNIX to the Linux system, using the Data Protector graphical user interface. For the step-by-step procedure for distributing the software, see "Remote installation" (page 76).

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

Troubleshooting remote installation

If you run into problems with remote installation on a Linux client system, ensure that the `root` account has rights to access the system either by using `exec` or `shell` services. To achieve this, do the following:

1. Edit the `/etc/xinetd.conf`. Find the definitions for `exec` and `shell` services and add the following line to the definition of these two services:

   ```
   server_args = -h
   ```

   For example:

   ```
   service shell
   {
   socket_type = stream
   protocol = tcp
   wait = no
   user = root
   server = /usr/sbin/in.rshd
   server_args = -L -h
   }
   service exec
   {
   socket_type = stream
   protocol = tcp
   wait = no
   user = root
   server = /usr/sbin/in.rexecd
   server_args = -h
   }
   ```

   NOTE: Some Linux distributions have these services configured in separate files in the `/etc/xinetd.d` directory. In this case, locate the appropriate file (`/etc/xinetd.d/rexec` and `/etc/xinetd.d/rsh`) and modify it as described above.

2. Terminate the `inetd` process with the `HUP` signal:

   ```
   kill -HUP $(ps ax|grep inet|grep -v grep|cut -c1-6)
   ```

3. Create a `~root/.rhosts` file with the entry: *`SystemNameOfMyInstallationServeK`* `root`

   That will allow administration access from the Installation Server.

After you have installed Data Protector, you can remove the entry from the `-root/.rhosts` file, and the `-h` flag from the `/etc/xinetd.conf` (`/etc/inetd.conf` for Red Hat Enterprise Linux) file. Then repeat the `kill` command from the Step 2.

For more information, see the `rexecd`(8), `rexec`(3), `rshd`(8), `rsh`(1), or `pam`(8) man pages. If this fails, see "Local installation on UNIX and Mac OS X systems" (page 81).

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

Connecting a backup device to the Linux system

Once you have a Media Agent component installed on the Linux client, follow the steps below to connect a backup device to the system:

1. Run the `cat /proc/scsi/scsi` command to determine the available SCSI addresses for the drives and control device (robotics).
2. Set the SCSI address on the device. Depending on the device type, this can be done by switching on the device. For details, see the documentation that comes with the device.

   For details about supported devices, see http://support.openview.hp.com/selfsolve/manuals.
3. Connect the device to the system, switch on the device, then switch on the computer, and wait until the boot process completes. The device files are created during the boot process.

   On Red Hat Enterprise Linux systems, an application, Kudzu, is launched during the boot process when a new device is connected to the system. Press any key to start the application, and then click the `Configure` button.
4. To verify if the system correctly recognizes your new backup device, run `cat /proc/scsi/scsi` and then `dmesg |grep scsi`. The device files are listed for each connected backup device.

   ### Examples

   For robotics, the output of the `dmesg |grep scsi` command is:

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

   and for drives:

   ```
   Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
   ```
5. Device files are created in the `/dev` directory. To check if the links to the device files were created, execute:

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

   For example:

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

   The output of this command is:

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

   where `/dev/sg2` is a link to the device file `/dev/sgc`. This means that the device files to be used by Data Protector are `/dev/sgc` for robotics and `/dev/st0` for drive. Device files for robotics are `sga`, `sgb`, `sgc`,... `sgh`, and for the drives `st0`, `st1`,... `st7`.

What's next?

Once the installation procedure has been completed and the backup devices have been properly connected to the Linux client system, see the *HP Data Protector Help* index: "configuring, backup devices" for information about configuring backup devices and media pools, or other configuration tasks.

Installing ESX Server clients

ESX Server is a modified Linux operating system. For details on how to install Data Protector components on ESX Server systems, see "Installing Linux clients" (page 59).

Installing Mac OS X clients

Mac OS X clients can be installed remotely using the Installation Server for UNIX, or locally from the UNIX installation DVD-ROM (for HP-UX or Linux).

Only the Disk Agent (DA) is supported.

Prerequisites

- For system requirements, disk space requirements, supported OS versions, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Remote installation

You install the Mac OS X client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

Installing IBM AIX clients

IBM AIX clients can be installed remotely using the Installation Server for UNIX, or locally from the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation process, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
- Before installing the `Disk Agent` component, check that the port mapper is up and running on the selected system. In the `/etc/rc.tcpip` file, there must be the line that starts the port mapper:

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

  The `src_running` flag is set to 1 if the `srcmstr` daemon is running. The `srcmstr` daemon is the System Resource Controller (SRC). The `srcmstr` daemon spawns and controls subsystems, handles short subsystem status requests, passes requests on to a subsystem, and handles error notifications.

IBM HACMP cluster

In IBM High Availability Cluster Multi-Processing environment for AIX, install the Data Protector `Disk Agent` component on all the cluster nodes. For information on how to install Data Protector in a cluster environment with a cluster-aware application database installed, see "Installing the Data Protector integration clients" (page 89).

After the installation, import the cluster nodes and the *virtual server* (virtual environment package IP address) to the Data Protector cell.

Remote installation

You install the AIX client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

After the installation

On IBM AIX 5.3 systems, if you have applied the Data Protector patch bundle 7.03 to a Data Protector 7.00 installation, additionally perform the following steps to finalize the patch bundle installation process:

1. Open a Terminal window.
2. Change current directory to `/usr/omni/bin`.
3. For each binary file in this directory whose filename contains the suffix `_32`, rename the file by removing the suffix from its filename.

   For example, to properly rename the Disk Agent binary used to perform volume backup, rename the file `vbda_32` to `vbda` (so that the existing file `vbda` is overwritten) by executing the command:

   ```
   mv -f vbda_32 vbda
   ```

Connecting a backup device to an AIX client

Once you have a Media Agent component installed on an AIX client, proceed as follows:

1. Shut down the computer and connect your backup device to the SCSI bus. Check that no other device is using the same SCSI address which has been selected for your backup device.

   For details about supported devices, see http://support.openview.hp.com/selfsolve/manuals.

2. Switch on the computer and wait until the boot process completes. Start the AIX system `smit` management tool and verify that the system correctly recognizes your new backup device.

IMPORTANT: Use `smit` to change the device's default block size to `0` (variable block size).

3. Select the appropriate device files from the `/dev` directory and configure your Data Protector backup device.

IMPORTANT: Use only non-rewind-style device files. For example, select `/dev/rmt0.1` instead of `/dev/rmt0`.

What's next?

Once the installation procedure has been completed and your backup devices have been properly connected to the AIX system, see the *HP Data Protector Help* index: "configuring, backup devices" for information on configuring backup devices, media pools, or other Data Protector configuration tasks.

Installing Tru64 clients

Tru64 clients can be installed remotely using the Installation Server for UNIX, or locally by using the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Remote installation

You install the Tru64 client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

Tru64 Cluster

You must have `root` permissions on every target system.

Data Protector has to be installed remotely or locally on the shared disk of the Tru64 Cluster. Use one of the cluster nodes to perform an installation.

After the installation, the cluster virtual hostname and individual nodes have to be imported to the Data Protector cell. For a detailed procedure, see "Importing a cluster-aware client to a cell" (page 134).

Connecting a backup device to Tru64 client

Once you have a Media Agent component installed on an Tru64 client, proceed as follows:

1. Shut down the computer and connect your backup device to the SCSI bus.

   NOTE: It is not recommended to connect the backup device on the same SCSI bus as the hard disk drive.

   Check that no other device is using the same SCSI address which has been selected for your backup device.

   For details about supported devices, see http://support.openview.hp.com/selfsolve/manuals.
2. Switch on the computer and wait until the boot process completes. Verify that the system correctly recognizes your new backup device.

What's next?

Once the installation procedure has been completed and your backup devices have been properly connected to the Tru64 system, see the *HP Data Protector Help* index: "configuring, backup devices" for information on configuring backup devices, media pools, or other Data Protector configuration tasks.

Installing SCO clients

SCO clients can be installed remotely using the Installation Server for UNIX, or locally by using the UNIX installation DVD-ROM (for HP-UX or Linux).

Note that for the UnixWare, remote installation is not available.

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26) for instructions.

Remote installation

You install the SCO client software from the Installation Server for UNIX to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

Local installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the UNIX installation DVD-ROM (for HP-UX or Linux). For instructions, see "Local installation on UNIX and Mac OS X systems" (page 81).

As soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

Connecting a backup device to an SCO system

Once you have a Media Agent component installed on the SCO client system, follow the steps below to connect a backup device to the system:

1. Find out which SCSI addresses are still free by checking the `/etc/conf/cf.d/mscsi` file. This file shows the currently connected SCSI devices.

   See http://support.openview.hp.com/selfsolve/manuals/ for details about supported devices and the documentation that comes with the device.
2. Shut down your computer, and then connect your backup device to the SCSI bus.
3. Restart your computer.
4. Configure your device using the `mkdev tape` command. In the list of tape drive types, select the `Generic SCSI-1 / SCSI-2 tape drive`.

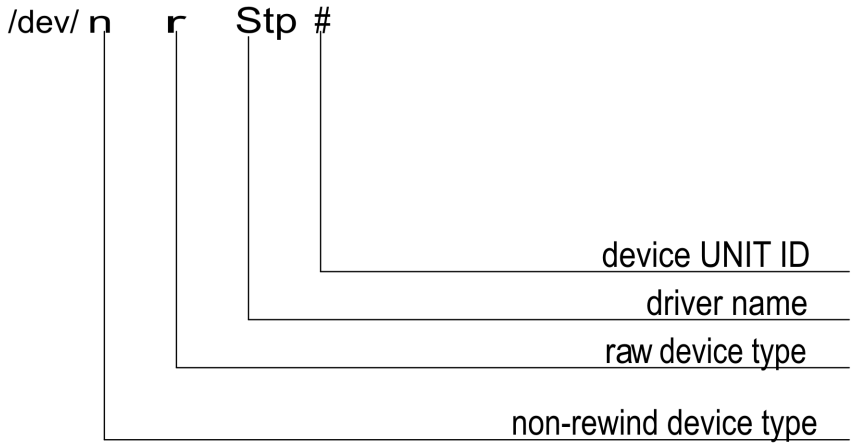
   NOTE: Remember the UNIT ID, which is displayed when you run the `mkdev tape` command. You will need it in order to recognize the device filename.
5. After you have configured the device and restarted the system, check in the `/etc/conf/cf.d/mscsi` file if your device was connected properly.

6. Select the appropriate device filename from the `/dev` directory.

   Use the `nrStp#` name, where # stands for UNIT ID of the device. The UNIT ID of the device is defined in the Step 4. The `/dev/nrStp#` device filename is explained in "Format of a device filename" (page 67).

CAUTION: Use only non-rewind-style device files with a variable block size. Verify whether the block size is variable by using the `tape -s getblk /dev/nrStp#` command. The value for a variable block size should be 0. If the value is not 0, use the `tape -a 0 setblk /dev/nrStp#` command to set the value of the block size to 0.

Figure 18 Format of a device filename



What's next?

Once the installation procedure has been completed and the backup devices have been properly connected to the SCO client system, see the *HP Data Protector Help* index: "configuring, backup devices" for information about configuring backup devices and media pools or other configuration tasks.

Installing HP OpenVMS clients

The installation procedure for OpenVMS clients has to be performed locally on a supported OpenVMS system. Remote installation is not supported.

You can install the Data Protector Disk Agent, General Media Agent, and the User Interface (command-line interface only) on systems running OpenVMS 7.3-2/IA64 8.2-1. You can also install the Oracle Integration component on systems running OpenVMS 7.3-2 or later. For information on Data Protector components, see "Data Protector components" (page 45).

For information on supported devices, OpenVMS platform versions, as well as for limitations, known problems and workarounds, see the *HP Data Protector Product Announcements, Software Notes, and References*.

For more OpenVMS specific information, see the *OpenVMS Release Notes* located in the default help document directory on OpenVMS, for example:
`SYS$COMMON:[SYSHLP]DPA0700.RELEASE_NOTES.`

Prerequisites

Before you install a Data Protector client on the OpenVMS platform, check the following:

- Make sure the HP TCP/IP transport protocol is installed and running.
- Set the TIMEZONE features of your system by executing the command `SYS$MANAGER:UTC$TIME_SETUP.COM`.

- Log in to the `SYSTEM` account of the OpenVMS system. Note that you must have appropriate permissions.
- Make sure that you have access to the Data Protector installation DVD-ROM containing the HP OpenVMS client installation package.

Installation

The installation procedure can be performed from the Data Protector Windows installation DVD-ROM. Note that the OpenVMS installation is not a part of the Installation Server functionality.

To install a Data Protector client on an OpenVMS system, proceed as follows:

1. If you already have the PCSI installation file go to Step 2. To get the PCSI installation file, mount the installation DVD-ROM on an OpenVMS Server and copy it to the desired location. You may also ftp the PCSI file from a Windows system.
2. Run the following command:

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

   where *`device:[directory]`* is the location of the .PCSI installation file.
3. Verify the version of the kit by responding `YES` to the prompt:

   ```
   The following product has been selected: HP AXPVMS DP A06.20-xx
   Layered Product Do you want to continue? [YES]
   ```
4. Choose the software components you wish to install. You may take the defaults and the Disk Agent, General Media Agent, and User Interface will be installed. You may also select each component individually.

   You will be asked to choose options, if any, for each selected product and for any product that may be installed to satisfy software dependency requirements.

   #### Example

   ```
   HP IA64VMS DP A06.20-xx: HP OpenVMS IA64 Data Protector V6.20
   COPYRIGHT HEWLETT-PACKARD COMPANY 2010
   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 X06.20-xx: HP OpenVMS IA64 Data Protector V6.20
   [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
```

The default and only location for the Data Protector directories and files is:

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

The directory structure will be created automatically and the files will be placed in this directory tree.

The Data Protector startup and shutdown command procedures will be placed in

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

There are four files that are always present for an OpenVMS client and a fifth file that only exists if you chose the CLI option. The five files concerned are:

- `SYS$STARTUP:OMNI$STARTUP.COM` This is the command procedure that starts Data Protector on this node.
- `SYS$STARTUP:OMNI$SYSTARTUP.COM` This is the command procedure that defines the `OMNI$ROOT` logical name. Any other logical names required by this client may be added to this command procedure.
- `SYS$STARTUP:OMNI$SHUTDOWN.COM` This is the command procedure that shuts down Data Protector on this node.
- `OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM` This is the command procedure that is used to start the `TCP/IP INET` process, which then executes the commands sent by the Cell Manager.
- `OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM` This is the command procedure that defines the symbols needed to invoke the Data Protector CLI. It will only exist on the system if you chose the CLI option during installation.

  Execute this command procedure from the `login.com` procedures for all users who will use the CLI interface. Several logical names are defined in this procedure which are necessary to execute the CLI commands correctly.

5. Insert the following line in `SYS$MANAGER:SYSTARTUP_VMS.COM`:

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

6. Insert the following line in `SYS$MANAGER:SYSHUTDWN.COM`:

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

7. Ensure that you can connect from the OpenVMS client to all possible TCP/IP aliases for the Cell Manager.
8. Import the OpenVMS client to the Data Protector cell using the Data Protector graphical user interface as described in "Importing clients to a cell" (page 132).

An account with the name OMNIADMIN gets created during the installation. The `OMNI` service runs under this account.

The login directory for this account is `OMNI$ROOT:[LOG]` and it holds the log file `OMNI$STARTUP_INET.LOG` for each startup of a Data Protector component. This log file contains

the name of the process executing the request, the name of Data Protector image used and the options for the request.

Any unexpected errors are logged in the `DEBUG.LOG` in this directory.

NOTE: On OpenVMS 8.3 and later, the Data Protector installation displays the following message:

```
%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0700
-XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
is not signed and therefore has no manifest file
```

To avoid the warning being issued, run the product install command using `/OPTION=NOVALIDATE_KIT`.

Installation in a cluster environment

If you use a common system disk, the client software needs to be installed only once. However, the `OMNI$STARTUP.COM` procedure needs to be executed for each node to be usable as a Data Protector client. If you do not use a common system disk the client software needs to be installed on each client.

If you use a cluster TCP/IP alias name, you can define a client for the alias name as well if you are using a cluster common system disk. With the alias client defined you do not have to configure the individual client nodes. You can choose either client definition or alias definition to run your backups and restores in a cluster. Depending on your configuration, the save or restore may or may not use a direct path to your tape device or tape library.

Disk Agent configuration

The Data Protector Disk Agent on OpenVMS supports mounted `FILES-11 ODS-2` and `ODS-5` disk volumes. There is no need to configure the OpenVMS Disk Agent. There are, however, some points to bear in mind when setting up a backup specification that will use it. These are described below:

- The file specifications entered into the GUI or passed to the CLI must be in UNIX style syntax, for instance:

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

  - The string must begin with a slash, followed by the disk, directories and filename, separated by slashes.
  - Do not place a colon after the disk name.
  - A period should be used before the version number instead of a semi-colon.
  - File specifications for OpenVMS files are case-insensitive, except for the files residing on `ODS-5` disks.

Example

An OpenVMS file specification of:

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

must be specified to Data Protector in the form:

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

NOTE: There is no implicit version number. You must always specify a version number and only the file version specified for the backup will be backed up.

For some options which allow wildcards the version number can be replaced with an asterisk '*'.

To include all versions of the file in a backup, you should select them all in the GUI or, in the CLI, include the file specifications under the `-only` option, using wildcards for the version number, as follows:

```
/DKA1/dir1/filename.txt.*
```

Media Agent configuration

You should configure devices on your OpenVMS system using OpenVMS and hardware documentation as a guide. The pseudo devices for the tape library must be created first using SYSMAN, as follows:

```
$ RUN SYS$SYSTEM:SYSMAN
SYSMAN> IO CONNECT gcan/NOADAPTER/DRIVER=SYS$GcDRIVER
```

where:

- `c` = K for direct connected SCSI tape libraries.
- `a` = A,B,C, …the adapter character for the SCSI controller.
- `n` = the unit number of the tape library's robotic control device.

NOTE: This command sequence must be executed after a system boot.

For SAN attached tape libraries the tape drives and robot device name should show up automatically under OpenVMS once the SAN devices have been configured according to SAN guidelines.

If you are installing tape jukeboxes for use with Data Protector, you should verify that the hardware is working correctly before configuring it within Data Protector. You may use the Media Robot Utility (MRU), available from Hewlett-Packard, to verify the hardware.

NOTE: You can generally use the Data Protector GUI to manually configure or auto-configure these devices.

However, certain older tape libraries and all tape libraries connected to HSx controllers cannot be auto-configured. Use manual configuration methods to add these devices to Data Protector.

Media Agent in a cluster

When dealing with devices attached to cluster systems:

1. Configure each tape device and tape library so that it can be accessed from each node.
2. Add the node name to the end of the device name to differentiate between the devices.
3. For tape devices, set a common `Device Lock Name` under `Devices/Properties/Settings/Advanced/Other`.

Example

In a cluster with nodes A and B, a TZ89 is connected to node A and MSCP served to node B. Configure a device named `TZ89_A`, with node A as the client and configure a device named `TZ89_B`, with node B as the client. Both devices get a common device lock name of `TZ89`. Now Data Protector can use the devices via either path, knowing that this is actually only one device. If you run a backup on node B using `TZ89_A`, Data Protector moves the data from node B to the device on node A. If you run a backup on node B using `TZ89_B` the OpenVMS MSCP server moves the data from node B to the device on node A.

NOTE: For MSCP served tape devices in a cluster, for all tape devices connected via an HSx controller and for all tape devices connected via Fibre Channel, follow the guidelines for SAN configurations in the *HP Data Protector Help* index: "SAN, configuring devices in".

Command-line interface

Before you can use the Data Protector command-line interface on OpenVMS you must run the CLI command setup procedure, as follows:

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

For a description of the available CLI commands, see the *HP Data Protector Command Line Interface Reference*.

Oracle integration

After you installed the Oracle integration and configured it as described in the *HP Data Protector Integration Guide for Oracle and SAP*, verify that the `-key Oracle8` entry is present in `OMNI$ROOT:[CONFIG.CLIENT]omni_info`, for example:

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId 12172 -flags
0x7 -ntpath "" -uxpath "" -version 7.00
```

If the entry is not present, copy it from `OMNI$ROOT:[CONFIG.CLIENT]omni_format`. Otherwise, the Oracle integration will not be shown as installed on the OpenVMS client.

What's next?

For information on additional configuration tasks, see the *HP Data Protector Help* Help index: "HP OpenVMS".

Installing Novell NetWare clients

The installation procedure of the Novell NetWare clients has to be performed from a supported Windows system that is connected to the Novell network.

You can install the Data Protector Disk Agent and General Media Agent on the systems running Novell NetWare. For information on Data Protector components, see "Data Protector components" (page 45).

For details about supported devices, Novell NetWare platform versions, as well as for known problems and workarounds, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Prerequisites

Before you install Data Protector on the Novell NetWare platform, check the following:

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Make sure the TCP/IP transport protocol is installed and functional.
- Make sure that one of the following services is running on the Windows system:
  - A Gateway Service for Novell NetWare.

    This service should run on Windows when an installation is executed from the Windows Server.
  - A Novell Client for Windows or a Microsoft Client Service for NetWare.

    This service should run on the Windows when an installation is executed from the Windows workstation.

- Log in to the target NetWare server (or the appropriate NDS/eDirectory tree) from the Windows system.
- Ensure that you have supervisor rights for the SYS: volume on the target NetWare server.
- Make sure that you have at least one local device name free on your Windows system.

Cluster-aware clients

Additional prerequisites are required for installing cluster-aware clients. For more details, see "Installing cluster-aware clients" (page 129).

Installation

The installation procedure can be performed from the Data Protector Windows DVD-ROM. Note that the Novell NetWare installation is not a part of the Installation Server functionality.

To install Data Protector on the Novell NetWare server, proceed as follows:

1. Run a command prompt on your Windows system and change the current path to the DVD-ROM root directory.
2. Run the installation script.

   To install the Data Protector Novell NetWare client, change the current path to the `NetWare` directory and type:

   `NWInstall` *`target server name`* `ALL|DA|MA` *`port_number`*

   The second parameter defines which part of the Data Protector Novell Client will be installed:

   - Type `ALL` to install the whole Data Protector Novell NetWare client functionality.
   - Type `DA` to install only the Data Protector Disk Agent for Novell NetWare.
   - Type `MA` to install only the Data Protector General Media Agent for Novell NetWare.

   NOTE: For the Data Protector installation on each Novell NetWare version, the port number is optional. If it is not specified, the default port 5555 will be used.

   If your Novell NetWare OS version is not supported by Data Protector, the installation is still possible but you receive a corresponding warning.

   The installation now verifies whether Data Protector files are already present on the target server. If so, the old Data Protector installation will be moved to the `SYS:\usr\Omni.old` directory.

   Depending on the installed NetWare client version, check whether `OMNIINET.NLM`, `HPINET.NLM` or `HPBRAND.NLM` is running on the server. If one of these programs is running, unload it by typing the following command at the Novell NetWare console:

   `UNLOAD HPINET` (`UNLOAD OMNIINET` / `UNLOAD HPBRAND`)

   The installation automatically creates a Data Protector directory structure and copies all Data Protector files to the target server.
3. Make sure that you have loaded the following modules on your system:
   - `NETDB.NLM`
   - `TSAFS.NLM`
   - `TSANDS.NLM`

   This way you enable the loader to resolve public symbols while trying to load `HPINET.NLM`.

   If you have configured Novell NetWare Cluster Services on your Novell NetWare 6.x system, make sure that you have loaded the `NCSSDK.NLM` module.

4. To load HPINET.NLM, type at the Novell NetWare console:

   ```
   SEARCH ADD SYS:USR\OMNI\BIN
   LOAD HPINET.NLM
   ```

   NOTE: When not using the default port number 5555, specify the port number by adding the `-port port_number` option to the LOAD command. For example:

   ```
   LOAD HPINET.NLM -port port_number
   ```

   To enable automatic recognition of the Data Protector Cell Manager by the Novell NetWare server, the installation will automatically add the console commands to the AUTOEXEC.NCF file, so that the HPINET.NLM file is always loaded and ready to connect to the Data Protector Cell Manager.

NOTE: You should verify your AUTOEXEC.NCF file after the installation is finished. If the necessary console commands were not added to the AUTOEXEC.NCF file during installation, you have to add them manually.

To enable backup and restore of the NDS/eDirectory database, complete the following steps:

1. Define the user account to be used when performing backup and restore of NDS/eDirectory.
2. From the Novell NetWare console, load the HPLOGIN.NLM module:

   ```
   LOAD HPLOGIN.NLM
   ```

3. Provide the following user information to the HPLOGIN.NLM file to enable successful login to the NDS/eDirectory database:

   - NDS/eDirectory Context:

     The context describes the container where the user objects reside. The container name must be a fully distinguished name syntax. For example:

     ```
     OU=SDM.O=MYDOMAIN
     ```

   - NDS/eDirectory Object Name:

     This is the Common Name of the user object that will be used as a valid NDS/eDirectory user for logging in to the NDS/eDirectory database when Data Protector Disk Agent performs backup or restore of the NDS/eDirectory. The selected user must be located in the previously applied context. For example:

     ```
     CN=MarcJ
     ```

     if the selected user's fully distinguished name has `.CN=MarcJ.OU=SDM.O=MYDOMAIN` syntax.

   - NDS/eDirectory Object Password:

     A valid user password that is used with the user name for logging in to the NDS/eDirectory database when a backup or restore of the NDS/eDirectory database is started.

     User information entered in the HPLOGIN module is encoded and stored to the SYS:SYSTEM directory. It is also used in conjunction with Novell NetWare SMS modules that must be loaded and functional.

   NOTE: The user account selected in the HPLOGIN module must have permissions to perform backup and restore of the NDS/eDirectory database.

   If changes are made on the NDS/eDirectory used object (moved to another container, deleted, renamed, changed password), the information encoded in the SYS:SYSTEM directory must be updated in the HPLOGIN module.

4. To back up and restore NDS/eDirectory with Novell NetWare Storage Management Services (SMS), the SMDR.NLM and TSANDS.NLM modules must be loaded on at least one server in the NDS/eDirectory tree. You can download the latest versions of TSANDS.NLM and SMDR.NLM from the Web at http://support.novell.com/filefinder/.

   The installation automatically adds the LOAD TSANDS.NLM line to the AUTOEXEC.NCF file, so the Novell NetWare server can immediately recognize TSANDS.NLM. The Novell NetWare SMS module SMDR.NLM is loaded as soon as TSANDS.NLM is loaded.

NOTE: If the installation did not add console commands to the AUTOEXEC.NCF file, you should do it manually.

TIP: To minimize network traffic during the backup process, load the modules on the server containing a replica of the largest NDS/eDirectory partition.

Now you have fulfilled the requirements for the backup and restore of NDS/eDirectory. For instructions about additional configuration tasks, see the *HP Data Protector Help* index: "configuring".

Media Agent configuration

At this stage, all Data Protector components are already installed. However, if you selected ALL or the MA parameter at the beginning of the installation procedure, you have to perform a few additional configuration tasks to enable the Data Protector General Media Agent to use backup devices connected to the Novell NetWare server.

Data Protector supports the Adaptec SCSI host adapter controller and its corresponding .HAM driver. The Data Protector Media Agent can directly communicate with the .HAM driver in order to access the SCSI host adapter. Therefore, you need to have the SCSI host adapter driver installed. For example, you can download the latest versions of Adaptec drivers from http://www.adaptec.com.

The driver can be loaded automatically whenever the server is restarted if you add a LOAD command to the STARTUP.NCF file. The command must specify the location of the driver, any available options, and the slot number. For the list of available options and calculation of the slot number, see the *Adaptec Driver User's Guide*.

Example

To automatically load the AHA-2940 Adaptec driver on the Novell NetWare 6.x server whenever the server is restarted, add the following lines to the STARTUP.NCF file:

```
SET RESERVED BUFFERS BELOW 16 MEG=200
LOAD AHA2940.HAM SLOT=4 lun_enable=03
```

where SLOT defines the location of the host adapter device and the lun_enable mask enables scanning for specific LUNs on all targets.

A scan for every LUN is enabled for all SCSI addresses by 1 in its corresponding bit position. For example, lun_enable=03 enables scanning for LUNs 0 and 1 on all targets.

NOTE: lun_enable is required only if you use devices which have SCSI LUNs higher than 0. For example, when you configure an HP 12000e tape library device.

TIP: To automatically scan for all devices connected to the Novell NetWare server and their LUNs whenever the server is restarted, add the following lines to the `AUTOEXEC.NCF` file:

```
SCAN FOR NEW DEVICES
SCAN ALL LUNS
```

The General Media Agent configuration is now complete.

What's next?

Once you have the General Media Agent software successfully installed on the Novell NetWare platform, it is advisable to check the Data Protector General Media Agent installation. See "Checking the General Media Agent Installation on Novell NetWare systems" (page 252).

As soon as you have verified the installation, you are ready to import the Novell NetWare client to the Data Protector cell using the Data Protector graphical user interface. For information on additional configuration tasks, see the *HP Data Protector Help* index: "Novell NetWare".

Remote installation

This section describes the procedure for distributing the Data Protector software to clients using the Installation Server (remote installation or upgrade).

Distribute the software to clients using the Data Protector user interface. Cross-platform client installation is supported.

Prerequisites

- For prerequisites and recommendations on the installation, see the section that describes the installation procedure for that particular client. The references are listed in "Installing Data Protector client systems" (page 43) and in "Installing integrations" (page 44).
- For the information on supported platforms, Data Protector components, and for disk space requirements, see http://support.openview.hp.com/selfsolve/manuals and the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and the Installation Server(s) installed on your network.
- The Installation Server for Windows must reside in a shared directory so that it is visible throughout the network.

Recommendation

- ***UNIX systems:*** For security reasons, it is recommended to use secure shell for the Data Protector remote installation. If secure shell is not available, the legacy UNIX tools `rsh` and `rexec` are automatically used by the Data Protector remote installation.

  To use secure shell, install and set up OpenSSH on both, the client and Installation Server. If your private key is encrypted, install and set up keychain on the Installation Server. See "Remote installation using secure shell" (page 77).

NOTE: You cannot distribute software to clients in another Data Protector cell. However, if you have an independent Installation Server, you can import it into more than one cell. You can then distribute software within different cells by using the GUI connected to each Cell Manager in turn.

Remote installation using secure shell

Secure shell installation helps you protect your client and Installation Server by installing Data Protector components in a secure way. High level of protection is achieved by:

- Authenticating the Installation Server user to the client in a secure way through the public-private key pair mechanism.
- Sending encrypted installation packages over the network.

NOTE: Secure shell installation is supported on UNIX systems only.

Setting up OpenSSH

Install and set up OpenSSH on both, the client and Installation Server:

1. Ensure that OpenSSH is installed on your system. For details, see the documentation of your operating system or distribution.

   If the OpenSSH package is not a part of your OS distribution, download OpenSSH from http://www.openssh.org and install it on both the Data Protector client and Installation Server.

   Alternately, on HP-UX, you can use the HP-UX Secure Shell.

   NOTE: The default location for the secure shell installation is `/opt/ssh`.

2. On the Installation Server, run `ssh-keygen` to generate a public-private key pair. Keep the private key on the Installation Server while transferring the public key to the client. Note that if you use an encrypted private key (that is, protected by a passphrase), you need to set up keychain on the Installation Server (for details, see "Setting up a keychain" (page 78)).

   For information on `ssh-keygen`, see http://www.openbsd.org/cgi-bin/man.cgi?query=ssh-keygen&sektion=1.

3. Store the public key in the `$HOME/.ssh` directory on the client under the name `authorized_keys`.

   NOTE: `$HOME/.ssh` is usually the home directory of the `root` user.

   To set an SSH protocol version (SSH1 or SSH2), modify the `protocol` parameter in the following files:

   1. ***On the Installation Server:***

      `ssh_install_directory``/ssh/etc/ssh_config`

      This file will be used by the `ssh` command.

   2. ***On the client:***

      `ssh_install_directory``/ssh/etc/sshd_config`

      This command will be used by the `ssh` daemon (`sshd`).

   Note that these two files must be in sync.

   NOTE: The default SSH protocol version is SSH2.

4. On the client, start the `ssh` daemon:

   `ssh_install_directory``/ssh/sbin/sshd`

5. Add the client to a list of known hosts (located in `$HOME/.ssh/known_hosts` on the Installation Server) by running:

   `ssh root@`*`client_host`*

   where *`client_host`* must be the fully qualified DNS name, for example:

   `ssh root@client1.company.com`

6. On the Installation Server, set the `omnirc` option `OB2_SSH_ENABLED` to `1`. For more information on `omnirc` options, see the *HP Data Protector Troubleshooting Guide*.

Setting up a keychain

Keychain is a tool eliminating the need to manually supply a passphrase when decrypting the private key. It is needed only if the private key is encrypted. To set up keychain:

1. Download keychain from http://www.gentoo.org/proj/en/keychain/index.xml to the Installation Server.
2. Add the following two lines to `$HOME/.profile`:

   HP-UX and Solaris systems:

   ```
   keychain_install_directory/keychain-keychain_version/keychain
   $HOME/.ssh/private_key
   . $HOME/.keychain/'hostname'-sh
   ```

   Linux systems:

   ```
   /usr/bin/keychain $HOME/.ssh/private_key
   . $HOME/.keychain/'hostname'-sh
   ```

3. On the Installation Server, set the `OB2_ENCRYPT_PVT_KEY` omnirc option to `1`. For more information on `omnirc` options, see the *HP Data Protector Troubleshooting Guide*.

What's next?

After you set up OpenSSH and keychain, add clients to the cell using the GUI as described on "Adding clients to the cell" (page 78) or using the CLI by running the `ob2install` command. For information on CLI commands and their parameters, see the *HP Data Protector Command Line Interface Reference*.

NOTE: If secure shell installation cannot be performed because the execution of its command fails, a warning message is issued. However, the installation continues using the standard Data Protector remote installation method.

Adding clients to the cell

Adding clients to the cell

To distribute the Data Protector software to the clients that are not in the Data Protector cell yet, proceed as follows:

1. Start the Data Protector GUI:
   - Original Data Protector GUI (on Windows only):
     - **Start** > **Programs** > **HP Data Protector** > **Data Protector Manager**.
   - Data Protector Java GUI:

     Windows systems: Select **Start** > **Programs** > **HP Data Protector** > **Data Protector Java GUI Manager**.

     In the Connect to a Cell Manager dialog, select or type the name of a Cell Manager and click `Connect`.

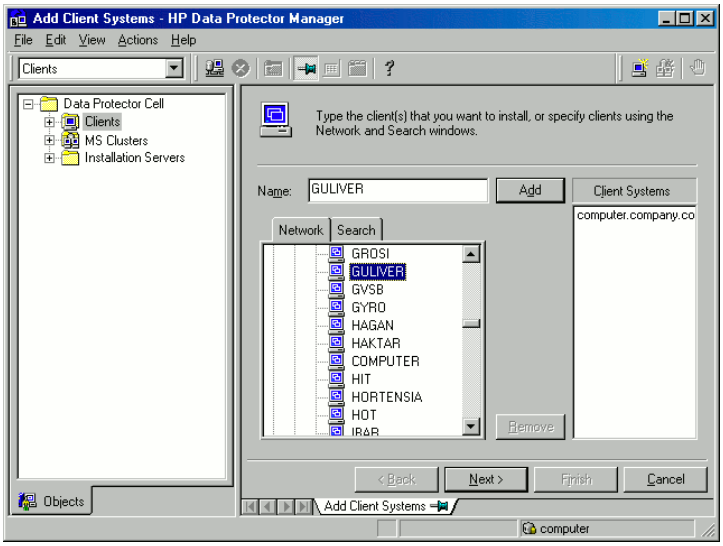
     UNIX systems: Execute:

     ```
     /opt/omni/java/client/bin/javadpgui.sh
     ```

   For details on the Data Protector graphical user interface, see "The Data Protector graphical user interface" (page 25) and the *HP Data Protector Help*.
2. In the Data Protector Manager, switch to the **Clients** context.
3. In the Scoping Pane, right-click **Clients** and click **Add Clients**.

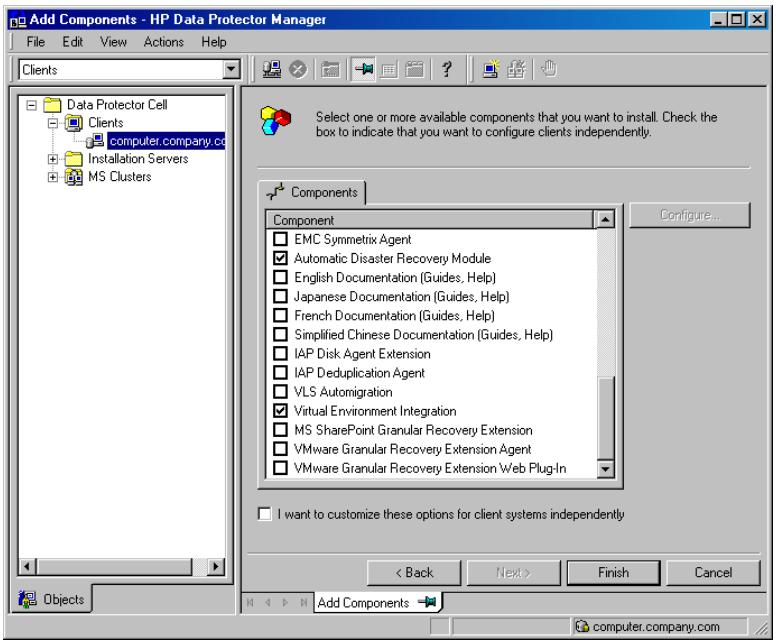
4. If you have more than one Installation Server configured, select the platform of the clients you want to install (UNIX or Windows) and the Installation Server to be used for installing the clients. Click **Next**.
5. Type the names of the clients or search for the clients (on Windows GUI only) you want to install as shown in "Selecting clients" (page 79). Click **Next**.

Figure 19 Selecting clients



6. Select the Data Protector components you want to install as shown in "Selecting components" (page 79). Note that you can select only one type of Media Agent. See "Data Protector components" (page 45).

Figure 20 Selecting components



To change the default user account and target directory (on Windows only) for the installation, click **Options**.

If you selected more than one client and you would like to install different components on each client, click **I want to customize this option for client systems independently** and then click **Next**. Select the components you want to install for each client independently.

Click **Finish** to start the installation.

7. During the installation and when asked, provide the data required (username, password, and on Windows also domain) to access the specific client system and click **OK**.

As soon as a system has the Data Protector software installed and is added to the Data Protector cell, it becomes a Data Protector client.

NOTE: Before you start using the Data Protector GUI on the client system, add a user from that system to an appropriate Data Protector user group. For the procedure and the descriptions of available user rights, see the *HP Data Protector Help*.

Troubleshooting

When the remote installation is finished, you can restart any failed installation procedures using the GUI by clicking **Actions** and **Restart Failed Clients**. If the installation fails again, see "Troubleshooting installation" (page 208).

Adding components to clients

You can install additional Data Protector software components on your existing clients and the Cell Manager. Components can be added remotely or locally. For local installation, see "Changing Data Protector software components" (page 157).

MC/ServiceGuard clients

In the MC/ServiceGuard cluster environment, make sure that the node to which you add the components is active.

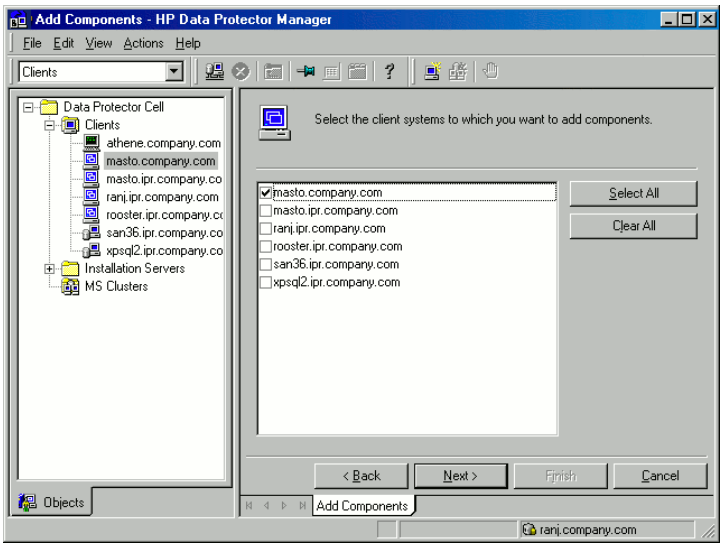
Prerequisite

The corresponding Installation Server must be available.

To distribute the Data Protector software to clients in the Data Protector cell, proceed as follows:

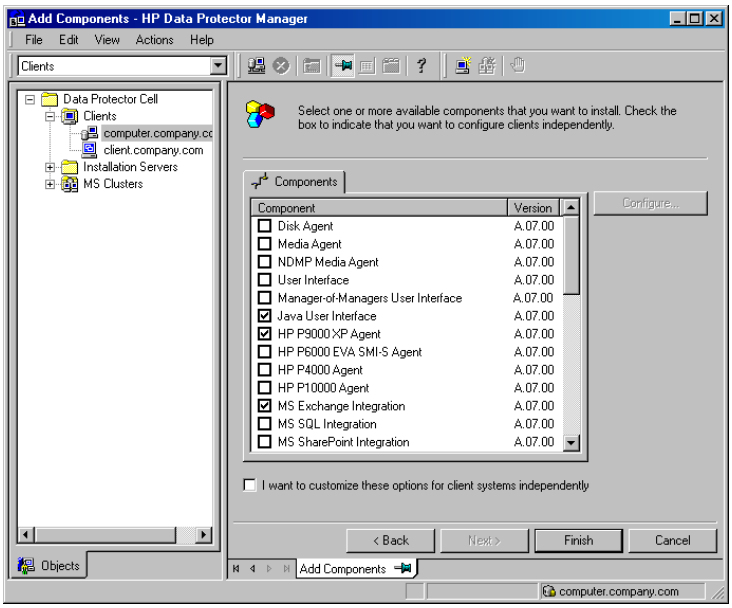
1. In the Data Protector Manager, switch to the **Clients** context.
2. In the Scoping Pane, expand Clients, right-click a client, and then click **Add Components**.
3. If you have more than one Installation Server configured, select the platform of the clients on which you want to install the components (UNIX or Windows) and the Installation Server to be used for installing the components. Click **Next**.
4. Select the clients on which you want to install the components as shown in "Selecting clients" (page 80). Click **Next**.

Figure 21 Selecting clients



5. Select the Data Protector components you want to install as shown in "Selecting components" (page 81). Note that you can select only one type of Media Agent. See "Data Protector components" (page 45).

Figure 22 Selecting components



If you selected more than one client and you want to install different components on each client, click **I want to customize this option for client systems independently** and then click **Next**. Select the components for each client independently.

Click **Finish** to start the installation.

Local installation on UNIX and Mac OS X systems

If you do not have an Installation Server for UNIX installed on your network, or if for some reason you cannot remotely install a client system, Data Protector clients can be installed locally from the UNIX installation DVD-ROM (for HP-UX or Linux).

Before starting the installation procedure, decide which components you need to install on your client system. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- You must have `root` permissions on every target system.
- A POSIX shell (`sh`) must be used for the installation.

NOTE: You can also use the following procedure to upgrade the UNIX clients locally. The script will detect a previous installation and will prompt you to perform the upgrade.

Procedure

Follow the procedure below to install UNIX and Mac OS X clients locally:

1. Insert and mount the UNIX installation DVD-ROM (for HP-UX or Linux).

   Note that the DVD-ROM filesystem uses the Rock Ridge extensions.

2. From the *MountPoint*/LOCAL_INSTALL directory execute the `omnisetup.sh` command.

   The syntax of the command is as follows:

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

   where:

   - *`directory`* is the location where the installation DVD-ROM is mounted. If not specified, the current directory is used.
   - *`name`* is a full hostname of the Cell Manager of the cell to which you want to import the client. If not specified, the client will not be automatically imported to the cell.

     NOTE: In case of upgrading the client that resides on the Cell Manager or Installation Server, you do not need to specify `-install` *`component_list`*. In this case, the setup will select the same components that were installed on the system before the upgrade without issuing a prompt.

   - *`component_list`* is a comma-separated list of component codes to be installed. No spaces are allowed. If the `-install` parameter is not specified, Setup will prompt you separately about installing each available component on the system.

     NOTE: In case of upgrading the client, the setup will select the same components that were installed on the system before the upgrade started, without issuing a prompt.

     The list of the components is presented in the table below. The exact list of the components is subject to the availability on the particular system. For the description of the components, see "Data Protector components" (page 45).

Table 7 Data Protector component codes

Component code	Component
`cc`	User Interface
`da`	Disk Agent
`ma`	General Media Agent
`ndmp`	NDMP Media Agent
`informix`	Informix Integration
`lotus`	Lotus Integration
`oracle8`	Oracle Integration
`vmware`	VMware Integration (Legacy)
`vepa`	Virtual Environment Integration
`ov`	HP Network Node Manager
`sybase`	Sybase Integration
`sap`	SAP R/3 Integration
`sapdb`	SAP DB Integration
`saphana`	SAP HANA Integration
`db2`	DB2 Integration
`emc`	EMC Symmetrix Agent
`smisa`	HP P6000 EVA SMI-S Agent

Table 7 Data Protector component codes *(continued)*

Component code	Component
ssea	HP P9000 XP Agent
vls_am	VLS Automigration
autodr	Automatic Disaster Recovery
javagui	Java Graphical User Interface (graphical user interface, Manager-of-Managers User Interface)
docs	English Documentation (Guides, Help)
fra_ls	French Documentation (Guides, Help)
jpn_ls	Japanese Documentation (Guides, Help)
chs_ls	Simplified Chinese Documentation (Guides, Help)

Example

The example below shows how you can install the `Disk Agent`, `General Media Agent`, `User Interface`, and `Informix Intergration` components on a client that will be automatically imported to the cell with the Cell Manager `computer.company.com`:

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

3. Setup informs you if the installation was completed and if the client was imported to the Data Protector cell.

   The `CORE` component is installed the first time any software component is selected for installation.

   The `CORE-INTEG` component is installed the first time any integration software component is selected for installation or reinstallation.

Running the installation from the hard disk

To copy the installation DVD-ROM to your computer and run the installation or upgrade of UNIX and Mac OS X clients from the hard disk, copy at least the `hpux/DP_DEPOT` and the `LOCAL_INSTALL` directories.

NOTE: The Linux depot does not support local installation. You must copy the HP-UX depot, even on Linux systems.

For example, if you copy installation packages to `/var/dp62`, the directories must be a subdirectory of `/var/dp62`:

```
# pwd
/var/dp62
# ls
DP_DEPOT
LOCAL_INSTALL
```

After you have copied this to the hard disk, change to the `LOCAL_INSTALL` directory and execute the following command:

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

For example:

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

Note, that if you copied the `DP_DEPOT` directory to a different directory (for example due to disk space constraints), the `-source` option is also required.

What's next?

If you did not specify the name of the Cell Manager during the installation, the client will not be imported to the cell. In this case, you should import it using the Data Protector graphical user interface. For the procedure, see "Importing clients to a cell" (page 132). For information on additional configuration tasks, see the *HP Data Protector Help*.

Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library

Data Protector provides a dedicated ADIC/GRAU and StorageTek ACS library policies used to configure an ADIC/GRAU library or StorageTek ACS library as a Data Protector backup device. You need to install a Data Protector Media Agent (the General Media Agent or the NDMP Media Agent) on every system that will be physically connected to a drive in an ADIC/GRAU or StorageTek library. Also, for multihost configurations, you must install a Data Protector Media Agent on the systems that control the ADIC/GRAU or StorageTek library robotics. Note that multihost configuration is a configuration where the library and drive are not connected to the same computer.

For the ADIC/GRAU library, each system on which you install a Media Agent software and it accesses the library robotics through the GRAU/ADIC DAS Server is called a **DAS Client**. For the STK ACS integration, each system on which you install a Media Agent software and it accesses the library robotics through the STK ACS Server is called an **ACS Client**.

NOTE: You need special licenses that depend on the number of drives and slots used in the StorageTek library. For more information, see "Data Protector licensing" (page 187).

Connecting library drives

Physically connect the library drives to the systems where you intend to install a Media Agent software.

For details about supported ADIC/GRAU or STK libraries, see http://support.openview.hp.com/selfsolve/manuals.

For information about how to physically attach a backup device to the system, see "Installing HP-UX clients" (page 51) and the documentation that comes with the ADIC/GRAU or StorageTek library.

For information on how to physically attach a backup device to a supported Windows system, see "Installing Windows clients" (page 48) and the documentation that comes with the ADIC/GRAU or StorageTek library.

Preparing Data Protector clients to use the ADIC/GRAU Library

The following steps pertain to configuring an ADIC/GRAU library, and should be completed before you install a Media Agent software:

1. If the DAS server is based on OS/2, before you configure a Data Protector ADIC/GRAU backup device, create/update the `C:\DAS\ETC\CONFIG` file on the DAS server computer. In this file, a list of all DAS clients must be defined. For Data Protector, this means that each Data Protector client that can control the library robotics must be defined in the file.

   Each DAS client is identified with a unique client name (no spaces), for example `DP_C1`. For example, the contents of the `C:\DAS\ETC\CONFIG` file should look like this:

```
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. On each Data Protector client with a Data Protector Media Agent installed that needs to access ADIC/GRAU DAS library robotics, edit the `omnirc` file (*`Data_Protector_home`*`\omnirc` file on Windows systems, `/opt/omni/.omnirc` file on HP-UX, Solaris, and Linux systems, or `/usr/omni/omnirc` file on AIX systems) and set the following options:

   `DAS_CLIENT` — A unique GRAU client name defined on the DAS server. For example, if the name of the client is "DP_C1", the appropriate line in the `omnirc` file is `DAS_CLIENT=DP_C1`.

   `DAS_SERVER` — The name of the DAS server.

3. You must find out how your ADIC/GRAU library slot allocation policy has been configured, either statically or dynamically. For information on how to check what type of allocation policy is used, see the *AMU Reference Manual*.

   The static policy has a designated slot for each volser, while the dynamic allocation policy assigns the slots randomly. Depending on the policy that has been set, you need to configure Data Protector accordingly.

   If the static allocation policy has been configured, you need to add the following omnirc option to your system controlling the robotics of the library:

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

   NOTE: This applies to HP-UX and Windows.

   For further questions on the configuration of your ADIC/GRAU library, contact your local ADIC/GRAU support or review your ADIC/GRAU documentation.

Installing a Media Agent to use the ADIC/GRAU Library

Prerequisites

The following prerequisites for installation must be met before installing a Media Agent on a system:

- The ADIC/GRAU library must be configured and running. See the documentation that comes with the ADIC/GRAU library.
- Data Protector must be installed and configured. See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
- DAS server must be up and running.

  To control the ADIC/GRAU library, the DAS software is required. Every DAS client must have DAS client software installed. Each media- and device-related action initiated by Data Protector first goes from the DAS client to the DAS server. Then, it is passed to the internal part (AMU - AML Management Unit) of the ADIC/GRAU library which controls the robotics and moves or loads media. After a completed action, the DAS server replies to the DAS client. See the documentation that comes with the ADIC/GRAU library.

- The following information must be obtained before you install a Media Agent:
  - The hostname of the DAS Server (an application that runs on an OS/2 host).
  - The list of available drives with the corresponding DAS name of the drive. The obtained drive names are to be used when configuring the ADIC/GRAU drives in Data Protector.

    If you have defined the DAS clients for your ADIC/GRAU system, you can get this list with one of the following `dasadmin` commands:

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

    where *`client`* is the DAS client for which the reserved drives are to be displayed.

    The `dasadmin` command can be called from the `C:\DAS\BIN` directory on the OS/2 host, or, if installed on other systems, from the directory where the DAS client software

has been installed. On a UNIX client system, this directory is usually the `/usr/local/aci/bin` system directory.

- The list of available Insert/Eject Areas, with corresponding format specifications.

  You can get the list of available Insert/Eject Areas in the Graphical Configuration of AMS (AML Management Software) on an OS/2 host:

  1. Start this configuration from the menu `Admin > Configuration`.
  2. Open the **EIF-Configuration** window by double-clicking the **I/O unit** icon, and then click the **Logical Ranges** field. In the text box, the available Insert/Eject Areas are listed.

     NOTE: One Data Protector library device can handle only one media type. It is important to remember which media type belongs to each one of the specified Insert and Eject Areas, because you will need this data later for configuring Insert/Eject Areas for the Data Protector library.

- A list of UNIX device files for the drives, if you want to install a Media Agent on a UNIX system.

  Run the `ioscan -fn` system command on your system to display the required information.

  For more information on UNIX device files, see "Connecting a backup device to HP-UX systems" (page 53).

- A list of SCSI addresses for the drives, if you want to install a Media Agent on a Windows system. For example, `scsi4:0:1:0`.

  For more information on SCSI addresses, see "Connecting a backup device to Windows systems" (page 50).

Installation

The installation procedure consists of the following steps:

1. Distribute a Media Agent component to clients, using the Data Protector graphical user interface and Installation Server. See "Remote installation" (page 76).

2. Install the ADIC/GRAU library:
   - On a Windows system, do the following:
     a. Copy the `aci.dll`, `winrpc32.dll` and `ezrpc32.dll` libraries to the *`Data_Protector_home`*`\bin` directory. (These three libraries are part of the DAS client software shipped with the ADIC/GRAU library. They can be found either on the installation media or in the `C:\DAS\AMU\` directory on the AMU-PC.)
     b. Copy these three files to the *`%SystemRoot%`*`\system32` directory as well.
     c. Copy `Portinst` and `Portmapper service` to the DAS client. (These requirements are part of the DAS client software shipped with the ADIC/GRAU library. They can be found on the installation media.)
     d. In the Control Panel, go to `Administrative Tools, Services` and start `portinst` to install `portmapper`. The DAS client needs to be restarted to run the `portmapper` service.
     e. After restarting the system, check if `portmapper` and both `rpc services` are running (in the Control Panel, go to **Administrative Tools, Services** and check the status of the services.
   - On an HP-UX system, copy the `libaci.sl` shared library into the `/opt/omni/lib` directory. You must have permissions to access this directory. Make sure that the shared library has read and execute permissions for everyone (root, group and others). The `libaci.sl` shared library is part of the DAS client software shipped with the ADIC/GRAU library. It can be found on the installation media.
   - On an AIX system, copy the `libaci.o` shared library into the `/usr/omni/lib` directory. You must have permissions to access this directory. Make sure that the shared library has read and execute permissions for everyone (root, group and others). The `libaci.o` shared library is part of the DAS client software shipped with the ADIC/GRAU library. It can be found on the installation media.

At this stage, you should have your hardware connected and your DAS software properly installed.

Run the following command to check whether the library drives are properly connected to your system:

Windows systems: *`Data_Protector_home`*`\bin\devbra -dev`

HP-UX systems: `/opt/omni/lbin/devbra -dev`

AIX systems: `/usr/omni/bin/devbra -dev`

See the library drives with corresponding device files displayed in the list.

What's next?

Once a Media Agent is installed and the ADIC/GRAU library is physically connected to the system, see the *HP Data Protector Help* index: "configuring, backup devices" for information about additional configuration tasks, such as configuring backup devices and media pools.

Preparing Data Protector clients to use the StorageTek Library

The following prerequisites for installation must be met before installing a Media Agent:

- The StorageTek library must be configured and running. See the documentation that comes with the StorageTek library.
- Data Protector must be installed and configured. See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

- The following information must be obtained before you start installing a Media Agent software:
  - The *hostname* of the host where ACSLS is running.
  - A list of ACS drive IDs that you want to use with Data Protector. The obtained drive IDs are to be used when configuring the StorageTek drives in Data Protector. To display the list, log in on the host where ACSLS is running and execute the following command:

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

    You will have to enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

    ```
    ACSSA> query drive all
    ```

    The format specification of an ACS drive must be the following:

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

  - A list of available ACS CAP IDs and the ACS CAP format specification. To display the list, login on the host where ACSLS is running and execute the following command:

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

    Enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

    ```
    ACSSA> query cap all
    ```

    The format specification of an ACS CAP must be the following:

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

  - A list of UNIX device files for the drives, if you want to install a Media Agent on a UNIX system.

    Run the `ioscan -fn` system command on your system to display the required information.

    For more information on UNIX device files, see "Connecting a backup device to HP-UX systems" (page 53).

  - A list of SCSI addresses for the drives, if you want to install a Media Agent on a Windows system. For example, `scsi4:0:1:0`.

    For more information on SCSI addresses, see "Connecting a backup device to Windows systems" (page 50).

- Make sure that the drives that will be used for Data Protector are in the `online` state. If a drive is not in the `online` state, change the state with the following command on the ACSLS host: `vary drive drive_id online`
- Make sure that the CAPs that will be used for Data Protector are in the state `online` and in `manual` operating mode.

  If a CAP is not in the `online` state, change the state using the following command:

  ```
  vary cap cap_id online
  ```

  If a CAP is not in `manual` operating mode, change the mode using the following command:

  ```
  set cap manual cap_id
  ```

Installing a Media Agent to use the StorageTek Library

The installation procedure consists of the following steps:

1. Distribute a Media Agent component to clients using the Data Protector graphical user interface and Installation Server for UNIX. See "Remote installation" (page 76).

2. Start the ACS `ssi` daemon for every ACS client:

   Windows systems:

   Install the `LibAttach` service. For details, see the ACS documentation. Make sure that during the configuration of `LibAttach` service the appropriate ACSLS hostname is entered. After successful configuration, the `LibAttach` services are started automatically and will be started automatically after every system restart as well.

   HP-UX, Solaris, and Linux systems:

   Run the following command:

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

   AIX systems:

   Run the following command:

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

   NOTE: After you have installed the `LibAttach` service, check if the `libattach\bin` directory has been added to the system path automatically. If not, add it manually.

   For more information on the `LibAttach` service, see the documentation that comes with the StorageTek library.

3. Run the following command to check whether or not the library drives are properly connected to your system:
   - On HP-UX, Solaris, and Linux ACS client: `/opt/omni/lbin/devbra -dev`
   - On Windows ACS client: *`Data_Protector_home`*`\bin\devbra -dev`
   - On AIX ACS client: `/usr/omni/bin/devbra -dev`

   See the library drives with corresponding device files/SCSI addresses displayed in the list.

What's next?

Once a Media Agent is installed and the StorageTek library is physically connected to the system, see the *HP Data Protector Help* index: "configuring, backup devices" for information about additional configuration tasks, such as configuring backup devices and media pools.

Installing the Data Protector integration clients

Data Protector integrations are software components that allow you to run an online backup of the database applications, such as Oracle Server or Microsoft Exchange Server, with Data Protector. Data Protector ZDB integrations are software components that allow you to run zero downtime backup and instant recovery using disk arrays, such as HP P6000 EVA Disk Array Family.

The systems running database applications are called **integration clients**; the systems using ZDB disk arrays for backing up and storing data are called **ZDB integration clients**. Such clients are installed with the same installation procedure as any other clients on Windows or on UNIX, provided that the appropriate software component has been selected (for example, `MS Exchange Integration` component for backing up the Microsoft Exchange Server database, `HP P6000 EVA SMI-S Agent` component for ZDB and IR with HP P6000 EVA Disk Array Family, and so on).

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- You need a license to use the Data Protector integration with a database application. For information about licensing, see "Data Protector 7.00 product structure and licenses" (page 204).
- At this point, you should have the Cell Manager and Installation Server (optionally, for remote installation) already installed on your network. For instructions, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Before starting the installation procedure, decide which other Data Protector software components you want to install on your client together with an integration component. For the list of the Data Protector software components and their descriptions, see "Data Protector components" (page 45).

Note that in the cases stated below you need to install the following Data Protector components:

- The `Disk Agent` component to be able to back up filesystem data with Data Protector. You can use the Disk Agent for the following purposes:
  - To run a filesystem backup of important data that *cannot* be backed up using a database application backup.
  - To run a filesystem test backup of a database application server (for example, Oracle Server or Microsoft SQL Server). You need to test a filesystem backup *before* configuring the Data Protector integration with a database application and resolve communication and other problems related to the application and Data Protector.
  - To run zero downtime backup of filesystems or disk images.
  - To restore from backup media to the application system on LAN in case of SAP R/3 ZDB integrations.
- The `User Interface` component to gain access to the Data Protector GUI and the Data Protector CLI on the Data Protector integration client.
- The `General Media Agent` component if you have backup devices connected to the Data Protector integration client. On Data Protector clients used to access an NDMP dedicated drive through the NDMP Server, the `NDMP Media Agent` is required.

Integration clients can be installed remotely using the Installation Server for Windows or for UNIX, or locally from the Windows or from the UNIX installation DVD-ROM (for HP-UX or Linux).

For additional information on specific integration clients, see the corresponding sections below:

- "Microsoft Exchange Server clients" (page 92)
- "Microsoft SQL Server clients" (page 94)
- "Microsoft SharePoint Server clients" (page 94)
- "Microsoft Volume Shadow Copy Service clients" (page 96)
- "Sybase Server clients" (page 96)
- "Informix Server clients" (page 96)
- "SAP R/3 clients" (page 97)
- "SAP MaxDB clients" (page 97)
- "SAP HANA Appliance clients" (page 97)
- "Oracle Server clients" (page 97)
- "IBM DB2 UDB clients" (page 98)
- "Lotus Notes/Domino Server clients" (page 98)

- "VMware clients" (page 98)
- "Microsoft Hyper-V clients" (page 100)
- "HP NNM clients" (page 101)
- "NDMP Server clients" (page 101)
- "HP P4000 SAN Solutions clients" (page 101)
- "HP P6000 EVA Disk Array Family clients" (page 102)
- "HP P9000 XP Disk Array Family clients" (page 106)
- "HP P10000 Storage Systems clients" (page 111)
- "EMC Symmetrix clients" (page 111)
- "VLS automigration clients" (page 114)

After you have installed the integration clients, HP recommends that you enable invocations of the Data Protector commands from any directory by adding the command locations to the appropriate environment variable on each client. Procedures in the Data Protector documentation assume the variable value has been extended. Command locations are listed in the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* and the `omniintro` man page.

After the installation, also see the *HP Data Protector Integration Guide*, the *HP Data Protector Zero Downtime Backup Administrator's Guide*, or the *HP Data Protector Zero Downtime Backup Integration Guide* to configure Data Protector integration clients.

Remote installation

You install the client software from the Installation Server to clients using the Data Protector graphical user interface. For the step-by-step procedure for remotely installing the software, see "Remote installation" (page 76).

After the remote installation, the client system automatically becomes a member of the Data Protector cell.

Local installation

If you do not have an Installation Server for the respective operating system installed in your environment, you have to perform local installation from the Windows, or from the UNIX installation DVD-ROM (for HP-UX or Linux), depending on the platform you install a client to. For instructions, see "Installing Windows clients" (page 48) or "Local installation on UNIX and Mac OS X systems" (page 81).

If you do not choose a Cell Manager during the installation, the client system has to be manually imported into the cell after the local installation. See "Importing clients to a cell" (page 132).

Installing cluster-aware integrations

The Data Protector cluster-aware integration clients must be installed locally, from the DVD-ROM, on each cluster node. During the local client setup, install, in addition to the other client software components, the appropriate integration software components (such as `Oracle Integration` or `HP Data Protector P6000 EVA SMI-S Agent`).

You can also install a cluster-aware database application and a ZDB Agent on the Data Protector Cell Manager. Select the appropriate integration software component during the Cell Manager setup.

The installation procedure depends on a cluster environment where you install your integration client. See the clustering related sections corresponding to your operating system:

- "Installing Data Protector on MC/ServiceGuard" (page 119)
- "Installing Data Protector on Microsoft Cluster Server" (page 120)

- "Installing Data Protector on a Microsoft Hyper-V cluster" (page 128)
- "Installing Data Protector clients on a Veritas Cluster" (page 129)
- "Installing Data Protector clients on a Novell NetWare Cluster" (page 129)
- "Installing Data Protector on IBM HACMP Cluster" (page 130)

For more information on clustering, see the *HP Data Protector Help* index: "cluster, MC/ServiceGuard" and the *HP Data Protector Concepts Guide*.

What's next?

When the installation has been completed, see the *HP Data Protector Integration Guide* for information on configuring the integration.

Microsoft Exchange Server clients

Data Protector components that need to be installed on Microsoft Exchange Server systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- "Data Protector Microsoft Exchange Server 2003/2007 integration" (page 92)
- "Data Protector Microsoft Exchange Server 2010 integration" (page 92)
- "Data Protector Microsoft Exchange Server Single Mailbox integration" (page 93)
- "Data Protector Microsoft Volume Shadow Copy Service integration" (page 93)
- "Data Protector Granular Recovery Extension for Microsoft Exchange Server" (page 93)

Data Protector Microsoft Exchange Server 2003/2007 integration

It is assumed that your Microsoft Exchange Server is up and running.

To be able to back up the Microsoft Exchange Server databases, install the `MS Exchange Integration` component on the Microsoft Exchange Server system.

The Microsoft Exchange Single Mailbox integration agent will be installed as part of the Data Protector Microsoft Exchange Server integration component.

Data Protector Microsoft Exchange Server 2010 integration

It is assumed that your Microsoft Exchange Server 2010 environment is up and running.

To be able to back up Microsoft Exchange Server databases, ensure that the following Data Protector components are installed on all the Microsoft Exchange Server systems:

- `MS Exchange Server 2010 Integration`
- `MS Volume Shadow Copy Integration`
- The appropriate Data Protector disk array agent (if Microsoft Exchange Server data resides on a disk array)

NOTE: For VSS transportable backup sessions, the `MS Volume Shadow Copy Integration` component and the appropriate Data Protector disk array agent must also be installed on the backup systems.

In DAG environments, the DAG virtual system (host) must also be imported to the Data Protector cell. On how to import a client to a Data Protector Cell, see the *HP Data Protector Help* index: "importing, client systems".

NOTE:

- Because the Data Protector Microsoft Exchange Server 2010 integration is based on VSS technology, Data Protector automatically installs the `MS Volume Shadow Copy Integration` component when you install the `MS Exchange Server 2010 Integration` component. If the `MS Volume Shadow Copy Integration` component is already installed, it is upgraded.
- If you remove the `MS Exchange Server 2010 Integration` component from a system, the `MS Volume Shadow Copy Integration` component is not removed automatically. Also note that you cannot remove the `MS Volume Shadow Copy Integration` component from a system where the `MS Exchange Server 2010 Integration` component is installed.

Data Protector Microsoft Exchange Server Single Mailbox integration

It is assumed that your Microsoft Exchange Server is up and running.

To be able to back up the Microsoft Exchange Server Mailbox and Public Folder items, install the `MS Exchange Integration` component on the Microsoft Exchange Server system. In a DAG environment, install the component on all Microsoft Exchange Server systems that are part of a DAG.

On Microsoft Exchange Server 2007 systems, you need to install an additional package to enable the functionality of the Data Protector Microsoft Exchange Single Mailbox integration. The package is named Microsoft Exchange Server MAPI Client and Collaboration Data Objects (`ExchangeMapiCdo.EXE`), and can be downloaded free of charge from the Microsoft web site http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en.

Data Protector Microsoft Volume Shadow Copy Service integration

See "Microsoft Volume Shadow Copy Service clients" (page 96).

Data Protector Granular Recovery Extension for Microsoft Exchange Server

You must use this Data Protector extension to be able to recover individual Microsoft Exchange Server mailbox items. Depending on the configuration of your Microsoft Exchange Server environment, you should install the corresponding Data Protector component on:

- single Microsoft Exchange Server system: this system
- multiple Microsoft Exchange Server systems: each Exchange Server system on which the Mailbox Server role is configured
- Microsoft Exchange Server Database Availability Group (DAG) environment: any of the Exchange Server systems in DAG

Prerequisites

- On the chosen Microsoft Exchange Server system, the following must be installed:
  - The Data Protector component `MS Exchange Server 2010 Integration`
  - All required non-Data Protector components

    For details, see the installation chapter in the *HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server*.
- On the chosen Microsoft Exchange Server system, the TCP/IP port 60000 must be free.

For instructions on how to locally or remotely install the Data Protector `MS Exchange Granular Recovery Extension` component, see the *HP Data Protector Help* index: "installing, client systems".

Microsoft SQL Server clients

It is assumed that your Microsoft SQL Server is up and running.

To be able to back up the Microsoft SQL Server database, you need to select the `MS SQL Integration` component during the installation procedure.

Microsoft SharePoint Server clients

Data Protector components that need to be installed in a Microsoft SharePoint Server environment vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- "Data Protector Microsoft SharePoint Server 2003 integration" (page 94)
- "Data Protector Microsoft SharePoint Server 2007/2010/2013 integration" (page 94)
- "Data Protector Microsoft SharePoint Server 2007/2010/2013 VSS based solution" (page 94)
- "Data Protector Microsoft Volume Shadow Copy Service integration" (page 95)
- "Data Protector Granular Recovery Extension for Microsoft SharePoint Server" (page 95)

Data Protector Microsoft SharePoint Server 2003 integration

It is assumed that your Microsoft SharePoint Portal Server and related Microsoft SQL Server instances are up and running.

To be able to back up Microsoft SharePoint Portal Server objects, install the following Data Protector components:

- `MS SharePoint Integration` - on Microsoft SharePoint Portal Server systems
- `MS SQL Integration` - on Microsoft SQL Server systems

Data Protector Microsoft SharePoint Server 2007/2010/2013 integration

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to back up Microsoft SharePoint Server objects, install the following Data Protector components:

- `MS SharePoint 2007/2010/2013 Integration` – on Microsoft SharePoint Server systems (Microsoft SQL Server systems are excluded)
- `MS SQL Integration` – on Microsoft SQL Server systems

NOTE: If a system has both the Microsoft SQL Server and Micosoft SharePoint Server installed, install both Data Protector components on it.

Data Protector Microsoft SharePoint Server 2007/2010/2013 VSS based solution

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to back up Microsoft SharePoint Server objects, install the following Data Protector components:

- `MS Volume Shadow Copy Integration` on the Microsoft SQL Server systems and the Microsoft SharePoint Server systems that have at least one of the following services enabled:

  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`

- The Data Protector `User Interface` component on one of the Microsoft SharePoint Server systems with the Data Protector `MS Volume Shadow Copy Integration` component installed and on which you plan to configure and start a backup.

Data Protector Microsoft Volume Shadow Copy Service integration

See "Microsoft Volume Shadow Copy Service clients" (page 96).

Data Protector Granular Recovery Extension for Microsoft SharePoint Server

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to recover individual Microsoft SharePoint Server objects, install the `MS SharePoint Granular Recovery Extension` on the Microsoft SharePoint Server Central Administration system.

- When installing the component locally, the Data Protector installation wizard will display the MS SharePoint GRE options dialog box. Specify the Farm Administrator user name and password.
- To install this component remotely, select the `MS SharePoint Granular Recovery Extension`, click **Configure** and specify the Farm Administrator user name and password in the MS SharePoint GRE options dialog box.

NOTE:

- You can install the Granular Recovery Extension only to systems with Microsoft SharePoint Server installed.
- Ensure that the Data Protector components that are needed to back up Microsoft SharePoint Server data are also installed in the Microsoft SharePoint Server environment.

Microsoft Volume Shadow Copy Service clients

To back up VSS writers or only the filesystem using VSS, install the following Data Protector software components on the application system (*local backup*) or on both the application and backup system (*transportable backup*):

- `MS Volume Shadow Copy Integration`.
- If you are using a disk array (with hardware providers), the appropriate disk array agent (`HP P4000 Agent`, `HP P6000 EVA SMI-S Agent`, `HP P9000 XP Agent`, or `HP P10000 Agent`).

After you have installed the VSS integration, you need to resolve the source volumes on the application system if you will perform the ZDB-to-disk and ZDB-to-disk+tape sessions (instant recovery–enabled sessions). Run the resolve operation from any VSS client in the cell as follows:

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

However, if you do not resolve or fail to resolve the application system, it will be resolved automatically, as long as the `OB2VSS_DISABLE_AUTO_RESOLVE` option in the `omnirc` file is set to `0` (default). In this case, the backup time for creating a replica is prolonged.

For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

Sybase Server clients

It is assumed that your Sybase Backup Server is running.

For backing up the Sybase database, you need to select the following Data Protector component during the installation procedure:

- `Sybase Integration` - to be able to back up a Sybase database
- `Disk Agent` - install the Disk Agent for two reasons:
  - To run a filesystem backup of Sybase Backup Server. Make this backup *before* configuring your Data Protector Sybase integration and resolve all problems related to Sybase Backup Server and Data Protector.
  - To run a filesystem backup of important data that *cannot* be backed up using Sybase Backup Server.

Informix Server clients

It is assumed that your Informix Server is up and running.

For backing up the Informix Server database, you need to select the following Data Protector component during the installation procedure:

- `Informix Integration` - to be able to back up an Informix Server database
- `Disk Agent` - install the Disk Agent for two reasons:
  - To run a filesystem backup of Informix Server. Make this backup *before* configuring your Data Protector Informix Server integration and resolve all problems related to Informix Server and Data Protector.
  - To run a filesystem backup of important Informix Server data (such as, ONCONFIG file, `sqlhosts` file, ON-Bar emergency boot file, `oncfg_`*`INFORMIXSERVER`*`.`*`SERVERNUM`*, configuration files, and so on) that *cannot* be backed up using ON-Bar.

IBM HACMP Cluster

If Informix Server is installed in the IBM HACMP cluster environment, install the `Informix Integration` component on all the cluster nodes.

SAP R/3 clients

Prerequisites

- Ensure that the following Oracle software is installed and configured:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 software
  - SQL*Plus
- It is assumed that your SAP R/3 Database Server is up and running.

NOTE: The Data Protector SAP R/3 integration backup specifications are fully compatible with the previous version of Data Protector. Data Protector will run all backup specifications created by earlier Data Protector versions. You cannot use backup specifications created by the current version of Data Protector on older versions of Data Protector.

To be able to back up the SAP R/3 database, select the following components during the installation procedure:

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

  Data Protector requires a Disk Agent to be installed on Backup Servers (clients with filesystem data to be backed up).

SAP MaxDB clients

It is assumed that your SAP MaxDB Server is up and running.

To be able to back up the SAP MaxDB database, you need to select the following Data Protector components during the installation procedure:

- `SAP DB Integration` - to be able to run an integrated online backup of an SAP MaxDB database
- `Disk Agent` - to be able to run a filesystem backup of an SAP MaxDB database

SAP HANA Appliance clients

To integrate Data Protector with your SAP HANA Appliance (SAP HANA), install the following Data Protector software components on the SAP HANA system:

- `SAP HANA Integration`

  This component enables integrated backup of a complete SAP HANA database and the SAP HANA redo logs.

- `Disk Agent`

  This component enables non-integrated backup of the SAP HANA configuration files using the Data Protector filesystem backup functionality. After a disaster, having a backup image of the SAP HANA configuration files available helps you more easily identify and restore your changes.

In case of a distributed SAP HANA environment, install the above components on each SAP HANA system that constitutes such environment.

Oracle Server clients

It is assumed that your Oracle Server is up and running.

To be able to back up the Oracle database, you need to select the `Oracle Integration` component during the installation procedure.

HP OpenVMS

On HP OpenVMS, after you installed the Oracle integration and configured it as described in the *HP Data Protector Integration Guide for Oracle and SAP*, verify that the `-key Oracle8` entry is present in `OMNI$ROOT:[CONFIG.CLIENT]omni_info`, for example:

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId 12172 -flags
0x7 -ntpath "" -uxpath "" -version 7.00
```

If the entry is not present, copy it from `OMNI$ROOT:[CONFIG.CLIENT]omni_format`. Otherwise, the Oracle integration will not be shown as installed on the OpenVMS client.

IBM DB2 UDB clients

It is assumed that your DB2 Server is up and running.

To be able to back up the DB2 database, you need to select the `DB2 Integration` and the `Disk Agent` components during the installation procedure.

In a physically partitioned environment, install the `DB2 Integration` and `Disk Agent` components on every physical node (system) on which the database resides.

NOTE: Log in as user `root` to perform the installation.

Lotus Notes/Domino Server clients

It is assumed that your Lotus Notes/Domino Server is up and running.

To be able to back up the Lotus Notes/Domino Server database, you need to select the `Lotus Integration` and the `Disk Agent` components during the installation procedure. You will need the `Disk Agent` component to be able to back up filesystem data with Data Protector in the following purposes:

- Backing up important data that *cannot* be backed up using Lotus Integration Agent. These are so called non-database files, which need to be backed up to provide a complete data protection solution for a Lotus Notes/Domino Server, such as `notes.ini`, `desktop.dsk`, all `*.id files`.
- Testing the filesystem backup to resolve communication and other problems related to the application and Data Protector.

Lotus Domino Cluster

Install the `Lotus Integration` and the `Disk Agent` components on the Domino servers that will be used for backup, and, if you plan to restore Domino databases to other Domino servers containing replicas of these databases, install the components on these Domino servers as well.

VMware clients

Data Protector components that need to be installed on VMware systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- "Data Protector Virtual Environment integration" (page 98)
- "Data Protector VMware (Legacy) integration" (page 99)
- "Data Protector Granular Recovery Extension for VMware vSphere" (page 99)

Data Protector Virtual Environment integration

It is assumed that all systems on which you intend to install components are up and running.

On systems that should control backup and restore sessions (**backup hosts**), install the following Data Protector components:

- `Virtual Environment Integration`
- `Disk Agent`

NOTE:

- The `Disk Agent` component enables you to use the **Browse** button when restoring to a directory on the backup host. If the component is not installed, you must type the target directory yourself.
- The client that you intend to use as a backup host should *not* have the VMware Consolidated Backup (VCB) software installed.

Data Protector VMware (Legacy) integration

It is assumed that VirtualCenter Server systems (if they exist) and ESX Server systems are up and running. To be able to install VMware clients remotely, first set OpenSSH. For details, see the *HP Data Protector Help* index: "installing, client systems".

Install the Data Protector `VMware Integration (Legacy)` component on the following clients:

- All ESX Server systems from which you plan to back up virtual machines
- VirtualCenter systems (if they exist)
- Backup proxy systems (if you plan to use the **VCBfile** and **VCBimage** backup methods)
- Windows systems (physical or virtual) to which you plan to restore filesystems of virtual machines

NOTE: The Data Protector `VMware Integration (Legacy)` component cannot be installed on ESXi Server systems. Consequently, not all backup and restore functionality is available for virtual machines running on ESXi Server systems.

Clusters

Install the `VMware Integration (Legacy)` component on both cluster nodes, regardless of whether you have ESX Server systems or VirtualCenter systems in a cluster.

Data Protector Granular Recovery Extension for VMware vSphere

It is assumed that the Data Protector Virtual Environment integration is installed and configured as described in the *HP Data Protector Integration Guide for Virtualization Environments*. The virtual machines you plan to restore data to must have VMware tools 4.x or later installed.

Limitations

- Only remote installation of the Data Protector Granular Recovery Extension for VMware vSphere is supported.

Installation procedure

Mount proxy system:

- Remotely install the following Data Protector components to the mount proxy system:
  - `Virtual Environment Integration`
  - `VMware Granular Recovery Extension Agent`

  For installation instructions, see the *HP Data Protector Help* index: "installing, client systems".

vCenter Servers (VirtualCenter Servers):

1. If no Data Protector component is installed on the vCenter Server, remotely install the Data Protector `Disk Agent` component to this system.

2. Import the vCenter Server to the Data Protector cell as a Data Protector client. For details, see the *HP Data Protector Help* index: "importing, client systems".

   Follow the steps:

   1. In the Import Client wizard, in the **Type** drop-down list, select **VMware vCenter**.
   2. In the Import Client wizard, specify the login credentials:
      - **Port**: Specify the port that VMware vSphere is using. By default, VMware vSphere uses the port 443.
      - **User name** and **Password**: Specify an operating system user account that has the following VMware vSphere privileges:

        Web service root

        Optionally, change the web service entry point URI. Default: `/sdk`.

3. Follow the steps:

   vCenter Server 5.1:

   - To perform installation by using the automatic deployment feature of VMware Web Server:
     1. In the VMware Web Server folder `installation_directory` (default path: `C:\Program Files\VMware\Infrastructure\tomcat`), in the `conf` subfolder, open the configuration file `server.xml`.
     2. In the Host node, change the value of the `autoDeploy` parameter from `false` to `true`.
     3. In the Control Panel, under Administrative Tools, open Services and restart the VMware VirtualCenter Management Webservices service.
     4. Remotely install the `VMware Granular Extension Web Plug-In` component to the vCenter Server.
   - To perform installation without using the automatic deployment feature of VMware Web Server:
     1. Remotely install the `VMware Granular Extension Web Plug-In` component to the vCenter Server.

        The VMware GRE post-installation script will fail.
     2. In the VMware Web Server folder `installation_directory`, in the `webapps` subfolder, extract the `VMWareGRE.war` file to a new directory named `VMWareGRE` (case sensitive).
     3. From the `Data_Protector_home\bin` folder, execute:

        ```
        perl -I "..\lib\perl" vmwgre_wp.pl -install
        ```
     4. In the Control Panel, under Administrative Tools, open Services and restart the VMware VirtualCenter Management Webservices service.

   Earlier vCenter Server versions:

   Remotely install the Data Protector `VMware Granular Extension Web Plug-In` component to the vCenter Server.

Microsoft Hyper-V clients

Data Protector components that need to be installed on Microsoft Hyper-V systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- "Data Protector Virtual Environment integration" (page 98)
- "Data Protector Microsoft Volume Shadow Copy Service integration" (page 101)

Data Protector Virtual Environment integration

It is assumed that all systems on which you intend to install components are up and running.

On systems that should control backup and restore sessions (**backup hosts**), install the following Data Protector components:

- `Virtual Environment Integration`
- `MS Volume Shadow Copy Integration`
- `Disk Agent`

NOTE: The `Disk Agent` component enables you to use the **Browse** button when restoring to a directory on the backup host. If the component is not installed, you must type the target directory yourself.

On Microsoft Hyper-V systems, install the following Data Protector component:

- `MS Volume Shadow Copy Integration`

NOTE: If your Microsoft Hyper-V systems are configured in a cluster, they must be installed as cluster-aware clients. For details, see "Installing Data Protector on a Microsoft Hyper-V cluster" (page 128).

On backup systems (applicable for VSS transportable backups), install the following Data Protector component:

- `MS Volume Shadow Copy Integration`

NOTE: A *backup host* and a *backup system* are not one and the same system.

Data Protector Microsoft Volume Shadow Copy Service integration

For details on which components need to be installed on Microsoft Hyper-V systems, see "Microsoft Volume Shadow Copy Service clients" (page 96).

HP NNM clients

It is assumed that your NNM system is up and running.

To be able to back up the NNM database, you need to select the `HP NNM Backup Integration` and the `Disk Agent` components during the installation procedure. You will need the Disk Agent to run pre-backup and post-backup scripts used for backup purposes.

NDMP Server clients

It is assumed that your NDMP Server is up and running.

During the installation procedure, select the `NDMP Media Agent` and install it to all Data Protector clients accessing the NDMP dedicated drives.

NOTE: If a Data Protector client will not be used to access an NDMP dedicated drive through the NDMP Server, but it will be used only to control the robotics of the library, either the `NDMP Media Agent` or the `General Media Agent` can be installed on such a client.

Note that only one Media Agent can be installed on one Data Protector client.

HP P4000 SAN Solutions clients

To integrate HP P4000 SAN Solutions with Data Protector, install the following Data Protector software components on the application and backup systems:

- `MS Volume Shadow Copy Integration`
- `HP P4000 Agent`

To perform ZDB-to-disk+tape or ZDB-to-tape sessions, additionally install the following Data Protector software component on the backup system:

- `General Media Agent`

HP P6000 EVA Disk Array Family clients

To integrate HP P6000 EVA Disk Array Family with Data Protector, install the following Data Protector software components on the application and backup systems:

- `HP P6000 EVA SMI-S Agent`
- `General Media Agent`

  Install the `General Media Agent` component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- `Disk Agent`

  Install the `Disk Agent` component on the application and backup systems to run zero downtime backup of filesystems or disk images. Clients without the Disk Agent installed are not listed in the `Application system` and `Backup system` drop-down lists when creating a ZDB backup specification.

IMPORTANT: On Microsoft Windows Server 2008 systems, two Windows Server 2008 hotfixes must be installed to enable normal operation of the Data Protector HP P6000 EVA Disk Array Family integration. You can download the required hotfix packages from the Microsoft websites http://support.microsoft.com/kb/952790 and http://support.microsoft.com/kb/971254.

This additional requirement does not apply to Windows Server 2008 R2 systems.

Installing in a cluster

You can install the HP P6000 EVA Disk Array Family integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with other applications

To install the HP P6000 EVA Disk Array Family integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the HP P6000 EVA Disk Array Family integration with Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, and Microsoft Volume Shadow Copy Service.

HP P6000 EVA Disk Array Family integration with Oracle Server

Prerequisites

- The following software must be installed and configured on the application system and on the backup system for the backup set ZDB method:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL*Plus

  The Oracle software on the backup system must be installed in the same directory as on the application system. The binaries should be identical to the binaries on the application system. You can achieve this either by copying the files and system environment from the application

system to the backup system, or by a clean installation of the Oracle binaries on the backup system with the same installation parameters as on the application system.

- The Oracle datafiles on the application system must be installed on source volumes that will be replicated using the SMI-S agent you have installed.

  Depending on the location of the Oracle control file, online redo log files, and Oracle SPFILE, the following two options are possible:

  - Oracle control file, online redo log files, and Oracle SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

    By default, instant recovery is enabled for such configuration.

  - Oracle control file, online redo log files, and Oracle SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

    By default, instant recovery is *not* enabled for such configuration. You can enable instant recovery by setting the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options. For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

  The Oracle archive redo log files do not have to reside on source volumes.

  If some Oracle data files are installed on symbolic links, then these links have to be created on the backup system too.

Installation procedure

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
   - `HP P6000 EVA SMI-S Agent` – on both the application system and backup system
   - `Oracle Integration` – on both the application system and backup system

NOTE:

- The Data Protector `Oracle Integration` component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector `Oracle Integration` and `HP P6000 EVA SMI-S Agent` components on all the systems where the Oracle instances are running.
- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

Prerequisites

- The following Oracle software must be installed on the application system.
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or filesystems.
  - The Oracle datafiles *must* reside on a disk array.
  - For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
  - For *offline backup*, the control file and online redo logs *must* reside on a disk array.
  - Archived redo log files do not have to reside on a disk array.

  If the Oracle control file, online redo logs, and Oracle SPFILE reside on the *same* LVM volume group or source volume as Oracle datafiles, set the Data Protector `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF`, and `ZDB_ORA_INCLUDE_SPF` `omnirc` options. Otherwise, you cannot run ZDB–to–disk and ZDB–to–disk+tape sessions. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

  NOTE: If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

  UNIX systems: If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX, ensure that the following users exist on the application system:
  - `ora`*`ORACLE_SID`* with the primary group `dba`
  - *`ORACLE_SID`*`adm` in the UNIX group `sapsys`
- The SAP R/3 software must be correctly installed on the application system.

  The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

  NOTE: The location of the directories is dependent on the environment (UNIX systems) or registry (Windows system) variables. For more information, see the SAP R/3 documentation.

  - *`ORACLE_HOME`*`/dbs` (UNIX systems) *`ORACLE_HOME`*`\database` (Windows systems) - the Oracle and SAP profiles)
  - *`ORACLE_HOME`*`/bin` (UNIX systems) *`ORACLE_HOME`*`\bin` (Windows systems) - the Oracle binaries
  - *`SAPDATA_HOME`*`/sapbackup` (UNIX systems) *`SAPDATA_HOME`*`\sapbackup` (Windows systems) - the SAPBACKUP directory with BRBACKUP log files

- *SAPDATA_HOME*/saparch (UNIX systems) *SAPDATA_HOME*\saparch (Windows systems) - the SAPARCH directory with BRARCHIVE log files
- *SAPDATA_HOME*/sapreorg (UNIX systems) *SAPDATA_HOME*\sapreorg (Windows systems)
- *SAPDATA_HOME*/sapcheck (UNIX systems) *SAPDATA_HOME*\sapcheck (Windows systems)
- *SAPDATA_HOME*/saptrace (UNIX systems) *SAPDATA_HOME*\saptrace (Windows systems)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIX systems)

  c:\Oracle*ORACLE_SID*\sys\exe\run (Windows systems)

NOTE: If you plan to do instant recovery, ensure that the sapbackup, saparch, and sapreorg directories reside on different source volumes than the Oracle data files.

UNIX systems

On UNIX systems, if the last six directories do not reside at the above specified destinations, create appropriate links to them.

On UNIX systems, the directory /usr/sap/*ORACLE_SID*/SYS/exe/run must be owned by the UNIX user ora*ORACLE_SID*. The owner of the SAP R/3 files must be the UNIX user ora*ORACLE_SID* and the UNIX group dba with setuid bit set (chmod 4755 ...). The exception is the file BRRESTORE, which must be owned by the UNIX user *ORACLE_SID*adm.

UNIX example

If *ORACLE_SID* is PRO, then the permissions inside the directory /usr/sap/PRO/SYS/exe/run should look like:

```
-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
```

Installation procedure

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
   - HP P6000 EVA SMI-S Agent
   - SAP R/3 Integration
   - Disk Agent

NOTE: You need to install SAP R/3 Integration on the backup system only if you plan to run SAP compliant ZDB sessions in which BRBACKUP is started on the backup system.

On Windows systems, the Data Protector software components must be installed using the SAP R/3 administrator user account, and this account must be included in the ORA_DBA or ORA_*SID*_DBA local group on the system where the SAP R/3 instance is running.

HP P6000 EVA Disk Array Family integration with Microsoft Exchange Server

Prerequisite

The Microsoft Exchange Server database must be installed on the application system source volumes. The following objects must be located on the source volumes:

- Microsoft Information Store (MIS)
- optionally, Key Management Service (KMS)
- optionally, Site Replication Service (SRS)

To be able to back up transaction logs, disable Circular Logging on the Microsoft Exchange Server.

Installation procedure

Install the following Data Protector software components:

- `HP P6000 EVA SMI-S Agent` – on both the application and backup systems
- `MS Exchange Integration` – on the application system only

HP P6000 EVA Disk Array Family integration with Microsoft SQL Server

Prerequisite

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However, if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

Installation procedure

Install the following Data Protector software components on both the application and the backup systems:

- `HP P6000 EVA SMI-S Agent` – on both the application and backup systems
- `MS SQL Integration` – on the application system only

HP P9000 XP Disk Array Family clients

To integrate HP P9000 XP Disk Array Family with Data Protector, install the following Data Protector software components on the application and backup systems:

- `HP P9000 XP Agent`
- `General Media Agent`

  Install the `General Media Agent` component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- `Disk Agent`

  Install the `Disk Agent` component on the application and backup systems to run zero downtime backup of filesystems or disk images. Clients without the Disk Agent installed are not listed in the `Application system` and `Backup system` drop-down lists when creating a ZDB backup specification.

IMPORTANT: On Microsoft Windows Server 2008 systems, two Windows Server 2008 hotfixes must be installed to enable normal operation of the Data Protector HP P9000 XP Disk Array Family integration. You can download the required hotfix packages from the Microsoft websites http://support.microsoft.com/kb/952790 and http://support.microsoft.com/kb/971254.

This additional requirement does not apply to Windows Server 2008 R2 systems.

Installing in a cluster

You can install the HP P9000 XP Disk Array Family integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with other applications

To install the HP P9000 XP Disk Array Family integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the HP P9000 XP Disk Array Family integration with Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, and Microsoft Volume Shadow Copy Service.

HP P9000 XP Disk Array Family integration with Oracle Server

Prerequisites

- The following software must be installed and configured on the application system and on the backup system for the backup set ZDB method:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL*Plus

  The Oracle software on the backup system must be installed in the same directory as on the application system. The binaries should be identical to the binaries on the application system. You can achieve this either by copying the files and system environment from the application system to the backup system, or by a clean installation of the Oracle binaries on the backup system with the same installation parameters as on the application system.
- The Oracle data files on the application system must be installed on HP P9000 XP Disk Array Family LDEVs that are mirrored to the backup system.

  In case of the backup set method, if some Oracle data files are installed on symbolic links, then these links have to be created on the backup system too.

  Depending on the location of the Oracle control file, online redo log files, and Oracle SPFILE, the following two options are possible:

  - Oracle control file, online redo log files, and Oracle SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

    By default, instant recovery is enabled for such configuration.
  - Oracle control file, online redo log files, and Oracle SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

    By default, instant recovery is *not* enabled for such configuration. You can enable instant recovery by setting the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options. For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

  The Oracle archive redo log files do not have to reside on source volumes.

Installation procedure

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
   - `HP P9000 XP Agent` – on both the application system and backup system
   - `Oracle Integration` – on both the application system and backup system

NOTE:

- The Data Protector `Oracle Integration` component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector `Oracle Integration` and `HP P9000 XP Agent` components on all the systems where the Oracle instances are running.
- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

HP P9000 XP Disk Array Family integration with SAP R/3

Prerequisites

- The following Oracle software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or filesystems.
  - The Oracle datafiles *must* reside on a disk array.
  - For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
  - For *offline backup*, the control file and online redo logs *must* reside on a disk array.
  - Archived redo log files do not have to reside on a disk array.

  If the Oracle control file, online redo logs, and Oracle SPFILE reside on the *same* LVM volume group or source volume as Oracle datafiles, set the Data Protector `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF`, and `ZDB_ORA_INCLUDE_SPF` `omnirc` options. Otherwise, you cannot run ZDB–to–disk and ZDB–to–disk+tape sessions. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

NOTE: If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

UNIX systems: If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX, ensure that the following users exist on the application system:
  - ora*ORACLE_SID* with the primary group dba
  - *ORACLE_SID*adm in the UNIX group sapsys
- The SAP R/3 software must be correctly installed on the application system.

  The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

NOTE: The location of the directories is dependent on the environment (UNIX systems) or registry (Windows system) variables. For more information, see the SAP R/3 documentation.

- *ORACLE_HOME*/dbs (UNIX systems)

  ORACLE_HOME\database (Windows systems) - the Oracle and SAP R/3 profiles)
- *ORACLE_HOME*/bin or (UNIX systems)

  ORACLE_HOME\bin (Windows systems) - the Oracle binaries
- *SAPDATA_HOME*/sapbackup (UNIX systems)

  SAPDATA_HOME\sapbackup (Windows systems) - the SAPBACKUP directory with BRBACKUP log files
- *SAPDATA_HOME*/saparch (UNIX systems)

  SAPDATA_HOME\saparch (Windows systems) - the SAPARCH directory with BRARCHIVE log files
- *SAPDATA_HOME*/sapreorg (UNIX systems)

  SAPDATA_HOME\sapreorg (Windows systems)
- *SAPDATA_HOME*/sapcheck (UNIX systems)

  SAPDATA_HOME\sapcheck (Windows systems)
- *SAPDATA_HOME*/saptrace (UNIX systems)

  SAPDATA_HOME\saptrace (Windows systems)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIX systems)

  c:\Oracle*ORACLE_SID*\sys\exe\run (Windows systems)

  NOTE: If you plan to do instant recovery, ensure that the sapbackup, saparch, and sapreorg directories reside on different source volumes than the Oracle data files.

UNIX systems

On UNIX systems, if the last six directories do not reside at the above specified destinations, create appropriate links to them.

On UNIX systems, the directory /usr/sap/*ORACLE_SID*/SYS/exe/run must be owned by the UNIX user ora*ORACLE_SID*. The owner of the SAP R/3 files must be the UNIX user

ora*ORACLE_SID* and the UNIX group dba with setuid bit set (chmod 4755 ...). The exception is the file BRRESTORE, which must be owned by the UNIX user *ORACLE_SID*adm.

UNIX example

If *ORACLE_SID* is PRO, then the permissions inside the directory /usr/sap/PRO/SYS/exe/run should look like:

```
-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
```

Installation procedure

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
   - HP P9000 XP Agent
   - SAP R/3 Integration
   - Disk Agent

NOTE: You need to install SAP R/3 Integration on the backup system only if you plan to run SAP compliant ZDB sessions in which BRBACKUP is started on the backup system.

On Windows systems, the Data Protector software components must be installed using the SAP R/3 administrator user account, and this account must be included in the ORA_DBA or ORA_*SID*_DBA local group on the system where the SAP R/3 instance is running.

HP P9000 XP Disk Array Family integration with Microsoft Exchange Server

Prerequisite

The Microsoft Exchange Server database must be installed on the application system on the HP P9000 XP Disk Array Family volumes (LDEVs), which are mirrored to the backup system. The mirroring can be HP BC P9000 XP or HP CA P9000 XP and the database installed on a filesystem. The following objects must be located on volumes that are mirrored:

- Microsoft Information Store (MIS)
- optionally, Key Management Service (KMS)
- optionally, Site Replication Service (SRS)

To be able to back up transaction logs, disable Circular Logging on the Microsoft Exchange Server.

Installation procedure

Install the following Data Protector software components:

- HP P9000 XP Agent – on both the application and the backup system
- MS Exchange Integration – on the application system only

HP P9000 XP Disk Array Family integration with Microsoft SQL Server

Prerequisite

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However,

if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

Installation procedure

Install the following Data Protector software components on both the application and the backup systems:

- `HP P9000 XP Agent`
- `MS SQL Integration`

HP P10000 Storage Systems clients

To integrate HP P10000 Storage Systems with Data Protector, install the following Data Protector software components on the application and backup systems:

- `MS Volume Shadow Copy Integration`
- `HP P10000 Agent`

  You can only install this component remotely, as this component is only available with patch bundle set 7.01 and superseding updates for the Data Protector version 7.00.

Additionally, reinstall the following component remotely, as only the updated version from the patch bundle set 7.01 and superseding updates for the Data Protector version 7.00 supports HP P10000 Storage Systems:

- `User Interface`

To perform ZDB-to-disk+tape or ZDB-to-tape sessions, additionally install the following Data Protector software component on the backup system:

- `General Media Agent`

EMC Symmetrix clients

To integrate EMC Symmetrix with Data Protector, install the following Data Protector software components on the application and backup systems:

- `EMC Symmetrix Agent` (SYMA)

  Before remotely installing the `EMC Symmetrix Agent` component, install the following two EMC components:

  - EMC Solution Enabler
  - EMC Symmetrix TimeFinder or EMC Symmetrix Remote Data Facility (SRDF) microcode and license.

- `General Media Agent`

  Install the `General Media Agent` component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- `Disk Agent`

  Install the `Disk Agent` component on the application and backup systems to run disk image and filesystem ZDB. Clients without Disk Agent installed are not listed in the `Application system` and `Backup system` drop-down lists when creating a ZDB backup specification.

Installing in a cluster

You can install the EMC Symmetrix integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with other applications

To install the EMC Symmetrix integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the EMC Symmetrix integration with Oracle and SAP R/3.

EMC Symmetrix Integration with Oracle

Prerequisites

- The following software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL*Plus
- The Oracle database files used by the application system must be installed on EMC Symmetrix devices which are mirrored to the backup system.

  The database can be installed on disk images, logical volumes or filesystems. The following Oracle files have to be mirrored:
  - Datafiles
  - Control file
  - Online redo log files

  The archive redo log files have to reside on non-mirrored disks.

Installation procedure

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
   - `EMC Symmetrix Agent` – on both the application system and backup system
   - `Oracle Integration` – on both the application system and backup system

NOTE:

- The Data Protector `Oracle Integration` component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector `Oracle Integration` and `EMC Symmetrix Agent` components on all the systems where the Oracle instances are running.
- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

EMC Symmetrix Integration with SAP R/3

Prerequisites

- The following Oracle software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 software
  - SQL*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or filesystems.
  - The Oracle datafiles *must* reside on a disk array.
  - For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
  - For *offline backup*, the control file and online redo logs *must* reside on a disk array.
  - The archived redo log files do not have to reside on a disk array.

NOTE: If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

UNIX systems: If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX, ensure that the following users exist on the application system:
  - `ora`*`ORACLE_SID`* with the primary group `dba`
  - *`ORACLE_SID`*`adm` in the UNIX group `sapsys`
- The SAP R/3 software must be correctly installed on the application system.

  The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

NOTE: The location of the directories depends on the environment variables. For more information, see the SAP R/3 documentation.

- *`ORACLE_HOME`*`/dbs` - the Oracle and SAP R/3 profiles
- *`ORACLE_HOME`*`/bin` - the Oracle binaries
- *`SAPDATA_HOME`*`/sapbackup` - the SAPBACKUP directory with BRBACKUP log files
- *`SAPDATA_HOME`*`/saparch` - the SAPARCH directory with BRARCHIVE log files
- *`SAPDATA_HOME`*`/sapreorg`
- *`SAPDATA_HOME`*`/sapcheck`
- *`SAPDATA_HOME`*`/saptrace`
- `/usr/sap/`*`ORACLE_SID`*`/SYS/exe/run`

NOTE: If you plan to do instant recovery, ensure that the `sapbackup`, `saparch`, and `sapreorg` directories reside on different source volumes than the Oracle data files.

If the last six directories do not reside at the above specified destinations, create appropriate links to them.

The directory `/usr/sap/ORACLE_SID/SYS/exe/run` must be owned by the UNIX user `ora`*`ORACLE_SID`*. The owner of the SAP R/3 files must be the UNIX user `ora`*`ORACLE_SID`* and the UNIX group `dba` with setuid bit set (chmod 4755 ...). The exception is the file BRRESTORE, which must be owned by the UNIX user *`ORACLE_SID`*`adm`.

Example

If *`ORACLE_SID`* is PRO, then the permissions inside the directory `/usr/sap/PRO/SYS/exe/run` should look like:

```
-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
```

Installation procedure

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
   - `EMC Symmetrix Agent`
   - `SAP R/3 Integration`
   - `Disk Agent`

NOTE: You need to install `SAP R/3 Integration` on the backup system only if you plan to run SAP compliant ZDB sessions in which BRBACKUP is started on the backup system.

EMC Symmetrix Integration with Microsoft SQL Server

Prerequisite

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However, if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

Installation procedure

Install the following Data Protector software components on both the application and the backup systems:

- `EMC Symmetrix Agent`
- `MS SQL Integration`

VLS automigration clients

The Data Protector media copy functionality allows you to copy media after performing a backup. The integration with the HP Virtual Library System (VLS) enhances this functionality by providing a solution that combines the internal VLS copy capabilities with the Data Protector media management and monitoring functionality.

To integrate Data Protector with VLS automigration to perform smart media copying, install the `VLS Automigration` Data Protector software component.

Prerequisites

Perform the following steps:

1. Configure the VLS virtual storage as required using the Command View VLS. For more information, see the VLS documentation.
2. Connect one or more physical tape libraries to the VLS.
3. Import the VLS client to the Data Protector cell.

Installing localized Data Protector user interface

Data Protector 7.00 provides a localized Data Protector user interface on Windows and UNIX systems. The user interface parts that are localized are the Data Protector GUI (original Data Protector GUI, Data Protector Java GUI) and messages and notifications of the Data Protector CLI. Localized documentation (guides and Help) is also provided. For more information on which parts of the Data Protector documentation set are localized, see the *HP Data Protector Product Announcements, Software Notes, and References*.

NOTE: By default, during the Data Protector installation, the language support for all supported languages is installed and the localized Data Protector user interface is started according to the locale environment set on the system.

On Linux systems, messages and notifications of the Data Protector CLI are only available in the English language.

Troubleshooting

If the English version of original Data Protector GUI is started after you installed a different language support, verify the following:

1. Check that the following files exist:

   For French Language Support:

   - Windows systems: *Data_Protector_home*\bin\OmniFra.dll
   - HP-UX systems: /opt/omni/lib/nls/fr.iso88591/omni.cat
   - Solaris systems: /opt/omni/lib/nls/fr.ISO8859-1/omni.cat

   For Japanese Language Support:

   - Windows systems: *Data_Protector_home*\bin\OmniJpn.dll
   - HP-UX systems: /opt/omni/lib/nls/ja.eucJP/omni.cat and /opt/omni/lib/nls/ja.SJIS/omni.cat
   - Solaris systems: /opt/omni/lib/nls/ja.eucJP/omni.cat and /opt/omni/lib/nls/ja.PCK/omni.cat

   For Simplified Chinese Language Support:

   - Windows systems: *Data_Protector_home*\bin\OmniChs.dll
   - HP-UX systems: /opt/omni/lib/nls/zh_CN.gb18030/omni.cat and /opt/omni/lib/nls/zh_CN.gb18030/omni.cat
   - Solaris systems: /opt/omni/lib/nls/zh_CN.GB18030/omni.cat and /opt/omni/lib/nls/zh_CN.GB18030/omni.cat

2. Check the locale environment settings on your system:

   Windows systems: In the Windows Control Panel, click Regional Options and check that you have an appropriate language selected in locale and language settings.

   UNIX systems: Run the following command to set the locale environment:

   ```
   export LANG=lang locale
   ```

   where *lang* represents the locale environment setting in the following format: language[_territory].codeset.

   For example, ja_JP.eucJP, ja_JP.SJIS, or ja_JP.PCK for Japanese locale; zh_CN.GB18030 for Simplified Chinese locale, and fr_FR.iso88591 for French locale. Note that the codeset part of the LANG variable is required and must match the codeset part of the corresponding directory name.

Installing the localized Data Protector documentation

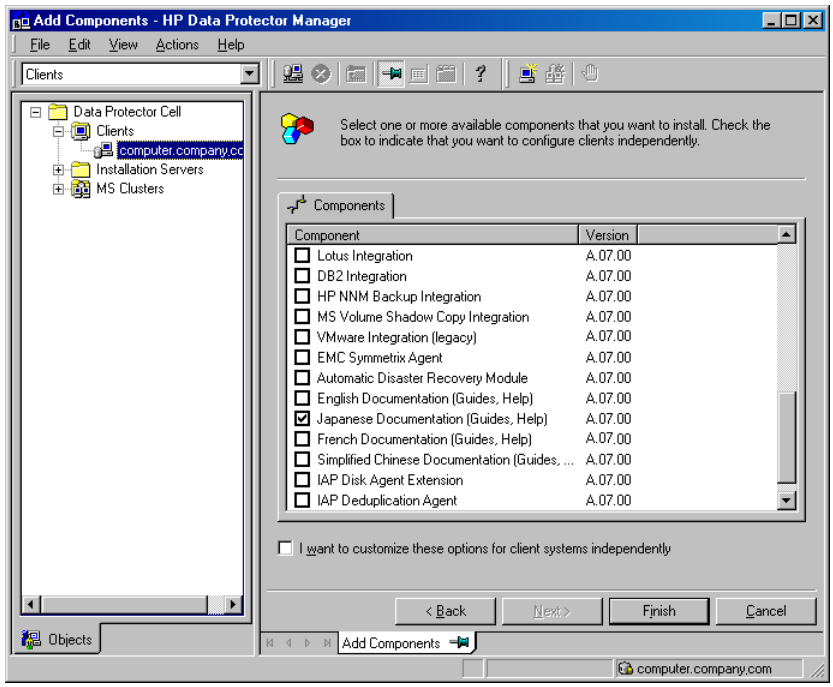
Installing localized Data Protector documentation on Windows systems

Remote installation

When distributing the Data Protector localized documentation remotely using the Installation Server, select the appropriate component in the **Component Selection** page of the **Add Components** wizard, as shown on "Installing localized documentation remotely" (page 117).

For the procedure on how to remotely add the Data Protector software components to clients, see "Remote installation" (page 76).

Figure 23 Installing localized documentation remotely

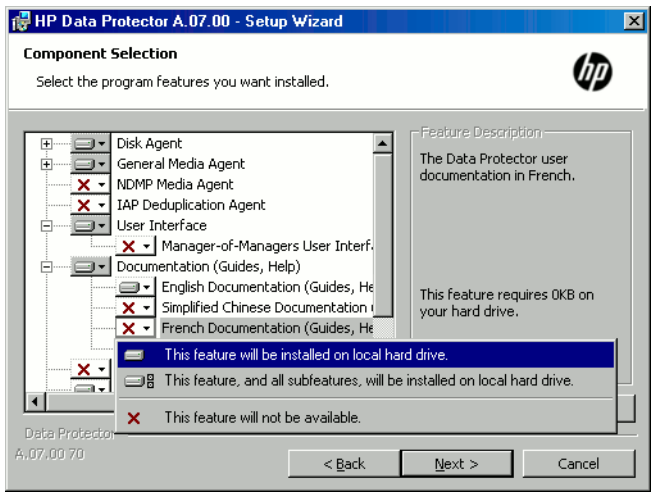


Local installation

To install the localized Data Protector documentation locally on Windows systems, select the appropriate component in the **Custom Setup** page of the **Setup** wizard, as shown on "Selecting localized documentation at setup" (page 117).

For the local installation procedure, see "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Figure 24 Selecting localized documentation at setup



Installing localized Data Protector documentation on UNIX systems

Remote installation

When distributing the Data Protector localized documentation remotely using the Installation Server, select the appropriate component in the **Component Selection** page of the **Add Components** wizard, as shown on "Installing localized documentation remotely" (page 117).

For the procedure on how to remotely add the Data Protector software components to clients, see "Remote installation" (page 76).

Local installation

You can install the French, Japanese, or Simplified Chinese documentation locally only on a Data Protector client using the `omnisetup.sh` command. Specify the `fra_ls`, `jpn_ls`, or `chs_ls` software components depending on the language support you need. For the detailed procedure, see "Local installation on UNIX and Mac OS X systems" (page 81).

If you are using the `swinstall`, `pkgadd`, or `rpm` utility to install the Data Protector Cell Manager or Installation Server, you can only install the English documentation. If you want the localized Data Protector documentation to reside on the same system with the Cell Manager or Installation Server, you need to install the additional language packs remotely.

Installing the Data Protector Single Server Edition

The Single Server Edition (SSE) of Data Protector is designed for small environments where backups run on only one device connected to a Cell Manager. It is available for supported Windows and for HP-UX platforms.

To install the Cell Manager and (optionally) Installation Server, follow the instructions in "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

Limitations

When considering the SSE license, be aware of the following limitations:

Limitations of SSE for Windows

- SSE supports backups to only one device concurrently, connected to a single Cell Manager.
- One 10-slot DDS autochanger only is supported.
- UNIX (also HP-UX) clients and servers are not supported. If a backup is attempted to a UNIX machine, the session is aborted.
- If a cell has a Windows Cell Manager, you can back up only Windows clients. Backup to Novell Netware clients is not supported.
- Adding extension products is not supported with SSE.
- Clustering is not supported with SSE.
- Disaster Recovery is not supported with SSE.

The number of Windows clients is not limited.

For supported devices, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Limitations of SSE for HP-UX

- SSE supports backups to only one device concurrently, connected to a single Cell Manager.
- One 10-slot DDS autochanger only is supported.
- On a UNIX Cell Manager, you cannot back up servers - only UNIX clients, Windows clients, Solaris clients, and Novell NetWare clients.
- Adding extension products is not supported with SSE.
- Clustering is not supported with SSE.

The number of clients (UNIX, Windows) is not limited.

For supported devices, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Installing a password

For the step-by-step instructions on how to install a password on the Cell Manager, see "Data Protector passwords" (page 198).

Installing Data Protector web reporting

Data Protector Web Reporting is installed with other Data Protector components by default, and as such, you can use it locally from your system.

You can also install it on a Web server and in that way make it available on other systems which do not need to have any of the Data Protector software components installed.

Prerequisites

To use Data Protector Web Reporting on your system, see the *HP Data Protector Product Announcements, Software Notes, and References* for prerequisites and limitations.

Installation

To install Data Protector Web Reporting to a Web server, do the following:

1. Copy the following Data Protector Java reporting files to the server. The server does not have to be a Data Protector client.
   - On Windows systems with the Data Protector user interface installed, the files are located in the following directory:

     `Data_Protector_home\java\bin`
   - On a UNIX system with the Data Protector user interface installed, the files are located in the following directory:

     `/opt/omni/java/bin`
2. Open the `WebReporting.html` file in your browser to access the Data Protector Web Reporting.

   You must make the file available to the users of the Web reporting in the full URL form. For example, you can put a link to this file from your Intranet site.

TIP: By default, no password is needed to use Data Protector Web Reporting. You can provide one and in that way restrict the access to the Web reporting. For the procedure, see the *HP Data Protector Help* index: "Web reports, limiting access to".

What's next?

When the installation has been completed, see the *HP Data Protector Help* index: "Web reporting interface, configuring notifications" for more information on configuration issues and creating your own reports.

Installing Data Protector on MC/ServiceGuard

Data Protector supports MC/ServiceGuard (MC/SG) for HP-UX and Linux. For details on supported operating system versions, see the *HP Data Protector Product Announcements, Software Notes, and References*.

If your Cell Manager is to be cluster-aware, note that the virtual server IP address should be used for licenses.

Installing a cluster-aware Cell Manager

Prerequisites

Before you install a Data Protector Cell Manager on MC/ServiceGuard, check the following:

- Decide which systems are going to be the Primary Cell Manager and the Secondary Cell Manager(s). All of them must have MC/ServiceGuard installed and must be configured as cluster members.
- Data Protector Cell Manager, with recommended patches, and all other Data Protector software components for the integrations you want to have in the cluster, must be installed on the Primary node and each of the Secondary nodes.

  The installation procedure is standard procedure for installing the Cell Manager system. See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

What's next?

When the installation has been completed, you must configure the installed Primary Cell Manager and the Secondary Cell Manager(s), and the Cell Manager package. For more information on configuring MC/ServiceGuard with Data Protector, see the *HP Data Protector Help* index: "cluster, MC/ServiceGuard".

Installing an Installation Server on cluster nodes

You can install the Installation Server on a secondary MC/ServiceGuard node and use if for remote installation."Installing Installation Servers for UNIX systems" (page 38).

Installing cluster-aware clients

IMPORTANT: The Data Protector cluster-aware clients must be installed on all the cluster nodes.

The installation procedure is standard procedure for installing Data Protector on an UNIX client. For detailed instructions, see "Installing HP-UX clients" (page 51) and "Installing Linux clients" (page 59).

What's next?

When the installation has been completed, you must import the virtual server (the hostname specified in the cluster package) to the Data Protector cell. See "Importing a cluster-aware client to a cell" (page 134).

For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuration".

Installing Data Protector on Microsoft Cluster Server

For supported operating systems for Microsoft Cluster Server integration, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

NOTE:

If your Cell Manager is to be cluster-aware, the Cell Manager's virtual server IP address should be used for licenses.

Installing a cluster-aware Cell Manager

Prerequisites

Before you install the cluster-aware Data Protector Cell Manager, the following prerequisites must be fulfilled:

- Clustering functionality must be installed properly on all cluster nodes. For example, you must be able to move groups from one to another node as many times as needed, without problems with shared disks.
- Make sure resources with the following names do not exist on the cluster:

  `OBVS_MCRS`, `OBVS_VELOCIS`, `OmniBack_Share`

  Data Protector uses these names for the Data Protector virtual server. If such resources exist, delete or rename them.

  This can be done as follows:

  1. Click **Start** > **Programs** >**Administrative Tools** > **Cluster Administrator**.
  2. Check the resource list and delete or rename these resources, if necessary.
- At least one group in the cluster should have a file cluster resource defined. Data Protector will install some of its data files in this file cluster resource under a specific folder.

  Windows Server 2008 and Windows Server 2012: Data files are installed on the *`File Server`* resource under the shared folder selected by the user at installation.

  Other Windows systems: Data files are installed on the *`File Share`* resource under the folder specified when the file cluster resource was created.

  For instructions on how to define a file cluster resource, see the cluster-specific documentation. Note that the file share name of the file cluster resource cannot be `OmniBack`.
- If the virtual server does not exist in the same group as the file cluster resource, create a new virtual server using a free registered IP address and associate a network name with it.
- The file cluster resource where Data Protector is to be installed must have the `IP Address`, `Network Name`, and `Physical Disk` set among the file cluster resource dependencies. This ensures that the Data Protector cluster group can run on any node independently of any other group.
- Ensure that only the cluster administrator has access to shared folder of the file cluster resource, and they should have full access to it.
- Data Protector is installed on the same location (drive and path name) on all cluster nodes. Ensure that these locations are free.
- If you start the cluster-aware Cell Manager installation from a network share, you must have access to this share from all cluster nodes.
- Ensure no other Microsoft Installer-based installations are running on any cluster node.
- Each system (node) of the cluster should be running and functioning properly.
- To enable installation of the cluster-aware Data Protector Cell Manager on a server cluster with Microsoft Cluster Service (MSCS) running on Windows Server 2008 or Windows Server 2012, perform the procedure described in "Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation" (page 228).

Considerations

- Setup must be started under the cluster service account on the system (node) where the file cluster resource is active, so that shared folder of the file cluster resource can be accessed

directly. The resource owner (the system where the resource is active) can be determined using Cluster Administrator.

- To properly install and configure cluster-aware Data Protector Cell Manager, a domain account with the following user rights must be provided during installation:
  - Administrator rights on the Cell Manager system
  - Cluster Administrator rights within the cluster
  - Password Never Expires
  - Logon as a service
  - User Cannot Change Password
  - All logon hours are allowed

IMPORTANT: An account with administrator rights on all the cluster systems (nodes) is required for Microsoft Cluster Server installation. You should use this account to install Data Protector as well. Failing to do so results in Data Protector services running in the ordinary instead of the cluster-aware mode.

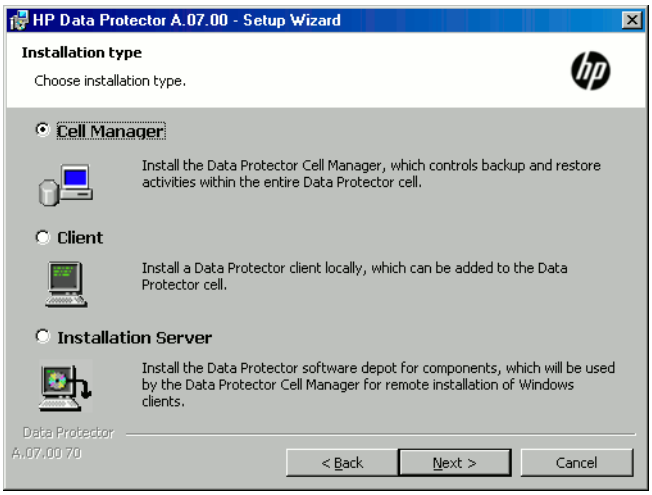
Local installation procedure

The cluster-aware Data Protector Cell Manager must be installed locally, from the DVD-ROM. Perform the following:

1. Insert the Windows installation DVD-ROM.

   On Windows Server 2008 and Windows Server 2012, the User Account Control dialog is displayed. Click **Continue** to proceed with the installation.
2. In the HP Data Protector window, select **Install Data Protector** to start the Data Protector Setup Wizard.
3. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
4. In the Installation Type page, select **Cell Manager** and then click **Next** to install Data Protector Cell Manager software.

Figure 25 Selecting the installation type



5. Setup automatically detects that it is running in a cluster environment. Select **Install cluster-aware Cell Manager** to enable a cluster setup.

   Select the cluster group, the virtual hostname, and the file cluster resource on which Data Protector shared files and the database will reside.

NOTE: If you select **Install Cell Manager on this node only**, the Cell Manager will *not* be cluster aware. See "Installing a Windows Cell Manager" (page 32).

Figure 26 Selecting the cluster resource on Windows Server 2008

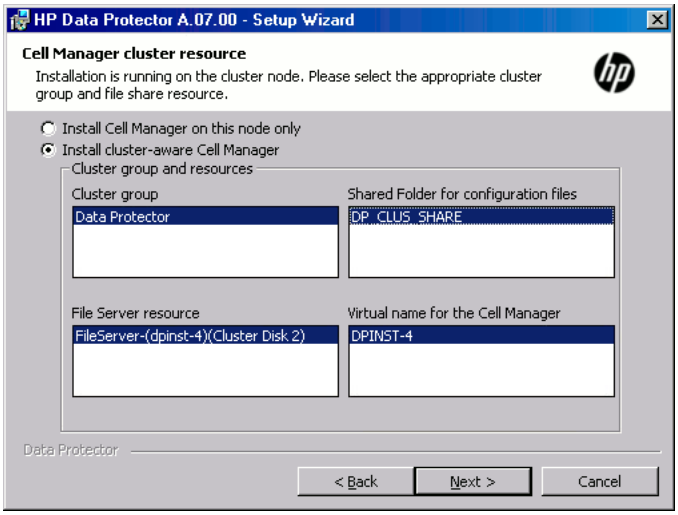
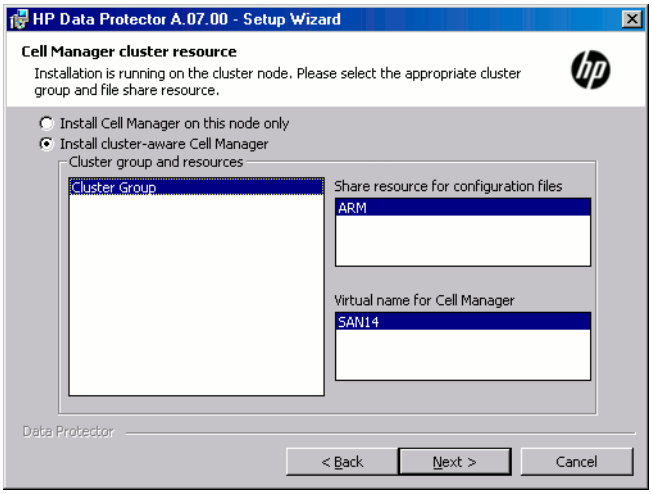
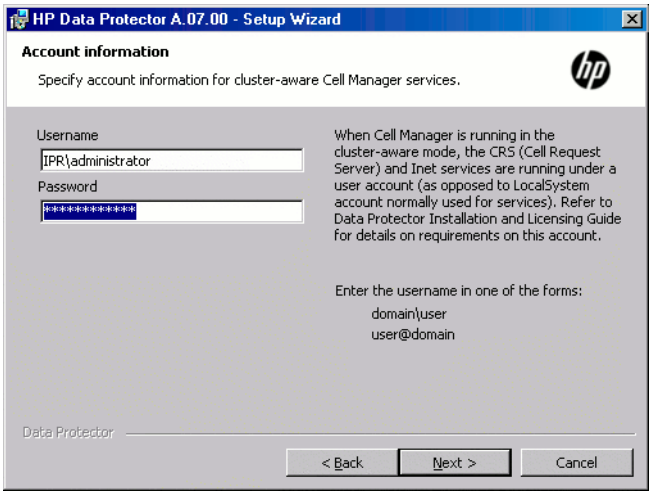


Figure 27 Selecting the cluster resource on other Windows systems



6. Enter the username and password for the account that will be used to start Data Protector services.

Figure 28 Entering the account information



7. Click **Next** to install Data Protector on the default folder.

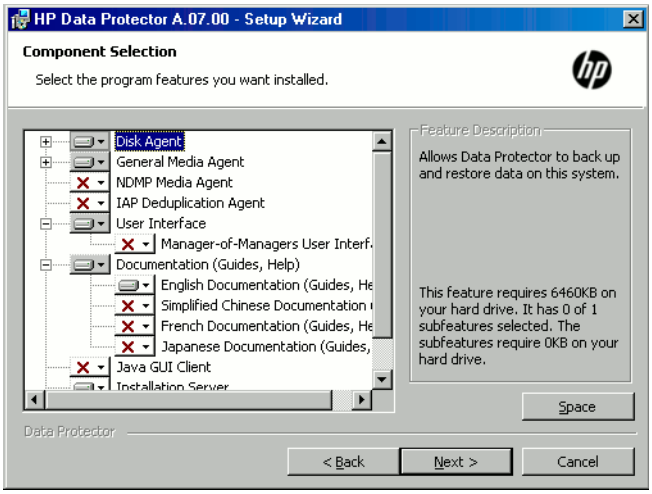
   Otherwise, click **Change** to open the Change Current Destination Folder window and enter a new path.

8. In the Component Selection window, select the components you want to install on all cluster nodes and cluster virtual servers. Click **Next**.

   The MS Cluster Support files are installed automatically.

   The selected components will be installed on all the cluster nodes.

Figure 29 Component selection page



9. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

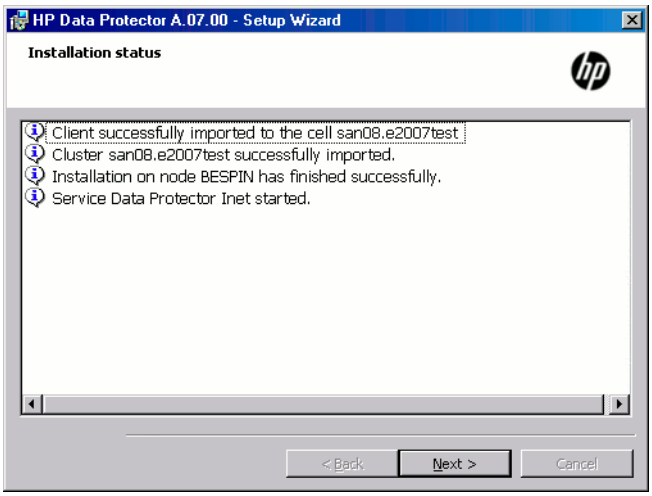
   Note that only inbound firewall rules are automatically created and you must manually create any outbound firewall rules. For the required port ranges, see the *HP Data Protector Help* index: "firewall support".

   Click **Next**.

10. The component selection summary page is displayed. Click **Install**.

11. The Installation setup page is displayed. Click **Next**.

Figure 30 Installation status page



12. To start Data Protector immediately after install, select **Start the Data Protector Manager GUI**.

    To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

    On operating systems other than Windows Server 2003 x64, Windows Server 2008 x64, and Windows Server 2012 x64, to install or upgrade the HP AutoPass utility, select the **Start AutoPass installation** or **Upgrade AutoPass installation** option.

    It is *not* recommended to install the AutoPass utility on Microsoft server cluster, because it will be installed only on one node and not on all nodes. However, if you install AutoPass, you must uninstall Data Protector from the same node on which it was installed, when you decide to remove Data Protector from the system.

    On Window Server 2003 x64, Windows Server 2008 x64, and Windows Server 2012 x64, systems, HP AutoPass is not installed.

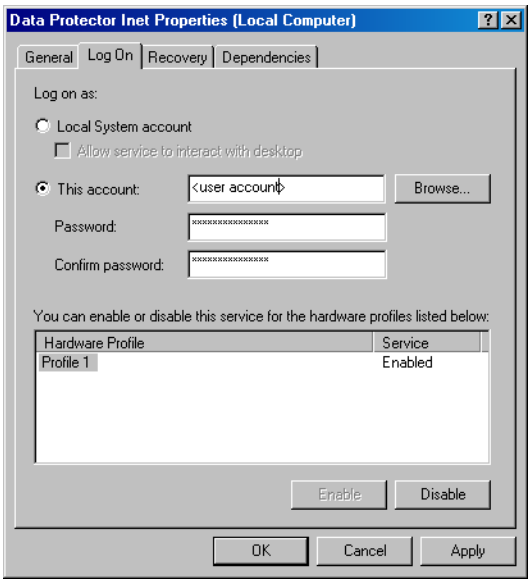
13. Click **Finish** to complete the installation.

Checking the installation

When the setup procedure has been completed, you can check whether or not the Data Protector software has been properly installed. Proceed as follows:

1. Check if the Cluster service account is assigned to the Data Protector `Inet` service on each cluster node. Make sure the same user is also added to the Data Protector admin user group. The logon account type should be set to `This account` as shown in "Data Protector user account" (page 126).

Figure 31 Data Protector user account



2. Execute the following command:

   `omnirsh` *`host`* `INFO_CLUS`

   where *`host`* is the name of the cluster virtual server (case-sensitive). The output should list the names of the systems within the cluster and the name of virtual server. If the output returns `0 "NONE"`, Data Protector is not installed in the cluster-aware mode.

3. Start the Data Protector GUI, select the **Clients** context, and then click **MS Clusters.** See the newly installed systems listed in the Results Area.

Data Protector Inet and CRS services

If needed, change the accounts under which the Data Protector `Inet` and `CRS` services are running.

Installing cluster-aware clients

Prerequisites

Before you install a cluster-aware Data Protector client, the following prerequisites must be fulfilled:

- Clustering functionality must be installed properly on all cluster nodes. For example, you must be able to move groups from one to another node as many times as needed, without problems with shared disks.
- Each system of the cluster should be running and functioning properly.
- To enable installation of the cluster-aware Data Protector client on a server cluster with Microsoft Cluster Service (MSCS) running on Windows Server 2008 or on Windows Server 2012, perform the procedure described in "Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation" (page 228).

Local installation procedure

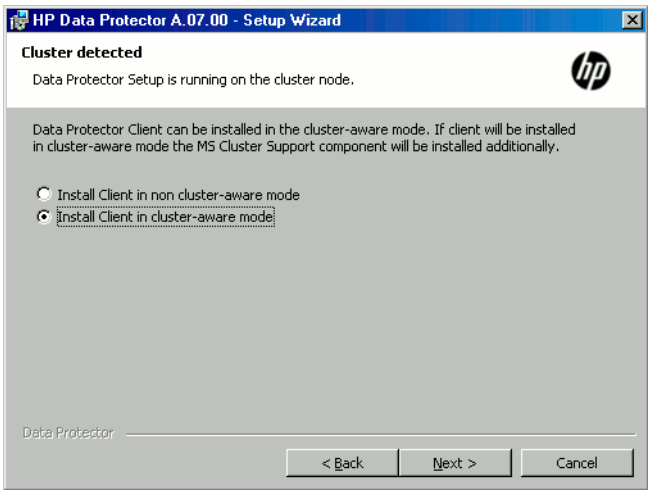
The cluster-aware Data Protector clients must be installed locally, from the DVD-ROM, on each cluster node. The cluster nodes (Data Protector cluster clients) are imported to the specified cell during the installation process. You need to import the virtual server name afterwards.

The cluster Administrator account is required to perform the installation. Apart from that, the cluster client setup is the same as for the ordinary Windows client setup. The MS Cluster Support files are installed automatically.

For information on how to locally install a Data Protector Windows client system, see "Installing Windows clients" (page 48).

The Data Protector installation reports that a cluster was detected. Select **Install client in cluster-aware mode**.

Figure 32 Selecting cluster-aware installation mode



If you are installing the Data Protector Oracle integration, the setup procedure must be performed on all cluster nodes and on the virtual server of the Oracle resource group.

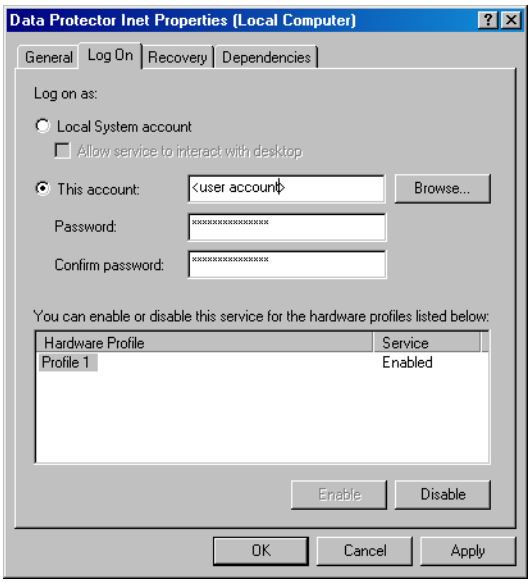
NOTE: You can import a cluster-aware client to the Data Protector cell that is managed using either the standard Cell Manager or the cluster-aware Cell Manager.

Checking the installation

When the setup procedure has been completed, you can check whether or not the Data Protector software has been properly installed. Proceed as follows:

1. Check if the Cluster service account is assigned to the Data Protector `Inet` service on each cluster node. Make sure the same user is also added to the Data Protector `admin` user group. The logon account type should be set to **This account** as shown in "Data Protector user account" (page 128).

Figure 33 Data Protector user account



2. Execute:

   `omnirsh` *`host`* `INFO_CLUS`

   where *`host`* is the name of the cluster client system. The output should return the name of the cluster-aware client system. If the output returns `0 "NONE"`, Data Protector is not installed in the cluster-aware mode.

Veritas Volume Manager

If you have Veritas Volume Manager installed on the cluster, additional steps are required after you have completed the installation of Data Protector on Microsoft Cluster Server. For the additional steps to be performed, see "Installing Data Protector on Microsoft Cluster Server with Veritas Volume Manager" (page 229).

What's next?

When the installation has been completed, you must import the virtual server hostname (cluster-aware application) to the Data Protector cell. See "Importing a cluster-aware client to a cell" (page 134).

For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuring".

Changing the Inet and CRS accounts

If needed, change the accounts under which the Data Protector `Inet` and `CRS` services are running.

Installing Data Protector on a Microsoft Hyper-V cluster

Installing Data Protector on Microsoft Hyper-V systems that are configured in a cluster using the Microsoft Failover Clustering feature is similar to installing Data Protector on Microsoft Cluster Server; Microsoft Hyper-V systems must become Data Protector cluster-aware clients. For details, see "Installing Data Protector on Microsoft Cluster Server" (page 120).

NOTE: Once the Microsoft Hyper-V systems become cluster-aware clients, you can install any additional Data Protector components on them remotely, using the Data Protector Installation Server.

Installing Data Protector clients on a Veritas Cluster

Data Protector clients can be installed on Veritas Cluster nodes, with a Cell Manager outside of the cluster. Using this configuration, backup of the local disks is supported.

In order to back up shared disks or cluster-aware applications, the virtual server IP address should be used for licenses.

IMPORTANT: For Data Protector, cluster-aware backups with failover are not supported.

Installing cluster-aware clients

The installation procedure is standard procedure for installing Data Protector on a Solaris client system. For detailed instructions, see "Installing Solaris clients" (page 54).

What's next?

When the installation has been completed:

- To back up the virtual server, you should import it into the cell.
- To back up the physical nodes, you should also import them into the cell.

See "Importing a cluster-aware client to a cell" (page 134). For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuring".

Installing Data Protector clients on a Novell NetWare Cluster

Data Protector clients can be installed on Novell NetWare Cluster Services cluster nodes, with a Cell Manager outside of the cluster. Using this configuration, backup of local disks is supported, as well as backup of shared cluster pools via the virtual server. For supported operating systems for Novell NetWare Cluster, see the *HP Data Protector Product Announcements, Software Notes, and References*.

In order to back up shared disks or cluster-aware applications, the virtual server IP address should be used for licenses.

IMPORTANT: Cluster-aware backups with failover are not supported. In case of failover, backup or restore sessions have to be restarted manually.

Backup devices should be configured on cluster nodes and not on the virtual server, because cluster nodes control the devices.

Installing cluster-aware clients

Before installation

Before installing Data Protector clients on Novell NetWare Cluster Services cluster nodes, it is recommended that you edit unload scripts for *every* virtual server in the cluster so that the secondary IP address remains active during the migration of the virtual server to another node. You can edit the unload scripts using the Novell's Console One utility or NetWare Remote Manager as described in the Novell NetWare documentation.

Example

The default unload script for every virtual server is:

```
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
nss /pooldeactivate=FIRST /overridetype=question
```

The modified unload script for every virtual server is:

```
nss /pooldeactivate=FIRST /overridetype=question
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

The modified unload script will first dismount and deactivate all cluster shared pools on the virtual server, and only then will delete the secondary IP address. This means that the secondary IP address will remain active during the migration.

To activate the modified unload script, put the virtual server offline and then back online on the preferred node.

Editing the smsrun.bas script

After you have edited the unload script(s), you have to edit the `smsrun.bas` script to include loading of the `TSA600.NLM` module (or `TSAFS.NLM` - depending on which module you are using) with the appropriate parameter which disables support for the cluster. For more information, see the Novell Support Knowledge database for "Known Backup/Restore Issues for NetWare 6.x".

Perform the following steps to edit the `smsrun.bas` script:

1. Change the write protection for the `SYS:NSN/user/smsrun.bas` script from `read only` to `read/write` and open it in a standard console editor.
2. Change the `nlmArray = Array("SMDR", "TSA600", "TSAPROXY")` (or `nlmArray = Array("SMDR", "TSAFS /NoCluster")`) line in the `Sub Main()` section to:
   - `nlmArray = Array("SMDR", "TSA600 /cluster=off", "TSAPROXY")` if you have `TSA600` installed.
   - `nlmArray = Array("SMDR", "TSAFS /NoCluster")` if you have `TSAFS` installed.

   Save the changes.
3. At the file server console, type `SMSSTOP`.
4. At the file server console, type `SMSSTART`.

Cluster shared volumes are now seen by the `TSA600.NLM` (`TSAFS.NLM`) module.

Installation

The installation procedure is the standard procedure for local installation of Data Protector on a Novell Netware client. For detailed instructions, see "Installing Novell NetWare clients" (page 72).

What's next?

When the installation has been completed:

- To back up the physical nodes, you should also import them into the cell.
- To back up the virtual server (shared cluster volumes), you should import it into the cell.

See "Importing a cluster-aware client to a cell" (page 134). For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuring".

Installing Data Protector on IBM HACMP Cluster

Data Protector supports IBM High Availability Cluster Multi-Processing for AIX.

IMPORTANT: Install the Data Protector Disk Agent component on all the cluster nodes.

Installing cluster-aware clients

To install Data Protector components on a cluster node, use the standard procedure for installing Data Protector on UNIX systems. For details, see "Remote installation" (page 76) or "Local installation on UNIX and Mac OS X systems" (page 81).

What's next?

After the installation, import the cluster nodes and the virtual server (virtual environment package IP address) to the Data Protector cell. See "Importing a cluster-aware client to a cell" (page 134).

For information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuration".

3 Maintaining the installation

In this chapter

This chapter describes the procedures most frequently performed to modify the configuration of your backup environment. The following sections provide information about:

- How to import clients to a cell using the graphical user interface. See "Importing clients to a cell" (page 132).
- How to import an Installation Server to a cell using the graphical user interface. See "Importing an installation server to a cell" (page 133).
- How to import clusters/virtual servers using the graphical user interface. See "Importing a cluster-aware client to a cell" (page 134).
- How to export clients using the graphical user interface. See "Uninstalling Data Protector software" (page 150).
- How to ensure security using the graphical user interface. See "Security considerations" (page 137).
- How to verify which Data Protector patches are installed. See "Verifying which Data Protector patches are installed" (page 149).
- How to uninstall the Data Protector software. See "Uninstalling Data Protector software" (page 150).
- How to add or remove Data Protector software components. See "Changing Data Protector software components" (page 157).

Importing clients to a cell

When you distribute Data Protector software to clients using the Installation Server, the client systems are automatically added to the cell. As soon as the remote installation has finished, the client becomes a member of the cell.

When to import?

Some of the clients, such as Novell NetWare, HP OpenVMS, and Windows XP Home Edition, that were installed locally from the installation CD-ROM must be imported to the cell after the installation. **Importing** means manually adding a computer to a cell after the Data Protector software has been installed. When added to a Data Protector cell, the system becomes a Data Protector client. Once the system is a member of the cell, information about the new client is written to the IDB, which is located on the Cell Manager.

A client can only be a member of one cell. If you wish to move a client to a different cell, you first *export* it from its current cell and then *import* it to the new cell. For the procedure on how to export clients, see "Exporting clients from a cell" (page 136).

IMPORTANT: After you have installed Data Protector clients and imported them to a cell, it is highly recommended to protect the clients from access by unwanted cell authorities. See "Securing clients" (page 139).

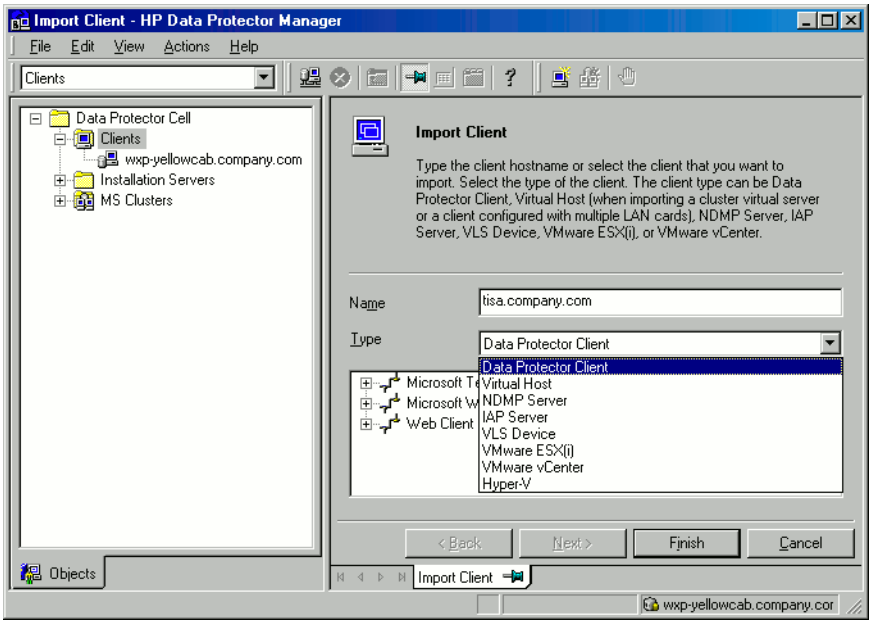
How to import?

You import a client system using the graphical user interface by performing the following steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Import Client**.

3. Type the name of the client or browse the network to select the client (on Windows GUI only) you want to import. See "Importing a client to the cell" (page 133).

Figure 34 Importing a client to the cell



If you are importing a client configured with multiple LAN cards, select the **Virtual Host** option. With this option you must import all names of the same system.

If you are importing an NDMP client, select the **NDMP Server** option and click **Next**. Specify the information about the NDMP Server.

If you are importing an HP OpenVMS client, type the TCP/IP name of the OpenVMS client in the `Name` text box.

If you are importing a VLS device, select the **VLS Device** option and click **Next**. Specify the information about the VLS device.

If you are importing a Microsoft Exchange Server 2010 DAG virtual host for the Data Protector Microsoft Exchange Server 2010 integration, select **Virtual Host**.

If you are importing a client for the Data Protector Virtual Environment integration, select either **VMware ESX(i)** for a standalone VMware ESX(i) Server system, **VMware vCenter** for a VMware vCenter Server system, or **Hyper-V** for a Microsoft Hyper-V system. Click **Next** and specify login credentials.

Click **Finish** to import the client.

The name of the imported client is displayed in the Results Area.

Importing an installation server to a cell

When to add?

An Installation Server must be added to a cell in the following circumstances:

- If it is installed as an independent UNIX Installation Server, for example, it is not installed on a Cell Manager.

  In this case, it will not be possible to remotely install any clients within a cell until the Installation Server has been added to that cell.

- If it is installed on a Cell Manager, but you also want to use it to perform remote installations in another cell. It must then be added to the other cell (using the GUI connected to the Cell Manager of the other cell).

Unlike a client, an Installation Server can be a member of more than one cell. Therefore it does not have to be deleted (exported) from one cell before it can be added (imported) to another cell.

How to add?

The process for importing an Installation Server is similar to that for importing a client. The task is performed using the Data Protector GUI (connected to the Cell Manager of the cell to which the Installation Server is to be added) by performing the following steps:

1. In the Context List, click **Clients.**
2. In the Scoping Pane, right-click **Installation Servers**, and then click **Import Installation Server** to start the wizard. See "Importing a client to the cell" (page 133).
3. Enter or select the name of the system that you want to import. Click **Finish** to import the Installation Server.

Importing a cluster-aware client to a cell

After you have locally installed the Data Protector software on a cluster-aware client, import the virtual server representing the cluster-aware client to the Data Protector cell.

Prerequisites

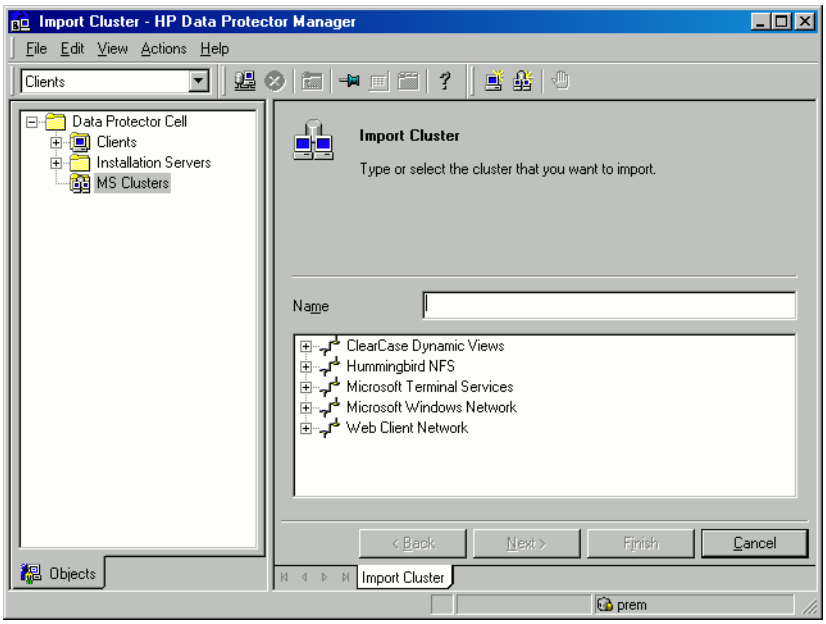
- Data Protector must be installed on all cluster nodes.
- All cluster packages must be running within the cluster.

Microsoft Cluster Server

To import a Microsoft Cluster Server client to the Data Protector cell, proceed as follows:

1. In the Data Protector Manager, switch to the Clients context.
2. In the scoping pane, right-click **MS Clusters** and click **Import Cluster**.
3. Type the name of the virtual server representing the cluster client to be imported or browse the network to select the virtual server. See "Importing a Microsoft Cluster Server client to a cell" (page 134).

Figure 35 Importing a Microsoft Cluster Server client to a cell



4. Click **Finish** to import the cluster client.

TIP: To import a specific cluster node or a virtual server, right click its cluster in the Scoping Pane and click **Import Cluster Node** or **Import Cluster Virtual Server**.

Other clusters

Tru64 Cluster prerequisites

Before importing cluster hostnames, make sure that:

- Data Protector is installed on the shared disk in the cluster
- All Tru64 Cluster nodes are running within the Tru64 Cluster
- Data Protector `inetd` process is running on each node

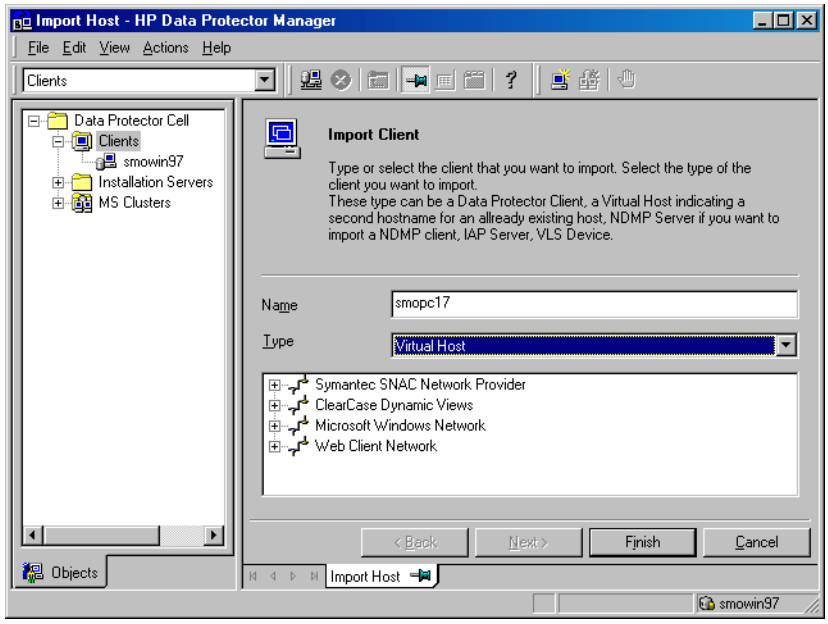
Procedure

To import an MC/ServiceGuard, Veritas, Tru64 Cluster, IBM HACMP Cluster, or Novell NetWare Cluster Services client to the Data Protector cell, proceed as follows:

1. In the Data Protector Manager, switch to the Clients context.
2. In the Scoping Pane, right-click **Clients** and click **Import Client**.
3. Type the hostname of the virtual server as specified in the application cluster package, or browse the network to select the virtual server (on Windows GUI only) you want to import.

   Select the **Virtual Host** option to indicate that this is a cluster virtual server. See "Importing a MC/ServiceGuard, Veritas, or Novell NetWare Cluster Services client to a cell" (page 135).
4. Click **Finish** to import the virtual server.

Figure 36 Importing a MC/ServiceGuard, Veritas, or Novell NetWare Cluster Services client to a cell



TIP: To configure backups of data on the local disks of the cluster nodes, you need to import the cluster nodes representing the Data Protector clients. For the procedure, see "Importing clients to a cell" (page 132).

Exporting clients from a cell

Exporting a client from a Data Protector cell means removing its references from the IDB on the Cell Manager without uninstalling the software from the client. This can be done using the Data Protector GUI.

You may want to use the export functionality if you:

- Want to move a client to another cell
- Want to remove a client from the Data Protector cell configuration which is no longer part of the network
- Want to resolve problems related to licensing

  By exporting a client from a cell, the license becomes available to some other system.

Prerequisites

Before you export a client, check the following:

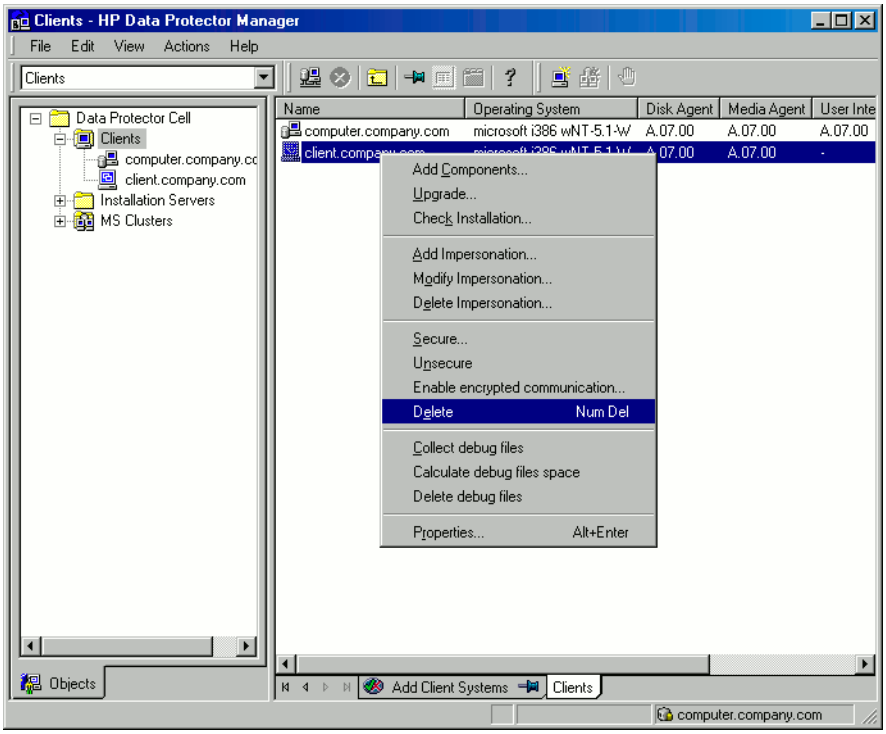
- All the occurrences of the client have been removed from backup specifications. Otherwise, Data Protector will try to back up unknown clients and this part of the backup specification will fail. For instructions on how to modify backup specifications, see the *HP Data Protector Help* index: "modifying, backup specification".
- The client does not have any connected and configured backup devices or disk arrays. Once the system is exported, Data Protector can no longer use its backup devices or disk arrays in the original cell.

How to export?

You export a client using the Data Protector GUI by performing these steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, click **Clients**, right-click the client system that you want to export, and then click **Delete**. See "Exporting a client system" (page 136).

Figure 37 Exporting a client system



3. You will be asked whether you want to uninstall Data Protector software as well. Click **No** to export the client, and then click **Finish**.

The client will be removed from the list in the Results Area.

NOTE: You cannot export or delete a Data Protector client if the Cell Manager is installed on the same system as the client you would like to export. However, you can export the clients from systems where only the client and Installation Server are installed. In this case, Installation Server is also removed from the cell.

Microsoft Cluster Server clients

To export a Microsoft Cluster Server client from the Data Protector cell, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **MS Clusters**, right-click the cluster client that you want to export, and then click **Delete**.
3. You are asked if you also want to uninstall the Data Protector software. Click **No** to only export the cluster client.

The cluster client will be removed from the list in the Results Area.

TIP: To export a specific cluster node or a virtual server, right-click the cluster node or virtual server in the Scoping Pane and click **Delete**.

Security considerations

This section describes the security elements of Data Protector. It describes the advanced settings that can be used to enhance the security of Data Protector with prerequisites and considerations that have to be taken into account.

Since enhancing security in an entire environment requires additional effort, many security features cannot be enabled by default.

The considerations described in this chapter apply not only when the security settings are changed, but must also be followed when configuring new users, adding clients, configuring Application Agents, or making any other changes these considerations apply to. Any changes in the security settings can have cell-wide implications and should be carefully planned.

Security layers

Security has to be planned, tested and implemented on different security-critical layers to ensure the secure operation of Data Protector. Such layers are Data Protector clients, Cell Manager, and users. This section explains how to configure security on each of these layers.

Client security

Data Protector agents installed on clients in the cell provide numerous powerful capabilities, like access to all the data on the system. It is important that these capabilities are available only to the processes running on **cell authorities** (Cell Manager and Installation Server), and that all other requests are rejected.

Before securing clients, it is important to determine a list of trusted hosts. This list must include:

- Cell Manager
- Relevant Installation Servers
- For some clients also a list of clients that will access the robotics remotely.

IMPORTANT: The list must contain all possible hostnames (or IP addresses) where connections can come from. Multiple hostnames may be needed if any of the above clients is multihomed (has multiple network adapters and/or multiple IP addresses) or is a cluster.

If the DNS configuration in the cell is not uniform, additional considerations may apply. For more information, see "Securing clients" (page 139).

While it may not always be necessary to secure each and every client in the cell, it is important that the computers that other clients will trust are secured themselves:

- Cell Manager / MoM
- Installation Servers
- Media Agent (MA) clients.

NOTE: User interface clients do not need to be added to the list of trusted clients. Depending on the user rights, you can either use the GUI to access the complete Data Protector functionality or to access only specific contexts.

Data Protector users

Consider the following important aspects when configuring Data Protector users:

- Some user rights are very powerful. For example, the `User configuration` and `Clients configuration` user rights enable the user to change the security settings. `Restore to other clients` user right is also very powerful, especially if (but not only if) combined with either the `Back up as root` or `Restore as root` user right.
- Even less powerful user rights bear an inherent risk associated with them. Data Protector can be configured to restrict certain user rights to reduce these risks. These settings are described later on in this chapter. See also "Start backup specification user right" (page 146).
- Data Protector comes with only a few predefined user groups. It is recommended to define specific groups for each type of user in the Data Protector environment to minimize the set of rights assigned to them.
- In addition to assigning user rights by user group membership, you may want to further restrict actions of certain user groups to only specific systems of the Data Protector cell. You can implement this policy by configuring the user_restrictions file. For more information, see the *HP Data Protector Help*.
- The configuration of users is connected with user validation (see "Strict hostname checking" (page 144)). Enhanced validation can be worthless without careful user configuration and the other way round - even the most careful user configuration can be worked around without the enhanced validation.
- It is important that there are no "weak" users in the Data Protector user list.

  NOTE: The *host* part of a user specification is the strong part (especially with the enhanced validation), while *user* and *group* parts cannot be verified reliably. Any user with powerful user rights should be configured for the specific client they will use for Data Protector administration. If multiple clients are used, an entry should be added for each client, rather than specifying such a user as *user*, *group*, *<Any>*. Non-trusted users should not be allowed to log on to any of those systems.

For details on configuring users, see the *HP Data Protector Help* index: "configuring, users".

Cell Manager security

Cell Manager security is important because the Cell Manager has access to all clients and all data in the cell.

Security of the Cell Manager can be enhanced via the strict hostname checking functionality. However, it is important that the Cell Manager is also secured as a client and that Data Protector users are configured carefully.

While it may not always be necessary to secure each and every client in the cell, it is important that the computers that other clients will trust are secured themselves. These are besides the Cell Manager also the Installation Server and Media Agent clients.

Security of a Cell Manager and subsequently all clients in the Data Protector cell can be additionally enhanced by enabling encrypted control communication.

For details, see the "Strict hostname checking" (page 144), "Securing clients" (page 139), and "Enabling secure communication" (page 145).

Other security aspects

There are also some other security related aspects you should consider:

- Users should not have access to any of the trusted clients (Cell Manager, Installation Servers, MA, and robotics clients). Even granting `anonymous` log on or `ftp` access could introduce a serious risk to overall security.
- Media and tape libraries (and the clients they are connected to) must be physically protected from unauthorized or untrusted personnel.
- During backup, restore, object or media copying, object consolidation or object verification, data is generally transferred via network. If sufficient separation from the untrusted network cannot be achieved with network segmentation, use locally attached devices, Data Protector encryption techniques, or a custom encoding library. Note that after changing the encoding library, you should perform a full backup.
- In addition, enabling encrypted control communication in a Data Protector cell helps preventing unauthorized access to your system and enhances security.

For other security related aspects, see the *HP Data Protector Help* and the *HP Data Protector Concepts Guide*.

Securing clients

After you have installed Data Protector clients and imported them to a cell, it is highly recommended to protect the clients from access by unwanted clients.

Data Protector allows you to specify from which cell authorities (Cell Manager, MoM, and Installation Servers) a client will accept requests on the Data Protector port `5555`. Consequently, other computers will not be able to access such a client. See "Client security" (page 137).

NOTE: Clients that will access library robotics remotely should be added to the cell authorities list for the library robotics clients.

For tasks like backup and restore, starting pre- or post-execution scripts, or importing and exporting clients, the client checks whether the computer which triggers one of these tasks via the Data Protector port (default `5555`) is allowed to do so. This security mechanism instructs the client to accept such actions only from the specified cell authorities.

Consider exceptional situations

Before limiting the access to clients, consider the following circumstances which may cause problems:

- A cell authority has several LAN cards and several IP addresses/client names.
- The Cell Manager is cluster-aware.
- A tape library has robotics configured on a separate (or dedicated) system.

Data Protector lets you specify not only one but a list of systems that are explicitly authorized to connect as a cell authority to the client. To avoid failure, prepare in advance such a list of all possible valid client names for alternate cell authorities.

The list should include:

- All additional client names (for all LAN cards) of the cell authority.
- Client names of all cluster nodes where the Cell Manager might failover, as well as a cluster virtual server hostname.
- The target system name to which a cell authority will be moved in case of a total hardware failure of the cell authority. This target system has to be defined in the disaster recovery strategy.
- For clients that are allowed to access a client that controls the robotics of a library, all clients that use the drives of that library.

The concept of allowing and denying access can be applied to all systems with Data Protector installed. For example, you can allow or deny access of Cell Managers to clients, Cell Managers to Cell Managers, Installation Servers to clients, or clients to clients.

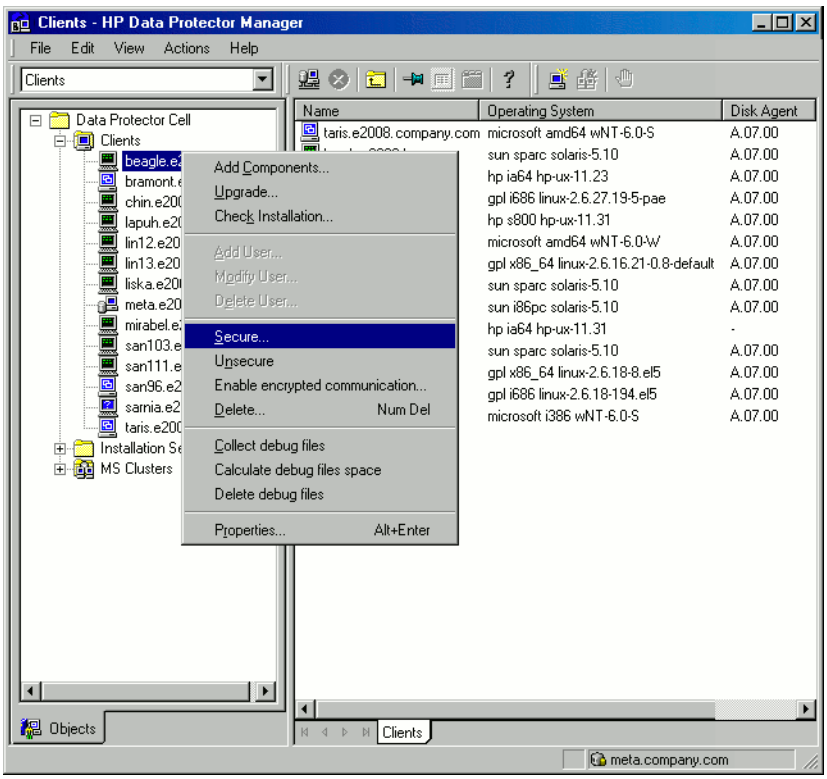
NOTE: If an Installation Server residing on a system other than the Cell Manager is not added to the list of allowed clients, it will not have access to a secured client. In this case, the operations dependent on the Installation Server (such as checking installation, adding components and removing clients) will fail. If you want these operations to be available on the secured client, add the Installation Server to the list of allowed clients.

How to secure a client

To enable verification of a cell authority on the client side (secure a client), perform the following steps in the Data Protector GUI:

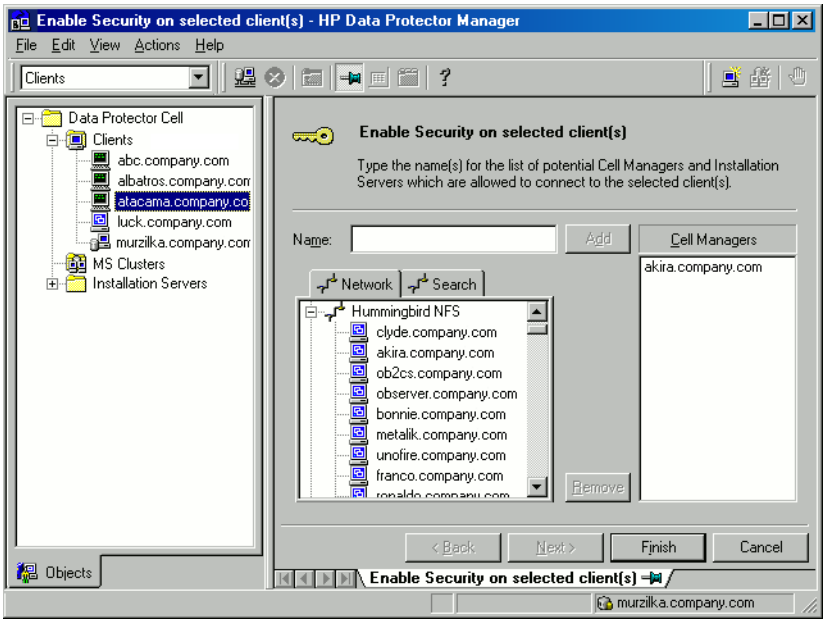
1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand Clients, right-click the client(s) you want to secure, and click **Secure**. See "Securing a client" (page 140).

Figure 38 Securing a client



3. Type the names of the systems that will be allowed to access the selected client(s) or search for the systems using the Network tab (on Windows systems only) or Search tab. Click **Add** to add each system to the list. See "Enabling security on selected client(s)" (page 141).

Figure 39 Enabling security on selected client(s)



The Cell Manager is automatically provided with access and added to the list of trusted clients. You cannot exclude the Cell Manager from the list.

4. Click **Finish** to add the selected systems to the `allow_hosts` file.

What happens?

Clients will verify the source for each request from other clients and allow only those requests received from clients selected in the Enable Security on selected client(s) window. These clients are listed in the `allow_hosts` file. If a request is denied, the event is logged to the `inet.log` file in the following directory:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *`Data_Protector_program_data`*`\log`

Other Windows systems: *`Data_Protector_home`*`\log`

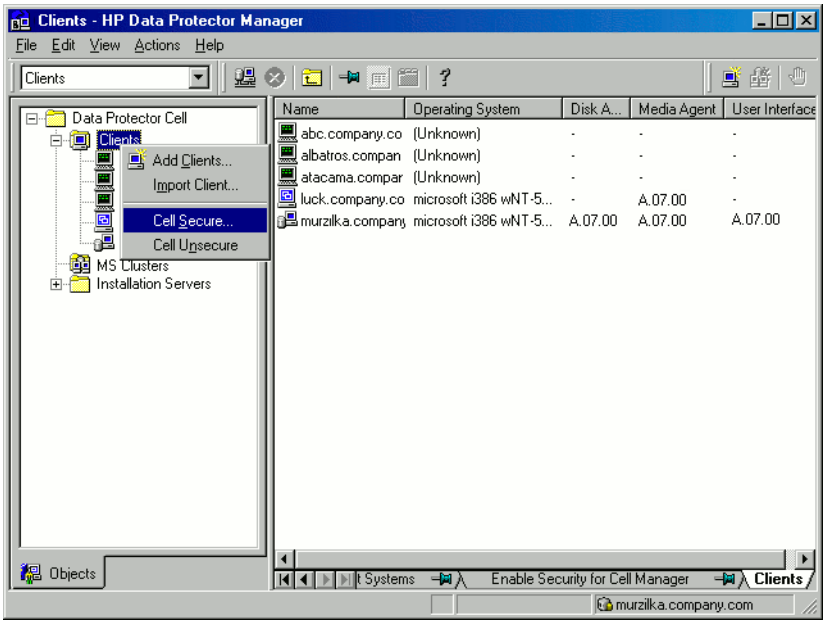
HP-UX, Solaris, and Linux systems: `/var/opt/omni/log`

Other UNIX systems and Mac OS X systems: `/usr/omni/log`

To secure all clients in the cell, perform the following steps in the Data Protector GUI:

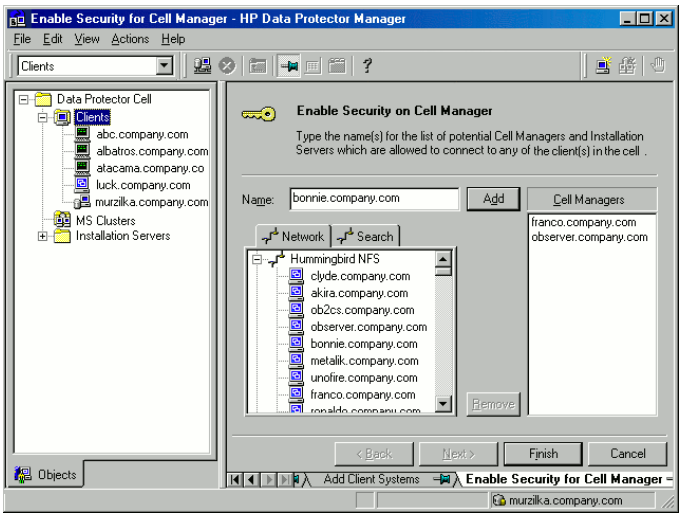
1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Cell Secure**. See "Securing a cell" (page 142).

Figure 40 Securing a cell



3. Type the names of the systems that will be allowed to access all clients in the cell or search for the systems using the `Network` (on Windows GUI only) or Search tabs. Click **Add** to add each system to the list. See "Enabling security for all clients in the cell" (page 142).

Figure 41 Enabling security for all clients in the cell



4. Click **Finish** to add the selected systems to the `allow_hosts` file.

What happens?

Clients will verify the source of each request and allow only those requests received from clients selected in the Enable Security on Cell Manager window. These clients are listed in the `allow_hosts` file. If a request is denied, the event is logged to the `inet.log` file in the following directory:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *`Data_Protector_program_data`*`\log`

Other Windows systems: *`Data_Protector_home`*`\log`

HP-UX, Solaris, and Linux systems: `/var/opt/omni/log`

Other UNIX systems and Mac OS X systems: `/usr/omni/log`

When you secure an entire cell, all clients residing in this cell at the time are secured. When you add new clients to the cell, you should also secure them.

How to remove security

To remove security from the selected system(s), perform the following steps in the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click the client(s) from which you want to remove security and click **Unsecure**.
3. Click **Yes** to confirm that you allow access to the selected client(s).

To remove security from all the clients in the cell, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Cell Unsecure**.
3. Click **Yes** to confirm that you allow access to all client(s) in your cell.

The allow_hosts and deny_hosts files

When you secure a client, the client names of the systems allowed to access a client are written to the `allow_hosts` file. You can also explicitly deny access to a client from certain computers by adding their names to the `deny_hosts` file. These files are located in the following directory:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *Data_Protector_program_data*`\Config\client`

Other Windows systems: *Data_Protector_home*`\Config\client`

HP-UX, Solaris, and Linux systems: `/etc/opt/omni/client`

Other UNIX systems and Mac OS X systems: `/usr/omni/config/client`

Specify each client name in a separate line.

NOTE: If you accidentally lock out a client, you can manually edit (or delete) the `allow_hosts` file on this client.

On Windows systems, the files are in double-byte format (Unicode), whereas on HP-UX, Solaris, and Linux systems, the files are in single-byte format or multi-byte format (for example, Shift-JIS).

Excessive logging to the inet.log file

If the clients are not secured and the Cell Manager is configured in the MC/ServiceGuard environment or has multiple names or IP numbers, the `inet.log` file may contain many entries of the following type:

`A request 0 came from host` *`name.company.com`* `which is not a Cell Manager of this client.`

This happens because the client, which is not secured, recognizes only the primary hostname of the Cell Manager. Requests from any other clients are allowed, but logged to the `inet.log` file.

When a client is secured, requests from the clients listed in the `allow_hosts` file are accepted, and are thus not logged. Requests from other clients are denied.

Securing clients can be used as a workaround to prevent unnecessary entries in `inet.log` files. However, all possible client names for the Cell Manager should be listed in the `allow_hosts` file on each client. This enables access to the client also in case of a failover.

If this workaround is for any reason not possible in your environment, you can secure the clients and specify `*` as an IP address range for the systems you want to allow access. This means that your clients will accept requests from all systems (any IP address) and will practically not be secured, but you will still resolve the excessive logging issue.

Strict hostname checking

By default, the Cell Manager uses a relatively simple method for validating users. It uses the hostname as known by the client where a user interface or an Application Agent is started. This method is easier to configure and it provides a reasonable level of security in environments where security is considered as "advisory" (for example, malicious attacks are not expected).

The strict hostname checking setting on the other hand, provides enhanced validation of users. The validation uses the hostname as it is resolved by the Cell Manager using the reverse DNS lookup from the IP obtained from the connection. This imposes the following limitations and considerations:

Limitations

- IP based validation of users can only be as strong as the anti-spoof protection in the network. The security designer must determine whether the existing network provides a sufficient degree of anti-spoof safety for the particular security requirements. Anti-spoof protection can be added by segmenting the network with firewalls, routers, VPN, and such.
- The separation of users within a certain client is not as strong as the separation between clients. In a high security environment, one must not mix regular and powerful users within the same client.
- Hosts that are used in user specifications cannot be configured to use DHCP, unless they are bound to a fixed IP and configured in the DNS.

Be aware of the limitations in order to correctly assess the degree of safety that can be achieved with the strict hostname checking.

Hostname resolution

The hostname that Data Protector uses for validation may differ between the default user validation and strict hostname checking in the following situations:

- Reverse DNS lookup returns a different hostname. This can be either intentional or can indicate misconfiguration of either the client or the reverse DNS table.
- The client is multihomed (has multiple network adapters and/or multiple IP addresses). Whether this consideration applies to a specific multihomed client, depends on its role in the network and on the way it is configured in the DNS.
- The client is a cluster.

The nature of checks that are enabled with this setting may require reconfiguration of Data Protector users. Existing specifications of Data Protector users must be checked to see if they could be affected by any of the above reasons. Depending on the situation, existing specifications may need to be changed or new specifications added to account for all the possible IPs from which the connections can come.

Note that users have to be reconfigured also when reverting back to the default user validation, if you had to modify user specifications when you enabled the strict hostname checking. It is therefore recommended to decide which user validation you would like to use and keep using it.

A prerequisite for a reliable reverse DNS lookup is a secure DNS server. You must prevent physical access and log on to all unauthorized personnel.

By configuring users with IPs instead of hostnames, you can avoid some DNS related validation problems, but such configuration is more difficult to maintain.

Requirements

The enhanced validation does not automatically grant access for certain internal connections. Therefore, when this validation is used, a new user must be added for each of the following:

- Any Application Agent (OB2BAR) on Windows clients. For Windows clients, it is required to add the user `SYSTEM`, `NT AUTHORITY`, *`client`* for each client where an Application Agent

is installed. Note that if `Inet` on a certain client is configured to use a specific account, this account must have already been configured. For more information, see the *HP Data Protector Help* index: "strict hostname checking".

- If you are using Web Reporting, user `java`, `applet`, *`hostname`* must be added for every hostname from where Web Reporting will be used. Note that for full Web Reporting functionality the users must be in the `admin` group. Therefore, these clients must be trusted. Also, before making any data or functionality of Web Reporting available to other users (for example, via a web server), consider the security implications of making such data generally available.

For detailed information on user configuration, see the *HP Data Protector Help* index: "configuring, users".

Enabling the feature

To enable the strict hostname checking, set the `StrictSecurityFlags` flag to the value `0x0001` in the global options file.

For more information about the global options file, see the *HP Data Protector Troubleshooting Guide*.

Enabling secure communication

Data Protector encrypted control communication helps preventing unauthorized access to clients in Data Protector cell. Using the Data Protector GUI or the CLI, you can remotely enable encrypted control communication for all clients in the Data Protector cell.

To enable encrypted control communication from the CLI, execute:

```
omnicc -encryption -enable
```

For details, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

IMPORTANT: You can enable encrypted control communication only from the Cell Manager or any client in the cell for which encrypted control communication is already enabled.

How to enable encrypted control communication

To enable encrypted control communication, perform the following steps in the Data Protector GUI:

NOTE: You must first enable encrypted control communication on a Cell Manager then on the clients in the cell.

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
3. Click the client that you want to modify.
4. In the Connection property page, select the **Encrypted control communication** option.
5. In the **Certificate Chain** drop-down list, select the certificate.
6. In the **Private Key** drop-down list, select the private key.
7. In the **Trusted Certificate** drop-down list, select the trusted certificate.
8. Click **Apply** to save the changes.

To enable encrypted control communication for multiple clients, perform the following steps in the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
3. Right-click the client from which you want to enable encrypted control communication, and click **Enable encrypted communication**.
4. Select one or more clients for which you want to enable encrypted control communication. Click **Next**.

5. In the **Certificate Chain** drop-down list, select the certificate.
6. In the **Private Key** drop-down list, select the private key.
7. In the **Trusted Certificate** drop-down list, select the trusted certificate.
8. Click **Finish** to save the changes.

What happens?

Encryption is enabled on a per-client basis, which means that encryption is either enabled or disabled for all control communication with the selected client.

How to add a client to the Security Exceptions list

Clients that for some reason are not supposed to communicate confidentially can be placed in a Cell Manager exception list, which allows particular clients to communicate in non-encrypted mode.

To add a client to the Security Exceptions list, perform the following steps in the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
3. Click the Cell Manager that you want to modify.
4. Type the names of the systems that will be will be added to the Security Exceptions list in the cell or search for systems using the **Network** (on Windows GUI only) or **Search** tabs.
5. Click **Add** to add systems to the list, then click **Apply** to save the changes.

The server configuration file

The clients that are accepted in a plain text mode are written to the `server configuration` file, located on the Cell Manager in the directory:

Windows Vista, Windows 7, Windows Server 2008, Windows Server 2012:
`Data_Protector_program_data\Config\server\config`

Other Windows systems: `Data_Protector_home\Config\server\config`

HP-UX and Linux systems: `/etc/opt/omni/server/config`

To remove a system from the Security Exceptions list, perform steps 1 to 4 and click **Remove**, then click **Apply** to save the changes.

Limitation

- Communication between the client, which is using plain control communication and the client with enabled encrypted control communication is not supported. This means, that Data Protector operations will not be executed (for example, remote installation from an Installation Server, which is using plain control communication to the client with enabled encrypted control communication will not succeed).

  However, the Cell Manager can communicate with both types of clients in the Data Protector cell.

Start backup specification user right

For general information about the Data Protector users and user rights, see the *HP Data Protector Help* index: “users”.

The `Start backup specification` user right alone does not enable a user to use the Backup context in the GUI. The user is allowed to start a backup specification from the command line by using the omnib with the -datalist option.

NOTE: By combining the `Start Backup Specification` with the `Start Backup` user rights, a user is allowed to see the configured backup specifications in the GUI and is able to start a backup specification or an interactive backup.

Allowing users to perform interactive backups may not always be desired. To allow interactive backups only for users who also have the right to save a backup specification, set the StrictSecurityFlags flag 0x0200 in the global options file.

For more information on the global options file, see the *HP Data Protector Troubleshooting Guide*.

Hiding the contents of backup specifications

In a high security environment, the contents of saved backup specifications may be considered to be sensitive or even confidential information. Data Protector can be configured to hide the contents of backup specifications for all users, except for those who have the *Save backup specification* user right. To do so, set the StrictSecurityFlags flag 0x0400 in the global options file.

For more information about the global options file, see the *HP Data Protector Troubleshooting Guide*.

Host trusts

The host trusts functionality reduces the need to grant the Restore to other clients user right to users when they only need to restore the data from one client to another within a limited number of clients. You can define groups of hosts that will trust each other with the data.

Host trusts are typically used in the following situations:

- For clients in a cluster (nodes and virtual server).
- If the hostname of a client is changed and the data from the old backup objects needs to be restored.
- If there is a mismatch between the client hostname and backup objects due to DNS issues.
- If a user owns several clients and needs to restore the data from one client to another.
- When migrating data from one host to another.

Configuration

To configure host trusts, on the Cell Manager, create the file *Data_Protector_program_data*`\Config\Server\cell\host_trusts` (Windows 7, Windows 8, Windows Server 2008, Windows Server 2012), *Data_Protector_home*`\Config\Server\cell\host_trusts` (other Windows systems), or `/etc/opt/omni/server/cell/host_trusts` (UNIX systems).

The groups of hosts that trust each other are defined as lists of hostnames enclosed in curly brackets. For example:

Example

```
GROUP="cluster.domain.com"
{
    cluster.domain.com
    node1.domain.com
    node2.domain.com
}
GROUP="Bajo"
{
    computer.domain.com
    anothercomputer.domain.com
}
```

Monitoring security events

If you encounter problems using Data Protector, you can use the information in the log files to determine your problem. For example, logged events can help you to determine misconfigured users or clients.

Client security events

Client security events are logged in the `inet.log` file on every client in the cell in the directory:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *Data_Protector_program_data*`\log`

Other Windows systems: *Data_Protector_home*`\log`

HP-UX, Solaris, and Linux systems: `/var/opt/omni/log`

Other UNIX systems and Mac OS X systems: `/usr/omni/log`

Cell Manager security events

Cell Manager security events are logged in the `security.log` file in the following directory on the Cell Manager:

Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *Data_Protector_program_data*`\log\server`

Other Windows systems: *Data_Protector_home*`\log\server`

UNIX systems: `/var/opt/omni/server/log`

Managing Data Protector patches

Data Protector patches are provided through HP support and can be downloaded from the HP support website. Data Protector provides individual patches and patch bundles.

Installing patches

Cell Manager patches can be installed locally. However, in order to patch clients, Installation Server is required. Once the Installation Server is patched, you can then patch clients remotely.

IMPORTANT: On HP-UX systems, before patching the Cell Manager with a Cell Manager (`CS`) patch, stop the Data Protector services using the Data Protector `omnisv` command, and start them again after the patching process completes.

If individual patches are included into a patch bundle, you can only install the whole bundle. For details, see the installation instructions provided with the patch.

To verify which patches are installed on the system, you can use the Data Protector GUI or CLI. See "Verifying which Data Protector patches are installed" (page 149)

Installing and removing Data Protector patch bundles

If Data Protector is already installed on your system, you can also install a Data Protector patch bundle (a set of Data Protector patches) on this system.

To install a Data Protector patch bundle on UNIX systems, you can use the `omnisetup.sh` script. On Windows systems, a patch bundle installation is provided as an executable file.

You can also remove the patch bundle. After removing the patch bundle, the last Data Protector release version remains on the system.

Installing and removing Data Protector patch bundles on UNIX systems

To install a Data Protector patch bundle, use the `omnisetup.sh` command provided in the tar archive together with the patch bundle files. Use the `-bundleadd` option. For example:

```
omnisetup.sh -bundleadd b701
```

You can install a Data Protector patch bundle only on the Installation Server and the Cell Manager. If the installation fails or you stopped it, you can continue with the installation and install the rest of the patches (supported with Linux systems only), rollback the installed patches to the previous patch level, or exit the installation without installing all patches.

To remove the Data Protector patch bundle, use the `omnisetup.sh -bundlerem` command. For example:

```
omnisetup.sh -bundlerem b701
```

For details, see the installation instructions provided with the patch or patch bundle.

Installing and removing Data Protector patch bundles on Windows systems

A Data Protector patch bundle for Windows is provided as an executable file (for example, `DPWINBDL_00701.exe`). You can install a Data Protector patch bundle on the Installation Server, the Cell Manager, or the client system.

To install the patch bundle on a Windows system, execute the *`BundleName`*`.exe` command, for example:

```
DPWINBDL_00701.exe
```

The command recognizes, which components are installed on the system and upgrades them to the latest patch.

To remove the Data Protector patch bundle, use the `remove_patch.bat` command located at *`Data_Protector_home`*`\bin\utilns`:

`remove_patch` *`BundleName DPInstallationDepot`* where *`DPInstallationDepot`* is the location from which Data Protector (not the patch bundle) was installed. For example, to remove the patch bundle `b701`, where Data Protector was installed from `D:\WINDOWS_OTHER`, execute:

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

You can remove a Data Protector patch bundle from the Installation Server, the Cell Manager, or the client system.

NOTE: On Windows systems, it is also possible to remove individual patches using the `remove_patch.bat` command. However make sure that if you do not remove the CORE patch until other individual patches are still installed on the system. Otherwise, you will not be able to remove other individual patches later.

Verifying which Data Protector patches are installed

You can verify which Data Protector patches are installed on a system in the cell. To verify which Data Protector patches are installed on a particular system in a cell, use the Data Protector GUI or CLI.

NOTE: After you install a site-specific patch or a patch bundle, it will always be listed in the patch report, even if it has been included into later patches.

Prerequisites

- To use this functionality, you should have the `User Interface` or `Java GUI Client` component installed.

Limitations

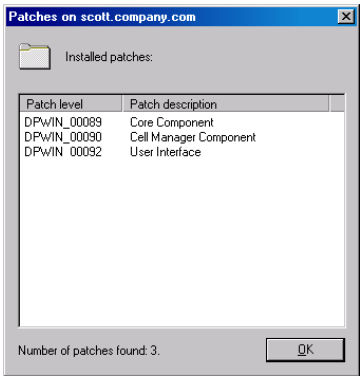
- Patch verification can check which patches are installed on systems within the same cell only.

Verifying Data Protector patches using the GUI

To verify which patches are installed on a particular client using the Data Protector GUI, follow the below procedure:

1. In the Context List, select **Clients**.
2. In the Scoping Pane, expand **Clients** and select a system in the cell for which you want to verify the patches installed.
3. In the Results Area, click **Patches** to open the **Patches on** window.

Figure 42 Verifying patches installed



If there are patches found on the system, the verification returns the level and the description of each patch and the number of the patches installed.

If there are no Data Protector patches on the system, the verification returns an empty list.

If the system verified is not a member of the cell, is unavailable, or an error occurs, the verification reports an error message.

4. Click **OK** to close the window.

Verifying Data Protector Patches Using the CLI

To verify which patches are installed on a particular client using the Data Protector CLI, execute the `omnicheck -patches -host` *`hostname`* command, where the *`hostname`* is the name of the system to be verified.

For more information on the `omnicheck` command, see the `omnicheck` man page.

Uninstalling Data Protector software

If your system configuration changes, you may want to uninstall the Data Protector software from the system or remove some software components.

Uninstalling is removing all the Data Protector software components from the system, including *all* references to this system from the IDB on the Cell Manager computer. However, by default, the Data Protector configuration data remains on the system because you may need this data in the future upgrade of Data Protector. To remove the configuration data after uninstalling the Data Protector software, delete the directories where Data Protector was installed.

If you have some other data in the directory where Data Protector is installed, make sure you copied this data to another location before uninstalling Data Protector. Otherwise, the data will be removed during the uninstallation process.

Uninstalling the Data Protector software from a cell consists of the following steps:

1. Uninstalling the Data Protector client software using the GUI. See "Uninstalling a Data Protector client" (page 151).
2. Uninstalling Data Protector Cell Manager and Installation Server. See "Uninstalling the Cell Manager and Installation Server" (page 152).

You can also uninstall Data Protector software components without uninstalling the Cell Manager or client. See "Changing Data Protector software components" (page 157).

On UNIX, you can also manually remove the Data Protector software. See "Manual removal of Data Protector software on UNIX" (page 156).

Prerequisites

Before you uninstall the Data Protector software from a computer, check the following:

- Make sure that all references to the computer are removed from the backup specifications. Otherwise, Data Protector will try to back up unknown systems and this part of the backup specification will fail. For instructions on how to modify backup specifications, see the *HP Data Protector Help* index: "modifying, backup specification".
- Make sure that no backup devices or disk arrays are connected and configured on the system that you want to uninstall. Once the system is exported, Data Protector can no longer use its backup devices or disk arrays in the original cell.

Uninstalling a Data Protector client

NOTE: The remote uninstallation procedure requires the Installation Server to be installed for the platforms from which you are uninstalling the Data Protector software.

You uninstall a client remotely by performing these steps in the Data Protector GUI:

1. In the Context List, switch to the **Clients** context.
2. In the Scoping Pane, expand **Clients**, right-click the client you want to uninstall, and then click **Delete**. You will be asked whether you want to uninstall the Data Protector software as well.
3. Click **Yes** to uninstall all the software components from the client, and then click **Finish**.

The client will be removed from the list in the Results Area and the Data Protector software will be deleted from its hard disk.

Note that the Data Protector configuration data remains on the client system. To remove the configuration data, delete the directories where Data Protector was installed.

Uninstalling Data Protector also removes the Java GUI Client. Unless the **Permanently delete configuration data** checkbox is selected when uninstalling Data Protector, the Java GUI configuration data remains on the system.

Cluster clients

If you have cluster aware clients in your Data Protector environment and you want to uninstall them, you must do this locally. The procedure is the same as for uninstalling Cell Manager or Installation Server. See "Uninstalling the Cell Manager and Installation Server" (page 152).

The cluster client will be removed from the list in the Results Area and the Data Protector software will be deleted from its hard disk.

TruCluster

To uninstall TruCluster clients, export the virtual node first. Then uninstall Data Protector clients from the node(s).

HP OpenVMS clients

A Data Protector OpenVMS client cannot be removed remotely using an Installation Server. It must be uninstalled locally.

To uninstall a Data Protector client from an OpenVMS system, follow these steps:

1. First export the client concerned from the Data Protector cell using the Data Protector GUI, as described in "Exporting clients from a cell" (page 136).

   When asked whether you want to uninstall the Data Protector software as well, select **No**.

2. To delete the actual Data Protector client software, log in to the `SYSTEM` account on the OpenVMS client and execute the following command: `$ PRODUCT REMOVE DP`. Respond to the prompt with `YES`.

IMPORTANT: This will shut down the Data Protector service and delete all the directories, files, and accounts associated with Data Protector on the OpenVMS system.

Uninstalling the Cell Manager and Installation Server

This section describes the procedure of uninstalling the Data Protector Cell Manager and Installation Server software from Windows, HP-UX and Linux systems.

Uninstalling from Windows systems

Uninstalling from a Microsoft server cluster

If you have installed HP AutoPass utility together with Data Protector on a Microsoft server cluster node, you must uninstall Data Protector from the same node, otherwise AutoPass will *not* be uninstalled.

To uninstall Data Protector software from a Windows system, follow these steps:

1. Make sure you have terminated all Data Protector sessions and exited the GUI.
2. In Windows Control Panel, click **Add/Remove Programs**.
3. Depending on whether you installed HP AutoPass or not, and whether you want to remove the Data Protector configuration data or not, different actions apply.

IMPORTANT: If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, during the installation choose the option that will remove the configuration data.

Proceed as follows:

- If AutoPass utility was installed together with Data Protector:

  Select **HP Data Protector 7.00** and click **Change** and then **Next**. In the Program Maintenance dialog box, select **Remove**. To permanently remove the Data Protector configuration data, select **Permanently remove the configuration data**. Otherwise, click **Next**.

  If AutoPass was installed together with Data Protector and Data Protector is the only application using it, AutoPass is removed. Otherwise, AutoPass is only unregistered with Data Protector but remains installed. To manually remove AutoPass, execute:

  ```
  msiexec.exe /X Package_GUI_ID /qr INSTALLSTANDALONE=1
  ```

  You can obtain the GUI ID by reading the registry entry `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HpOvLic`.

- If AutoPass has not been installed:

  - To uninstall Data Protector and leave the Data Protector configuration data on the system, select **HP Data Protector 7.00** and click **Remove**.
  - To uninstall Data Protector and remove the Data Protector configuration data, select **HP Data Protector 7.00**, click **Change** and then **Next**. In the Program Maintenance dialog box, select **Remove**. Select **Permanently remove the configuration data** and click **Next**.

4. When uninstalling is completed, click **Finish** to exit the wizard.

   If AutoPass was removed during the uninstallation of the Cell Manager, press **F5** in the Add/Remove Program window to refresh the list of installed programs and components.

Uninstalling from HP-UX systems

The Cell Manager for HP-UX is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `swremove` utility.

IMPORTANT: If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, after the uninstallation remove the remaining Data Protector directories from your system.

Prerequisites

- Remove any installed Data Protector patch bundles using the `omnisetup.sh -bundlerem` command. See "Installing and removing Data Protector patch bundles on UNIX systems" (page 148).

Procedure

Before you start uninstalling Data Protector software, shut down Data Protector processes running on the Cell Manager and/or Installation Server system:

1. Log in as root and execute the `omnisv -stop`.
2. Enter the `ps -ef | grep omni` command to verify whether or not all the processes have been shut down. There should be no Data Protector processes listed after executing `ps -ef | grep omni`.

   If you have any Data Protector processes running, stop them using the `kill`*`process_ID`* command before you proceed with uninstalling.
3. Run `/usr/sbin/swremove DATA-PROTECTOR` to uninstall Data Protector software.
4. The HP AutoPass utility is not removed during the Data Protector uninstallation. You can manually remove it by running the `/usr/sbin/swremove HPOVLIC` command as the user root.

To remove the remaining Data Protector directories from your system, see "Manual removal of Data Protector software on UNIX" (page 156).

Uninstalling the Cell Manager and/or Installation Server configured on MC/ServiceGuard

If your Cell Manager and/or Installation Server is configured on an MC/ServiceGuard cluster, perform the following steps to uninstall the software.

Primary node

Log on to the primary node and perform the following steps:

1. Stop the Data Protector package:

   `cmhaltpkg` *`pkg_name`*

   where *`pkg_name`* stands for the name of the cluster package.

   For example:

   `cmhaltpkg ob2cl`
2. Deactivate the cluster mode for the volume group:

   `vgchange -c n` *`vg_name`*

(where *vg_name* stands for the path name of the volume group located in the subdirectory of the /dev directory).

For example:

```
vgchange -c n /dev/vg_ob2cm
```

3. Activate the volume group:

   ```
   vgchange -a y -q y vg_name
   ```

   For example:

   ```
   vgchange -a y -q y /dev/vg_ob2cm
   ```

4. Mount the logical volume to the shared disk:

   ```
   mount lv_path shared_disk
   ```

   (where *lv_path* stands for the path name of the logical volume and *shared_disk* stands for the mount point or shared directory).

   For example:

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

5. Remove Data Protector by using the swremove utility.
6. Remove the soft links:

   ```
   rm /etc/opt/omni
   rm /var/opt/omni
   ```

7. Remove the backup directories:

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```

8. Remove the Data Protector directory with its contents:

   ```
   rm -rf /opt/omni
   ```

9. You can remove the HP AutoPass utility by running the `/usr/sbin/swremove HPOVLIC` command as the user root.
10. Dismount the shared disk:

    ```
    umount shared_disk
    ```

    For example:

    ```
    umount /omni_shared
    ```

11. Deactivate the volume group:

    ```
    vgchange -a n vg_name
    ```

    For example:

    ```
    vgchange -a n /dev/vg_ob2cm
    ```

Secondary node

Log on to the secondary node and perform the following steps:

1. Activate the volume group:

   ```
   vgchange -a y vg_name
   ```

2. Mount the shared disk:

   ```
   mount lv_path shared_disk
   ```

3. Remove Data Protector by using the `swremove` utility.
4. Remove the soft links:

   ```
   rm /etc/opt/omni
   ```

```
rm /var/opt/omni
```

5. Remove the backup directories:

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```

6. Remove the Data Protector directory with its contents:

   ```
   rm -rf /opt/omni
   ```

7. Remove the directories in the shared filesystem:

   ```
   rm -rf shared_disk/etc_opt_omni
   rm -rf shared_disk/var_opt_omni
   ```

   For example:

   ```
   rm -rf /omni_shared/etc_opt_omni
   rm -rf /omni_shared/etc_opt_omni
   ```

8. You can remove the HP AutoPass utility by running the `/usr/sbin/swremove HPOVLIC` command as the user root.
9. Dismount the shared disk:

   ```
   umount shared_disk
   ```

10. Deactivate the volume group:

    ```
    vgchange -a n vg_name
    ```

Data Protector is completely removed from the system.

Uninstalling from Linux systems

Prerequisites

- Remove any installed Data Protector patch bundles using the `omnisetup.sh -bundlerem` command. See "Installing and removing Data Protector patch bundles on UNIX systems" (page 148).

Cell Manager

The Cell Manager for Linux is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `rpm` utility.

IMPORTANT: If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, after the uninstallation remove the remaining Data Protector directories from your system.

To uninstall the Data Protector Cell Manager, proceed as follows:

1. Make sure you have terminated all Data Protector sessions and exited the graphical user interface.
2. Enter the `rpm -qa | grep OB2` command to list all the Data Protector components installed on the Cell Manager.

   The components associated with the Cell Manager are as follows:

OB2-CORE	Data Protector Core software
OB2-CORE-IS	Installation Server software
OB2-CS	Cell Manager software
OB2-CC	Cell Console software, containing the command-line interface

If Data Protector clients or an Installation Server are also installed on the system, other components will also be listed.

NOTE: To leave any other Data Protector components installed, you must leave the OB2-CORE component installed, since it is a dependency for other components.

3. In reverse order to the sequence in which they were installed, remove the components mentioned in the previous step using the `rpm -e package name` command and follow the prompts.

Installation Server

The Installation Server for UNIX on Linux is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `rpm` utility.

To uninstall the Data Protector Installation Server, proceed as follows:

1. Make sure you have terminated all Data Protector sessions and exited the GUI.
2. Enter the `rpm -qa | grep OB2` command to list all the Data Protector components and remote installation packages stored on the Installation Server system.

   The components and remote installation packages associated with the Installation Server are as follows:

OB2-CORE	Data Protector Core software
OB2-CORE-IS	Installation Server Core software
OB2-CFP	Common Installation Server remote installation packages for all UNIX systems.
OB2-CCP	Cell Console remote installation packages for all UNIX systems.
OB2-DAP	Disk Agent remote installation packages for all UNIX systems.
OB2-MAP	Media Agent remote installation packages for all UNIX systems.

   If other Data Protector components are installed on the system, other components will also be listed.

   For a complete list of components and their dependencies, see "Data Protector software component dependencies on Linux" (page 159).

   NOTE: To leave any other Data Protector components installed, you must leave the OB2-CORE component installed, since it is a dependency for other components.

3. In reverse order to the sequence in which they were installed, remove the components mentioned in the previous step using the `rpm -e package name` command and follow the prompts.

Manual removal of Data Protector software on UNIX

Before uninstalling a UNIX client, you should export it from the cell. For procedure, see "Exporting clients from a cell" (page 136).

HP-UX systems

To manually remove the files from an HP-UX system, do the following:

1. Run `/usr/sbin/swremove DATA-PROTECTOR` to remove the Data Protector software.
2. Remove the following directories using the `rm` command:

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   At this stage, Data Protector references no longer reside on your system.

Solaris systems

To manually remove files from a Solaris system, delete them from the following directories and then delete the directories using the `rm` command:

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Linux systems

To manually remove files from a Linux system, delete them from the following directories and then delete the directories using the `rm` command:

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Other UNIX systems and Mac OS X systems

Delete the files from the following directory and then delete the directories using the `rm` command:

```
rm -fr /usr/omni
```

Changing Data Protector software components

This section describes the procedure for removing and adding Data Protector software components from or to Windows, HP-UX, Solaris, and Linux systems. For the list of supported Data Protector components for a particular operating system, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Data Protector software components can be added on the Cell Manager or on a client using the Data Protector GUI. You perform the remote installation of selected components using the Installation Server functionality. For the detailed procedure, see "Remote installation" (page 76).

The Data Protector components can be removed locally on the Cell Manager or on a client.

On Windows systems

To add or remove the Data Protector software components on a Windows system, follow the steps below:

1. In the Windows Control Panel, click **Add or Remove Programs**.
2. Select **HP Data Protector 7.00** and click **Change**.
3. Click **Next**.
4. In the Program Maintenance window, click **Modify** and then **Next**.
5. In the Custom Setup window, select the components you want to add and/or unselect the software components you want to remove. Click **Next**.
6. Click **Install** to start the installing or removing the software components.
7. When the installation is completed, click **Finish**.

Cluster-Aware clients

If you are changing the Data Protector software components on the cluster-aware clients, it must be done locally, from the DVD-ROM, on each cluster node. After that, the virtual server hostname has to be manually imported to the Data Protector cell using the GUI.

On HP-UX systems

You can add new components using the Installation Server functionality. On an HP-UX system, some Data Protector software components depend on each other and cannot operate properly, if

you remove one of them. The table below presents the components and their dependencies on each other:

Table 8 Data Protector software component dependencies on HP-UX

Components	Depend on
Cell Manager	
OMNI-CC	OMNI-CORE
OMNI-CS	OMNI-CORE, OMNI-CC
OMNI-DA, OMNI-MA, OMNI-JAVAGUI, OMNI-DOCS	OMNI-CORE
Installation Server	
OMNI-CORE-IS	OMNI-CORE
OMNI-CF-P	OMNI-CORE-IS
OMNI-CC-P, OMNI-JGUI-P, OMNI-DA-P, OMNI-MA-P, OMNI-NDMP-P, OMNI-AUTODR-P, OMNI-DOCS-P, OMNI-CHS-LS-P, OMNI-FRA-LS-P, OMNI-JPN-LS-P, OMNI-PEGASUS-P, OMNI-INTEG-P, OMNI-VMW-P	OMNI-CORE-IS, OMNI-CF-P
OMNI-DB2-P, OMNI-EMC-P, OMNI-INF-P, OMNI-LOTUS-P, OMNI-OR8-P, OMNI-OV-P, OMNI-SAPDB-P, OMNI-SAP-P, OMNI-SSEA-P, OMNI-SYB-P	OMNI-INTEG-P, OMNI-CORE-IS, OMNI-CF-P
OMNI-SMISA-P, OMNI-VLSAM-P	OMNI-CORE-IS, OMNI-CF-P, OMNI-PEGASUS-P

Procedure

Perform the following procedure to remove Data Protector software components:

1. Log in as `root` and run the `swremove` command.
2. Double-click **B6960MA**, **DATA-PROTECTOR**, and then **OB2-CM** to display a list of the Data Protector components.
3. Select the components you want to remove.
4. In the **Actions** menu, click **Mark for Remove** to mark the components you want to remove.
5. When the components you want to remove are marked, click **Remove** in the **Actions** menu, and then click **OK**.

NOTE: When you mark the Data Protector components you want to remove, and if the remaining components cannot operate properly, the **Dependency Message Dialog** box appears with a list of dependent components.

Oracle specifics

After uninstalling the Data Protector Oracle integration on an Oracle server system, the Oracle server software is still linked to the Data Protector Database Library. You have to remove this link, otherwise the Oracle server cannot be started after removing the integration. See the *HP Data Protector Integration Guide*, "Using Oracle after removing the Data Protector Oracle integration".

On Solaris systems

You can add new components using the Installation Server functionality. On Solaris systems, some Data Protector software components depend on each other and cannot operate properly, if you remove one of them. The table below presents the components and their dependencies on each other:

Table 9 Data Protector software component dependencies on Solaris

Components	Depend on
Cell Manager	
OB2-CC, OB2-DA, OB2-MA, OB2-JAVAGUI, OB2-DOCS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
Installation Server	
OB2-C-IS	OB2–CORE
OB2-CF-P	OB2-C-IS
OB2-CCP, OB2-JGUIP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTGP, OB2-VMWP	OB2-C-IS, OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTGP, OB2-C-IS, OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-C-IS, OB2-CF-P, OB2-PEG-P

On Linux systems

You can add new components using the Installation Server functionality. On Linux systems, some Data Protector components depend on each other and cannot operate properly, if you remove one of them. The table below presents the components and their dependencies on each other:

Table 10 Data Protector software component dependencies on Linux

Components	Depend on
Cell Manager	
OB2-CC, OB2-DA, OB2-MA, OB2-JAVAGUI, OB2-DOCS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
Installation Server	
OB2-CORE-IS	OB2-CORE
OB2-CF-P	OB2-CORE-IS
OB2-CCP, OB2-JGUIP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP	OB2-CORE-IS, OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-CORE-IS, OB2-CF-P, OB2-PEG-P

Procedure

Perform the following procedure to remove Data Protector components from the Linux systems:

1. Make sure you terminated all Data Protector sessions and exited the GUI.
2. Enter the command `rpm | grep OB2` to list all the Data Protector components installed.
3. In reverse order to the sequence in which they were installed, remove the components mentioned in Step 2 using the `rpm -e package name` command and follow the prompts.

Other UNIX systems

When manually removing components from a Data Protector client on a UNIX system other than Solaris or HP-UX, update the `omni_info` file in `/usr/omni/bin/install/omni_info`.

For each of the removed components, remove the associated component version string from the `omni_info` file.

If you are only removing components from a Data Protector client and have not exported the client from the cell, you will need to update the cell configuration in the `cell_info` file (on the Cell Manager). This can be done by executing the following command on a system in the cell with the Cell Console installed:

```
omnicc -update_host HostName
```

4 Upgrading to Data Protector 7.00

In this chapter

This chapter provides instructions for performing Data Protector upgrade and migration tasks.

Upgrade overview

Before you begin

Before upgrading an existing product version to Data Protector 7.00, consider the following:

- For information about supported and discontinued platforms and versions, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
- After the upgrade, the Cell Manager, and Installation Server must have the same Data Protector version installed. Although older Data Protector Disk Agent and Media Agent versions are supported in the same cell, it is highly recommended that the clients also have the same version of Data Protector components installed.

  For constraints imposed by older Disk Agent and Media Agent versions after an upgrade, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- After the upgrade of a multiple-cell (MoM) environment, all Cell Managers must have the same Data Protector version installed.
- If you have a permanent license for Data Protector A.06.10, Data Protector A.06.11, or Data Protector 6.20 it can be used with Data Protector 7.00.

  Otherwise, be aware that you work with an Instant-On license, which will be valid for 60 days from the date of original installation.

  For details about licensing, see "Data Protector licensing" (page 187).

Prerequisite

- Perform a backup of the existing Cell Manager system and the internal database (IDB).
- When migrating the Cell Manager from a system with Data Protector A.06.10, Data Protector A.06.11, or Data Protector 6.20 to a system with Data Protector 7.00, you must first upgrade the existing Cell Manager to Data Protector 7.00.

Limitations

- The upgrade to Data Protector 7.00 is only supported for Data Protector A.06.10, Data Protector A.06.11, and Data Protector 6.20.
- A backup of the Internal Database, created with previous versions of Data Protector, cannot be restored with Data Protector 7.00. After upgrading the Cell Manager, backup the Internal Database before you continue using Data Protector.
- Changing the Cell Manager platform is not supported in the 7.00 release of Data Protector. Upgrades are only supported on the same Cell Manager platform (HP-UX to HP-UX, Linux to Linux, and Windows to Windows).

Upgrade sequence

To upgrade your cell from the earlier versions of the product to Data Protector 7.00, proceed as follows:

1. Upgrade the Cell Manager and Installation Server to Data Protector 7.00. The steps are different for UNIX and Windows platforms.

   Note that you must first upgrade the Cell Manager in the current cell before you can upgrade the Installation Server.
2. Upgrade the GUI clients.
3. Upgrade the clients that have an online application integration installed, such as Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server, and other.
4. Upgrade the clients that have a Media Agent (MA) installed. You can perform backups as soon as MA is upgraded on all MA clients of the same platform as the Cell Manager.
5. HP recommends that you upgrade the clients that have the filesystem Disk Agent (DA) installed within the next two weeks.

Upgrading in a MoM environment

To upgrade your MoM environment to Data Protector 7.00, you need to upgrade the MoM Manager system first. After this is done, all Cell Managers of the previous versions, which have not been upgraded yet, are able to access the Central MMDB and central licensing, perform backups, but other MoM functionality is not available. Note that device sharing between the Data Protector 7.00 MoM cell and the cells with earlier versions of the product installed is not supported. During the upgrade in a MoM environment, none of the Cell Managers in the MoM environment should be operational.

Upgrading from Data Protector A.06.10, A.06.11, and 6.20

The Data Protector A.06.10, A.06.11, and 6.20 release versions can be directly upgraded to Data Protector 7.00 for UNIX and Windows platforms.

Licenses

The existing Data Protector A.06.10, A.06.11, and 6.20 licenses are fully compatible and valid for use with Data Protector 7.00. For details about licensing, see "Data Protector licensing" (page 187).

Before you begin

Before you begin with the upgrade, see "Upgrade overview" (page 161) for information on limitations and the upgrade sequence.

Upgrading the UNIX Cell Manager and Installation Server

Prerequisites

- Stop all Data Protector services using the `omnisv -stop` command.
- A POSIX shell (`sh`) is required for the installation.
- You must have `root` permissions to perform the upgrade.

If the HP-UX or Linux Installation Server is installed together with the Cell Manager, it is upgraded automatically when the `omnisetup.sh` command is executed.

If the HP-UX or Linux Installation Server is installed on a separate system, see "Upgrading an Installation Server" (page 164).

Upgrading a Cell Manager

The HP-UX or Linux Cell Manager is upgraded automatically when the `omnisetup.sh` command is executed.

On HP-UX, this command directly upgrades the installed components using the `swinstall` utility. On Linux, this command directly upgrades the installed components using the `rpm` utility.

If the Installation Server is installed with client components, it will be removed by the `omnisetup.sh` command. In this case, install a new Installation Server depot using the `omnisetup.sh -IS` command, and then re-import the upgraded Installation Server. For details, see "Importing an installation server to a cell" (page 133).

MC/ServiceGuard

The upgrade procedure for the Cell Manager, configured on MC/SG differs from the upgrade procedure for the Cell Manager not running in the MC/SG environment. The detailed steps you need to follow are described in "Upgrading the Cell Manager configured on MC/ServiceGuard" (page 181).

Setting kernel parameters

On HP-UX systems, it is recommended that you set the kernel parameter `maxdsiz` (Max Data Segment Size) or `maxdsiz_64` (for 64bit systems) to at least 134217728 bytes (128 MB), and the kernel parameter `semmnu` (Number of Semaphore Undo Structures) to at least 256. After you commit these changes, recompile the kernel and restart the system.

Upgrade procedure

To upgrade the HP-UX or Linux Cell Manager to Data Protector 7.00, follow the procedure described below:

1. Insert and mount the UNIX installation DVD-ROM (for HP-UX or Linux) to a mount point, for example to `/dvdrom`.

   Optionally, you can install Data Protector from a depot on the disk, perform the following:

   - Copy the `DP_DEPOT`, `AUTOPASS`, and `LOCAL_INSTALL` directories, where the installation files are stored:

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/platform_dir/AUTOPASS directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     Where *`platform_dir`* is:

`hpux`	HP-UX on IA-64 and PA-RISC systems
`linux`	Linux systems

   - Copy the whole DVD-ROM to your local disk:

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. Execute the `omnisetup.sh` command from the DVD-ROM:

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh
   ```

   To start the installation from disk, execute the following:

   - If you have copied the `DP_DEPOT`, `AUTOPASS`, and `LOCAL_INSTALL` directories to your local disk under *`directory`*, go to the directory where the `omnisetup.sh` command is stored, and execute:

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh
     ```

   - If you have copied the whole DVD-ROM to *`dvd_image_dir`*, execute the `omnisetup.sh` command without any parameters:

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ```

```
./omnisetup.sh
```

3. `omnisetup.sh` prompts you to install or upgrade the HP AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, see the *AutoPass License Management Online Help*. It is recommended to install AutoPass.

   If AutoPass is installed on MC/ServiceGuard, it must be installed or upgraded on all nodes.

   When prompted, press **Return** to install or upgrade AutoPass. If you do not want to install or upgrade AutoPass, enter **n**.

   After the A.06.10, A.06.11, or 6.20 version of Data Protector is detected, the upgrade procedure is automatically started. To perform a clean installation (the database of previous version will be deleted), uninstall the old version and restart the installation.

   For details about installation, see "Installing a UNIX Cell Manager" (page 27) and "Installing Installation Servers for UNIX systems" (page 38).

As soon as the procedure is completed, you can start using Data Protector.

For the description of the `omnisetup.sh` command, see the `README` file located in the *`Mount_point`*`/LOCAL_INSTALL` directory on the DVD-ROM or *HP Data Protector Command Line Interface Reference* located in the *`Mount_point`*`/DOCS/C/MAN` directory on the DVD-ROM.

What's next?

- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See "Checking configuration changes" (page 168).
- You must manually adjust the library capacity (`VTLCAPACITY`) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade to Data Protector 7.00 by default set to 1 TB. See "Checking configuration changes" (page 168).
- On HP-UX 11.31 (Itanium) and SUSE Linux Enterprise Server (x86-64) the maximum size of database files can exceed the default maximum size of 2 GB. Consequently, during an upgrade to Data Protector 7.00 a warning message is displayed with an advice to adjust the maximum size of database files. This adjustment should be done after the upgrade, as it may take a significant amount of time, depending on the database size. See "Troubleshooting upgrade" (page 214).

Upgrading an Installation Server

The HP-UX or Linux Installation Server is upgraded automatically when the `omnisetup.sh` command is executed.

On HP-UX, this command directly upgrades the installed components and stored remote installation packages using the `swinstall` utility. On Linux, this command directly upgrades the installed components and stored remote installation packages using the `rpm` utility.

If the Installation Server is installed with client components, it will be removed by the `omnisetup.sh` command. In this case, install a new Installation Server depot using the `omnisetup.sh -IS` command, and then re-import the upgraded Installation Server. For details, see "Importing an installation server to a cell" (page 133).

IMPORTANT: You cannot upgrade the Installation Server unless you upgraded the Cell Manager first.

Upgrade procedure

To upgrade the HP-UX or Linux Installation Server to Data Protector 7.00, follow the procedure described below:

1. Insert and mount the UNIX installation DVD-ROM (for HP-UX or Linux) to a mount point, for example to `/dvdrom`.

   Optionally, to install Data Protector from a depot on the disk, perform the following:

   - To copy the `DP_DEPOT`, and `LOCAL_INSTALL` directories, where the installation files are stored, on your local disk, proceed as follows:

     ```
     mkdir directory
     cp -r /dvdrom/platform_dir/DP_DEPOT directory
     cp -r /dvdrom/platform_dir/AUTOPASS directory
     cp -r /dvdrom/LOCAL_INSTALL directory
     ```

     Where *`platform_dir`* depends on the operating system and processor platform on which you upgrade Data Protector:

`hpux_ia`	HP-UX on IA-64 systems
`hpux_pa`	HP-UX on PA-RISC systems
`linux`	Linux systems

   - To copy the whole DVD-ROM to your local disk, execute:

     ```
     cp -r /dvdrom dvd_image_dir
     ```

2. Execute the `omnisetup.sh` command from the DVD-ROM:

   ```
   cd /dvdrom/LOCAL_INSTALL
   ./omnisetup.sh
   ```

   To start the installation from disk, perform one of the following steps:

   - If you have copied the `DP_DEPOT`, and `LOCAL_INSTALL` directories to your local disk under *`directory`*, go to the directory where the `omnisetup.sh` command is stored, and execute:

     ```
     cd directory/LOCAL_INSTALL
     ./omnisetup.sh
     ```

   - If you have copied the whole DVD-ROM to *`dvd_image_dir`*, execute the `omnisetup.sh` command without any parameters:

     ```
     cd dvd_image_dir/LOCAL_INSTALL
     ./omnisetup.sh
     ```

As soon as the procedure is completed, you can start using Data Protector.

For the description of the `omnisetup.sh` command, see the `README` file located in the *`Mount_point`*`/LOCAL_INSTALL` directory on the DVD-ROM or *HP Data Protector Command Line Interface Reference* located in the *`Mount_point`*`/DOCS/C/MAN` directory on the DVD-ROM.

What's next?

Once the Installation Server system is upgraded, check if you have to apply any modifications to your configuration files. See "Checking configuration changes" (page 168).

Upgrading the Windows Cell Manager and Installation Server

When the previous version of Data Protector is detected, the same component set as installed is assumed by the operating system (without obsolete components). The installed components are removed and the new components are installed as for a new (clean) installation.

The Windows Installation Server is upgraded automatically during the upgrade procedure if it is installed on the same system as the Cell Manager. The old Installation Server depot is removed

and if the `Installation Server` component is selected during the installation, the new Installation Server depot is copied to its place.

If the Installation Server is installed together with the Data Protector client, and this client is upgraded remotely (using the Data Protector GUI), the Installation Server is upgraded as well.

IMPORTANT: Re-import the upgraded Installation Server after the installation procedure has finished. For details, see "Importing an installation server to a cell" (page 133).

Microsoft Cluster Server

The upgrade procedure for the Cell Manager, running in the Microsoft Cluster Server environment, is different from the upgrade procedure for the Cell Manager not configured for use with Microsoft Cluster Server. The detailed steps you need to follow are described in "Upgrading the Cell Manager configured on Microsoft Cluster Server" (page 184).

Upgrade procedure

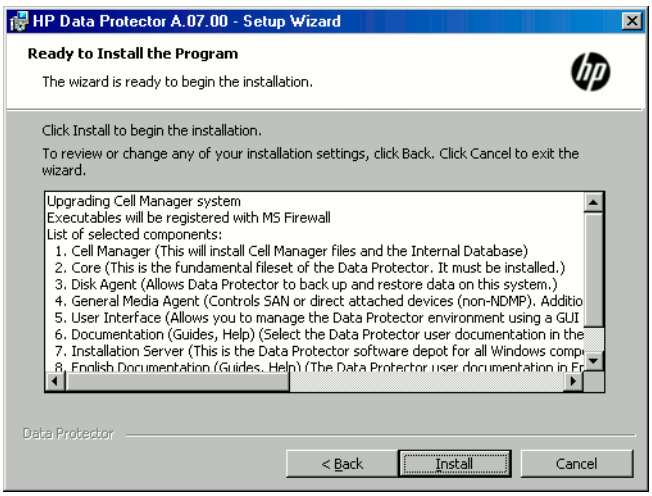
To upgrade the Windows Cell Manager and Installation Server to Data Protector 7.00, follow the procedure described below:

1. Insert the Windows installation DVD-ROM and run the `\Windows_other\i386\setup.exe` command. Setup detects the old Data Protector installation. Click **Next** to start the upgrade.
2. In the **Component Selection** page, the components previously installed on the system are selected. Note that you can change the component set by selecting or deselecting additional components. For a description of selected components, see the next step of the wizard. Click **Next**.
3. *If Data Protector detects Windows Firewall on your system*, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the **Initially, enable newly registered Data Protector binaries to open ports as needed** option is selected. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

   Note that only inbound firewall rules are automatically created and you must manually create any outbound firewall rules. For the required port ranges, see the *HP Data Protector Help* index "firewall support".

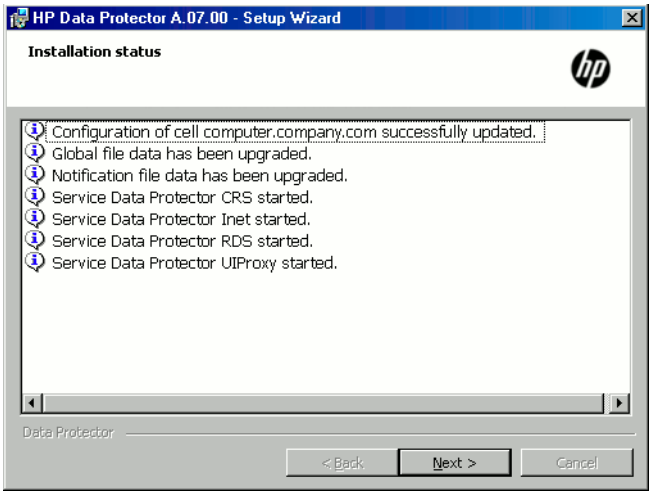
   Click **Next**.
4. The component summary list is displayed. Click **Install** to perform the upgrade.

Figure 43 Component selection summary page



5. The **Installation status** page is displayed. Click **Next**.

Figure 44 Installation status page



6. This step is performed only for a Cell Manager upgrade. If the Installation Server installed on a client other than the Cell Manager is being upgraded, this step does not occur.

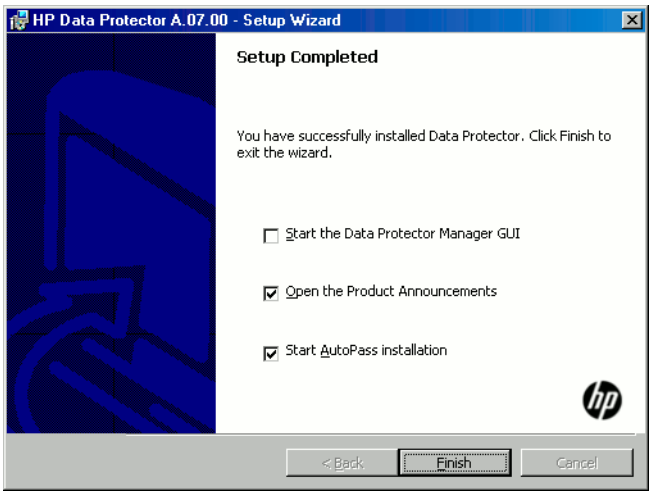
   The Setup Wizard enables you to install or upgrade the HP AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, see "Obtaining and installing permanent passwords using the HP AutoPass utility" (page 199).

   By default, the **Start AutoPass installation** or the **Upgrade AutoPass installation** option is selected. It is recommended to install the HP AutoPass utility. If you do not want to install or upgrade AutoPass, deselect the option.

   To start using Data Protector immediately after setup, select **Start the Data Protector Manager GUI**.

   To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

Figure 45 Selecting AutoPass for installation



7. Click **Finish**.

As soon as the procedure is completed, you can start using Data Protector.

What's next?

- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See "Checking configuration changes" (page 168).
- You must manually adjust the library capacity (`VTLCAPACITY`) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade to Data Protector 7.00 by default set to 1 TB. See "Checking configuration changes" (page 168).

Checking configuration changes

Global options file

During the upgrade, the contents of the *old* global options file, residing on the Cell Manager in the *Data_Protector_program_data*`\Config\server\Options` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*`\Config\server\Options` (other Windows systems), or `/etc/opt/omni/server/options` (UNIX systems) directory, are merged with the contents of the *new (default)* global options file on the Cell Manager, located at:

Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012: *Data_Protector_program_data*`\NewConfig\Server\Options`

Other Windows systems: *Data_Protector_home*`\NewConfig\Server\Options`

UNIX systems: `/opt/omni/newconfig/etc/opt/omni/server/options`

The *merged* file `global` resides at the same location on the Cell Manager as the old one, in the *Data_Protector_program_data*`\Config\server\Options` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*`\Config\server\Options` (other Windows systems), or `/etc/opt/omni/server/options` (UNIX systems) directory, and is used by the upgraded version of the product. The *old* global options file is renamed to `global.1`, `global.2`, and so on, depending on the number of upgrades performed.

The following applies when the merged file is created:

- Global options that were active (uncommented) in the old file remain active in the merged file. The following comment, stating that the value of the option was copied from the old file, is added to the merged file:

  ```
  Option=Value
  # Data Protector 7.00
  # This value was automatically copied from previous version.
  ```

- Global options that are not used anymore, are commented (made inactive) in the merged file and added the following comment stating that the option is no longer in use:

  ```
  #Option=Value
  # Data Protector 7.00
  # This value is no longer in use.
  ```

- Options with values, not supported anymore, are commented (made inactive) in the merged file. The following comment is added, containing a template line (*DefaultValue*) and stating the previous value of this option:

  ```
  # Option=DefaultValue
  # Data Protector 7.00
  # This variable cannot be transferred automatically.
  # The previous setting was:
  # Option=Value
  ```

- Comments are not transferred to the newly merged file.

On Windows systems, the global options file is in the Unicode format and can be edited using, for example, Notepad. After editing this file, make sure that you saved it in the Unicode format.

Descriptions of the new options are in the merged global options file on the Cell Manager in the *Data_Protector_program_data*\Config\server\options\global (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*\Config\server\options\global (other Windows systems), or /etc/opt/omni/server/options/global (UNIX systems) directory. For details on how to use global options, see the *HP Data Protector Troubleshooting Guide*.

Manual steps

The following list summarizes the steps you must perform manually once the upgrade procedure has successfully completed:

- Omnirc file

  After upgrading the Cell Manager and Installation Server systems, you may want to edit the omnirc file. For the information on how to edit it, see "Using Omnirc Options" in the *HP Data Protector Troubleshooting Guide*.

- Command line

  For a list of commands that have been changed or provided with extended functionality, see "Command line changes after upgrading to Data Protector 7.00" (page 256). You have to check and modify the scripts that use the old commands. For usage synopsis, see the corresponding man page or the *HP Data Protector Command Line Interface Reference*.

- Maximum size per DCBF directory

  Settings for already existing DCBF directories are not changed after an upgrade, only the newly created directories will have the maximum size set to the default value of 16 GB. When you increase the default maximum size, you should also adjust the free disk space needed for a DCBF binary file (10 to 15% of the maximum size is recommended). To manually change the maximum size of DC directory, execute:

  omnidbutil -modify_dcdir *directory* -maxsize *size_MB* -spacelow *size_MB*

  You need to change the settings when drives with large capacity, for example LTO 4, are used, and more than 10 million files are backed up on tape. In addition, make sure that the file system where DC directories reside supports large files.

- Verify that the hosts file contains the fully qualified domain names (FQDNs) in computer.company.com format. Otherwise configure the host's file with the FQDN. The location of the file depends on the operating system:

  Windows systems: %SystemRoot%\system32\drivers\etc\

  UNIX systems: /etc/hosts

- Advanced backup to disk licensing

  The library capacity (VTLCAPACITY) of a virtual tape library, which was created with a previous version of Data Protector, is after the upgrade to Data Protector 7.00 by default set to 1 TB. Consequently, you must enter the estimated library capacity value manually through the graphical user interface (GUI) or via the command-line interface (CLI).

  #### Example

  Before the upgrade to Data Protector 7.00, the information about configured virtual tape library named "VTL" looks like this:

  ```
  #omnidownload -library VTL
  NAME "VTL"
  DESCRIPTION ""
  HOST computer.company.com
  ```

```
POLICY SCSI-II
TYPE DDS
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

After the upgrade to Data Protector 7.00, a new string `VTLCAPACITY` is added and the library capacity is by default set to 1 TB.

```
#omnidownload -library VTL
NAME "VTL"
DESCRIPTION ""
HOST computer.company.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 1
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

To modify the library capacity (`VTLCAPACITY`) of a virtual tape library named "VTL" in an ASCII file named "libVTL.txt" in the directory "C:\Temp", execute:

```
omnidownload -library VTL -file C:\Temp\libVTL.txt
```

Enter the estimated library capacity value, for example `163` and execute:

```
omniupload -modify_library VTL -file C:\Temp\libVTL.txt
```

NOTE: The estimated virtual library capacity consumption value (`VTLCAPACITY`) in terabytes (TB) must be an integer to avoid the error message `Invalid VTL capacity specified`.

To verify library configuration, execute:

```
omnidownload -library VTL
```

```
#omnidownload -library VTL
NAME "VTL"
DESCRIPTION ""
HOST computer.company.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 163
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

What's next?

Once the Cell Manager and Installation Server(s) are installed and all required modifications implemented, it is recommended that you distribute the software to clients. See "Upgrading the clients" (page 170).

Upgrading the clients

Upgrade sequence

For information about the sequence in which the client upgrade is performed, see "Upgrade overview" (page 161).

Upgrading clients remotely

For the procedure on how to upgrade the clients using the Installation Server, see "Remote installation" (page 76). On UNIX systems, you must upgrade the already present components before you add new components. After new components are added, the components from previous versions are not displayed by Data Protector. In this case, you have to reinstall them.

Upgrading clients locally

If you do not have an Installation Server installed on your network, or if for some reason you cannot distribute the Data Protector software to a client system, Data Protector clients can be upgraded locally.

To upgrade Windows clients locally, see "Installing Windows clients" (page 48).

To upgrade UNIX clients locally, see "Local installation on UNIX and Mac OS X systems" (page 81).

Upgrade-related operating system specifics

Upgrading Windows, HP-UX, and Linux clients

During an upgrade to Data Protector 7.00, the enhanced incremental backup database is not migrated to the new release version. The old enhanced incremental backup repository is deleted from the directory *Data_Protector_home*\enhincrdb*MountPoint* (Windows systems) or /var/opt/omni/enhincrdb (UNIX systems). During the first full backup after the client upgrade, a new repository is created at the same location. Ensure the type of your first backup performed after the upgrade is full.

Upgrading Linux clients

If the xinetd service is used instead of inetd, the /etc/xinetd.d/omni file is *not* replaced and thus the settings remain unchanged. To check if the xinetd service is running, run the following command:

```
ps -e | grep xinetd
```

To replace your settings with the default Data Protector settings or to replace a corrupted file, remove the file and remotely upgrade any Data Protector software component from the Data Protector GUI. The /etc/xinetd.d/omni file is then installed with the default settings.

IMPORTANT: By replacing the /etc/xinetd.d/omni file, your modifications are lost. To retain your modifications, create a backup copy in advance and manually transfer the settings to the newly installed file after the upgrade.

Upgrading IBM AIX clients

On IBM AIX 5.3 systems, if you have applied the Data Protector patch bundle 7.03 to a Data Protector installation previously upgraded to the product version 7.00, additionally perform the following steps to finalize the patch bundle installation process:

1. Open a Terminal window.
2. Change current directory to /usr/omni/bin.
3. For each binary file in this directory whose filename contains the suffix _32, rename the file by removing the suffix from its filename.

   For example, to properly rename the Disk Agent binary used to perform volume backup, rename the file vbda_32 to vbda (so that the existing file vbda is overwritten) by executing the command:

   ```
   mv -f vbda_32 vbda
   ```

Upgrading Novell NetWare clients

After upgrading any Novell NetWare client, you need to perform some additional steps that will enable you to perform any backup and restore of the NDS/eDirectory database. For details, see "Installing Novell NetWare clients" (page 72).

Upgrading clients configured in MC/ServiceGuard

If you are upgrading the client that uses MC/ServiceGuard, and if the Data Protector integration component to be upgraded is installed on the same node as the Cell Manager, first upgrade the physical nodes, and then perform the following:

1. Export the virtual host by executing:

   ```
   omnicc -export_host virtual_hostname
   ```

2. Re-import the virtual host by executing:

   ```
   omnicc -import_host virtual_hostname -virtual
   ```

Upgrading integration clients

If you are upgrading a Data Protector client that has the integration installed (such as the integration for Oracle, SAP R/3, Microsoft Volume Shadow Copy Service, or HP P6000 EVA Disk Array Family, the Automatic Disaster Recovery module, the integration for Microsoft Exchange Server, Microsoft SQL Server, HP P9000 XP Disk Array Family, or EMC Symmetrix, and so on), follow the steps described in sections below to successfully perform the upgrade:

- For instructions on how to upgrade the Oracle integration, see "Upgrading the Oracle integration" (page 172).
- For instructions on how to upgrade the SAP R/3 integration, see "Upgrading the SAP R/3 integration" (page 173).
- For instructions on how to upgrade the Microsoft Volume Shadow Copy Service integration, see "Upgrading the Microsoft Volume Shadow Copy Service integration" (page 174).
- For instructions on how to upgrade the HP P6000 EVA Disk Array Family integration, see "Upgrading the HP P6000 EVA Disk Array Family integration" (page 174).
- For instructions on how to upgrade the Microsoft Exchange Server, Microsoft SQL Server, HP P9000 XP Disk Array Family, or EMC Symmetrix integration, or any other integration, see "Upgrading other integrations" (page 174).

Upgrading the Oracle integration

The clients that have the Oracle integration installed are upgraded either locally, by running the `omnisetup.sh -install oracle8` command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, by remotely installing the Oracle integration agent to the client using the Data Protector GUI. Note that on UNIX, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-install oracle8` option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

User root is no longer required

On UNIX clients, the Data Protector Oracle Server integration no longer configures, checks the configuration of, and browses Oracle databases under the user `root`. Now, these operations run under the operating system user account that you specify in a backup specification. Therefore, you can safely remove the user `root` from the Data Protector user group.

NOTE: For ZDB and instant recovery sessions, the user `root` is still required.

After the upgrade, it is also recommended to perform a configuration check for each Oracle database, during which Data Protector copies the operating system user account (backup owner)

from the backup specification to the corresponding Data Protector Oracle database configuration file.

If the configuration check is not performed, the configuration file is not updated. In such cases, during restore, Data Protector browses Oracle databases under the backup owner of the last backup session. If such a backup session has not been created in the last three months, the `root` user is used as the last option.

Configuring an Oracle instance for instant recovery

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you must either reconfigure the Oracle instance or set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options. See the *HP Data Protector Zero Downtime Backup Integration Guide*.

Oracle ASM configurations using HP P6000 EVA Disk Array Family for data storage

To enable support for creation of consistent replicas of the Oracle Server data on P6000 EVA Array in configurations in which Automatic Storage Management (ASM) is used, you need to upgrade both Data Protector components, the Oracle Integration and the HP P6000 EVA SMI-S Agent, on the application system as well as on the backup system.

Upgrading the SAP R/3 integration

The clients that have the SAP R/3 integration installed are upgraded either locally, by executing the `omnisetup.sh -install sap` command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, by remotely installing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that on UNIX, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-install sap` option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

SAP compliant ZDB sessions

SAP standards recommend that BRBACKUP is started on the backup system during ZDB sessions (SAP compliant ZDB sessions). Data Protector 7.00 enables you to comply with these standards. First, configure the backup system as described in the SAP guide for Oracle (split mirror backup, software configuration) and install the Data Protector `SAP R/3 Integration` component on the backup system. Then, configure Data Protector for SAP compliant ZDB sessions as described in the *HP Data Protector Zero Downtime Backup Integration Guide*.

Configuring an Oracle instance for instant recovery

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you have three options:

- Reconfigure the Oracle instance.
- Set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options.
- Configure Data Protector to start BRBACKUP on the backup system (SAP compliant ZDB sessions).

For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

Upgrading the Microsoft Volume Shadow Copy Service integration

Instant recovery-enabled backup sessions after upgrading from HP Data Protector A.06.10, HP Data Protector A.06.11, or HP Data Protector 6.20

After you upgraded the VSS integration from an older version of Data Protector, you need to resolve the source volumes on the application system if you will perform the ZDB-to-disk and ZDB-to-disk+tape sessions. Otherwise, the ZDB-to-disk sessions will fail and ZDB-to-disk+tape session will complete only with backups to tape not leaving the replicas on the disk array. Execute the resolve operation from any VSS client in the cell as follows:

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

For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

Upgrading the HP P6000 EVA Disk Array Family integration

Considerations

- When upgrading a pre-6.20 version of Data Protector to Data Protector 7.00, note that the *Loose* snapshot policy for replica creation on P6000 EVA Array was no longer supported starting with the Data Protector version 6.20. The *Strict* snapshot policy is implied for all ZDB sessions involving this disk array. After the upgrade, when a ZDB session using the *Loose* snapshot policy is run, a warning is reported and the *Strict* snapshot policy is used instead, but the ZDB backup specification itself is not updated. To avoid such warnings, you need to manually update such ZDB backup specifications.

  To manually update a ZDB backup specification to use the now implicit *Strict* snapshot policy, open the backup specification in the Data Protector GUI, change any of its options and change it back, and finally save the backup specification by clicking **Apply**.

  For information on snapshot policies for replica creation on P6000 EVA Array, see the *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Help*.

Upgrading the Virtual Environment integration

When upgrading the Data Protector Virtual Environment integration component from the Data Protector version 6.20 or earlier, run the following command after the new version has been installed on the corresponding clients:

```
vepa_util.exe --upgrade-cell_info
```

This is needed due to a change in password encoding in the `cell_info` file. It will re-encode the passwords used by the Virtual Environment integration, first creating a `cell_info.bak` file.

Upgrading other integrations

If the Data Protector client has the Microsoft Exchange Server, Microsoft SQL Server, HP P9000 XP Disk Array Family, or EMC Symmetrix integration, or any other integration installed, upgrade such client either locally, using the `omnisetup.sh -install` *`component_list`* command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, using the Data Protector GUI. For a list of the Data Protector component codes, see "Local installation on UNIX and Mac OS X systems" (page 81). Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-install` *`component_list`* option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

Upgrading in a MoM environment

You can upgrade a MoM Environment sequentially. However, note the following limitations:

Limitations

- You cannot use **distributed file media format** with your file libraries until all Cell Managers have been upgraded to Data Protector 7.00.

To upgrade your MoM environment to Data Protector 7.00, proceed as follows:

1. Upgrade the MoM Manager/CMMDB Server to Data Protector 7.00.

   During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with the old Cell Managers.

2. Upgrade each client Cell Manager in a MoM environment.

   For the upgrade procedure, see "Upgrading the UNIX Cell Manager and Installation Server" (page 162) and "Upgrading the Windows Cell Manager and Installation Server" (page 165).

3. Upgrade clients with configured devices.
4. Upgrade clients with application integrations.

   After this part of the upgrade is finished, you can backup and restore filesystems and integrations with the Data Protector 7.00 MoM GUI.

Upgrading from the Single Server Edition

You can perform the upgrade from one of the following:

- From earlier versions of the Single Server Edition (SSE) to Data Protector 7.00 Single Server Edition. For details, see "Upgrading from earlier versions of SSE to Data Protector 7.00 SSE" (page 175).
- From Data Protector 7.00 Single Server Edition to Data Protector 7.00. For details, see "Upgrading from Data Protector 7.00 SSE to Data Protector 7.00" (page 175).

Upgrading from earlier versions of SSE to Data Protector 7.00 SSE

The upgrade procedure from earlier versions of SSE to Data Protector 7.00 SSE is the same as the upgrade procedure from earlier versions of Data Protector to Data Protector 7.00. For the information, see "Upgrading from Data Protector A.06.10, A.06.11, and 6.20" (page 162).

Upgrading from Data Protector 7.00 SSE to Data Protector 7.00

Licenses

You need to have a license to perform the upgrade from Data Protector 7.00 Single Server Edition to Data Protector 7.00. For details about licensing, see "Data Protector licensing" (page 187).

The upgrade from Data Protector 7.00 Single Server Edition to Data Protector 7.00 is offered for two possible scenarios:

- If you have the Data Protector Single Server Edition installed on one system (Cell Manager) only. See "Upgrading the Cell Manager" (page 175).
- If you have the Data Protector Single Server Edition installed on multiple systems and you want to merge these cells. See "Upgrading from multiple installations" (page 176).

NOTE: To upgrade from a previous version of the Single Server Edition to a full Data Protector installation, first upgrade your Single Server Edition to the full installation of the same version level. To upgrade this full installation to Data Protector 7.00, see "Upgrading from Data Protector A.06.10, A.06.11, and 6.20" (page 162).

Upgrading the Cell Manager

To upgrade the Single Server Edition Cell Manager, do the following:

1. Remove the Single Server Edition license:

   Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012:

   `del Data_Protector_program_data\Config\server\Cell\lic.dat`

   Other Windows systems:

   `del Data_Protector_home\Config\server\Cell\lic.dat`

   UNIX systems:

   `rm /etc/opt/omni/server/cell/lic.dat`
2. Start the Data Protector GUI and add a permanent password.

Upgrading from multiple installations

To upgrade the Data Protector Single Server Edition installed on multiple systems, proceed as follows:

1. Select one of the existing Single Server Edition systems to be the new Cell Manager. See "Choosing the Cell Manager system" (page 23).
2. Upgrade the selected Cell Manager by performing the following:
   a. Remove the Single Server Edition license:

      `del Data_Protector_home\Config\server\Cell\lic.dat` (on Windows systems) or

      `rm /etc/opt/omni/server/cell/lic.dat` (on UNIX systems)

   b. Start the Data Protector GUI and add a permanent password.
3. Import the other Single Server Edition systems into the newly created Cell Manager system as clients using the GUI.
4. Uninstall the Data Protector Single Server Edition from the other systems. See "Uninstalling Data Protector software" (page 150).
5. If needed, import the media to the new Cell Manager.

   Perform this step if you intend to frequently restore from the media created on the other Single Server Edition systems. If the probability of these restores is relatively low, the `List from media` restore can be used. For the information about importing media and details about the `List from media` restore, see the *HP Data Protector Help* index: "importing, media".

Upgrading from Solaris 8 to Solaris 9

With Data Protector 7.00, upgrading the operating system on the Data Protector Disk Agent clients from Solaris 8 to Solaris 9 is no longer supported.

If you still have Disk Agent (DA) of an earlier Data Protector version installed on Solaris 8, to upgrade the operating system to Solaris 9, follow instructions in the corresponding section of the *HP Data Protector Installation and Licensing Guide* of the earlier product version.

Migrating from HP-UX 11.31 (PA-RISC) to HP-UX 11.31 (IA-64)

With Data Protector 7.00, migrating your existing Cell Manager from a PA-RISC architecture based HP-UX 11.11/11.23 system to an HP-UX 11.23/11.31 system for the Intel Itanium 2 (IA-64) architecture is no longer supported.

This section describes the procedure for migrating your existing Cell Manager from a PA-RISC architecture based HP-UX 11.31 system to an HP-UX 11.31 system for the Intel Itanium 2 (IA-64) architecture.

Limitations

For details on supported operating system versions, platforms, processor architectures and Data Protector components as well as required patches, general limitations, and installation requirements, see the *HP Data Protector Product Announcements, Software Notes, and References*.

- For the supported combinations of MoM configurations, see "MoM specifics" (page 178).

Prerequisites

- Before the migration, the Data Protector Cell Manager on a PA-RISC architecture based HP-UX 11.31 system must be upgraded to Data Protector 7.00.

Licenses

The new Cell Manager (IA-64 system) will have a different IP address as the old Cell Manager, therefore you should apply for the licenses migration prior to the migration. For a limited amount of time, licenses on both system will be operational. If licenses are based on an IP range and the new Cell Manager's IP address is within this range, no license reconfiguration is necessary. For details, see "License migration to Data Protector 7.00" (page 206).

Migration procedure

Perform the migration procedure as follows:

1. Install a Data Protector client on the IA-64 system and import it to the old Cell Manager's cell. If you are planning to configure Data Protector in a cluster, install the client on the primary node. See "Installing HP-UX clients" (page 51).
2. Execute the following command on the *old* Cell Manager to add the hostname of the IA-64 system to the list of trusted hosts on secured clients:

   `omnimigrate.pl -prepare_clients` *`New_CM_Name`*, where the *`New_CM_Name`* is the client name of the IA-64 system from the previous step.

   For more information about trusted hosts and securing Data Protector clients, see "Securing clients" (page 139) and "Host trusts" (page 147).
3. Back up the IDB. Make sure that the used media can later be accessed on the new Cell Manager system. See the *HP Data Protector Help* index: "IDB backup".
4. Restore the IDB to a temporary location on the IA-64 system. See the *HP Data Protector Help* index: "IDB restore".
5. Uninstall the Data Protector client from the IA-64 system. See "Uninstalling a Data Protector client" (page 151).
6. Install Data Protector Cell Manager on the IA-64 system. If you are planning to configure Data Protector in a cluster, install the Cell Manager on the primary node as a *standalone* Cell Manager (not cluster aware). See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).
7. If you changed the default Data Protector Inet port on the old Cell Manager, set the same Inet port also on the new Cell Manager. See "Changing the default Data Protector Inet port" (page 226).
8. Move the restored IDB (residing in a temporary location on the new Cell Manager), and configuration data to the same location on the new Cell Manager as it was on the old Cell Manager. See the *HP Data Protector Help* index: "IDB restore".

   If the old Cell Manager was cluster-aware, comment out the `SHARED_DISK_ROOT` and `CS_SERVICE_HOSTNAME` parameter in the `/etc/opt/omni/server/sg/sg.conf` file. This is necessary even if the new Cell Manager will be cluster-aware.

9. To migrate the IDB and clients to the new Cell Manager, and to reconfigure the Cell Manager's settings, perform the following steps on the *new* Cell Manager:
   - To configure a standalone IA-64 Cell Manager, execute the `omnimigrate.pl -configure` command. See the `omnimigrate.pl` man page.
   - To configure a cluster-aware IA-64 Cell Manager:
     a. Execute the `omnimigrate -configure_idb` command to configure the IDB from the old Cell Manager for use on the new Cell Manager. See the `omnimigrate.pl` man page.
     b. Execute the `omnimigrate -configure_cm` command to reconfigure the configuration data transferred from the old Cell Manager for use on the new Cell Manager. See the `omnimigrate.pl` man page.
     c. Export the old virtual server from the cell by executing the `omnicc -export_host` *`Old_CM_Name`*.
     d. Configure the primary and secondary Cell Manager. See the *HP Data Protector Help* index: "MC/ServiceGuard integration configuring".
     e. Execute the `omnimigrate -configure_clients` command to migrate the clients from the old Cell Manager to the new Cell Manager. Note that the old Cell Manager will keep the clients in the configuration files although it will not be their Cell Manager anymore.

     NOTE: If the `/etc/opt/omni/server` directory is located on the shared cluster volume, the configuration changes made by the `omnimigrate.pl` script will affect all nodes in the cluster.

   NOTE: The old Cell Manager will automatically become a client in the new cell. You can uninstall the Cell Manager component from the old Cell Manager, because it is not necessary anymore. See "Changing Data Protector software components" (page 157).
10. Configure the licenses on the new Cell Manager. See "Data Protector 7.00 product structure and licenses" (page 204).
11. Additional steps are required if the following is true:
    - Your cell is a part of the MoM environment. See "MoM specifics" (page 178).
    - Your cell works across a firewall. Reconfigure all firewall related settings on the new Cell Manager. See the *HP Data Protector Help* index: "firewall environments".
    - You want to have an Installation Server on your new Cell Manager. See "Installation Server specifics" (page 179).

MoM specifics

If the new Cell Manager will be configured in the MoM, additional steps are required after the basic migration procedure has been completed. The required steps depend on the configuration of the MoM for the old and new Cell Managers in your environment. The supported combinations are:

- The old Cell Manager was a MoM client; the new Cell Manager will be a MoM client of the same MoM Manager.

  Perform the following steps:

  1. On the MoM Manager, export the old Cell Manager from the MoM Manager cell and import the new Cell Manager. See the *HP Data Protector Help* index: "client systems exporting".

2. Add the MoM administrator to the users list on the new Cell Manager. See the *HP Data Protector Help* index: "MoM administrator, adding".

- The old Cell Manager was a MoM Manager; the new Cell Manager will be a MoM Manager.

  If the old MoM Manager was the only client in the MoM, no action is necessary. Otherwise, perform the following steps:

  1. On the old MoM Manager (the old Cell Manager), export all MoM clients.
  2. On the new MoM Manager (the new Cell Manager), import all MoM clients.
  3. Add the MoM administrator to the users list on all MoM clients.

Installation Server specifics

The migration of the Installation Server is not done as part of the Cell Manager migration. If Installation Server is installed on your old Cell Manager, it will not be migrated to the new Cell Manager and will stay the Installation Server for your cell.

To use the new Cell Manager also as an Installation Server, install the Installation Server component on the new Cell Manager after the migration and import it in the cell. See the *HP Data Protector Help* index: "Installation Server".

Migrating to a different Windows system

This section describes the procedure for migrating your existing Cell Managerfrom a 32-bit Windows system to a 64-bit Windows system, or from a 64-bit Windows system to a 64-bit Windows Server 2008 or Windows Server 2012 system.

Limitations

- For details on supported operating system versions, platforms, processors, and Data Protector components as well as required patches, general limitations, and installation requirements, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Prerequisites

- Before the migration, the Data Protector Cell Manager on a 32-bit Windows system must be upgraded to Data Protector 7.00.

Licenses

The new Cell Manager will have a different IP address than the old Cell Manager, therefore you should apply for license migration prior to the migration. For a limited amount of time, licenses on both systems will be operational. If your licenses are based on an IP range and the new Cell Manager's IP address is within this range, no license reconfiguration is necessary. For details, see "License migration to Data Protector 7.00" (page 206).

Migration procedure

Perform the migration as follows:

1. Install a Data Protector client on the system that will become your new Cell Manager. For details, see "Installing Windows clients" (page 48).
2. Import the system to the old Cell Manager's cell.
3. On the *old* Cell Manager, add the hostname of the new Cell Manager to the list of trusted hosts on secured clients. Execute:

   ```
   perl winomnimigrate.pl -prepare_clients New_CM_Name
   ```

   New_CM_Name is the client name of the new Cell Manager from the previous step. For details on `winomnimigrate.pl`, see the *HP Data Protector Command Line Interface Reference*.

   For more information about trusted hosts and securing Data Protector clients, see "Securing clients" (page 139) and "Host trusts" (page 147).

4. Back up the IDB. Make sure that the used media can later be accessed on the new Cell Manager system. See the *HP Data Protector Help* index: "IDB backup".
5. Restore the IDB to a temporary location on the new Cell Manager. Depending on which option you choose for the IDB backup, you may have to configure the device and import the catalog from the appropriate media. Once the IDB backup object is in the IDB, you can restore the IDB in order to move the configuration data to the new system. See the *HP Data Protector Help* index: "IDB restore".
6. Uninstall the Data Protector client from the new Cell Manager. See "Uninstalling a Data Protector client" (page 151).
7. Install Data Protector Cell Manager on the new Cell Manager. See "Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)" (page 26).

   Make sure that you install the Cell Manager in the same path as the original Cell Manager.
8. If you changed the default Data Protector Inet port on the old Cell Manager, set the same Inet port on the new Cell Manager. See "Changing the default Data Protector Inet port" (page 226).
9. Move the restored IDB (residing in a temporary location on the new Cell Manager) and configuration data to the same location on the new Cell Manager as it was on the old Cell Manager. Do not restart the Data Protector services. See the *HP Data Protector Help* index: "IDB restore".

   NOTE: During the migration from to a different Windows system, the IDB files are relocated to the new default location. For this reason, you need to ensure the IDB files are located in the same directory as they were before the migration, under `Data_Protector_home` and not `Data_Protector_program_data`.
10. To migrate the IDB and clients to the new Cell Manager and to reconfigure the Cell Manager's settings, perform the following steps on the *new* Cell Manager:
    - Configure a standalone Cell Manager and execute:

      ```
      perl winomnimigrate.pl -configure
      ```

      If you are migrating the Cell Manager to a 64-bit Windows Server 2008 or Windows Server 2012 system, you can use the option `-keep_dcdirs` to unconditionally preserve references to additional DCBF directories in the migrated IDB:

      ```
      perl winomnimigrate.pl -configure -keep_dcdirs
      ```
    - To configure a cluster-aware Cell Manager:
      a. Execute `perl winomnimigrate.pl -configure_idb` to configure the IDB from the old Cell Manager for use on the new Cell Manager.

      If you are migrating the Cell Manager to a 64-bit Windows Server 2008 or Windows Server 2012 system, you can use the option `-keep_dcdirs` to unconditionally preserve references to additional DCBF directories in the migrated IDB: `perl winomnimigrate.pl -configure_idb -keep_dcdirs`

      b. Execute `perl winomnimigrate.pl -configure_cm` to reconfigure the configuration data transferred from the old Cell Manager for use on the new Cell Manager.

      c. Export the old virtual server from the cell by executing `omnicc -export_host Old_CM_Name`.

      d. Execute `perl winomnimigrate.pl -configure_clients` to migrate the clients from the old Cell Manager to the new Cell Manager. Note that the old Cell Manager will keep the clients in the configuration files although it will not be their Cell Manager anymore.

NOTE: The old Cell Manager will automatically become a client in the new cell. You can uninstall the Cell Manager component from the old Cell Manager, because it is not necessary anymore. See "Changing Data Protector software components" (page 157).

11. If you installed the new 64-bit Cell Manager in a different directory than the one in which the old Cell Manager was installed, the internal links in the IDB still include the old Cell Manager paths. Manually add the new paths of the Detail Catalog Directories on the new Cell Manager using the Data Protector GUI. See the *HP Data Protector Help* index: "creating DC directories".
12. Configure the licenses on the new Cell Manager. See "Data Protector 7.00 product structure and licenses" (page 204).
13. Additional steps are required if:
    - Your cell is a part of the MoM environment. See "MoM specifics" (page 181).
    - Your cell works across a firewall. Reconfigure all firewall related settings on the new Cell Manager. See the *HP Data Protector Help* index: "firewall environments".
    - You want to have an Installation Server on your new Cell Manager. See "Installation Server specifics" (page 181).

MoM specifics

If the new Cell Manager will be configured in the MoM, additional steps are required after the basic migration procedure has been completed. The required steps depend on the configuration of the MoM for the old and new Cell Managers in your environment. The supported combinations are:

- The old Cell Manager was a MoM client; the new Cell Manager will be a MoM client of the same MoM Manager.

  Perform the following steps:

  1. On the MoM Manager, export the old Cell Manager from the MoM Manager cell and import the new Cell Manager. See the *HP Data Protector Help* index: "client systems, exporting".
  2. Add the MoM administrator to the user list on the new Cell Manager. See the *HP Data Protector Help* index: "MoM administrator, adding".

- The old Cell Manager was a MoM Manager; the new Cell Manager will be a MoM Manager.

  If the old MoM Manager was the only client in the MoM, no action is necessary. Otherwise, perform the following steps:

  1. On the old MoM Manager (the old Cell Manager), export all MoM clients.
  2. On the new MoM Manager (the new Cell Manager), import all MoM clients.
  3. Add the MoM administrator to the user list on all MoM clients.

Installation Server specifics

The migration of the Installation Server is not performed as part of the Cell Manager migration. If Installation Server is installed on your old Cell Manager, it will not be migrated to the new Cell Manager.

To use the new Cell Manager also as an Installation Server, install the Installation Server component on the new Cell Manager after the migration and import it to the cell. See the *HP Data Protector Help* index: "Installation Server".

Upgrading the Cell Manager configured on MC/ServiceGuard

During an upgrade procedure, only the database is upgraded, and the old version of the product is removed. Data Protector 7.00 is installed with the default selection of agents, and other agents

are removed. In order to obtain a configuration equivalent to the state before the upgrade, you must manually select any other agents during the upgrade procedure or reinstall them afterwards on each physical node.

The upgrade procedure from Data Protector A.06.10, A.06.11, or 6.20 consists of upgrading the primary and secondary nodes. Follow the steps described below:

Primary node

Log on to the primary node and perform the following steps:

1. Stop the old Data Protector package by running the `cmhaltpkg` *`pkg_name`* command (where *`pkg_name`* is the name of the cluster package). For example:

   ```
   cmhaltpkg ob2cl
   ```

2. Activate the volume group in exclusive mode:

   ```
   vgchange -a e -q y vg_name
   ```

   For example:

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```

3. Mount the logical volume to the shared disk:

   ```
   mount lv_path shared_disk
   ```

   The *`lv_path`* parameter is the path name of the logical volume, and *`shared_disk`* is the mount point or a shared directory. For example:

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

4. Upgrade the Cell Manager following the procedure described in the sections below. Note that some of the steps are different depending on the product version you are upgrading from to Data Protector 7.00. See "Upgrading the UNIX Cell Manager and Installation Server" (page 162).
5. Stop the Data Protector services if they are running:

   ```
   omnisv -stop
   ```

6. Dismount the shared disk:

   ```
   umount shared_disk
   ```

   For example:

   ```
   umount /omni_shared
   ```

7. Deactivate the volume group:

   ```
   vgchange -a n vg_name
   ```

   For example:

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

Secondary node

Log on to the secondary node and perform the following steps:

1. Activate the volume group in exclusive mode:

   ```
   vgchange -a e -q y vg_name
   ```

2. Mount the logical volume to the shared disk:

   ```
   mount lv_path shared_disk
   ```

3. Upgrade the Cell Manager. The steps are different depending on the product version you are upgrading from to Data Protector 7.00. Follow the steps described in "Upgrading the UNIX Cell Manager and Installation Server" (page 162).

4. Rename the `csfailover.sh` and `mafailover.ksh` startup scripts in the `/etc/opt/omni/server/sg` directory (for example, to `csfailover_DP55.sh` and `mafailover_DP55.ksh`) and copy the new `csfailover.sh` and the `mafailover.ksh` scripts from the `/opt/omni/newconfig/etc/opt/omni/server/sg` directory to the `/etc/opt/omni/server/sg` directory.

   If you customized your old startup scripts, reimplement the changes also in the new startup scripts.
5. Stop the Data Protector services if they are running:

   ```
   omnisv -stop
   ```
6. Dismount the shared disk:

   ```
   umount shared_disk
   ```
7. Deactivate the volume group:

   ```
   vgchange -a n vg_name
   ```

Primary node

Log on to the primary node again and perform the following steps:

1. Restart the Data Protector package:

   ```
   cmrunpkg pkg_name
   ```

   Make sure that the package switching and switching for nodes options are enabled.
2. Configure the Cell Manager. Make sure not to be positioned in the `/etc/opt/omni` or `/var/opt/omni` directory or their subdirectories when running the script. Make also sure to have no mounted subdirectories in the `/etc/opt/omni` or `/var/opt/omni`. Esecute:

   ```
   omniforsg.ksh -primary -upgrade
   ```
3. Stop the Data Protector services if they are running:

   ```
   omnisv -stop
   ```
4. Dismount the shared disk:

   ```
   umount shared_disk
   ```
5. Deactivate the volume group:

   ```
   vgchange -a n vg_name
   ```

Secondary node

Log on to the secondary node again and perform the following steps:

1. Restart the Data Protector package:

   ```
   cmrunpkg pkg_name
   ```

   Make sure that the package switching and switching for nodes options are enabled.
2. Configure the Cell Manager. Make sure not to be positioned in the `/etc/opt/omni` or `/var/opt/omni` directory or their subdirectories when running the script. Make also sure to have no mounted subdirectories in the `/etc/opt/omni` or `/var/opt/omni`. Execute:

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
   ```
3. Stop the Data Protector services if they are running:

   ```
   omnisv -stop
   ```
4. Dismount the shared disk:

   ```
   umount shared_disk
   ```

5. Deactivate the volume group:

   ```
   vgchange -a n vg_name
   ```

Primary node

Log on to the primary node again and perform the following steps:

1. Restart the Data Protector package:

   ```
   cmrunpkg pkg_name
   ```

   Make sure that the package switching and switching for nodes options are enabled.
2. Re-import the virtual host:

   ```
   omnicc -import_host virtual_hostname -virtual
   ```
3. Change the Cell Manager name in the IDB:

   ```
   omnidbutil -change_cell_name
   ```
4. If you have the Installation Server in the same package as the Cell Manager, import the Installation Server virtual hostname:

   ```
   omnicc -import_is virtual_hostname
   ```

NOTE: All requests coming from the Cell Managers are logged in the `/var/opt/omni/log/inet.log` file on clients. To prevent unnecessary log entries, secure the clients. See "Security considerations" (page 137) for information on how to secure a cell.

Upgrading the Cell Manager configured on Microsoft Cluster Server

The upgrade of Data Protector A.06.10, A.06.11, or 6.20 Cell Manager to Data Protector 7.00 on Microsoft Cluster Server (MSCS) is performed locally, from the Windows installation DVD-ROM.

Prerequisites

- The upgrade option is supported only if the previously installed Data Protector software is the Cell Manager installed in cluster-aware mode. If a system in the cluster has the Data Protector software installed as non-cluster-aware, you need to uninstall it prior to starting the setup.

Upgrade procedure

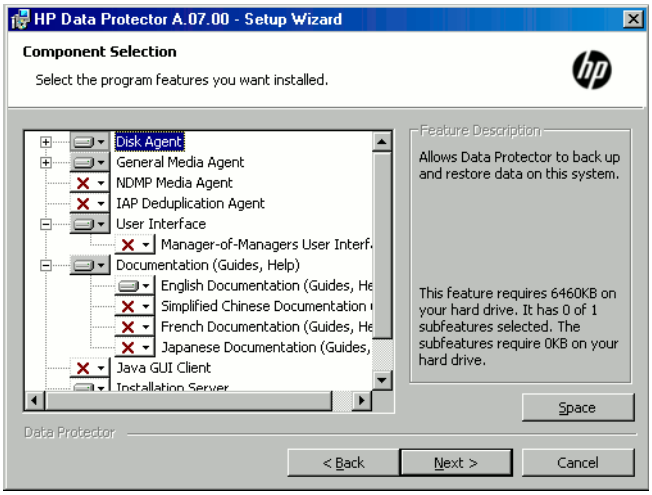
To perform the upgrade, proceed as follows:

1. Insert the Windows installation DVD-ROM and run `\Windows_Other\i386\setup.exe`. It is recommended to start the setup on the currently active virtual server node.

   Setup automatically detects the old version of the product and prompts you to upgrade it to Data Protector 7.00.

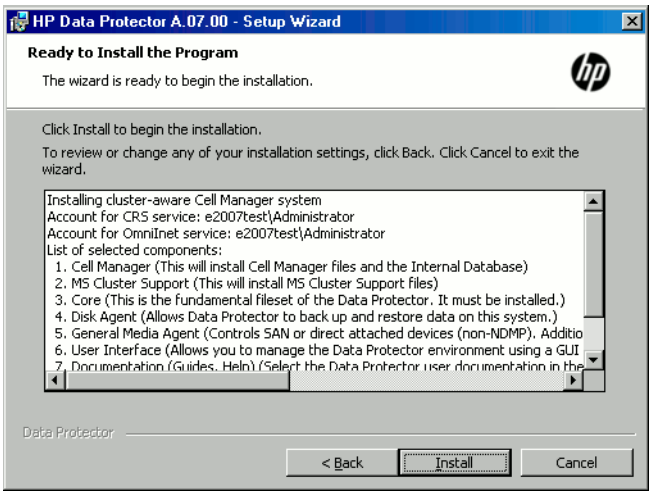
   Click **Next** to continue.
2. Data Protector automatically selects the components that were installed.

Figure 46 Selecting the components



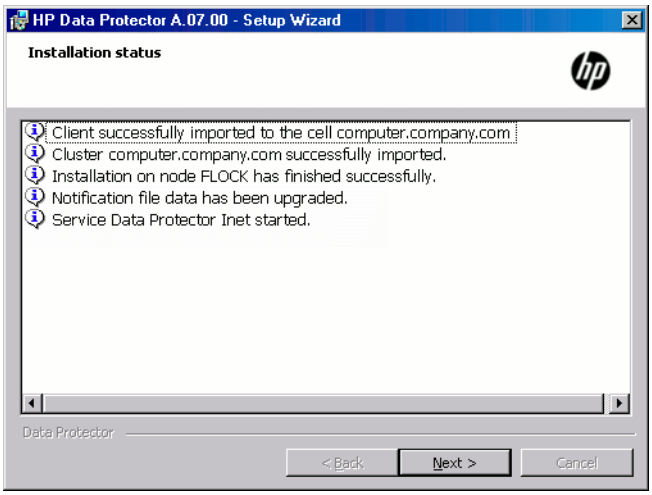
3. The component selection summary list is displayed. Click **Install** to perform the upgrade. Note that after the upgrade, every node has the same component set.

Figure 47 Component selection summary page



4. The **Installation status** page is displayed. Click **Next**.

Figure 48 Installation status page



5. To start using Data Protector immediately after setup, select **Start the Data Protector Manager GUI**.

   To view the *HP Data Protector Product Announcements, Software Notes, and References*, select **Open the Product Announcements**.

   It is *not* recommended to install the HP AutoPass utility on Microsoft Cluster Server, because it will be installed only on one node and not on all nodes. However, if you install AutoPass, you must uninstall Data Protector from the same node on which it was installed, when you decide to remove Data Protector from the system.

   Click **Finish**.

NOTE: If you are upgrading cluster-aware clients, first upgrade every cluster node separately, and then re-import the virtual server. The remote upgrade is not supported.

5 Data Protector licensing

In this chapter

This chapter contains information about:

- Data Protector license checking and reporting
- obtaining and installing Data Protector passwords
- Data Protector product structure and licenses

Overview

The Data Protector 7.00 product structure and licensing consists of three main categories:

1. Starter Packs
2. Drive extensions and Library extensions
3. Functional Extensions

NOTE: The UNIX product licenses operate on all platforms, providing the functionality regardless of the platform, while the Windows product licenses operate on the Windows, Linux, and Novell NetWare platforms only.

Licenses of the *Starter Pack* and *Drive extensions and Library extensions* categories and the corresponding passwords are bound to the Cell Manager and cover the entire Data Protector cell, regardless of the number of Data Protector clients involved in the sessions. Licenses of the *Functional Extensions* category either apply only to a specific client that is protected or cover the entire cell, depending on the license type.

For example, filesystem and disk image backup is covered by the *Starter Pack* licenses. You therefore need only one license for backing up filesystems and disk images from an arbitrary number of clients in the same cell.

License checking and reporting

Data Protector licenses are checked and if missing, reported during various Data Protector operations, for example:

- As a part of the Data Protector checking and maintenance mechanism, the licenses are checked and, if missing, reported in the Data Protector Event Log. The Data Protector Event Log is located on the Cell Manager in *Data_Protector_program_data*`\log\server\Ob2EventLog.txt` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*`\log\server\Ob2EventLog.txt` (other Windows systems), or `/var/opt/omni/server/log/Ob2EventLog.txt` (UNIX systems). For more information on Data Protector checking and maintenance mechanism, see the *HP Data Protector Help* index: “Event Log, Data Protector“.
- When the Data Protector User Interface is started, if there are any missing licenses reported in the Data Protector Event Log, an Event Log notification is displayed. For more information on Data Protector Event Log, see the *HP Data Protector Help* index: “Event Log, Data Protector“.
- When a Data Protector session is started, the licenses are checked and, if missing, reported.

Data Protector licenses are with regard to their characteristics grouped as follows:

- Cell Manager related licenses
- entity based licenses
- capacity based licenses

Cell Manager related licenses

The Data Protector Cell Manager related licenses are:

- Starter packs
- Manager-of-Managers Extension
- Single Server Edition

When a certain Data Protector component, such as the Cell Manager (included in the Starter Pack) or the Manager-of-Managers (MoM) is present in the cell, only the presence of the required basic or special license is checked.

Entity based licenses

The Data Protector entity based licenses are:

- Library extension for one library with 61-250 slots and for one library with unlimited slots
- Drive extension for SAN / all platforms and Drive extension for Windows / NetWare / Linux
- On-line extension for one UNIX system and On-line extension for one Windows / Linux system
- Data Protector encryption extension for one client system
- Granular recovery extension for one database server

When any of the items that are the subject of the source based licenses is configured in the cell, the presence and number of the required entity based licenses is checked.

Data Protector checks the number of configured entity based items against the number of entity based licenses. If there are less licenses than configured items, Data Protector issues a notification.

With the first two licenses from the above list the following applies:

When a backup device is configured in a SAN environment for several Data Protector clients, multipath functionality must be used for Data Protector to recognize it as a single backup device.

Capacity based licenses

The Data Protector capacity based licenses are:

- UNIX Zero Downtime Backup for 1 TB and 10 TB
- UNIX Instant Recovery for 1 TB and 10 TB
- Linux Zero Downtime Backup for 1 TB and 10 TB
- Linux Instant Recovery for 1 TB and 10 TB
- Windows Zero Downtime Backup for 1 TB and 10 TB
- Windows Instant Recovery for 1 TB and 10 TB
- Direct Backup using NDMP for 1 TB and 10 TB
- Advanced backup to disk for 1 TB, 10 TB, and 100 TB

When a capacity based license (other than the advanced backup to disk license) is being checked, the amount of *total* disk space on logical units that have been backed up is compared to the capacity of licenses installed.

License checking is done in such a way as not to prevent you from performing instant recovery or a backup even if you have run out of licensed capacity. In these circumstances a warning message appears during the backup session informing you that you have exceeded your licensed capacity.

Capacity of used disks is calculated based on historical information gathered during each ZDB backup session. The time interval taken into account is twenty-four hours. Data Protector calculates used disk capacity based on the disks that were used in all sessions in the last twenty-four hours and compares the calculated capacity with the licensed capacity.

If a license violation occurs, a warning message is issued during the backup. In addition, the license reporting tool is run daily and writes a notification to the Data Protector Event Log if the licensed capacity is exceeded.

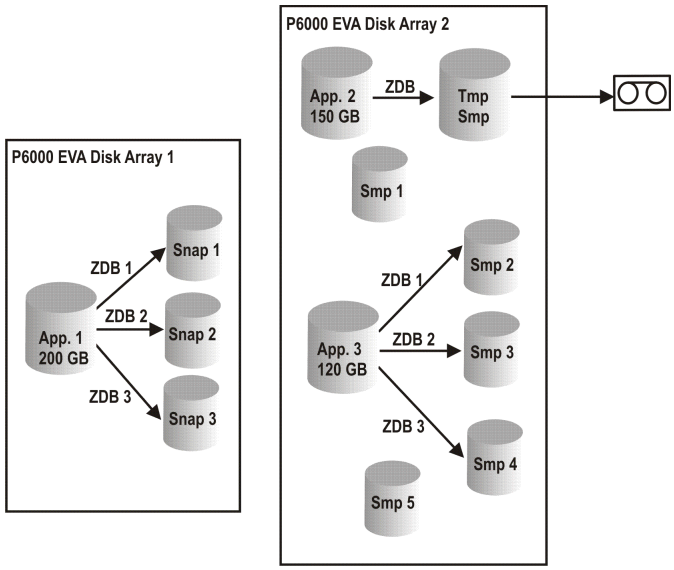
Used capacity calculation

The used capacity calculation calculates the licensed capacity of each disk array used in the past twenty-four hours. Disks used two or more times in the specified time interval are only counted once. Disk array units are identified by their identification numbers taken from each array. The use of array identification numbers means that it is possible to know when an array has already been counted.

If a ZDB backup has been run that includes instant recovery, the original unit's total capacity is calculated both for ZDB used capacity per disk array, and in addition, that used for instant recovery capacity per disk array.

For example, imagine a scenario where there are two P6000 EVA disk arrays. On one array there is a single disk (App.1) with a capacity of 200 GB being used for data protection. An instant recovery option is included with each backup session which are triggered three times a day. Three replicas at a time are kept, these are rotated for instant recovery purposes. On the second disk array there are two disks (App.2 and App.3) with capacities of 150 GB and 120 GB respectively. Backup is run once a day on App.2 disk and the snapshot is deleted after the data is moved to tape. On App.3, backup is run three times a day and five different replicas are rotated for instant recovery. See "Used capacity calculation scenario" (page 189).

Figure 49 Used capacity calculation scenario



The calculation for ZDB used capacity counts all disks used in backup sessions in the last twenty-four hours 200 GB (App.1) + 150 GB (App.2) + 120 GB (App.3) = 470 GB.

Calculations for instant recovery used capacity count source capacity for ZDB sessions that left data for instant recovery purposes. The same disk is only counted once 200 GB (App.1) + 120 GB (App.3) = 320 GB.

The advanced backup to disk license

The advanced backup to disk license is required to back up to a Data Protector file library and to a Data Protector StoreOnce library, and can be used for a virtual tape library (VTL) instead of drive licenses.

- Usable native capacity of a Data Protector file library is the available size on disk for the file library, as reported by the filesystem.
  - Virtual full backups and the incremental backups that will be consolidated into a synthetic full or virtual full backup must be stored in the Data Protector file library, which requires this license.
- If Data Protector is using the VTL exclusively, it is recommended to license a quantity matching the physical capacity of the VTL, also referred as usable native capacity.
  - Usable native capacity of a virtual tape library (VTL) is the size on disk of the virtual tape library consumed by all protected HP Data Protector backups as reported by the VTL.
  - For each VTL, you can choose whether to use the backup to disk or tape drive licensing model. Within one VTL, both concepts must not been mixed.
  - If the VTL has a built-in capability to migrate backup data from the disk cache to another disk or tape, the migrated storage capacity needs to be fully licensed. No drive and library licenses are required for the tape library exclusively controlled by the VTL, but ***the used capacity of all tapes in the physical tape library needs to be licensed***. However, this is not applicable if Data Protector object copy functionality has been used to migrate the backup data to another disk or tape.
  - By default, Data Protector treats VTL devices as ordinary libraries (such as SCSI II libraries) and does not utilize capacity based licensing. To enable capacity based licensing, the device must be marked as a VTL during the device configuration.

    For more information on how to configure a VTL via the graphical user interface (GUI), see the *HP Data Protector Help* index: "virtual tape library". For more information on how to configure a VTL via the command-line interface (CLI), see the following "Example" (page 190).
- In case of central licensing with the Manager-of-Manager (MoM), you need to assign at minimum 1 TB to each cell using the advanced backup to disk functionality.

NOTE: Data Protector cannot report the required amount of licenses due to the missing instrumentation and interfaces of today's Virtual Tape Libraries and some files servers hosting the Data Protector file library. It is your responsibility to license the capacity consistently with the licensing definitions.

Example

If you configure a virtual tape library named "VTL_2011" via the command-line interface (CLI) by using the `omniupload` command, you must specify the estimated library capacity in the configuration file for the string `VTLCAPACITY`. This estimated value consequently adds up to used licenses capacity for advanced backup to disk in the license checker report.

NOTE: The estimated virtual library capacity consumption value (`VTLCAPACITY`) in terabytes (TB) must be an integer to avoid the error message `"Invalid VTL capacity specified"`.

In the configuration file named "libVTL.txt" in the directory "C:\Temp" type the estimated library capacity, for example `11` and execute:

```
omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt
```

To verify library configuration, execute:

```
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 ""
```

The license checker reports the license capacity in use, which is the sum of used space on disk for the file library (FL) and the estimated size of disk space on a virtual tape library. For example, you are using 2 TB of the disk space by backing up with the FL and 10 TB of disk capacity on the VTL. The total capacity in use is 12 TB. If there are only 5 TB licenses capacity installed, you get a notification that you need additional 7 Advanced Backup to disk for 1 TB licenses.

```
#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
```

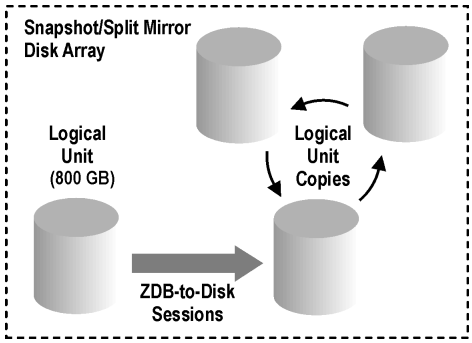
Capacity based licensing examples

This section provides examples of how capacity based licensing is calculated.

Example 1

Figure 50 (page 191) shows a situation where data from one 800 GB logical unit is backed up three times a day in a ZDB-to-disk session.

Figure 50 ZDB-to-disk sessions



Three split mirror or snapshot copies (replicas) are rotated and kept for the purpose of instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk sessions:

1 x 800 GB = 0.8 TB for the “Zero Downtime Backup for 1 TB” license.

Three replicas of the same 800 GB logical unit are kept for the purpose of instant recovery. Note that it is the capacity of source volumes and not the capacity of replica that is the subject of the license:

1 x 800 GB = 0.8 TB for the "Instant Recovery for 1 TB" license.

One "Zero Downtime Backup for 1 TB" license and one "Instant Recovery for 1 TB" license are sufficient for this situation.

Example 2

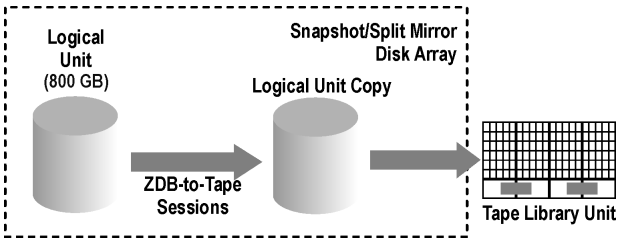
"ZDB-to-tape sessions" (page 192) shows a situation where data from one 800 GB logical unit is backed up twice a day in a ZDB-to-tape session. Split mirror or snapshot copies (replicas) are, therefore, not kept for instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk sessions:

1 x 800 GB = 0.8 TB for the "Zero Downtime Backup for 1 TB license.

One "Zero Downtime Backup for 1 TB" license is sufficient.

Figure 51 ZDB-to-tape sessions



Example 3

"ZDB-to-disk+tape sessions" (page 192) shows a situation where data from one 800 GB logical unit is backed up three times a day in a ZDB-to-disk+tape session. Five split mirror or snapshot copies (replicas) are rotated and kept for the purpose of instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk+tape sessions:

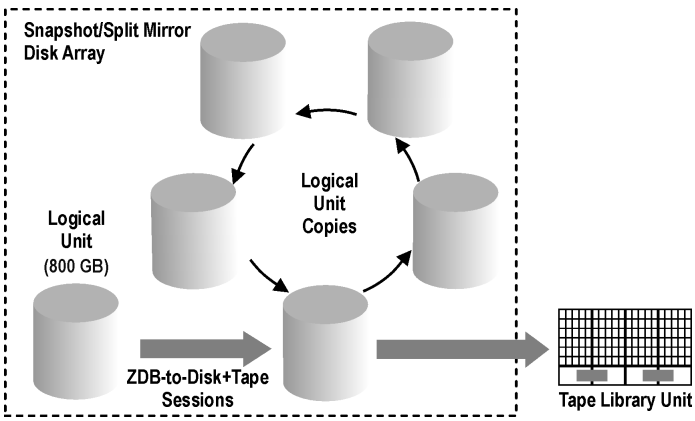
1 x 800 GB = 0.8 TB for the "Zero Downtime Backup for 1 TB" license.

Five replicas of the same 800 GB logical unit are kept for the purpose of instant recovery. Note that it is the capacity of source volumes and not the capacity of replica that is the subject of the license:

1 x 800 GB = 0.8 TB for the "Instant Recovery for 1 TB" license.

One "Zero Downtime Backup for 1 TB" license and one "Instant Recovery for 1 TB" license are sufficient.

Figure 52 ZDB-to-disk+tape sessions



Example 4

One 200 GB logical unit, one 500 GB logical unit, one 120 GB logical unit, and one 300 GB logical unit are used in ZDB sessions:

1 x 200 GB + 1 x 500 GB + 1 x 120 GB + 1 x 300 GB = 1.12 TB for the "Zero Downtime Backup for 1 TB" license.

Split mirror or snapshot copies of one 200 GB logical unit, one 120 GB logical unit, and one 300 GB logical unit are kept for the purpose of instant recovery:

1 x 200 GB + 1 x 120 GB + 1 x 300 GB = 0.62 TB for the "Instant Recovery for 1 TB" license.

One "Zero Downtime Backup for 1 TB" licenses and one "Instant Recovery for 1 TB" license are sufficient if all three examples in "ZDB-to-disk sessions" (page 191) through "ZDB-to-disk+tape sessions" (page 192) are configured in a cell.

Producing a license report on demand

To produce a report about licensing related information from the cell, execute:

```
omnicc -check_licenses [-detail]
```

If the `-detail` option is not specified, the command returns information on whether the Data Protector licensing is covered or not. The following information is returned: the time when the report was generated, the licensing mode, and the license server.

If the `-detail` option is specified, a detailed report is produced. The license checker returns the following information for every license in the cell: license name, licenses installed, licenses used, and additional licenses (capacity) required.

Note that for drive extension licenses-to-use, the license checker returns information about configured drives and recommended additional licenses. You need as many licenses as there are drives in use at any point in time. This is typically the total number of configured drives to allow all drives to be used simultaneously.

Note that the command does not list the expiration dates for the licenses. Depending on the environment and the number of licenses installed, the report may take some time to generate. To get the information on the licenses expiration dates, execute:

```
omnicc -password_info
```

IMPORTANT: In a MoM environment with the CMMDB configured, when producing a license report for the items that are subject to libraries and drives, the `omnicc` command must be run on the Cell Manager with the CMMDB installed.

For more information, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

Checking and reporting of pre-Data Protector 7.00 licenses

In Data Protector 7.00 the license checker maps certain licenses from previous Data Protector releases to the new Data Protector 7.00 product structure and reports them as new licenses. Note that certain limitations may still occur during license enforcement. For more information, see the limitations in the *HP Data Protector Product Announcements, Software Notes, and References*.

This chapter contains information about:

- "Reporting of multi-drive server licenses" (page 194)
- "Reporting of old on-line licenses" (page 195)
- "Reporting of licenses for direct backup using NDMP" (page 196)
- "Reporting of slot libraries licenses" (page 196)
- "Reporting of old ZDB and IR licenses" (page 197)

Reporting of multi-drive server licenses

The Multi-Drive Server for UNIX license-to-use is reported as 6 Drive extension for SAN / all platforms licenses.

Note that the Multi-drive license is used only on a device server, if the **Client is Device server** option is set in the **Client** context under **Advanced** tab when you select a client in the GUI. If this option is not set, the Multi-drive license is not used even if it is installed.

The number of installed Drive extension for SAN / all platforms licenses is increased by 6. For example, you have 1 Multi-Drive Server for UNIX license and 1 Drive extension for SAN / all platforms license installed on a device server. The license checker shows that you have 7 (1 single-drive + 6 from 1 multi-drive) Drive extension for SAN / all platforms licenses installed.

If you have 10 drives configured on a system, the license checker reports 3 Drive extension for SAN / all platforms licenses recommended to allow all drives to be used simultaneously.

```
#omnicc -check_licenses -detail
License Category         : Drive extension for SAN / all platforms
Licenses Installed       : 7
Drives Configured        : 10
Add. Licenses Recommended: 3

Summary
Description                          Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                          3

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

The same is done with licenses for Windows systems. The Multi-drive Server for Windows / NetWare license is removed from the license checker report as well and it is reported as 4 Drive extension for Windows / NetWare / Linux licenses. The number of Drive extension for Windows / NetWare / Linux licenses is increased by 4. In an environment with 10 configured drives where 1 multi-drive license and 1 single-drive license are installed, the license checker reports 5 (10 needed, 5 covered: 4 from 1 multi-drive, 1 from 1 single-drive) Drive extension for Windows / NetWare / Linux licenses recommended to allow all drives to be used simultaneously.

```
#omnicc -check_licenses -detail
License Category: Drive extension for Windows / NetWare / Linux
Licenses Installed       : 5
Drives Configured        : 10
Add. Licenses Recommended: 5

Summary
Description                        Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                          5

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

There are also old combined licenses, the Cell Manager & Multi-Drive Server for UNIX and the Cell Manager & Multi-Drive Server for Windows / NetWare.

If 1 Cell Manager & Multi-Drive Server for UNIX license is installed, the `omnicc` command reports that there is 1 Cell Manager for all platforms license and 1 Multi-Drive Server for UNIX license installed.

```
#omnicc
Licensing mode     : Local
License server     : computer.company.com

                Category                          Number of Licenses
 Cell Manager for all platforms                                   1
 Cell Manager for Windows / Linux                                 0
 Drive extension for SAN / all platforms                          0
 Drive extension for Windows / NetWare / Linux                    0
 Multi-Drive Server for UNIX                                      1
 Multi-Drive Server for Window / NetWare                          0
```

This combined license-to-use is reported as 1 Cell Manager & Single-Drive Server for UNIX license and 5 Drive extension for SAN / all platforms licenses. This means that the license checker reports 1 Cell Manager for all platforms license and 6 Drive extension for SAN / all platforms licenses.

If you have 10 drives configured in your system and 1 Cell Manager & Multi-Drive Server for UNIX license installed, the license checker reports 4 (10 needed, 6 covered by a multi-drive license) Drive extension for SAN / all platforms licenses recommended.

```
#omnicc -check_licenses -detail
License Category            : Cell Manager for all platforms
Licenses Installed          : 1
Licenses Used               : 1
Additional Licenses Required: 0

License Category: Drive extension for Windows / NetWare / Linux
Licenses Installed          : 6
Drives Configured           : 10
Add. Licenses Recommended   : 4

Summary
Description                     Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                     4

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

The same is done for the old combined license for Windows systems. The Cell Manager & Multi-Drive Server for Windows / NetWare license is reported as 1 Cell Manager & Single-Drive Server for Windows license and 4 Drive extension for Windows / NetWare / Linux licenses. The license checker reports 1 Cell Manager for Windows / Linux license and 5 Drive extension for Windows / NetWare / Linux licenses installed.

While the license checker may now report missing licenses, the checking of installed licenses during the backup is not changed. With the multi-drive license installed on a drive server it is still possible to use unlimited number of configured drives simultaneously. On the other hand, if you do not have a drive server configured but yet the multi-drive license installed, backup may not be possible, although the license checker reports enough single-drive licenses installed.

Reporting of old on-line licenses

The On-line Extension for UNIX system and the On-line Extension for Windows / Linux system licenses-to-use are valid for all clients in a cell. On-line licenses from previous Data Protector releases increase the number of installed current licenses by 1.

The license checker may now report that additional online licenses are required if there are a lot of systems in a cell. For example, there are 5 Windows systems in a cell using online backup and 1 On-line Extension for Windows license installed. Since 1 system is covered by the installed license, additional 4 are required for another 4 systems. The license checker reports that 4 On-line Extension for ONE Windows / Linux system licenses are required.

```
#omnicc -check_licenses -detail
License Category: On-line Extension for ONE Windows / Linux system
Licenses Installed    : 1
Licenses Used         : 5
Add. Licenses Required: 4

Summary
Description                                          Licenses Needed
On-line Extension for ONE Windows / Linux system                   4

Licensing is NOT covered.
```

If there are also 3 On-line Extension for ONE Windows / Linux system licenses installed, you get a notification that 1 (5 needed, 4 covered: 1 from the old one and 3 from ONE system) On-line Extension for ONE Windows / Linux system license is still needed.

```
#omnicc -check_licenses -detail
License Category: On-line Extension for ONE Windows / Linux system
Licenses Installed    : 4
Licenses Used         : 5
Add. Licenses Required: 1

Summary
Description                                           Licenses Needed
On-line Extension for ONE Windows / Linux system                    1

Licensing is NOT covered.
```

Reporting of licenses for direct backup using NDMP

The Extension for ONE NDMP Server license-to-use is reported as 1 Direct Backup using NDMP for 1 TB license. The first is an entity based license, which means that 1 license is needed per 1 NDMP server. The Direct Backup using NDMP for 1 TB license, however, is a capacity based license, which means that it is required to back 1 TB up on 1 NDMP server.

The quantity of licenses capacity installed for the Direct Backup using NDMP for 1 TB license is increased by the number of Extension for ONE NDMP Server licenses installed. For example, 1 Direct Backup using NDMP for 1 TB license and 1 Direct Backup using NDMP for 1 TB license installed give together 2 TB of licenses capacity installed. Consequently, the license checker may now report that additional licenses are required. For example, you are backing up 5 TB using the NDMP and you have installed 1 Extension for ONE NDMP Server and 1 Direct Backup using NDMP for 1 TB license. The license checker reports 3 (5 needed, 2 covered: 1 from the old and 1 from the new license) Direct Backup using NDMP for 1 TB licenses required.

```
#omnicc -check_licenses -detail
License Category               : Direct Backup using NDMP for 1 TB
Licenses Capacity Installed    : 2 TB
Licenses Capacity In Use       : 5.0 TB
Add. Licenses Capacity Required: 3 TB

Summary
Description                                          Licenses Needed
Direct Backup using NDMP for 1 TB                                  3
```

Reporting of slot libraries licenses

The platform specific library extensions licenses-to-use, 1 for Windows and 1 for UNIX systems, are reported as the platform independent licenses.

The number of the Extension for ONE 61-250 Slot Library licenses installed is increased by the number of the installed platform specific licenses for 61-250 slot libraries, and the platform specific unlimited licenses are added to the number of Extension for ONE Unlimited Slot Library licenses installed.

If you have installed 1 Unlimited Slot Libraries Extension for UNIX and 1 Unlimited Slot Libraries Extension for Windows license, then the license checker reports 2 Extension for ONE Unlimited Slot Library licenses installed.

```
#omnicc -check_licenses -detail
License Category      : Extension for ONE 61-250 Slot Library
Licenses Installed    : 2
Licenses Used         : 0
Add. Licenses Required: 0
License Category      : Extension for ONE Unlimited Slot Library
Licenses Installed    : 2
Licenses Used         : 0
Add. Licenses Required: 0
```

Due to the platform independent licenses for slot libraries, the license enforcement is stronger than the license checking. During the backup, Data Protector is checking the licenses for different platforms and the backup may not be possible because of the missing licenses for a specific platform, although the license checker reports enough appropriate licenses installed on the system.

Reporting of old ZDB and IR licenses

- The Zero Downtime Backup for 1 TB license-to-use (B7025CA) replaces disk array specific zero downtime backup licenses from previous Data Protector releases:
  - ZDB for 1 TB for HP Modular SAN Array 1000 (`Zero Downtime Backup for 1 TB HP Modular SAN Array 1000` (B7036AA))
  - ZDB for 1 TB for HP P6000 EVA Disk Array Family (`Zero Downtime Backup for 1 TB (generic license)` (B7025CA))
  - ZDB for 1 TB for HP P9000 XP Disk Array Family (`Zero Downtime Backup for 1 TB HP P9000 XP` (B7023CA))
  - ZDB for 1 TB for EMC Symmetrix / DMX (`Zero Downtime Backup for 1 TB EMC Symmetrix / DMX` (B6959CA))

  All disk array-specific licenses are reported by the license checker as 1 generic license Zero Downtime Backup for 1 TB (B7025CA). The quantity of generic licenses installed is increased by all specific array type licenses. License capacity in use is the sum of used data on all arrays. For example, you have installed 1 license for each disk array specific license category, together 4 ZDB licenses, and you are backing up 2 TB on EMC Symmetrix, 2 TB on P9000 XP Array, and 6 TB on P6000 EVA Array. Therefore, you need 10 licenses but you only have 4. The license checker reports 6 (10 needed, 4 installed) additional Zero Downtime Backup for 1 TB licenses needed.

  ```
  #omnicc -check_licenses -detail
  ------------------------------------------------------------
  License Category               : Zero Downtime Backup for 1 TB
  Licenses Capacity Installed    : 4 TB
  Licenses Capacity In Use       : 10.0 TB
  Add. Licenses Capacity Required: 6 TB

  Summary
  -------
  Description                                  Licenses Needed
  Zero Downtime Backup for 1 TB                              6

  Licensing is NOT covered.
  ```

Note that old unlimited ZDB licenses for EMC Symmetrix and P9000 XP Array are reported:

- EMC Split Mirror Extension (B6959AA) as 3 ZDB for 1 TB for EMC Symmetrix / DMX licenses (B6959CA)
- HP XP Split Mirror Extension (B7023AA) as 3 ZDB for 1 TB for HP P9000 XP Disk Array Family licenses (B7023CA)
- Zero Downtime Backup Extension for ONE EMC Symmetrix (B6959BA) as 3 ZDB for 1 for TB EMC Symmetrix / DMX licenses (B6959CA)
- Zero Downtime Backup Extension for ONE HP StorageWorks XP (B7023BA) as 3 ZDB for 1 TB for HP P9000 XP Disk Array Family licenses (B7023CA)

This means that the old licenses for EMC Symmetrix and P9000 XP Array are reported as 3 Zero Downtime Backup for 1 TB licenses as well.

For example, if you have installed on your system 1 ZDB license from each license category, the license checker reports 16 installed Zero Downtime Backup for 1 TB licenses-to-use (1+1+1+1+3+3+3+3).

- The Instant Recovery for 1 TB license-to-use (B7028AA) replaces disk array specific instant recovery licenses from previous Data Protector releases:
  - IR for 1 TB for HP Modular SAN Array 1000 (`Instant Recovery for 1 TB HP Modular SAN Array 1000` (B7037AA))
  - IR for 1 TB for HP P6000 EVA Disk Array Family (`Instant Recovery for 1 TB (generic license)` (B7028AA))
  - IR for 1 TB for HP P9000 XP Disk Array Family (`Instant Recovery for 1 TB HP P9000 XP` (B7026CA))

  All disk array-specific licenses are reported by the license checker as 1 generic license Instant Recovery for 1 TB. The quantity of generic licenses installed is increased by all disk array-specific licenses. License capacity is the sum of used data on all arrays.

```
#omnicc -check_licenses -detail
------------------------------------------------------
License Category               : Instant Recovery for 1 TB
Licenses Capacity Installed    : 3 TB
Licenses Capacity In Use       : 5.0 TB
Add. Licenses Capacity Required: 2 TB

Summary
-------
Description                                 Licenses Needed
Instant Recovery for 1 TB                                 2

Licensing is NOT covered.
```

Note that the license enforcement is stronger than the license checking. During the ZDB backup, the backup may not be possible due to the missing licenses for a specific storage array, although the license checker reports a sufficient number of the ZDB and IR licenses.

Data Protector passwords

Once you have installed Data Protector product, you can start using it for 60 days. After this period, you must install a permanent password on the Cell Manager to enable the software. You may load the software on the Data Protector Cell Manager, but you cannot perform configuration tasks without a permanent password, because the licenses required for particular Data Protector functionality require passwords.

The Data Protector licensing requires one of the following passwords:

- Instant-On password

  An Instant-On password is built in the product when first installed. You are able to use the software for 60 days after you have installed it on any system supported by Data Protector. Within this period you must request your permanent password from the *HP Password Delivery Center (PDC)* and then install it.

- Permanent passwords

  The Data Protector product is shipped with an *Entitlement Certificate* license that entitles you to obtain a permanent password. The permanent password permits you to configure a Data Protector cell with regard to your backup policy, provided that you have bought all required licenses. Before you request a permanent password, you must determine the Cell Manager system and understand your cell configuration requirements.

- Emergency password

  Emergency or fallback passwords are available in case the currently installed passwords do not match the current system configuration due to an emergency. They will allow operation on any system for a duration of 120 days.

  Emergency passwords are issued by the support organization. They must be requested by and are issued only to HP personnel. Refer to your support contact or see the HP Licensing site at: http://www.webware.hp.com.

  The purpose of an emergency password is to enable the backup operation while the original system configuration gets reconstructed or until you move to a new permanent installation. In case of moving the licenses, you need to fill out the License Move Form and send it to the *HP Password Delivery Center (PDC)* or go to the web page http://www.webware.hp.com where passwords can be generated, moved, and so on.

The recommended way of obtaining passwords is by using the HP AutoPass utility, which can be installed during the Cell Manager installation process. For instructions on how to obtain passwords using the HP AutoPass utility after it has been installed during the Cell Manager installation process, see "Obtaining and installing permanent passwords using the HP AutoPass utility" (page 199).

For instructions on how to obtain and install a password by means other than HP AutoPass utility, see "Other ways of obtaining and installing permanent passwords" (page 201).

Obtaining and installing permanent passwords using the HP AutoPass utility

The HP AutoPass utility lets you install passwords for your HP products' purchased licenses directly through the internet from the HP password delivery center web server. For more information on the HP AutoPass utility, see the *AutoPass License Management Online Help*.

Prerequisites

To obtain and install permanent passwords using the HP AutoPass utility, the following conditions must be fulfilled:

- Install the HP AutoPass utility with the Cell Manager. If you did not have this utility installed on your system before the Data Protector installation, you can install it using the `omnisetup.sh` script (UNIX systems) or during the Cell Manager installation (Windows systems).
- Install Java Runtime Environment (JRE) 1.5.0_06 or newer update on the Cell Manager.
- On MC/ServiceGuard, the HP AutoPass utility must be installed an all nodes.
- You need a permanent license entitlement certificate.
- You need the HP order number for the purchased licenses.
- You need the IP address of the Cell Manager or of the Manager-of-Managers.

Limitations

For HP AutoPass, the following limitations apply:

- The HP AutoPass utility is not installed on Windows 2003 x64, Windows Vista x64, Windows Server 2008 x64, Windows Server 2012 x64, and Linux operating systems.
- It is *not* recommended to install HP AutoPass in Microsoft Cluster, because it will be installed only on one node and not on all nodes.
- The `omniinstlic` command operates only if JRE 1.5.0_06 or newer update is installed on the Cell Manager.

For additional prerequisites and limitations, see the *AutoPass License Management Online Help*.

The passwords are installed on the Cell Manager and are valid for the entire cell.

Procedure

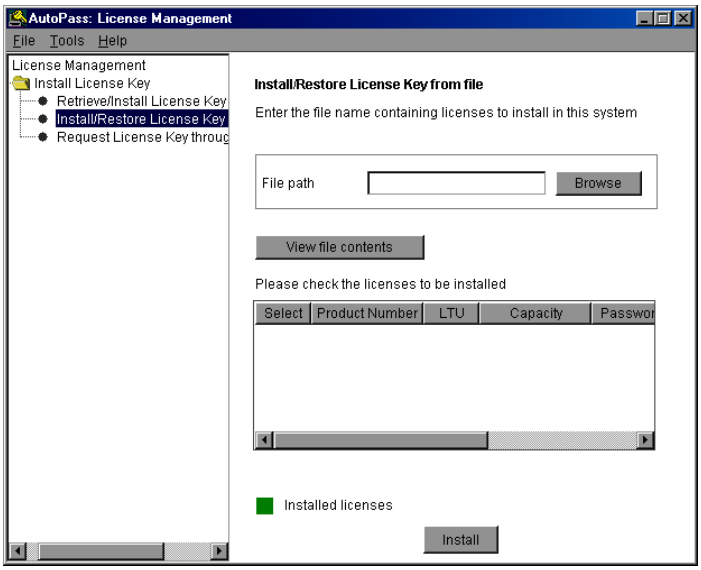
The following is the procedure to obtain and install a permanent password:

1. Gather the information required to obtain a permanent password. To see what information is required, see the *AutoPass License Management Online Help*.
2. Order the password online using the *HP AutoPass utility* by executing the `omniinstlic` command on the Cell Manager.

   NOTE: In a Manager-of-Managers (MoM) environment, the `omniinstlic` command must be run either on the MoM system (if Data Protector centralized licensing *is* used) or on the Cell Manager for which the passwords are being ordered and installed (if Data Protector centralized licensing *is not* used).

   For more information, see the `omniinstlic` man page or *HP Data Protector Command Line Interface Reference*.
3. Follow the *HP AutoPass utility* wizard and enter the required information.

Figure 53 HP AutoPass wizard



In the last step of the wizard, clicking **Get password** will transfer permanent passwords for the purchased licenses from the *HP Password Delivery Center* to the Cell Manager.

Clicking **Finish** will install permanent passwords for the purchased licenses on the Cell Manager.

4. For instructions how to verify the installed passwords, see "Verifying the password" (page 202).

Other ways of obtaining and installing permanent passwords

Obtaining

The following is the procedure to obtain permanent passwords:

1. Gather the information required in the Permanent Password *Request Form*. See "Data Protector licensing forms" (page 206) to find the location of the forms and get instructions on how to fill them out.
2. See "Data Protector 7.00 product structure and licenses" (page 204) for more information about the product structure. The *HP Password Delivery Center* will send your permanent password using the same method that you used when you sent your request. For example, if you sent your request by e-mail then you would receive your permanent password by e-mail.
3. Do one of the following:
   - Go to the online *HP Password Delivery Center* site at http://www.webware.hp.com.
   - Complete the *Permanent Password Request Form* and send it to the *HP Password Delivery Center* using one of the following (see the Entitlement Certificate shipped with the product for fax numbers, telephone numbers, email addresses, and hours of operation):
     - Faxing a form to the *HP Password Delivery Center*
     - Sending an e-mail to the *HP Password Delivery Center*

       You can use the electronic version of the license forms that are included in the following files on the Cell Manager and the installation media:

       On Windows Cell Manager: `Data_Protector_home\Docs\license_forms.txt`

       On UNIX Cell Manager: `/opt/omni/doc/C/license_forms_UNIX`

       On Windows installation DVD-ROM: `Disk_Label:\Docs\license_forms.txt`

       to "copy" and "paste" your message to the *HP Password Delivery Center (HP PDC)*.

       You will receive your permanent password within 24 hours of sending your *Permanent Password Request Form*.

Installing

This section describes the procedure to install a permanent password that the *HP Password Delivery Center (HP PDC)* has sent to you.

Prerequisite

You must have received permanent passwords sent from the *HP Password Delivery Center* and the Data Protector user interface must be installed on the Cell Manager. The passwords are installed on the Cell Manager and are valid for the entire cell.

Using the GUI

To install the permanent password using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Data Protector Cell** and click **Add License**.

3. Type the password exactly as it appears on the *Password Certificate*.

   A password consists of eight 4-character groups, separated by a space and followed by a string. Make sure that you do not have a line-feed or a return character within this sequence. The following is an example of a password:

   ```
   2VFF 9WZ2 C34W 43L7 RYY7 HBYZ S9MQ 1LZA JUUQ TA48 EPNB QFRN MR9F
   2A2A 7UEG 9QR3 Y3QW LZA9 AZA9 EQ97 "Product; Cell Manager for UNIX"
   ```

   After you have typed in the password, check the following:

   - Make sure the password appears correctly on the screen.
   - Make sure there are no leading or trailing spaces, or extra characters.
   - Double-check "1" (number one) characters and "l" (letter l) characters.
   - Double-check "O" (uppercase letter O) characters and "0" (number zero) characters.
   - Make sure that you have used the correct case. The password is case-sensitive.

   Click **OK**.

The password is written to the following file on the Cell Manager:

Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012: *Data_Protector_program_data*\Config\server\Cell\lic.dat

Other Windows systems: *Data_Protector_home*\Config\server\Cell\lic.dat

UNIX systems: /etc/opt/omni/server/cell/lic.dat

Using the CLI

To install the permanent password using the Data Protector CLI, proceed as follows:

1. Log on to the Cell Manager.
2. Execute the following command:

   ```
   omnicc -install_license password
   ```

   The *password* string must be entered exactly as it appears on the *Password Certificate*. It must be formatted as a single line and must not contain any embedded carriage returns. The password must be in quotes. If the password includes also a description in quotes, the quotes in this description must be preceded with backslashes. For an example and more information, see the omnicc man page or the *HP Data Protector Command Line Interface Reference*.

You can also append the password to the following file on the Cell Manager:

Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012: *Data_Protector_program_data*\config\server\cell\lic.dat

Other Windows systems: *Data_Protector_home*\config\server\cell\lic.dat

UNIX systems: /etc/opt/omni/server/cell/lic.dat

If the file does not exist, create it with an editor, such as vi or Notepad. For an example of a password, see Step 3 in the procedure for the graphical user interface.

Verifying the password

Using the GUI

To verify if the password for the license you have installed is correct, proceed as follows in the Data Protector GUI:

1. In the Help menu, click **About**.
2. Click the **License** tab. All installed licenses are displayed. If the password you entered is not correct, it is listed with the remark Password could not be decoded.

Using the CLI

To verify if the password for the license you have installed is correct, use the following command:

```
omnicc -password_info
```

This command displays all installed licenses. If the password you entered is not correct, it is listed with the remark `Password could not be decoded.`

Finding the number of installed licenses

Using the GUI

Once you have installed a permanent password, you can check how many licenses are currently installed on the Cell Manager:

1. Start the Data Protector Manager.
2. In the menu bar, click **Help**, and then **About**. The About Manager window will open, displaying the installed licenses.

Using the CLI

If you use the command line, proceed as follows:

1. Log on to the Cell Manager.
2. Execute the following command:

   ```
   omnicc -query
   ```

A table listing the currently installed licenses will be displayed.

Moving licenses to another Cell Manager System

You must contact the *HP Password Delivery Center* in any of the following cases:

- If you wish to move the Cell Manager to another system.
- If you plan to move a license, installed on a Cell Manager not currently in use in the cell, to another Data Protector cell.

NOTE: It is possible to move a UNIX license to another UNIX Cell Manager or to a Windows Cell Manager, but it is not possible to move a Windows license to a UNIX Cell Manager.

Use the following process to move licenses from one Cell Manager to another:

1. Fill out one *License Move Form* for each new Cell Manager and send it to the *HP Password Delivery Center*. To move licenses for products, which can no longer be purchased, you should use the *License Move Forms* delivered with the previous version of the product. See "Data Protector licensing forms" (page 206).

   On the form, you must specify the number of licenses you want to move from the existing Cell Manager.

2. Delete the following file:

   Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012:

   Data_Protector_program_data\config\server\cell\lic.dat

   Other Windows systems:

   Data_Protector_home\config\server\cell\lic.dat

   UNIX systems:

   /etc/opt/omni/server/cell/lic.dat

3. As soon as you have filled out the *License Move Form* and sent it to the *HP Password Delivery Center (PDC)*, you are legally obliged to delete all Data Protector passwords from the current Cell Manager.

4. Install the new passwords. You will receive one password for each new Cell Manager. You will also receive one new password for the current Cell Manager if licenses are left on the current Cell Manager. This new password replaces the current password entry on the current Cell Manager.

Centralized licensing

Data Protector allows you to configure centralized licensing for a whole multi-cell environment, which simplifies license management. All licenses are kept on the Manager-of-Managers (MoM) Manager system. Licenses are allocated to specific cells although they remain configured on the MoM Manager.

For more information on how to configure licenses, see the *HP Data Protector Help*.

NOTE: It is possible to assign a UNIX license to another UNIX Cell Manager or to a Windows Cell Manager, but it is not possible to assign a Windows license to a UNIX Cell Manager.

The MoM functionality allows you to move (re-assign) licenses among the MoM cells. For more information, see the *HP Data Protector Help* index: "MoM environment".

If you are installing a new Data Protector license, ensure that you check the MoM functionality before you request any licenses. If you decide to use centralized licensing at a later date, you will then have to go through the procedure of moving licenses.

NOTE: The MoM functionality allows centralized licensing. This means you can install all licenses on the MoM Manager and then distribute them to the Cell Managers that belong to the MoM cell. You can later move (re-distribute) licenses among the MoM cells. For more information, see the *HP Data Protector Help* index: "MoM environment".

Data Protector 7.00 product structure and licenses

This section explains how to use the Data Protector product structure, so that product numbers to be ordered can be easily identified.

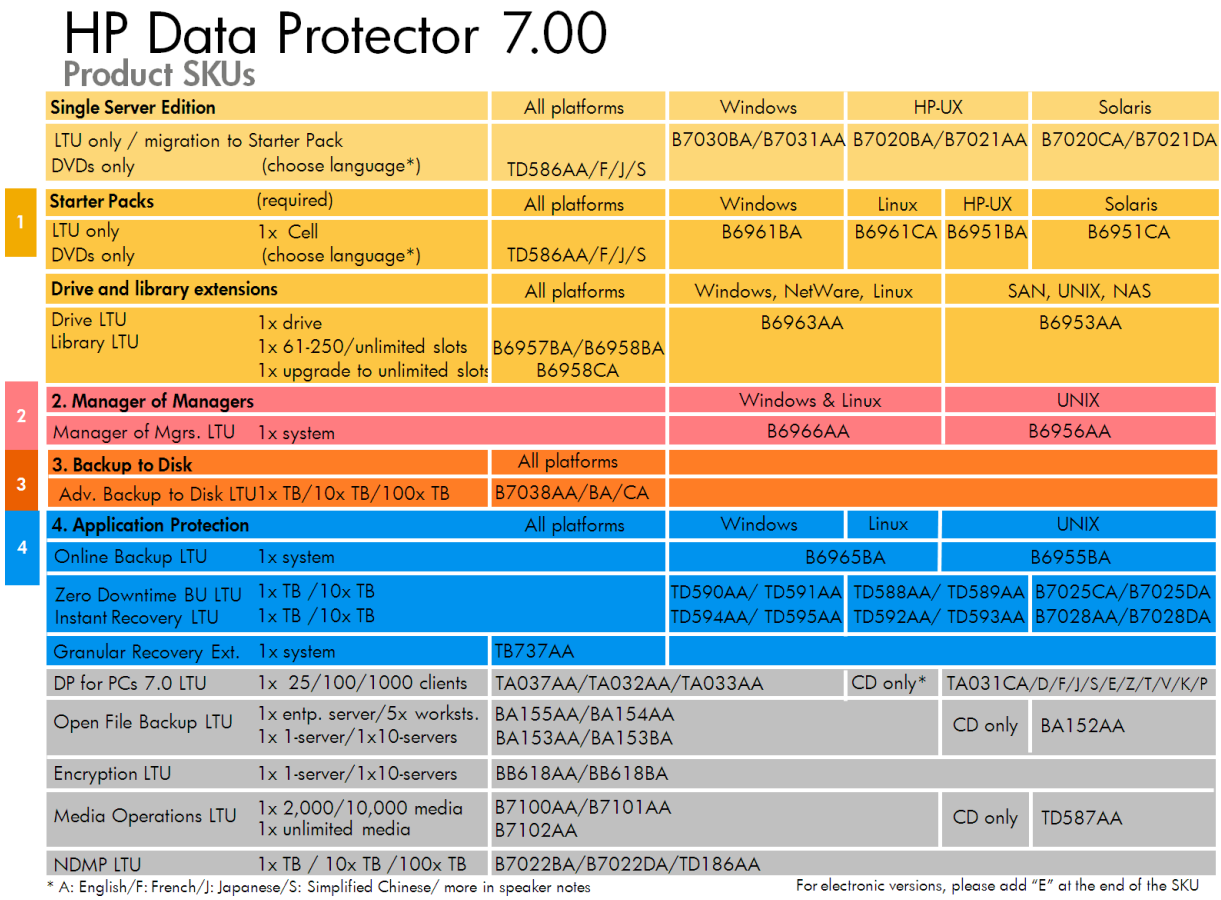
The product structure is divided in different sections, as shown in "HP Data Protector product structure" (page 205). When ordering a Data Protector solution, go through the sections as follows:

1. Select a Starter Pack. The appropriate product number depends on the operating system of your Cell Manager system.
2. Determine the number of configured drives in your environment and the tape libraries involved.
3. Identify what other functionality you need. The recommended functionality can range from on-line backup to instant recovery.

The required minimum is a Starter Pack license and media.

NOTE: The licenses delivered for the UNIX products can be applied to all operating systems.

Figure 54 HP Data Protector product structure



IMPORTANT: *The product structure in this manual is listed for illustration purposes only*. The latest official product structure is available on the Web at http://h18006.www1.hp.com/products/quickspecs/Division/Division.html#12647.

Data Protector leverages the product numbers of previous Data Protector versions. This is why existing Data Protector licenses remain valid after the migration.

Password considerations

Consider the following to help determine the right number of passwords.

- Instant-On passwords can be used on any Cell Manager candidate. For all other types of passwords, however, you must determine the related platform. This includes the system that will become the central Data Protector administration system, the Cell Manager. It is important to use Instant-On passwords to fully understand your cell configuration requirements before requesting a permanent password.
- Permanent licenses can be moved to a different Cell Manager. However, you need to use the License Move Form(s) and send them to the *HP Password Delivery Center (PDC)*.
- Passwords are installed on the Cell Manager and are valid for the entire cell.
- Centralized licensing is provided within the Manager-of-Managers (MoM) functionality. You can have all the licenses installed on the MoM system if you purchase multiple licenses for several cells.
- You need one Cell Manager license for each cell.

NOTE: Data Protector licensing (the IP-based licenses, time-limited or permanent, IP- or subnet-bound, except Instant-on licenses and Emergency Passwords) requires that the Cell Manager must have an IPv4 address. When running in an IPv6 environment, the Cell Manager must be configured in a dual-stack mode, thus having both IPv6 as well as IPv4 enabled. The Cell Manager's IPv4 address is used for licensing purposes.

If the system on which the Cell Manager is installed has more than one IP address (multihomed systems, RAS-servers, clusters), you can bind the license to any of the IPv4 addresses.

- The licenses are regularly checked by the software when you perform a Data Protector configuration task or start a backup session.
- Instant-On passwords can be used on any system, while evaluation and permanent passwords can be used only on the Cell Manager system for which you requested the licenses.

NOTE: To change the IP address of the Cell Manager, to move the Cell Manager to another system, or to move licenses from one cell to another (where MoM functionality is not used), you should contact the *HP Password Delivery Center (PDC)* in order to update the licenses. For information about contacting the HP Password Delivery Center, see "Other ways of obtaining and installing permanent passwords" (page 201).

License migration to Data Protector 7.00

Migrate directly to Data Protector 7.00. Licenses from previous Data Protector releases are automatically migrated.

Data Protector A.06.10, A.06.11, or 6.20 customers on support contract will receive Data Protector 7.00 free of charge. Once you upgrade your environment to Data Protector 7.00, the functionality you were using with A.06.10, A.06.11, or 6.20 will be available with Data Protector 7.00 at no additional cost. You only need to purchase new licenses if you want to acquire new functional extensions.

Data Protector licensing forms

This section discusses Data Protector Licensing forms. Fill them out to order permanent passwords using one of the following methods:

- Use the HP AutoPass utility to obtain and install permanent passwords directly through the internet from the HP password delivery center web server. For more information, see "Obtaining and installing permanent passwords using the HP AutoPass utility" (page 199). This is the recommended method.
- Order permanent passwords using the online *Password Delivery Center* site at http://www.webware.hp.com.
- Print the electronic version of the license forms that are included in the following files on the Cell Manager system and the installation media:

  HP-UX and Linux systems: `/opt/omni/doc/C/license_forms_UNIX`

  Windows installation DVD-ROM: `DriveLetter:Docs\license_forms.txt`

  or use the electronic files to "copy" and "paste" your message to the *Password Delivery Center (PDC)*.

IMPORTANT: Make sure that you type information clearly and that you do not forget the required fields.

The common fields in the licensing forms that you are required to fill out are briefly described beneath:

Personal Data	This field contains customer information, including to whom the new password should be delivered.
Licensing Data	Provide licensing information about your Data Protector cell.
Current Cell Manager	Enter the required information about your current Cell Manager.
New Cell Manager	Enter the required information about your New Cell Manager.
Order Number	Enter the *Order Number* printed on the *Entitlement Certificate.* The *Order Number* is required to verify that you are entitled to request a permanent password.
IP Address	This field defines for which system the *Password Delivery Center* will generate the passwords. In case you want to use centralized licensing (MoM environments only) then this system must be the MoM Manager system. If the Cell Manager has the several LAN cards, you can enter any of the IP addresses. We recommend that you enter the primary one. If you have Data Protector in a MC/ServiceGuard or Microsoft Cluster environment, enter the IP address of your virtual server. For more information on clusters, see the *HP Data Protector Help*.
The *Password Delivery Center* Fax Numbers	For contact information, see the *Entitlement Certificate* shipped with your product.
Product License Type	In the fields next to the *Product Numbers*, enter the quantity of licenses you want to install on this Cell Manager. The quantity can be all or a subset of the licenses purchased with the *Order Number*.

6 Troubleshooting installation

In this chapter

This chapter contains information specific to installation related problems. For general troubleshooting information, see the *HP Data Protector Troubleshooting Guide*.

This chapter includes information on:

Name resolution problems when installing the Windows Cell Manager

During the installation of the Data Protector Cell Manager on Windows, Data Protector detects and warns you if the DNS or the LMHOSTS file is not set up as required. In addition, Data Protector notifies you if the TCP/IP protocol is not installed on your system.

Problem

Name resolution fails when using DNS or LMHOSTS

If the name resolution fails, the "`error expanding hostname`" message is displayed and the installation is aborted.

- If you encounter resolution problems when using DNS, you get a warning message about your current DNS configuration.
- If you encounter resolution problems when using LMHOSTS file, you get a warning message to check your LMHOSTS file configuration.
- If you have not configured either DNS or LMHOSTS, you get a warning message to enable the DNS or the LMHOSTS resolution in the TCP/IP properties dialog.

Action

Check your DNS or LMHOSTS file configuration or activate it. See "Verifying DNS connections within Data Protector cell" (page 209).

Problem

The TCP/IP protocol is not installed and configured on your system

Data Protector uses the TCP/IP protocol for network communications; it must be installed and configured on every client in the cell. Otherwise, the installation is aborted.

Action

Check the TCP/IP setup. For information, see "Changing the default Data Protector Inet port" (page 226).

Verifying DNS connections within Data Protector cell

DNS (Domain Name System) is a name service for TCP/IP hosts. The DNS is configured with a list of host names and IP addresses, enabling users to specify remote systems by host names rather than by IP addresses. DNS ensures proper communication among the members of the Data Protector cell.

If DNS is not configured properly, name resolution problems may occur in the Data Protector cell and the members will not be able communicate with each other.

Data Protector provides the `omnicheck` command to verify the DNS connections among the members of the Data Protector cell. Although all possible connections in the cell can be checked with this command, it is enough to verify the following connections, which are essential in the Data Protector cell:

- Cell Manager to any other member of the cell and the other way round
- Media Agent to any other member of the cell and the other way round

Using the omnicheck command

Limitations

- The command verifies connections among the cell members only; it does not verify DNS connections in general.

The synopsis of the omnicheck command is:

```
omnicheck -dns [-host Client | -full] [-verbose]
```

You can verify the following DNS connections in the Data Protector cell using different options:

- To check that the Cell Manager and every Media Agent in the cell resolve DNS connections to every Data Protector client in the cell properly and the other way round, execute:

  ```
  omnicheck -dns [-verbose]
  ```

- To check that a particular Data Protector client resolves DNS connections to every Data Protector client in the cell properly and the other way round, execute:

  ```
  omnicheck -dns -host client [-verbose]
  ```

  where *client* is the name Data Protector client checked.

- To check all possible DNS connections in the cell, execute:

  ```
  omnicheck -dns -full [-verbose]
  ```

When the `[-verbose]` option is specified, the command returns all the messages. If this option is not set (default), only the messages that are the result of failed checks are returned.

For more information, see the `omnicheck` man page.

"Return messages" (page 209) lists return messages for the `omnicheck` command. If the return message indicates a DNS resolution problem, see the "Troubleshooting Networking and Communication" chapter of the *HP Data Protector Troubleshooting Guide*.

Table 11 Return messages

Return message	Meaning
client_1 cannot connect to *client_2*	Timeout connecting to *client_2*.
client_1 connects to *client_2*, but connected system presents itself as *client_3*	The *%SystemRoot%*\System32\drivers\etc\hosts/etc/hosts (UNIX systems) file on the *client_1* is not correctly configured or the hostname of the *client_2* does not match its DNS name.

Table 11 Return messages *(continued)*

Return message	Meaning
client_1 failed to connect to *client_2*	*client_2* is either unreachable (for example, disconnected) or the *%SystemRoot%*\System32\drivers\etc\hosts (Windows systems) or /etc/hosts (UNIX systems) file on the *client_1* is not correctly configured.
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.	

Troubleshooting installation and upgrade of Data Protector

Problem

One of the following error messages is reported

- 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.

After installation or upgrade to Data Protector 7.00, Windows may report that some applications are not installed or that a reinstall is required.

The reason is an error in the Microsoft Installer upgrade procedure. Microsoft Installer version 1.x data information is not migrated to the Microsoft Installer version 2.x that Data Protector installs on the computer.

Action

On how to solve the problem, see article Q324906 in the Microsoft Knowledge Base.

Problem

Cell Manager installation on a Windows system, which is not part of any Windows domain, fails

The following error message is reported:

Setup is unable to match the password with the given account name.

Actions

Two solutions are available:

- Make the Windows system, on which you are installing the Cell Manager, part of a domain.
- Use the local administrator account for the CRS service.

Problem

The following error message is reported

msvcr90.dll file is not found

The `MSVCR90.dll` library (upper case) cannot be found, because only `msvcr90.dll` (lower case) is available on the network share. Since `MSVCR90.dll` and `msvcr90.dll` are not treated as the same files, `setup.exe` fails to find the appropriate `dll`.

Action

Rename the file from `msvcr90.dll` (lower case) to `MSCVCR90.dll` (upper case) or reconfigure the network share not to be case-sensitive.

Problem

Canceling of installation does not uninstall already installed components

If you cancel the Data Protector installation while some components have been already installed, Data Protector does not uninstall them. The installation finishes with an error.

Action

Manually uninstall already installed components after you cancelled the installation.

Problems with remote installation of Windows clients

Problem

Error starting setup process

When using Data Protector remote installation to update Windows clients, you get the following error:

```
Error starting setup process, err=[1326] Logon failure: unknown user
name or bad password.
```

The problem is that the `Data Protector Inet` service on the remote computer is running under a user account that does not have access to the OmniBack share on the Installation Server computer. This is most probably a local user.

Action

Change the user for the `Data Protector Inet` service to one that can access the Data Protector share.

Troubleshooting installation of UNIX clients

Problem

Remote installation of UNIX clients fails

Remote installation or upgrade of a UNIX client fails with the following error message:

```
Installation/Upgrade session finished with errors.
```

When installing or upgrading UNIX clients remotely, the available disk space on a client system in the folder `/tmp` should be at least the size of the largest package being used for the installation. On Solaris client systems, the same amount of disk space should be available also in the `/var/tmp` folder.

Action

Check if you have enough disk space in the above mentioned directories and restart the installation or upgrade procedure.

For disk space requirements, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Problem

Problems with the installation of an HP-UX client

When adding a new HP-UX client to a Data Protector cell, the following error message is displayed:

```
/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.
```

Action

Stop the `swagent` daemon and restart it by either killing the process and then restarting it by running the `/opt/omni/sbin/swagentd` command, or by running the `/opt/omni/sbin/swagentd -r` command.

Ensure that you have a local host, loopback entry in the hosts file (`/etc/hosts`).

Problem

Problems with the installation of a Mac OS X client

When adding a Mac OS X client to a Data Protector cell, the `com.hp.omni` process is not started.

Action

On Mac OS X, `launchd` is used to start the `com.hp.omni` process.

To start the service, go to:

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

Execute:

```
launchctl load com.hp.omni
```

Problem

Inet process cannot be started after installing the UNIX Cell Manager

When starting the Cell Manager, the following error is displayed:

```
ERROR: Cannot start "omniinet" service, system error: [1053] Unknown
error 1053.
```

Action

Check if the `inetd` or `xinetd` service is running:

HP-UX systems: `ps -ef | grep inetd`

Linux systems: `ps -ef | grep xinetd`

To start the service, execute:

HP-UX systems: `/usr/sbin/inetd`

Linux systems: `rcxinetd start`

Troubleshooting installation of Windows clients

Problem

Remote installation of Windows clients fails

Remote installation of a Data Protector client to a Windows system fails and reports the following error message:

```
[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.
```

Action

1. On the Installation Server system, execute the following command to mark a user account from the local operating system Administrators user group to be used by the Installation Server during remote installation:

   ```
   omniinetpasswd -inst_srv_user User@Domain
   ```

   Note that the user account must already be added to the local Inet configuration. For details, see the `omniinetpasswd` command description in the *HP Data Protector Command Line Interface Reference*.
2. Start remote installation of the Data Protector client once again.

Problem

Remote installation of Windows clients fails (Windows XP)

When a Windows XP system is a member of a workgroup and the Simple File Sharing security policy setting is turned on, users attempting to access this system through the network are forced to use the Guest account. During remote installation of a Data Protector client, Data Protector repeatedly asks for a valid username and password because administrator rights are required for the remote installation.

Action

Turn off Simple File Sharing: in Windows XP, open **Windows Explorer** or **My Computer**, click the **Tools** menu, click **Folder Options**, click the **View** tab, then clear the **Use simple file sharing (Recommended)** check box.

The Simple File Sharing policy is ignored:

- when the computer is a member of a domain
- when the `Network access: Sharing and security model for local accounts` security policy setting is set to `Classic: Local users authenticate as themselves`

Verifying Data Protector client installation

Verifying Data Protector client installation consists of the following:

- Checking the DNS configuration on the Cell Manager and client systems, and ensuring that the results of the `omnicheck -dns` command on the Cell Manager and client system match the specified system.
- Checking the software components installed on the client.
- Comparing the list of files required for a certain software component to be installed with the files installed on the client.
- Verifying the checksum for every read-only file required for a certain software component.

Prerequisite

An Installation Server must be available for the type of client system (UNIX, Windows) that you select.

Limitation

The verification procedure is not applicable for Novell NetWare clients.

To verify a Data Protector installation using the Data Protector GUI:

1. In the Context List, click **Clients**.

2. In the Scoping Pane, expand **Clients**, right-click the Cell Manager system, and then click **Check Installation** to start the wizard.
3. Follow the wizard to verify the installation of the systems in the cell. The Check Installation window opens, displaying the results of the installation.

   For details, see the *HP Data Protector Help*.

If your installation has not succeeded, see "Using log files" (page 216).

On how to verify the installation on UNIX systems using the Data Protector CLI, see the `ob2install` man page.

Troubleshooting upgrade

Problem

IDB and configuration files are not available after upgrade

After upgrading the Cell Manager from a previous release version, the IDB and all configuration files are not available. This occurs if the upgrade procedure was interrupted for any reason.

Action

Restore Data Protector from the backup made before the upgrade, eliminate the reason of the interruption, and start the upgrade again.

Problem

Old Data Protector patches are not removed after upgrade

Old Data Protector patches are listed among installed programs if the `swlist` command is run after the Data Protector upgrade has finished. The patches were removed from your system during the upgrade, but they remained in the sw database.

To check which Data Protector patches are installed, see "Verifying which Data Protector patches are installed" (page 149).

Action

To remove the old patches from the sw database, run the following command:

`swmodify -u` *`patch`*`.\*` *`patch`*

For example, to remove a patch "`PHSS_30143`" from the sw database, run the following command:

```
swmodify -u PHSS_30143.\* PHSS_30143
```

Problem

Maximum size of database files exceeds 2 GB

On HP-UX 11.31 (Itanium) and SUSE Linux Enterprise Server (x86-64) the maximum size of database files (`dirs.dat`, `fnames.dat`, `fn?.ext`, and their extension files) can exceed the default maximum size of 2 GB. Consequently, during an upgrade to Data Protector 7.00 a warning message is displayed with an advice to adjust the maximum size of database files:

```
Please run omnidbutil –modifytblspace to adjust maximum size of database
files.
```

Action

This adjustment should be done after the upgrade, as the procedure for adjusting the maximum size of database files can be both, time and space consuming, depending on the size of the database. Until the adjustment is performed, Data Protector 7.00 will report incorrect tablespace sizes. However, it is still possible to perform backup and restore.

NOTE: Ensure that you have enough free disk space before starting the adjustment. You will need at least as much additional free space as the current size of the database that you intend to export.

Plan enough time for the entire operation. Exporting and importing of the database may take a significant amount of time (up to several days, depending on the complexity and size of your database) and you cannot perform a backup or restore while you are exporting or importing the database.

To resolve the issue, proceed as follows:

1. Perform a successful backup of the entire IDB.
2. Export the IDB to an existing temporary directory:

   ```
   omnidbutil -writedb -mmdb MMDBDirectory -cdb CDBDirectory
   ```

   where *CDBDirectory* and *MMDBDirectory* are temporary directories to which the CDB and MMDB are exported.
3. Initialize the IDB:

   ```
   omnidbinit
   ```
4. Add the required number of extension files for the tablespace file:

   ```
   omnidbutil -extendtblspace TablespaceFileName Pathname -maxsize
   Size_MB
   ```

   For example, if the size of the file `fnames.dat` was 7 GB, than you need to add 3 extension files with a maximum size of 2047 MB by executing the same command 3 times:

   ```
   omnidbutil -extendtblspace fnames.dat
   /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat
   /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat
   /var/opt/omni/server/db40/datafiles/cdb -maxsize 2047
   ```

   This will create 3 extension files, `fnames.dat1`, `fnames.dat2`, and `fnames.dat3`.
5. Adjust the maximum size of the existing database files:

   ```
   omnidbutil -modifytblspace
   ```

   Following the above example, `fnames.dat`, which previously reached a size of 7 GB, is now limited to 2 GB.
6. Import the IDB:

   ```
   omnidbutil -readdb -mmdb MMDBDirectory -cdb CDBDirectory
   ```

   If you did not create enough extension files, `omnidbutil` will exit with the following message:

   ```
   Tablespace TableSpaceName is running out of space.
   ```

   Add the required number of extension files and restart the import operation.
7. After the successful adjustment, remove the temporary files.

Problem

Upgrade of a Media Agent client which uses the StorageTek Library causes connectivity problems

After you upgrade the Data Protector Media Agent component on a system which uses the StorageTek Library, connectivity to the library is lost, and the Data Protector sessions which involve the library may stop responding or terminate abnormally.

Action

Restarting the StorageTek Library supporting service or daemon may solve the problem:

Windows systems: Using the administrative tool Services, restart the `LibAttach` service.

HP-UX and Solaris systems: Run the commands `/opt/omni/acs/ssi.sh stop` and `/opt/omni/acs/ssi.sh start` *`ACSLS_hostname`* where *`ACSLS_hostname`* is the name of the system on which the Automated Cartridge System library software is installed.

AIX systems: Run the commands `/usr/omni/acs/ssi.sh stop` and `/usr/omni/acs/ssi.sh start` *`ACSLS_hostname`* where *`ACSLS_hostname`* is the name of the system on which the Automated Cartridge System library software is installed.

Manual upgrade procedure

Normally, you upgrade Data Protector A.06.10, A.06.11, or 6.20 on UNIX Cell Manager and Installation Server by executing the `omnisetup.sh` command, which performs an automated upgrade procedure. However, you can also perform the upgrade manually. See "Upgrading on HP-UX and Linux systems using native tools" (page 223).

Using log files

If you run into problems installing Data Protector, you can examine any of the following log files to determine your problem:

- setup log files (Windows)
- system log files (UNIX)
- Data Protector log files

Which log files to check in case of installation problems depends on the type of the installation (local or remote) and on the operating system.

Local installation

In case of problems with local installation, check the following log files:

HP-UX Cell Manager:

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log` (for more details)

Linux Cell Manager:

`/var/opt/omni/log/debug.log`

Windows client (the system where setup is running):

- *`Temp`*`\SetupLog.log`
- *`Temp`*`\OB2DBG_`*`did`*`__setup_`*`HostName_DebugNo`*`_setup.txt` (for more details)

  where:

  - *`did`* (debugging ID) is the process ID of the first process that accepts the debugging parameters. This ID is used as an ID for the debugging session. All further processes will use this ID.
  - *`HostName`* is the name of the host where the trace file is created.
  - *`DebugNo`* is a number generated by Data Protector.
- *`Temp`*`\CLUS_DBG_`*`DebugNo`*`.TXT` (in cluster environments)

The location of the *`Temp`* directory is specified by the `TEMP` environment variable. To examine the value of this variable, run the `set` command.

Remote installation

In case of problems with remote installation, check the following log files:

UNIX Installation Server:

`/var/opt/omni/log/IS_install.log`

Windows client (the remote system to which components are to be installed):

- *SystemRoot*`\TEMP\OB2DBG_`*did*`_INSTALL_SERVICE_`*DebugNo*`_debug.txt`
- *SystemRoot*`\TEMP\CLUS_DBG_`*DebugNo*`.TXT`

The location of the *Temp* directory is specified by the `TEMP` environment variable, and *SystemRoot* is a path specified in the `SystemRoot` environment variable.

In case the setup log files are not created, run the remote installation with the debug option. See "Creating installation execution traces" (page 217).

Data Protector log files

The Data Protector log files listed below are located in:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012: *Data_Protector_program_data*`\log`

Other Windows systems: *Data_Protector_home*`\log`

HP-UX, Solaris, and Linux : `/var/opt/omni/log` and `/var/opt/omni/server/log`

Other UNIX systems and Mac OS X systems: `/usr/omni/log`

Novell NetWare systems: `SYS:\USR\OMNI\LOG`

The following log files are important for troubleshooting installation:

`debug.log`	Contains unexpected conditions. While some can be meaningful to you, the information is mainly used by the support organization.
`inet.log`	Contains requests made to the Data Protector `inet` service. It can be useful to check the recent activity of Data Protector on clients.
`IS_install.log`	Contains a trace of remote installation and resides on the Installation Server.
`omnisv.log`	Contains information on when Data Protector services were stopped and started.
`upgrade.log`	This log is created during upgrade and contains upgrade core part (UCP) and upgrade detail part (UDP) messages.
`OB2_Upgrade.log`	This log is created during upgrade and contains traces of the upgrade process.

For more log files, see the *HP Data Protector Troubleshooting Guide*.

Creating installation execution traces

Run the installation with the `debug` option if this is requested by the HP Customer Support Service. For more information on debugging, including the debug options below, and preparing data to be sent to the HP Customer Support Service, see the *HP Data Protector Troubleshooting Guide*.

Windows systems:

For debugging remote installation on a Windows system, run the Data Protector GUI with the debug option:

`Manager -debug 1-200` *DebugPostfix*

Once the session is finished/aborted, collect the debug output from the following locations:

- On the Installation Server system:

  Data_Protector_program_data\tmp\OB2DBG_*did*__BM_ *Hostname_DebugNo_DebugPostfix* (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012)

  Data_Protector_home\tmp\OB2DBG_*did*__BM_ *Hostname_DebugNo_DebugPostfix* (other Windows systems)

- On the remote system:

  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hostname_DebugNo_DebugPostfix*

UNIX systems:

For debugging the installation on a UNIX system, run the Data Protector GUI with the debug option:

```
xomni -debug 1-200 DebugPostfix
```

or

```
xomniadmin -debug 1-200 Debug_postfix
```

Once the session is finished/aborted, collect the debug output from the Installation Server system's `tmp` directory.

A Installing and upgrading Data Protector using UNIX native tools

In this appendix

This appendix describes how to install and upgrade Data Protector on UNIX systems, using the native installation tools — `swinstall` on HP-UX and `rpm` on Linux.

NOTE: The recommended method for installing or upgrading Data Protector is using the `omnisetup.sh` script. See "Installing a UNIX Cell Manager" (page 27) and "Upgrading the UNIX Cell Manager and Installation Server" (page 162).

Installing on HP-UX and Linux systems using native tools

NOTE: The native installation procedures on HP-UX and Linux are only documented if you intend to install an Installation Server with a limited set of remote installation packages. It is recommended to install Data Protector using `omnisetup.sh`.

Installing a Cell Manager on HP-UX systems using swinstall

To install the UNIX Cell Manager on an HP-UX system:

1. Insert and mount the HP-UX installation DVD-ROM and run the `/usr/sbin/swinstall` utility.
2. In the Specify Source window, select **Network Directory/CDROM**, and then enter *`Mountpoint`*`/hpux/DP_DEPOT` in the **Source Depot Path**. Click **OK** to open the SD Install - Software Selection window.
3. In the list of available packages for the installation, the Data Protector product is displayed under the name `B6960MA`.
4. Right-click **DATA-PROTECTOR**, and then click **Mark for Install** to install the whole software.

   In case you do not need all subproducts, double-click **DATA-PROTECTOR** and then right-click an item from the list. Click **Unmark for Install** to exclude the package or **Mark for Install** to select it for installation.

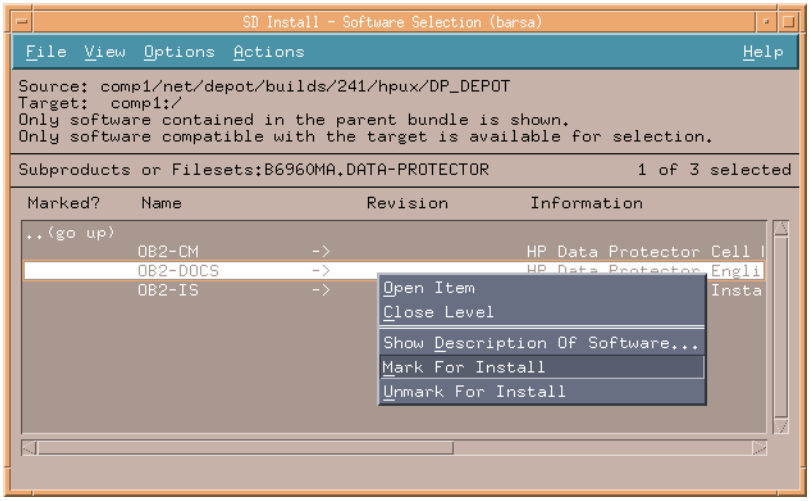
   The following subproducts are included in the product:

OB2-CM	Cell Manager software
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the *HP Data Protector Help* in the WebHelp format.
OB2-IS	The Data Protector Installation Server

   Make sure that the `Marked?` status value next to the `OB2-CM` package is set to `Yes` if you are installing the Cell Manager for UNIX on the system. See "SD install - software selection window" (page 220).

   NOTE: If you are using user IDs longer than 32 bits, you must remotely install the User Interface component (OMNI-CS) on the Cell Manager after you have installed the Core Cell Manager software component.

Figure 55 SD install - software selection window



5. In the Actions list, click **Install (analysis)**, then click **OK** to proceed. If the `Install (analysis)` fails, displaying an error message, click **Logfile** to view the file.

NOTE: To install software from a tape device across the network, you first need to mount the source directory on your computer.

Installing the Cell Manager on Linux systems using rpm

To install the Cell Manager on a Linux system:

1. Insert and mount the Linux installation DVD-ROM.
2. Change to the directory `linux_x86_64/DP_DEPOT`.
3. To install a component, execute:

   `rpm -i package_name-A.07.00-1.x86_64.rpm`

   where *package_name* is the name of the respective sub-product package.

   The following components must be installed:

OB2-CORE	Data Protector Core software.
OB2-CC	Cell Console software. This contains the command-line interface.
OB2-CS	Cell Manager software.
OB2-DA	Disk Agent software. This is required, otherwise it is not possible to back up the IDB.
OB2-MA	The General Media Agent software. This is required to attach a backup device to the Cell Manager.
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the *HP Data Protector Help* in the WebHelp format.
OB2-JAVAGUI	A Java-based graphical user interface. It contains the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface. To install the command-line interface on a client with Java GUI, you need to install the OB2–CC component.

IMPORTANT: The components on Linux are dependent on each other. You should install the components in the order in which they are listed above.

4. Restart the Data Protector services:

   ```
   omnisv stop
   omnisv start
   ```

Installing an Installation Server on HP-UX systems using swinstall

1. Insert and mount the HP-UX installation DVD-ROM and run the `/usr/sbin/swinstall` utility.
2. In the Specify Source window, select **Network Directory/CDROM**, and then enter *`Mountpoint`*`/hpux/DP_DEPOT` in the **Source Depot Path**. Click **OK** to open the SD Install - Software Selection window.
3. In the list of available components for the installation, the Data Protector product is displayed under the name B6960MA. Double-click it to display the DATA-PROTECTOR product for UNIX. Double-click it to display the contents.

   The following sub-product components are included in the product:

OB2-CM	Cell Manager software
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the *HP Data Protector Help* in the WebHelp format.
OB2-IS	The Data Protector Installation Server

4. In the SD Install - Software Selection window, double-click **DATA-PROTECTOR** to list the software for the installation. Right-click **OB2-IS**, and then click **Mark for Install**.
5. From the Actions menu, click **Install (analysis)**. Click **OK** to proceed.

When the installation is finished, the software depot for UNIX is located in the `/opt/omni/databases/vendor` directory.

IMPORTANT: If you do not install the Installation Server for UNIX on your network, you will have to install every UNIX client locally from the HP-UX installation DVD-ROM. Furthermore, patching of components on Data Protector clients will not be possible.

Installing an Installation Server on Linux systems using rpm

Local installation on Linux

To install the Installation Server for UNIX on a Linux system:

1. Insert the Linux installation DVD-ROM.
2. Change to the directory containing the installation archive (in this case *`Mount_point`*`/linux_x86_64/DP_DEPOT`.
3. For each component, execute:

   `rpm -i` *`package_name`*`-A.07.00-1.x86_64.rpm`

   The following components (*`package_name`*) related to Installation Server installation are included in the product:

OB2-CORE	Data Protector Core software. Note that this is already installed, if you are installing the Installation Server on the Cell Manager system.
OB2-CORE-IS	Installation Server Core software.
OB2-CFP	Common Installation Server Core software for all UNIX platforms.
OB2-CCP	Cell Console remote installation packages for all UNIX systems.
OB2-DAP	Disk Agent remote installation packages for all UNIX systems.
OB2-MAP	Media Agent remote installation packages for all UNIX systems.

   Also, if you are setting up an independent Installation Server (that is, not on the Cell Manager) and want to use the user interface:

OB2-CC	Cell Console software. This contains the command-line interface.
OB2-JAVAGUI	Java GUI software. It contains the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface.

4. Once you have installed these components, use `rpm` to install the remote installation package for all the components you will want to install remotely. For instance:

OB2-INTGP	Data Protector Integrations Core software. This component is necessary to install integrations.
OB2-JGUIP	Java GUI remote installation package. It contains the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface. To install the command-line interface on a client with Java GUI, you need to install the OB2-CC package.
OB2-SAPP	SAP Integration component.
OB2-VMWP	VMware Integration (Legacy) component.
OB2-SAPDBP	SAP DB Integration component.
OB2-SAPHANAP	SAP HANA Integration component.
OB2-INFP	Informix Integration component.
OB2-LOTP	Lotus Notes/Domino Integration component.
OB2-SYBP	Sybase Integration component.
OB2-OR8P	Oracle Integration component.
OB2-DB2P	DB2 Integration component.
OB2-EMCP	EMC Symmetrix Integration component.
OB2-SMISAP	HP P6000 EVA SMI-S Agent component.
OB2-SSEAP	HP P9000 XP Agent component.
OB2-NDMPP	The NDMP Media Agent component.
OB2-OVP	HP NNM Integration component.
OB2-FRAP	French Documentation (Guides, Help) component.
OB2-JPNP	Japanese Documentation (Guides, Help) component.
OB2-CHSP	Simplified Chinese Documentation (Guides, Help) component.
OB2-DOCSP	English Documentation (Guides, Help) component.
OB2-PEGP	PEGASUS package.
OB2-VLSAMP	VLS-AM component.

For a complete list of components and dependencies, see "Data Protector software component dependencies on Linux" (page 159).

When the installation is finished, the software depot for UNIX is located in the `/opt/omni/databases/vendor` directory.

IMPORTANT: If you do not install an Installation Server for UNIX on your network, you will have to install every UNIX client locally from the Linux installation DVD-ROM.

IMPORTANT: install Data Protector to linked directories, for instance:

```
/opt/omni/ -> /prefix/opt/omni/
/etc/opt/omni/ -> /prefix/etc/opt/omni/
/var/opt/omni/ -> /prefix/var/opt/omni/
```

you must create the links before the installation and ensure that the destination directories exist.

What's next?

At this point, you should have the Installation Servers for UNIX installed on your network. Now you should perform the following tasks:

1. If you have set up an independent Installation Server (that is, not on the Cell Manager) you must manually add (import) the system to the Data Protector cell. See "Importing an installation server to a cell" (page 133).

   NOTE: When an Installation Server is imported, the file `/etc/opt/omni/server/cell/installation_servers` on the Cell Manager is updated to list the installed remote installation packages. This can be used from the CLI to check the available remote installation packages. For this file to be kept up to date, you should export and re-import an Installation Server whenever remote installation packages are installed or deleted. This applies even if an Installation Server is installed on the same system as the Cell Manager.

2. Install the Installation Server for Windows in case you have any Windows systems in your Data Protector cell. See "Prerequisites" (page 40).
3. Distribute the software to clients. See "Installing Data Protector clients" (page 43).

Installing the clients

The clients are not installed during a Cell Manager or Installation Server installation. The clients must be installed either by using `omnisetup.sh` or by remotely installing the components from the Data Protector GUI. For detailed information on how to install the clients, see "Installing Data Protector clients" (page 43).

Upgrading on HP-UX and Linux systems using native tools

Upgrading Data Protector on HP-UX systems using swinstall

An upgrade of a Cell Manager must be performed from HP-UX installation DVD-ROM.

If you are upgrading a Cell Manager with an Installation Server installed, you must first upgrade the Cell Manager and then the Installation Server.

Client components that are installed on the Cell Manager system are *not* upgraded during a Cell Manager upgrade and must be upgraded either by using `omnisetup.sh` or by remotely installing the components from the Installation Server. For details, see "Local installation on UNIX and Mac OS X systems" (page 81) or "Remote installation" (page 76).

Upgrade procedure

To upgrade Data Protector A.06.10, A.06.11, or 6.20 to Data Protector 7.00, using `swinstall`, proceed as follows:

1. Log in as `root` and shut down the Data Protector services on the Cell Manager by running the `omnisv -stop` command.

   Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no Data Protector services listed after executing the `ps -ef | grep omni` command.

2. To upgrade a Cell Manager or/and an Installation Server, follow the procedures described "Installing a Cell Manager on HP-UX systems using swinstall" (page 219) or/and "Installing an Installation Server on HP-UX systems using swinstall" (page 221).

The installation procedure will automatically detect the previous version and upgrade *only the selected* components. If a component that was installed in the previous version of Data Protector is not selected, it is *not* upgraded. Therefore, you must ensure that you select all components that must be upgraded.

NOTE: The `Match what target has` option is *not* supported if you are upgrading both, the Cell Manager and Installation Server on the same system.

Upgrading Data Protector on Linux systems using rpm

To upgrade the Linux Cell Manager or Installation Server, uninstall the old version and install the new version of the product.

Client components that are installed on the Cell Manager system are *not* upgraded during a Cell Manager upgrade and must be upgraded either by using `omnisetup.sh` or by remotely installing the components from the Installation Server. For details, see "Local installation on UNIX and Mac OS X systems" (page 81) or "Remote installation" (page 76).

Upgrade procedure

To upgrade Data Protector A.06.10, A.06.11, or 6.20 to Data Protector 7.00 using `rpm`, proceed as follows:

1. Log in as `root` and shut down the Data Protector services on the Cell Manager by running the `omnisv -stop` command.

   Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no Data Protector services listed after executing the `ps -ef | grep omni` command.
2. Uninstall Data Protector using `rpm`.

   The configuration files and the database are preserved during this procedure.
3. Run the `rpm –q` command to verify that you uninstalled the old version of Data Protector. Old versions of Data Protector should not be listed.

   Verify that the database and configuration files are still present. The following directories should still exist and contain binaries:

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`
4. If you are upgrading a Cell Manager, insert and mount the Linux installation DVD-ROM and use `rpm` to install the Cell Manager. For detailed steps, see "Installing the Cell Manager on Linux systems using rpm" (page 220).

   If you are upgrading an Installation Server, insert and mount the Linux installation DVD-ROM and install the Installation Server. For detailed steps, see "Installing an Installation Server on Linux systems using rpm" (page 221).

B System preparation and maintenance tasks

In this appendix

This appendix provides some additional information about tasks that are beyond the scope of this guide but strongly influence the installation procedure. These tasks include system preparation and maintenance tasks.

Network configuration on UNIX systems

When you install Data Protector on a UNIX system, Data Protector `Inet` is registered as a network service. Typically this involves the following steps:

- Modification of the `/etc/services` file for registering a port on which Data Protector `Inet` will listen.
- Registration of Data Protector `Inet` in the system's `inetd` daemon or its equivalent (`xinetd`, `launchd`).

When you modify a network configuration, the initial Data Protector `Inet` configuration may become incomplete or even invalid. This happens whenever you add or remove Internet Protocol version 6 (IPv6) network interfaces, due to the system-specific settings for adding IPv6 support to network services. It may happen in other circumstances as well.

In order to update the Data Protector `Inet` configuration, you can use the `dpsvcsetup.sh` utility. This utility, also used by the installation, which gathers the necessary information and accordingly updates the system configuration, is located in the directory `/opt/omni/sbin` (HP-UX, Solaris, and Linux systems) or `/usr/omni/bin` (other UNIX systems).

- To update the Data Protector `Inet` configuration, execute:

  `dpsvcsetup.sh -update`.
- To register the Data Protector `Inet` as a network service, execute:

  `dpsvcsetup.sh -install`.
- To unregister the Data Protector `Inet` as a network service, execute:

  `dpsvcsetup.sh -uninstall`.

Checking the TCP/IP setup

An important aspect of the TCP/IP configuration process is the setup of a hostname resolution mechanism. Each system in the network must be able to resolve the address of the Cell Manager as well as all clients with Media Agents and physical media devices attached. The Cell Manager must be able to resolve the names of all clients in the cell.

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig/ifconfig` commands to verify the TCP/IP configuration.

Note that on some systems the `ping` command cannot be used for IPv6 addresses, the `ping6` command should be used instead.

1. At the command line, execute:

   Windows systems: `ipconfig /all`

   UNIX systems: `ifconfig` *`interface`* or `ifconfig -a` or `nestat -i`, depending on the system

   The precise information on your TCP/IP configuration and the addresses that have been set for your network adapter. Check if the IP address and subnet mask are set correctly.
2. Type `ping` *`your_IP_address`* to confirm the software installation and configuration. By default, you should receive four echo packets.

3. Type `ping default_gateway`.

   The gateway should be on your subnet. If you fail to ping the gateway, check if the gateway IP address is correct and that the gateway is operational.

4. If the previous steps have worked successfully, you are ready to test the name resolution. Enter the name of the system while running the `ping` command to test the hosts file and/or DNS. If your machine name was `computer`, and the domain name was `company.com`, you would enter: `ping computer.company.com`.

   If this does not work, verify that the domain name in the TCP/IP properties window is correct. You should also check the hosts file and the DNS. Be sure that the name resolution for the system, which is intended to be the Cell Manager, and the systems, which are intended to be the clients, is working in both ways:

   - On the Cell Manager you can ping each client.
   - On the clients you can ping the Cell Manager and each client with a Media Agent installed.

NOTE: When using the hosts file for the name resolution, the above test does not guarantee that name resolution works properly. In this case, you may want to use **DNS check tool** once Data Protector is installed.

IMPORTANT: If the name resolution, as specified above, is not working, Data Protector cannot be installed properly.

Also note that the Windows computer name must be the same as the hostname. Otherwise, Data Protector setup reports a warning.

5. After Data Protector has been installed and a Data Protector cell has been created, you can use the DNS check tool to check that the Cell Manager and every client with a Media Agent installed resolve DNS connections to all other clients in the cell properly and vice versa. You do this by executing the `omnicheck -dns` command. Failed checks and the total number of failed checks are listed.

   For detailed information on the `omnicheck` command, see the *HP Data Protector Command Line Interface Reference*.

Changing the default Data Protector ports

Changing the default Data Protector Inet port

The Data Protector `Inet` service (process), which starts other processes needed for backup and restore, should use the same port on each system within the Data Protector cell.

By default, `Inet` uses the port number 5555. To verify that this particular port is not used by another program, inspect the local `/etc/services` file (UNIX systems) or the output of the locally invoked `netstat -a` command (Windows systems). If the port is already in use by another program, you must reconfigure `Inet` to use an unused port. Such reconfiguration must be done on *each* system of the cell so that *all* systems in the cell use the same port.

Once changed on the Cell Manager which also acts as the Installation Server, or on a standalone Installation Server, the new port is automatically used by all clients which are remotely installed using this Installation Server. The `Inet` port can, therefore, be changed most easily when establishing the cell.

CAUTION: Do not change the default `Inet` listen port on systems that are prepared for disaster recovery. In the opposite case, if such systems are struck by a disaster, the disaster recovery process may fail.

UNIX systems

To change the `Inet` port on a UNIX system that will become your Cell Manager, Installation Server, or Data Protector client, follow the steps:

- Create the file `/tmp/omni_tmp/socket.dat` with the desired port number.

To change the `Inet` port on a UNIX system that is already your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. Edit the `/etc/services` file. By default, this file should contain the entry:

   ```
   omni 5555/tcp # DATA-PROTECTOR
   ```

   Replace the number `5555` with the number of an unused port.
2. If the files `/etc/opt/omni/client/customize/socket` and `/opt/omni/newconfig/etc/opt/omni/client/customize/socket` exist on the system, update their content with the desired port number.
3. Restart the `Inet` service by terminating the process concerned using the `kill -HUP` *`inetd_pid`* command. To determine the process ID (*`inetd_pid`*), run the `ps -ef` command.
4. If you are reconfiguring `Inet` on the Cell Manager, in the global options file, set a new value for the `Port` variable.
5. If you are reconfiguring `Inet` on the Cell Manager, restart the Data Protector services:

   ```
   omnisv stop
   omnisv start
   ```

Windows systems

To change the `Inet` port on a Windows system that will become your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. From the command line, run `regedit` to open the Registry editor.
2. Under the key `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Common`, create the registry entry `InetPort`:

   Name of the registry entry: `InetPort`

   Type of the registry entry: `REG_SZ (string)`

   Value of the registry entry: *`PortNumber`*

To change the `Inet` port on a Windows system that is already your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. From the command line, run `regedit` to open the Registry editor.
2. Expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Hewlett-Packard**, **OpenView**, **OmniBack**, and select **Common**.
3. Double-click **InetPort** to open the Edit String dialog box. In the Value data text box, enter the number of an unused port. The same must be done in the Parameters subfolder of the Common folder.
4. In the Windows Control Panel, open **Administrative Tools**, **Services**, then select the **Data Protector Inet** service, and restart the service by clicking the **Restart** icon on the toolbar.

Novell NetWare systems

To change the `Inet` port on a Novell NetWare Data Protector client system, follow the steps:

1. Ensure that no Data Protector sessions are running in the cell.
2. From the Novell NetWare console, run the command `UNLOAD HPINET`.
3. Open the `AUTOEXEC.NCF` file and locate the following line in it:

   ```
   LOAD HPINET.NLM -PORT 5555
   ```

   Replace the entry `5555` with the number of an unused port.
4. Open the `SYS:\ETC\SERVICES` file and add the following line into it:

   ```
   omni PortNumber/tcp
   ```

   `PortNumber` must be the same as the port number used in step 3 of this procedure.
5. From the Novell NetWare console, run the command `WS2_32 RELOAD SERVICES` so that the file `SYS:\ETC\SERVICES` is re-read.

6. Run the command `LOAD HPINET` to reload `HPINET`.

Changing the default Data Protector Java GUI port

To change the default port for Java GUI Server (port number 5556), follow the steps below:

1. Copy the `JGUI_BBC_SERVER_PORT` variable to the `omnirc` file and set its value to an unused port number.

   For example:

   ```
   JGUI_BBC_SERVER_PORT=5557
   ```

2. Restart the Data Protector services:

   ```
   omnisv -stop
   omnisv -start
   ```

A Java GUI Client has to use the same port in order to connect to the `UIProxy` service.

When connecting to the Cell Manager, type *`CellManagerName:PortNumber`* in the **Connect to a Cell Manager** dialog, and click **Connect**.

For example:

`mycellmanager:5557`

Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation

To enable installation of the cluster-aware Data Protector Cell Manager or Data Protector client on a server cluster with Microsoft Cluster Service (MSCS) running on the Windows Server 2008 or Windows Server 2012 operating system, you need to prepare the cluster in advance. Failing to do so may result in failed sessions for backing up the local `CONFIGURATION` object, which must be backed up during preparation for disaster recovery, and potentially even in a data loss.

Prerequisites

- Ensure that you are logged on to the system with a domain user account. The domain user account must be a member of the local `Administrators` group.

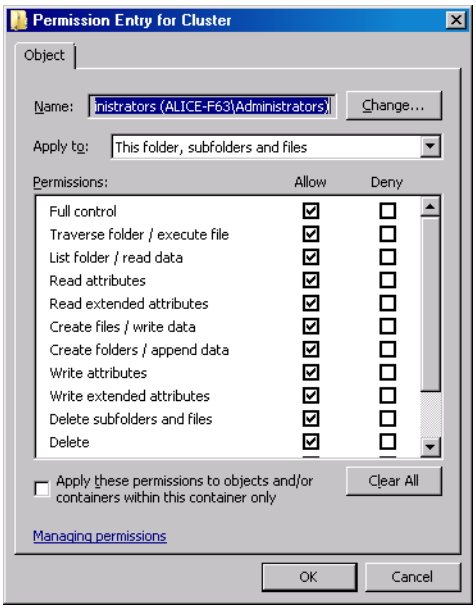
Preparation procedure

To properly prepare your cluster for Data Protector installation, perform the following:

1. On both cluster nodes, start Windows Firewall and enable exceptions for the program `File and Printer Sharing`.
2. On the active cluster node, start Failover Cluster Management, and verify that the witness disk in quorum resource is online. If the resource is offline, bring it online.

   Perform the steps that follow on the active cluster node only.
3. If you are preparing a cluster without a Majority Node Set (MNS) configured, start Windows Explorer and change ownership of the folder *`WitnessDiskLetter`*`:\Cluster` to the local `Administrators` group. While changing the ownership in the Advanced Security Settings for Cluster window, ensure that the option **Replace owner on subcontainers and objects** is selected. In the Windows Security dialog box, confirm the suggested action by clicking **Yes**, and confirm the notification that follows by clicking **Yes**.
4. If you are preparing a cluster without an MNS configured, in Windows Explorer, change permissions of the folder *`WitnessDiskLetter`*`:\Cluster` to allow full control for the `SYSTEM` and local `Administrators` groups. Verify that the permission settings for both groups match the settings shown on "Appropriate permissions for the Cluster folder and local users group Administrators" (page 229).

Figure 56 Appropriate permissions for the Cluster folder and local users group Administrators



5. If you are preparing a cluster which will take the role of the Data Protector Cell Manager, in Failover Cluster Management, add a `Cluster Access Point` resource. Select **Add a resource** and click **1- Client Access Point** to start the New Resource wizard:
   a. On the Client Acces Point pane, enter the network name of the virtual server in the Name text box.
   b. Enter the IP address of the virtual server in the Address text box.
6. If you are preparing a cluster which will take the role of the Data Protector Cell Manager, in Failover Cluster Management, add a shared folder to the cluster. Start the Provision a Shared Folder wizard by clicking **Add a shared folder**:
   a. On the Shared Folder Location pane, enter a directory path in the Location text box. Ensure that the chosen directory has sufficient free space to store data created during the Data Protector installation. Click **Next**.
   b. On the NTFS Permissions, Share Protocols, and SMB Settings panes, leave the default option values unchanged. Click **Next** to move to the next pane.
   c. On the SMB Permissions pane, select the option **Administrators have Full Control; all other users and groups have only Read Access and Write Access**. Click **Next**.
   d. On the DFS Namespace Publishing, leave the default option values. Click **Next**.
   e. On the Review Settings and Create Share pane, click **Create**.

Installing Data Protector on Microsoft Cluster Server with Veritas Volume Manager

To install Data Protector on Microsoft Cluster Server (MSCS) with Veritas Volume Manager, first follow the general procedure for installation of Data Protector on MSCS. See "Installing Data Protector on Microsoft Cluster Server" (page 120).

After you have completed the installation, some additional steps are required to enable the `Data Protector Inet` service to differentiate between local and cluster disk resources which use their own resource driver and not the Microsoft resource driver:

1. Execute the `omnisv -stop` command on the Cell Manager to stop the Data Protector services/processes:
2. Define a new system environment variable `OB2CLUSTERDISKTYPES` with `Volume Manager Disk Group` as a value, or set the `omnirc` option on both cluster nodes as follows:

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

To specify additional proprietary disk resources, such as NetRAID4 disk, simply append the resource type name to the OB2CLUSTERDISKTYPES environment variable value:

```
OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
```

For more information on using the omnirc file options, see the *HP Data Protector Troubleshooting Guide*.

3. Execute the omnisv -start command to start the services/processes:

Preparing a NIS server

This procedure enables your NIS server to recognize your Data Protector Cell Manager.

To add the Data Protector information to your NIS server, follow these steps:

1. Log in as root on the NIS server.
2. If you are managing the /etc/services file via NIS, append the following line to the /etc/services file:

   ```
   omni 5555/tcp # Data Protector for Data Protector inet server
   ```

   Replace 5555 with an alternative if this port it is not available. See "Changing the default Data Protector Inet port" (page 226).

   If you are managing the /etc/inetd.conf file via NIS, append the following line to the /etc/inetd.conf file:

   ```
   #Data Protector
   omni stream tcp nowait root /opt/omni/lbin/inet -log
   /var/opt/omni/log/inet.log
   ```

3. Run the following command so that the NIS server reads the file and updates the configuration.

   ```
   cd /var/yp; make
   ```

NOTE: In the NIS environment, the nsswitch.conf file defines the order in which different configuration files will be used. For example, you can define whether the /etc/inetd.conf file will be used on the local machine or from the NIS server. You can also insert a sentence in the file, stating that the nsswitch.conf file controls where the names are kept. See the man pages for detailed information.

If you have already installed Data Protector, you must prepare the NIS server, and then restart the inet service by killing the process concerned, using the command kill -HUP *pid* on every NIS client that is also a Data Protector client.

Troubleshooting

- If the Data Protector Inet service does not start after you have installed Data Protector in your NIS environment, check the /etc/nsswitch.conf file.

  If you find the following line:

  ```
  services: nis [NOTFOUND=RETURN] files
  ```

  replace the line with:

  ```
  services: nis [NOTFOUND=CONTINUE] files
  ```

Changing the Cell Manager name

When Data Protector is installed it uses the current hostname for the Cell Manager name. If you change the hostname of your Cell Manager, you need to update the Data Protector files manually.

IMPORTANT: It is necessary to update the client information about the Cell Manager name. Before changing the hostname of your Cell Manager, export the clients from the cell. For the procedure, see "Exporting clients from a cell" (page 136). After you have changed the hostname, import the clients back to the cell. For the procedure, see "Importing clients to a cell" (page 132).

NOTE: Any devices and backup specifications that were configured using the old Cell Manager name must be modified to reflect the correct name.

On UNIX systems

On a UNIX Cell Manager, do the following:

1. Change the Cell Manager hostname entries in the following files:

   ```
   /etc/opt/omni/client/cell_server
   /etc/opt/omni/server/cell/cell_info
   /etc/opt/omni/server/users/UserList
   ```

2. Verify that Name Resolution works among the members of a Data Protector cell.
3. Change the Cell Manager name in the IDB by executing:

   ```
   omnidbutil -change_cell_name [old_host]
   ```

On Windows systems

On a Windows Cell Manager, do the following:

1. Change the Cell Manager hostname entries in the following files:

   ```
   Data_Protector_home\config\server\cell\cell_info
   Data_Protector_home\config\server\users\userlist
   ```

2. Change the Cell Manager name in the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBack\Site\CellServer`

C Device and media related tasks

In this appendix

This Appendix provides some additional Data Protector specific information about tasks that are beyond the scope of this guide. These tasks include device driver configuration, managing SCSI robotics, maintaining the SCSI environment and similar.

Using tape and robotics drivers on Windows systems

Data Protector supports the native tape drivers that are loaded by default for an enabled tape drive attached to a Windows system. The Windows native drivers loaded for Medium changers (robotics) devices are not supported by Data Protector.

In the examples below, an HP 4mm DDS tape device is attached to the Windows system. The native driver loaded for medium changer devices needs to be disabled if the HP 4mm DDS tape device is connected to the Windows system and will be configured for use with Data Protector. This section describes the related procedures.

Tape drivers

A driver is usually delivered with Windows, if the device is listed in the Hardware Compatibility List (HCL). HCL is a list of the devices supported by Windows and can be found at the following site:

http://www.microsoft.com/whdc/hcl/default.mspx

The device drivers then load automatically for all enabled devices once the computer has been started. You do not need to load the native tape driver separately, but you can update it. To update or replace the native tape driver on a Windows system, proceed as follows:

1. In the Windows Control Panel, double-click **Administrative Tools**.
2. In the **Administrative Tools** window, double-click the **Computer Management**. Click **Device Manager**.
3. Expand Tape Drives. To check which driver is currently loaded for the device, right-click the tape drive and then click **Properties**.
4. Select the **Driver** tab and click **Update Driver**. Then, follow the wizard, where you can specify if you want to update the currently installed native tape driver or replace it with a different one.
5. Restart the system to apply the changes.

IMPORTANT: If a device has already been configured for Data Protector without using the native tape driver, you have to rename the device files for all configured Data Protector backup devices that reference the particular tape drive (for example, from `scsi1:0:4:0` to `tape3:0:4:0`).

For details, see "Creating device files (SCSI Addresses) on Windows systems" (page 233).

Robotics drivers

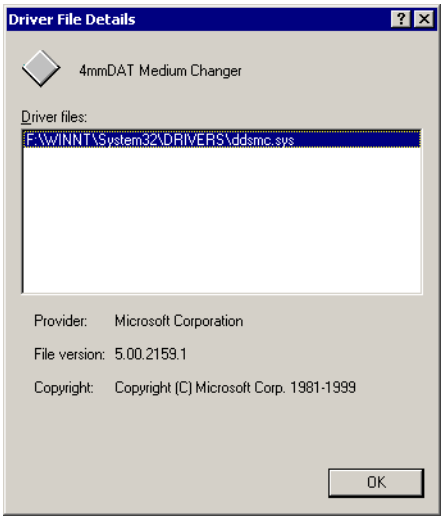
On Windows, the robotics drivers are automatically loaded for enabled tape libraries. In order to use the library robotics with Data Protector, you have to disable the respective driver.

An HP 1557A tape library using the 4mm DDS tapes is used in the example below. Proceed as follows to disable the automatically loaded robotics driver (`ddsmc.sys`) on a Windows system:

1. In the Windows Control Panel, double-click **Administrative Tools.**
2. In the Administrative Tools window, double-click the **Computer Management**. Click **Device Manager**.
3. In the Results Area of the Device Manager window, expand Medium Changers.
4. To check which driver is currently loaded, right-click the **4mm DDS Medium Changer** and then **Properties**.

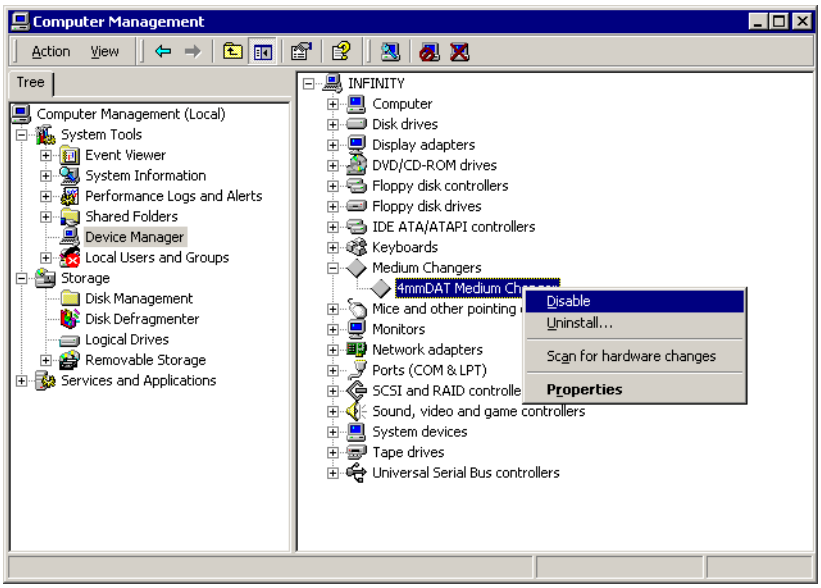
   Select the **Driver** tab and click **Driver details**. In this case, the following window will display:

Figure 57 Medium changer properties



To disable the native robotics driver, right-click the **4mm DDS Medium Changer** and then select **Disable**.

Figure 58 Disabling robotics drivers



5. Restart the system to apply the changes. The robotics can now be configured with Data Protector.

Creating device files (SCSI Addresses) on Windows systems

The tape device filename syntax depends on whether the native tape driver was loaded (`tapeN:B:T:L`) or unloaded (`scsiP:B:T:L`) for a tape drive.

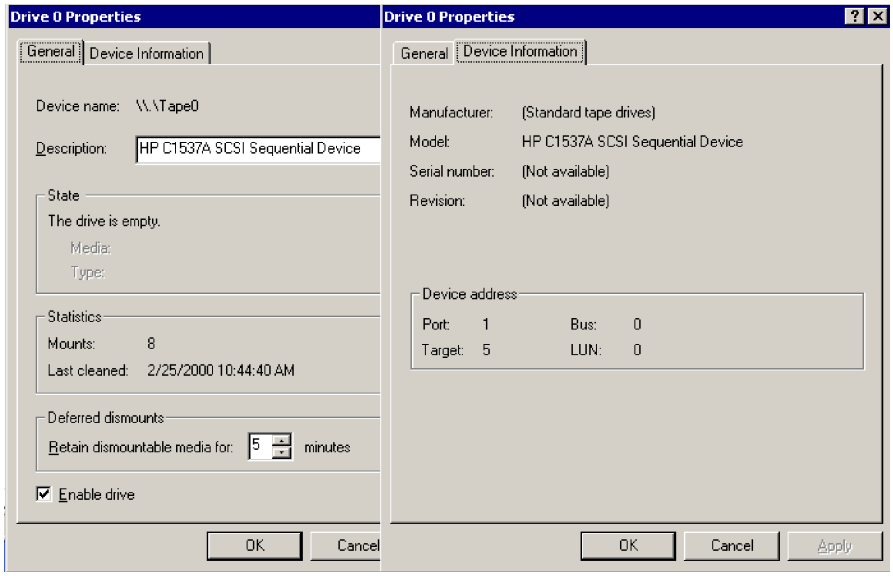
Windows using the native tape driver

To create a device file for a tape drive connected to a Windows system that uses the native tape driver, proceed as follows:

1. In the Windows Control Panel, double-click **Administrative Tools.**
2. In the Administrative Tools window, double-click the **Computer Management**. Expand Removable Storage, then Physical Locations. Right-click the tape drive and select **Properties**.

3. If the native tape driver is loaded, the device file name is displayed in the General property page. Otherwise, you can find the relevant information in the Device Information property page. See "Tape drive properties" (page 234).

Figure 59 Tape drive properties



The file name for the tape drive in "Tape drive properties" (page 234) is created as follows:

Native Tape Driver Used `Tape0 or Tape0:0:5:0`

Native Tape Driver NOT Used `scsii1:0:5:0`

Magneto-optical devices

If you connect a magneto-optical device to a Windows system, a drive letter is assigned to the device after you restart the system. This drive letter is then used when you create the device file. For example, `E:` is the device file created for a magneto-optical drive which has been assigned a drive letter `E`.

SCSI robotics configuration on HP-UX systems

On HP-UX systems, a SCSI Pass-Through Driver is used to manage the SCSI controller *and* control device (also referred to as robotics or picker) of the Tape Library devices (like HP 12000e). The control device in a library is responsible for loading/unloading media to/from the drives and importing/exporting media to/from such a device.

Figure 60 SCSI controlled devices

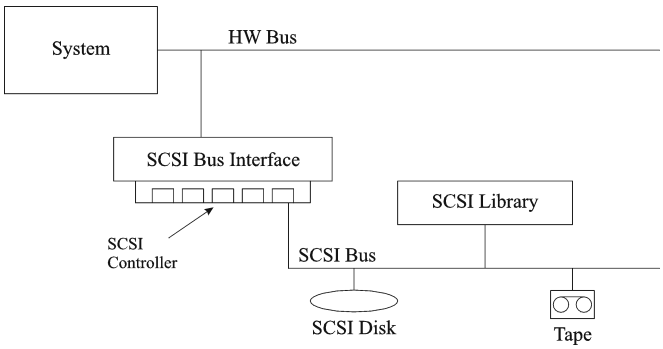
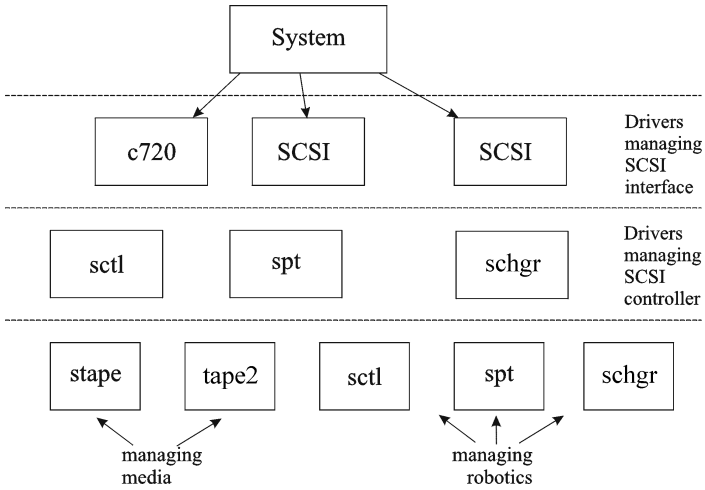


Figure 61 Managing devices



The type of SCSI Robotic Driver in use depends on the hardware. Systems equipped with the `GSC/HSC` or `PCI` bus have the SCSI Autochanger Driver named `schgr`, and systems equipped with the `EISA` bus have the SCSI Pass-Through Driver named `sctl`, which is already built in the kernel. However, the SCSI Pass-Through Driver used on HP Servers with an NIO Bus is named `spt`. It is installed on the system without being built into the kernel by default.

If the SCSI Robotic Driver driver has not already been linked to your current kernel, you have to add it yourself and assign it to the robotics of the connected Tape libraries.

The steps beneath explain how to *manually* add the SCSI Robotic Driver to the kernel and manually rebuild a new one.

TIP: On the HP-UX platform, you can also build the kernel using the *HP System Administration Manager (SAM)* utility. See "Installing HP-UX clients" (page 51).

Use the `/opt/omni/sbin/ioscan -f` command to check whether or not the SCSI Robotic Driver is assigned to the library that you want to configure.

Figure 62 Status of the SCSI pass-through driver (sctl)

```
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
```

In "Status of the SCSI pass-through driver (sctl)" (page 235), you can see the `sctl` SCSI Pass-Through Driver assigned to the control device of the Exabyte tape device. The matching hardware path (H/W Path) is `8/12.2.0`. (SCSI=2, LUN=0)

There is also a tape drive connected to the same SCSI bus, but the driver controlling the tape drive is `stape`. The matching hardware path (H/W Path) is `8/12.1.0`. (SCSI=0, LUN=0)

IMPORTANT: The SCSI address 7 is always used by SCSI controllers, although the corresponding line may not appear in the output of the `ioscan -f` command. In this example, the controller is managed by `sctl`.

Figure 63 Status of the SCSI pass-through driver (spt)

```
# 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
#
```

In "Status of the SCSI pass-through driver (spt)" (page 236), you can see an example of a connected tape device with robotics controlled by the `spt` SCSI Pass-Through Driver. The particular device is an HP 12000e tape library device that uses the SCSI address 4 and is connected to the SCSI bus with the H/W Path 52. The matching hardware path is 52.4.1. The robotics is correctly assigned to the `spt` SCSI Pass-Through Driver.

If the `sctl`, `spt`, or `schgr` driver is not assigned to the robotics, you have to add the H/W Path of the robotics to the driver statement in the `system` file and rebuild the kernel. Follow the procedure below.

The following procedure explains how to *manually* add a SCSI Robotic Driver to the kernel, assign it to the robotics, and then manually rebuild a new kernel:

1. Login as a *root* user and switch to the build directory:

   `cd /stand/build`

2. Create a new system file from your existing kernel:

   `/usr/lbin/sysadm/system_prep -s system`

3. Check which SCSI Robotic Driver is already built in your current kernel. From the `/stand` directory, enter the following command:

   `grep SCSI Robotic Driversystem`

   where the *`SCSI Robotic Driver`* can be either `spt`, `sctl`, or `schgr`. The system will display the corresponding line if the driver is already built in the current kernel.

4. Use an editor to append a driver statement:

   `driver H/W Path spt`

   to the `/stand/build/system` file, where *`H/W Path`* is the complete hardware path of the device.

   For the HP 12000e Tape library from the previous example you would enter:

   `driver 52.4.1 spt`

   For several libraries connected to the same system, you have to add a driver line for each library robotics with the appropriate hardware path.

   When configuring the `schgr` driver, append the following line to a driver statement:

   `schgr`

5. Enter the `mk_kernel -s./system` command to build a new kernel.

6. Save the original old system file using a different name and move the new system file to the original name so that it becomes the current one:

   ```
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
   ```

7. Save the old kernel with a different name and move the new kernel to the original name so that it becomes the current one:

   ```
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
   ```

8. Restart the system from the new kernel by entering the following command:

   ```
   shutdown -r 0
   ```

9. Once you have restarted the system, verify the changes you have made using the **`/usr/sbin/ioscan -f`** command.

Creating device files on HP-UX systems

Prerequisites

Before you create a device file, you should have the backup device already connected to the system. Use the `/usr/sbin/ioscan -f` command to check whether the device is properly connected. Use the `/usr/sbin/infs -e` command to create device files for some backup devices automatically.

If the device files that correspond to a particular backup device have not been created during the system initialization (boot process) or after running the `infs -e` command, you have to create them manually. This is the case with the device files required to manage the library control device (library robotics).

We will use an example of creating a device file for the robotics of the HP 12000e library device connected to an HP-UX system. The device file for the tape drive has already been created automatically after the restart of the system, while the device file for the control device must be created manually.

In "Status of the SCSI pass-through driver (spt)" (page 236), you can see the output of the `ioscan -f` command on the selected HP-UX system.

Figure 64 List of connected devices

```
# 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
#
```

The SCSI bus interface is controlled by the `scsi1` system driver. This is a `SCSI NIO` interface. To access the library robotics on the `SCSI NIO` bus we must use the `spt` SCSI Pass-Through driver that is already installed and assigned to the robotics of the HP 12000e Tape device that uses the hardware path `52.4.1`.

NOTE: If you do not use a `SCSI NIO` based bus interface, the `spt` driver is not required but the `sctl` driver is used instead.

To create the device file, you need to know the *Major number* character of the SCSI Pass-Through driver and the *Minor Number* character, which does not depend on the SCSI Pass-Through driver you use.

To obtain the character *Major number* belonging to `spt`, run the system command:

```
lsdev -d spt
```

In the example (see "List of connected devices" (page 237)) the command reported the *Major number* character `75`.

To obtain the character *Major number* belonging to `sctl`, run the system command:

```
lsdev -d sctl
```

In our case, the command reported the *Major number* character `203`.

The *Minor Number* character, regardless of which SCSI Pass-Through driver is in use, has the following format:

```
0xIITL00
```

`II` -> The *Instance number* of the SCSI bus interface (NOT of the device) reported by the `ioscan -f` output is in the second column, labeled with `I`. In the example, the instance number is `0`, so we must enter two hexadecimal digits, 00.

`T` -> The SCSI address of the library robotics. In the example, the SCSI address is `4`, so we must enter `4`.

`L` -> The LUN number of the library robotics. In the example, the LUN number is `1`, so we must enter `1`.

`00` -> Two hexadecimal zeroes.

Creating the device file

The following command is used to create the device file:

```
mknod /dev/spt/devfile_name c Major # Minor #
```

Usually the device files for `spt` are located in the `/dev/spt` or `/dev/scsi` directory. In this case, we will name the control device file `/dev/spt/SS12000e`.

Thus, the complete command for creating a device file named `SS12000e` in the `/dev/spt` directory is:

```
mknod /dev/spt/SS12000e c 75 0x004100
```

If we create a device file for `sctl`, which is named SS12000e and located in the `/dev/scsi` directory, the complete command is:

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

Setting a SCSI controller's parameters

Data Protector allows you to change the device's block size, which requires an additional configuration on some SCSI controllers: in order to enable writing of block sizes larger than 64K, some SCSI controllers need to have their parameters set differently.

On Windows systems, you set the SCSI controller's parameters by editing the registry value for Adaptec SCSI controllers, and for some controllers with Adaptec's chipsets:

1. Set the following registry value:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ aic78xx\Parameters\Device0\MaximumSGList`
2. Enter a `DWORD` value containing the number of 4 kB blocks, increased by one.

   ```
   MaximumSGList = (OBBlockSize in kB / 4) + 1
   ```

   For example, to enable block sizes up to 260 kB, `MaximumSGList` has to be at least `(260 / 4) + 1 = 66`.
3. Restart the system.

NOTE: This registry value sets the upper limit of the block size. The actual block size for a device must be configured using the Data Protector GUI for device configuration.

Finding the unused SCSI addresses on HP-UX systems

A backup device connected to an HP-UX system is accessed and controlled through a device file that must exist for each physical device. Before you can create the device file, you have to find out which SCSI addresses (ports) are still unused and available for a new device.

On HP-UX systems, the `/usr/sbin/ioscan -f` system command is used to display the list of the SCSI addresses that are already occupied. Thus, the addresses not listed in the output of the `/usr/sbin/ioscan -f` command are still unused.

In "Output of the ioscan -f command on an HP-UX system" (page 239), there is the output of the `/usr/sbin/ioscan -f` command on an HP-UX 11.x system.

Figure 65 Output of the ioscan -f command on an HP-UX system

```
# 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
#
```

Only the third `(H/W Path)` and the fifth `(S/W State)` columns are relevant for the purpose of determining the available SCSI addresses. A dismembered `(H/W Path)` format would look like this:

`SCSI_bus_H/W_Path.SCSI_address.LUN_number`

In this particular case, there is just one SCSI bus, using the H/W Path 52. On this bus, you can use the SCSI addresses `0` and 3 because they do not appear in the list.

You can see in "Output of the ioscan -f command on an HP-UX system" (page 239) which SCSI addresses on the selected SCSI bus are already occupied:

- SCSI address 1 by a SCSI disk
- SCSI address 2 by a CD-ROM
- SCSI address 4, LUN 0, by a tape drive
- SCSI address 4, LUN 1, by the tape library robotics
- SCSI address 5 by a SCSI disk
- SCSI address 6 by a SCSI disk
- SCSI address 7 by a SCSI controller

NOTE: The SCSI address number 7 is *not* listed although it is, by default, occupied by the SCSI controller.

All devices have the `S/W State` value set to `CLAIMED` and the `H/W Type` value set to `H/W DEVICE`, meaning that the devices are currently connected. If there was an `UNCLAIMED` value in the `S/W State` or `NO-HW` in the `H/W Type` column it would mean that the system cannot access the device.

The SCSI address 4 is claimed by the tape library that has the tape drive with LUN 0 and the robotics with LUN 1. The drive is controlled by the `tape2` driver and the robotics is controlled by the `spt` SCSI Pass-Through driver. Looking at the description, you can see that the device is an

HP 12000e library; it is easily recognized among the SCSI libraries because it uses the same SCSI address for the tape drive and robotics but uses different LUNs.

The whole SCSI bus is controlled by the `scsi1` interface module.

Finding the unused SCSI target IDs on Solaris systems

A backup device connected to a Solaris system is accessed and controlled through a device file. This device file is created automatically by the Solaris operating system, in the directory `/dev/rmt`, when the backup device is connected and the client system and backup device are powered up.

Before the backup device is connected, however, the available SCSI addresses must be checked and the address of the backup device set to an address not already allocated.

To list the available SCSI addresses on a Solaris system:

1. Stop the system by pressing **Stop** and **A**.
2. Run the **`probe-scsi-all`** command at the ok prompt:

   `probe-scsi-all`

   You may be asked by the system to start the `reset-all` command before executing the `probe-scsi-all` command.
3. To return to normal operation, enter **`go`** at the `ok` prompt:

   `go`

After listing the available addresses and choosing one to use for your backup device, you must update the relevant configuration files before connecting and starting up the device. See the next section for instructions on updating the configuration files.

Updating the device and driver configuration on Solaris systems

Updating configuration files

The following configuration files are used for device and driver configuration. They must be checked, and if necessary, edited before attached devices can be used:

- `st.conf`
- `sst.conf`

st.conf: all devices

This file is required on each Data Protector Solaris client with a tape device connected. It must contain device information and one or more SCSI addresses for each backup device connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

1. Check the unused SCSI addresses on the client, as described in the previous section, and choose an address for the device you want to attach.
2. Set the chosen SCSI address(es) on the backup device.
3. Power down the client system.
4. Attach the backup device.
5. First power up the device and then the client system.
6. Stop the system by pressing `Stop` and `A`.
7. Enter the **`probe-scsi-all`** command at the `ok` prompt:

   `probe-scsi-all`

   This will provide information on the attached SCSI devices, including the correct device ID string for the newly attached backup device.
8. Return to normal running:

   `go`

9. Edit the `/kernel/drv/st.conf` file. This file is used by the Solaris `st` (SCSI tape) driver. It contains a list of devices officially supported by Solaris and a set of configuration entries for third party devices. If you are using a supported device, it should be possible to connect the device and use it without any further configuration. Otherwise, you should add the following types of entries to `st.conf`:

   - A tape configuration list entry (plus a tape data variable definition). Example entries are supplied in the file, commented out. You can use one of these, if applicable, or modify one to suit your needs.

     The entry must come before the first `name=` entry in the file and the required format is as follows:

     tape-config-list= "*Tape unit*", "*Tape reference name*", "*Tape data*";

     where:

Tape unit	The vendor and product ID string for the tape device. This must be correctly specified as described in the device manufacturer's documentation.
Tape reference name	The name you choose, by which the system will identify the tape device. The name you provide does not change the tape product ID, but when the system boots, the reference name will be displayed in the list of peripheral devices recognized by the system.
Tape data	A variable that references a series of additional tape device configuration items. The variable definition must also be supplied and be correctly specified, as described in the device manufacturer's documentation.

     For example:

     ```
     tape-config-list= "Quantum DLT4000", "Quantum DLT4000", "DLT-data";
     DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
     ```

     The second parameter, `0x38`, designates the DLTtape tape type as "other SCSI drive". The value specified here should be defined in `/usr/include/sys/mtio.h`.

     NOTE: Ensure that the last entry in the tape-config-list is terminated with a semi-colon (;).

   - For multidrive devices, target entries as follows:

     ```
     name="st" class="scsi"
     target=X lun=Y;
     ```

     where:

     X is the SCSI port assigned to the data drive (or robotic mechanism).

     Y is the logical unit value.

     For example:

     ```
     name="st" class="scsi"
     target=1 lun=0;
     name="st" class="scsi"
     target=2 lun=0
     ```

     Normally target entries are required in `st.conf` only for the drives, not for the robotics mechanism, which is on a different target. Entries for these are usually provided in the `sst.conf` file (see below). However, there are some devices, for example the HP 24x6, that treat the robotics mechanism similar to another drive. In this case two entries with the same target are required (one for the drive and one for the robotics), but with different LUNs.

     For example:

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

sst.conf: library devices

This file is required on each Data Protector Solaris client to which a multi-drive library device is connected. Generally speaking, it requires an entry for the SCSI address of the robotic mechanism of each library device connected to the client (there are some exceptions, such as the HP 24x6 mentioned in the previous section).

1. Copy the `sst` driver (module) and configuration file `sst.conf` to the required directory:
   - For 32-bit operating systems:
     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
   - For 64-bit operating systems:
     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
2. Edit the `sst.conf` file and add the following entry:
   `name="sst" class="scsi" target=`*`X`*` lun=`*`Y`*`;`
   where:
   `X` is the SCSI address of the robotic mechanism.
   `Y` is the logical unit.
   For example:
   ```
   name="sst" class="scsi" target=6 lun=0;
   ```
3. Add the driver to the Solaris kernel:
   ```
   add_drv sst
   ```

Creating and checking device files

After setting up the configuration files and installing the drivers, you can create new device files as follows:

1. Remove all existing device files from the `/dev/rmt` directory:
   ```
   cd /dev/rmt rm *
   ```
2. Enter the following to shut down the system:
   ```
   shutdown -i0 -g0
   ```
3. Restart the system:
   ```
   boot -rv
   ```
   The `r` switch in the `boot` command enables a kernel compile and includes the creation of device special files used for communication with the tape device. The `v` switch enables verbose mode display of system startup. With verbose mode, the system should indicate that the device is attached by displaying the *`Tape reference name`* string you selected during the `/devices` directory configuration phase of boot.
4. Enter the following command to verify the installation:
   ```
   mt -t /dev/rmt/0 status
   ```
   The output of this command depends on the configured drive. It will be similar to the following:
   ```
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention residual=
   0 retries= 0 file no= 0 block no= 0
   ```

5. When the system restart has completed, you can check the device files that have been created using the command `ls -all`. For a library device, the output of this command might be:

   /dev/rmt/0hb for a first tape drive

   /dev/rmt/1hb for a second tape drive

   /dev/rsst6 for a robotic drive

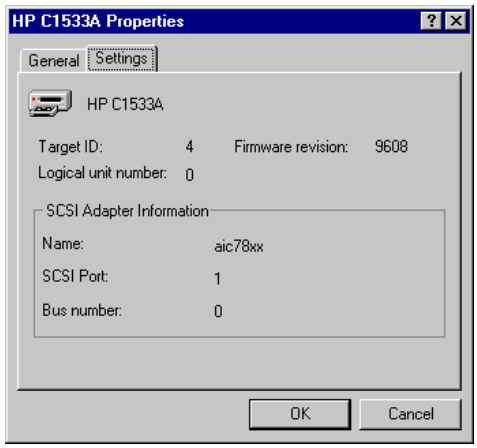
Finding unused SCSI target IDs on Windows systems

Follow the steps below to determine the unused SCSI Target IDs (SCSI Addresses) on a Windows system:

1. In the Windows Control Panel, click **SCSI Adapters**.
2. For each device connected to a SCSI Adapter in the list, check its properties. Double-click the name of a device, and then click **Settings** to open the property page. See "Device settings" (page 243).

   Remember the `SCSI Target IDs` and `LUNs(Logical Unit Numbers)` assigned to the device. This way you can find out which `SCSI Target IDs` and `LUNs` are already occupied.

Figure 66 Device settings



Setting SCSI IDs on an HP 330fx library

Once you have chosen the unused SCSI IDs for the robotics and drives, you can check and configure them using the Control Panel of the library device.

EXAMPLE: If you have a library model HP 330fx, you can find the configured SCSI IDs as follows:

1. From the READY state, press **NEXT**, and then `ADMIN*` will appear.
2. Press **ENTER**, and then you will be asked for the password. Enter the password.
3. `TEST*` will appear, press **NEXT** until `SCSI IDs*` appears.
4. Press **ENTER**. `VIEW IDs*` appears.
5. Press **ENTER**. `JKBX ID 6 LUN 0` appears.
6. Press **NEXT**. `DRV 1 ID 5 LUN 0` appears.
7. Press **NEXT**. `DRV 2 ID 4 LUN 0` appears, and so on.

You can return to the `READY` state by pressing CANCEL several times.

Connecting backup devices

The following procedure describes the general steps to follow in order to connect a backup device to an HP-UX, Solaris, Linux, or Windows system.

1. Select the client to which you will connect the backup device.
2. Install a Media Agent on the selected system. See "Remote installation" (page 76).
3. Determine the unused SCSI address that can be used by the device. For HP-UX systems, see "Finding the unused SCSI addresses on HP-UX systems" (page 239). For Solaris systems, see

"Finding the unused SCSI target IDs on Solaris systems" (page 240). For a Windows system, see "Finding unused SCSI target IDs on Windows systems" (page 243).

- If connecting to an HP-UX system, check that the required drivers are *installed* and *built* into the current kernel. See "Checking the kernel configuration on HP-UX" (page 52).

  If you need to configure a SCSI Pass-Through Driver, see "SCSI robotics configuration on HP-UX systems" (page 234).

- If connecting to a Solaris system, check that the required drivers are installed and the configuration files are updated for the device to be installed. See "Updating the device and driver configuration on Solaris systems" (page 240). This also tells you how to update the `sst.conf` file if you need to configure a SCSI Pass-Through Driver.
- If connecting to a Windows client, the native tape driver can be loaded or disabled, depending on the Windows system version. See "Using tape and robotics drivers on Windows systems" (page 232).

  If you load the native tape driver for a device which has been already configured in Data Protector and did not use the native tape driver, make sure that you rename the device filenames for all configured Data Protector logical devices that reference this specific device (for example, from `scsi1:0:4:0` to `tape3:0:4:0)`.

  For more information on an appropriate device filename, see "Creating device files (SCSI Addresses) on Windows systems" (page 233).

4. Set the SCSI addresses (IDs) on the device. Depending on the device type, this can be usually done using the switches on the device. For details, see the documentation that comes with the device.

   For an example, see "Setting SCSI IDs on an HP 330fx library" (page 243).

   For details about supported devices, see http://support.openview.hp.com/selfsolve/manuals.

   NOTE: On a Windows systems with the Adaptec SCSI adapter installed and a SCSI device connected, the `Host Adapter BIOS` option must be enabled so that the system does not have problems issuing SCSI commands.

   To set the Host Adapter BIOS option, press **`Ctrl+A`** during the boot of the system to enter the SCSI Adapter menu, then select **Configure/View Host Adapter Settings > Advanced Configuration Options** and enable Host Adapter BIOS.

5. First, switch on the device, and then the computer, and then wait until the boot process completes. Verify that the system correctly recognizes your new backup device.

   Windows systems: You can verify that the system correctly recognizes your new backup device if you use the `devbra` utility. In the *`Data_Protector_home`*`\bin` directory, execute:

   ```
   devbra -dev
   ```

   In the output of the `devbra` command you will find the following lines for each connected and properly recognized device:

   ```
   backup device specification
   hardware_path
   media_type
   ..........
   ```

   For example, the following output:

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

   means that an HP DDS tape device (with the native tape driver loaded) has the Drive instance number 3, and is connected to the SCSI bus 0, the SCSI Target ID 4 and LUN number 0.

   Or, the following output:

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

   means that an HP DDS tape device (with the native tape driver unloaded) is connected to the SCSI port 1, SCSI bus 0, and the tape drive has the SCSI Target ID 4, and LUN number 0.

   HP-UX systems: Run the command `/usr/sbin/ioscan -fn` to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

   If the device file has not been created automatically during the system startup process, you should create it manually. See "Creating device files on HP-UX systems" (page 237).

   Solaris systems: Run the `ls -all` command on the `/dev/rmt` directory to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

   Linux systems: Run the `ls -all` command on the `/dev/rmt` directory to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

   AIX systems: Run the command `lsdev -C` to display the list of connected devices with the corresponding device files.

Hardware compression

Most modern backup devices provide built-in hardware compression that can be enabled when you create a device file or SCSI address in the device configuration procedure. For detailed steps, see the *HP Data Protector Help*.

Hardware compression is done by a device that receives the original data from a Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

When software compression is used and hardware compression is disabled, the data is compressed by the Disk Agent and sent compressed to a Media Agent. The compression algorithm can take a substantial amount of resources from the Disk Agent system if software compression is used, but this reduces the network load.

To enable hardware compression on Windows, add "C" to the end of the device/drive SCSI address, for example: scsi:0:3:0C (or tape2:0:1:0C if tape driver is loaded). If the device supports hardware compression, it will be used, otherwise the C option will be ignored.

To disable hardware compression on Windows, add "N" to the end of the device/drive SCSI address, for example: scsi:0:3:0:N.

To enable/disable hardware compression on UNIX, select a proper device file. Consult the device and operating system documentation for details.

What's next?

At this stage, you should have the backup devices connected that enable you to configure backup devices and media pools. For more information about further configuration tasks, see the *HP Data Protector Help* index: "configuring, backup devices".

You must have a Media Agent installed on your system. See "Remote installation" (page 76).

The following sections describe how to connect an HP Standalone 24 Tape Device, HP 12000e Library, and HP DLT Library 28/48-Slot to an HP-UX and a Windows system.

Connecting an HP 24 standalone device

The 24 DDS backup device is a standalone tape drive based on DDS3 technology.

Connecting to an HP-UX system

Follow the steps below to connect the HP 24 Standalone device to an HP-UX system:

1. Check that the required drivers (`stape` or `tape2`) are *installed* and *built* into the current kernel. See "Checking the kernel configuration on HP-UX" (page 52).
2. Determine an unused SCSI address that can be used by the tape drive. See "Finding the unused SCSI addresses on HP-UX systems" (page 239).
3. Set the SCSI addresses (IDs) on the device. Use the switches at the back of the device.

   For details, see the documentation that comes with the device.
4. First, switch on the device, and then the computer, and wait until the boot process completes.
5. Verify that the system correctly recognizes the newly connected tape drive. Use the `ioscan` utility:

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

   to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected tape drive, which has the correct SCSI address. The device file for the drive has been created during the boot process.

What's next?

After properly connecting the device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Windows system

Follow the steps below to connect the HP 24 Standalone device to a Windows system:

1. Determine an unused SCSI address (Target ID) that can be used by the tape drive. See "Finding unused SCSI target IDs on Windows systems" (page 243).
2. Set the SCSI addresses (IDs) on the device. Use the switches at the back of the device. For details, see the documentation that comes with the device.
3. First, switch on the device, and then the computer, and then wait until the boot process completes.

4. Verify that the system correctly recognizes the newly connected tape drive. Run the `devbra` command from the *`Data_Protector_home`*`\bin` directory. Enter

   ```
   devbra -dev
   ```

   In the output of the `devbra command`, you should find the newly connected tape drive of the HP 24 Standalone device.

What's next?

After properly connecting the device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting an HP DAT Autoloader

Both the HP 12000e and the DAT24x6 libraries have a repository for six cartridges, one drive, and one robotic arm used for moving cartridges to and from the drive. The two libraries also have built-in dirty tape detection.

Connecting to an HP-UX system

Follow the steps below to connect the HP 12000e library device to an HP-UX system:

1. On the rear side of the autoloader, set the mode switch to `6`.
2. Check that the required drivers `(stape` or `tape2)` are *installed* and *built* into the current kernel. See "Checking the kernel configuration on HP-UX" (page 52).
3. Check that the required SCSI Pass-Through drivers `(sctl` or `spt`) are *installed* and *built* into the current kernel. See "SCSI robotics configuration on HP-UX systems" (page 234).
4. Determine an unused SCSI address that can be used by the tape drive and the robotics. See "Finding the unused SCSI addresses on HP-UX systems" (page 239).

   NOTE: The HP 12000e Library uses the same SCSI address for the tape drive and for the robotics, but uses different LUN numbers.

5. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.
6. First, switch on the device, and then the computer, and then wait until the boot process completes.
7. Verify that the system correctly recognizes the newly connected tape drive. Use the `ioscan` utility

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

   to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected tape drive, having the correct SCSI address.
8. The device file for the drive has been created during the boot process, while the device file for the robotics must be created manually. See "Creating device files on HP-UX systems" (page 237).
9. Verify that the system correctly recognizes the newly created device file for the library robotics. Run the `ioscan` utility:

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

   You should see your newly created device file in the output of the command.

What's next?

After properly connecting the library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Windows system

Follow the steps below to connect the HP 12000e library device to a Windows system:

1. On the rear side of the autoloader, set the mode switch to `6`.
2. Determine an unused SCSI address that can be used by the tape drive and for the robotics. See "Finding unused SCSI target IDs on Windows systems" (page 243).
3. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.

   NOTE: The HP 12000e Library uses the same SCSI address for the tape drive and for the robotics, but uses different LUN numbers.

4. First, switch on the device, and then the computer, and wait until the boot process completes.
5. Verify that the system correctly recognizes the newly connected tape drive and the robotics. In the *Data_Protector_home*`\bin` directory, execute:

   ```
   devbra -dev
   ```

   In the output of the `devbra` command, you should find the newly connected tape drive and the robotics of the HP 12000e Library device.

What's next?

After properly connecting the library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting an HP DLT Library 28/48-Slot

The HP DLT Library 28/48-Slot is a multi-drive library for enterprise environments with 80-600 GB to back up. It has four DLT 4000 or DLT 7000 drives with multiple data channels, a mail slot, and a barcode reader.

Connecting to an HP-UX system

Follow the steps below to connect the HP DLT Library 28/48-Slot library device to an HP-UX system:

1. Check that the required drivers `(stape` or `tape2)` drivers are *installed* and *built* into the current kernel. See "Checking the kernel configuration on HP-UX" (page 52).
2. Check that the required SCSI Pass-Through drivers `(sctl` or `spt)` are *installed* and *built* into the current kernel. See "SCSI robotics configuration on HP-UX systems" (page 234).
3. Determine an unused SCSI address that can be used by the tape drive and the robotics. See "Finding the unused SCSI addresses on HP-UX systems" (page 239).

   NOTE: The HP DLT Library 28/48-Slot has four tape drives and the robotics, so you need five unused SCSI addresses in case you will be using all tape drives. The tape drives and the robotics must use different SCSI addresses.

4. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.
5. Switch on the device, and then the computer, and wait until the boot process completes.
6. Verify that the system correctly recognizes the newly connected tape drives. Use the `ioscan` utility

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

   to display a list of connected devices with the corresponding hardware paths and device files, where you must find your newly connected tape drives, having the correct SCSI addresses.
7. The device files for the drives have been created during the boot process, while the device file for the robotics must be created manually. See "Creating device files on HP-UX systems" (page 237).
8. Verify that the system correctly recognizes the newly created device file for the library robotics. Use the `ioscan` utility:

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

   You should see your newly created device file in the output of the command.

What's next?

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Solaris system

To configure the HP C5173-7000 library device on a Solaris system, follow the steps below. For this example, it is assumed that two drives are to be allocated to Data Protector:

1. Copy the `sst` driver (module) and configuration file `sst.conf` to the required directory:
   - For 32-bit operating systems:

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

   - For 64-bit operating systems:

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

2. Add the driver to the Solaris kernel:

   ```
   add_drv sst
   ```

3. Remove all existing device files from the `/dev/rmt` directory:

   ```
   cd /dev/rmt rm *
   ```

4. Stop the system by pressing **Stop** and **A**.
5. Run the `probe-scsi-all` command at the "`ok`" prompt to check which SCSI addresses are available for use.

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

   The system may ask you to start the `reset-all` command before executing the `probe-scsi-all` command.

   In our case, we will use port 6 for the SCSI control device, port 2 for the first drive, and port 1 for the second drive; lun is 0)
6. Return to normal running:

   ```
   ok go
   ```

7. Copy the `st.conf` configuration file into the required directory:

   ```
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   ```

   The `st.conf` file is present on each Solaris Data Protector client and contains SCSI addresses for each backup device connected to the client.
8. Edit the `/kernel/drv/st.conf` file and add the following lines:

   ```
   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;
   ```

   These entries provide the SCSI addresses for drive 1, drive 2, and the robotic drive, respectively.
9. Edit the `sst.conf` file (that you copied across in Step 1 and add the following line:

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

NOTE: This entry must match that for the robotic drive in the `st.conf` file. See Step 8 above.

10. Power down the client system and attach the library device.
11. Power up the library device first and then the client system.

    The system will now boot and automatically create device files for the robotic drive and tape drives. These can be listed using the command `ls -all`. In our case:

    /dev/rmt/0hb for a first tape drive

    /dev/rmt/1hb for a second tape drive

    /dev/rsst6 for a robotic drive

What's next?

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Windows system

Follow the steps below to connect the HP DLT 28/48-Slot library device to a Windows system:

1. Determine the unused SCSI addresses (Target IDs) that can be used by the tape drive and by the robotics. See "Finding unused SCSI target IDs on Windows systems" (page 243).
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.

   NOTE: The HP DLT Library 28/48-Slot has four tape drives and the robotics, so you need five unused SCSI addresses in case you will be using all tape drives. The tape drives and the robotics must use different SCSI Target IDs.

3. First, switch on the device, then the computer, and then wait until the boot process completes.
4. Verify that the system correctly recognizes the newly connected tape drives and the robotics. In the *`Data_Protector_home`*`\bin` directory, execute:

   ```
   devbra -dev
   ```

   In the output of the `devbra` command, you should find the newly connected tape drives and the robotics of the HP DLT Library 28/48-Slot library device.

What's next?

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected library device.

Connecting a Seagate Viper 200 LTO Ultrium Tape Drive

The Seagate Viper 200 LTO Ultrium Tape Drive is a standalone device for enterprise environments with 100-200 GB to back up.

Connecting to a Solaris system

To configure the Seagate Viper 200 LTO Ultrium Tape Drive on a Solaris system, follow the steps below:

1. Determine the unused SCSI addresses that can be used by the tape drive. Run the `modinfo` or `dmesg` command to find the SCSI controllers in use and the SCSI target devices installed:

   ```
   dmesg | egrep "target" | sort | uniq
   ```

   The following output should be received:

   ```
   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
   ```

   NOTE: It is recommended that you use either a `glm` or `isp` SCSI controller when connecting the Viper 200 LTO device to a Solaris system. It is also recommended that you use either Ultra2 SCSI or Ultra3 SCSI controllers.

2. Edit the `/kernel/drv/st.conf` file and add the following lines:

   ```
   tape-config-list=
   "SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , \
   "SEAGATE_LTO";
   SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
   0x00, 1;
   ```

3. Power down the client system and attach the device.
4. Power up the device first and then the client system.

   The system will now boot and automatically create device files for the tape drive. These can be listed using the command `ls -all`.

What's next?

After properly connecting the Seagate Viper 200 LTO Ultrium Tape Drive, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Windows system

Follow the steps below to connect the Seagate Viper 200 LTO Ultrium Tape Drive to a Windows system:

1. Determine the unused SCSI addresses (Target IDs) that can be used by the tape drive. See "Finding unused SCSI target IDs on Windows systems" (page 243).
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.
1. First, switch on the device, then the computer, and then wait until the boot process completes.
2. Verify that the system correctly recognizes the newly connected tape drives and the robotics. In the *`Data_Protector_home`*`\bin` directory, execute:

   ```
   devbra -dev
   ```

   In the output of the `devbra` command, you should find the newly connected tape drive of the Seagate Viper 200 LTO Ultrium Tape Drive.

What's next?

After properly connecting the Seagate Viper 200 LTO Ultrium Tape Drive, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

NOTE: When configuring the Seagate Viper 200 LTO Ultrium Tape Drive with Data Protector, make sure that the compression mode is set. This is done by specifying the `C` parameter after the SCSI address of the drive, for example:

```
scsi2:0:0:0C
```

Checking the General Media Agent Installation on Novell NetWare systems

After you have installed the General Media Agent on the Novell NetWare platform, you should verify the installation by performing the following tasks:

- Identify the storage device.
- Test the General Media Agent startup at the Novell NetWare server's console.
- Test `HPUMA.NLM` and `HPDEVBRA.NLM` startup at the Novell NetWare server's console.

Identifying the storage device

Use the following convention to identify a storage device in the Novell NetWare environment:

`adapter identification number``:`*`target identification number`*`:`*`logical unit numbercompression`*

For example, string "`0:2:0N`" identifies a storage device as adapter ID 0, target ID 2, a logical unit number (LUN) 0, and no compression.

Another example is string "`1:1:0C`" that identifies a storage device as adapter ID 1, target ID 1, a Logical Unit Number (LUN) 0, with compression.

Testing the general Media Agent startup

Once you have the General Media Agent installed on the Novell NetWare system, you can test a startup of a backup Media Agent `HPBMA.NLM` at the Novell NetWare server's console.

The example below uses the `Adaptec` host bus adapter, `AHA-2940`, to access the exchanger tape device of the HP Tape 12000e library device.

The following conditions should be fulfilled before you start any of the Data Protector `*.NLM` components:

- `HPINET` must be up and running.
- The `Adaptec` SCSI host adapter driver must be up and running.
- The General Media Agent software must be located in the `SYS:USR\OMNI\BIN` directory.
- The storage device must be correctly installed and connected.
- The Adaptec host bus adapter and the TCP/IP communication protocol must be properly installed, and up and running.

Once the required conditions have been verified, proceed as follows:

1. Enter the following to load `HPBMA.NLM`:

   `LOAD HPBMA -name testbma -type` *`type_number`* `-policy` *`policy_number`* `-ioctl` *`control_device`* `-dev` *`data_device`* `-tty` *`tty_number`*

   The `type` *`type_number`* option is the Data Protector device type. Possible values for *`type_number`* are:

   - 1=DAT/DDS
   - 2 = Quarter Inch Cartridge(QIC)
   - 3 = 8mm - Exabyte
   - 9 = Generic Magnetic tape device
   - 10 = Digital Linear Tape (DLT)

   The `policy` *`policy_number`* option is the Data Protector way to use the device. Possible values are:

   - 1= standalone device
   - 10= SCSI - II library

   The `ioctl` *`control_device`* option defines the SCSI address of the robotics control. It has the following form:

   `adapter_identification_number``:`*`target_identification_number`*`:`

   `logical_unit_number`

   For example:

   - `0:1:1` =>The control device (robotics) uses the SCSI adapter 0, has the SCSI address 1, and has the LUN 1.

   The `dev` *`data_device`* option defines the SCSI address of the robotics control. It has the following form:

   `adapter_identification_number``:`*`target_identification_number`*`:`*`logical_unit_number`*

   `compression`

   For example:

   - `0:1:1C` =>The control device (robotics) is uses SCSI adapter 0, has the SCSI address 1, and has the LUN 1. The data compression has been set.

   The `-tty` *`tty_number`* is the TCP/IP communication protocol port number.

   The Console Media Agent, `HPCONMA.NLM`, starts and you will be prompted by the following screen:

   ```
   *** MA listening on port: number
   SLOT: [Load(2), Peek(2), Stop(0), Abort(0)]
   SLOT: _
   ```

   The currently available commands are:

   `Load(2)` - The command is used for loading the tape into the drive and requires two arguments:

   `Load` *`Slot numberflipping flag`*

   The flipping flag can be set either to 0 or to 1, meaning that the medium does not flip if the value is 0 or it flips if the value is 1.

   `Stop(0)` - Completes the current session normally.

   `Abort(0)` - Aborts the current session.

   In this example, you will load the tape from `SLOT 3` with no flipping of the medium.

2. Enter the command to load the tape from `SLOT 3` with no flipping of the medium.

   ```
   SLOT:LOAD 3 0
   ```

Once the tape is loaded in the drive, the following message will be displayed:

```
CHECK: [Deny(0), Init(1), Seek(2), Abort(0)]
CHECK: _
```

The available commands are:

`Deny(0)` - Denies the current action.

`Init(1)` - Initializes the loaded tape and requires one parameter:

`Init(1) medium_id`

`Seek(2)` - Seeks to the requested position. The argument string is:

`Seek segment_numberblock number`

`Abort(0)` - Aborts the current session.

3. To initialize the tape, enter

   `CHECK: Init test`

4. Switch from Backup Media Agent screen to the Novell NetWare console and start the backup session using the General Media Agent action/request command.

   NOTE: The Data Protector Disk Agent should be started at the selected host using `load -ma host port` to enable proper General Media Agent and Disk Agent communication and to display the correct backup session operations port number as the `HPCONMA.NLM` starts. A message will appear after the successful backup session.

5. To successfully terminate the Backup Media Agent, press **CTRL-C** at the Backup Media Agent screen. The `Console Attention Request` prompt appears after a short time-out:

   `ATT:[Stop(0), Abort(0), Disconnect(1)]` Run `Stop` to successfully complete the session.

Testing the HPUMA.NLM and the HPDEVBRA.NLM startup

Loading `HPUMA.NLM` at the server's console allows you to test the SCSI commands manually.

Load `HPUMA.NLM` with the following command:

`LOAD HPUMA.NLM -ioctl control_device -dev data_device -tty`

The `ioctl control_device` option defines the SCSI address of the robotics control. It has the following form:

adapter_identification_number:*target_identification_number*:*logical_unit_number*

For example:

- `0:1:1` =>The control device (robotics) uses the SCSI adapter 0, has the SCSI address 1, and uses the LUN 1.

The `dev data_device` option defines the SCSI address of the robotics control. It has the form:

adapter_identification_number:*target_identification_number*:*logical_unit_number*:*compression*

For example:

- `0:1:1C` =>The control device (robotics) uses SCSI adapter 0, has the SCSI address 1, and uses the LUN 1. The data compression has been set.

The `-tty` option is necessary to interact with the Novell NetWare server's console.

The HPUMA starts and you are prompted with the following screen:

`prompt`

where prompt has the following form:
`adapter_identification_number:target_identification_number:logical_unit_number` For example,

`0:2:1`

To see the available commands, type `HELP` in the HPUMA screen. For example, to see which slots and drive(s) are full or empty, type `STAT` at the prompt.

When you have finished, type `BYE` to close the HPUMA screen.

Loading `HPDEVBRA.NLM` locally enables you to get information on the devices both installed and detected on the Novell NetWare server.

To load `HPDEVBRA.NLM` at the server console, enter the following command:

```
LOAD HPDEVBRA.NLM -dev
```

where the `-dev` option is necessary to list all devices attached onto the Novell NetWare server.

To see the currently available commands, load `HPDEVBRA.NLM` with `HELP` option:

```
LOAD HPDEVBRA -HELP
```

D Command line changes after upgrading to Data Protector 7.00

The commands listed in this chapter have been changed or provide extended functionality in terms of new options in Data Protector 7.00. Commands and options marked with an asterisk (*) are only introduced, changed, or made obsolete in the most recent set of patches for this Data Protector release version. Check and modify the scripts that use the old commands. For usage synopses, see the *HP Data Protector Command Line Interface Reference* or the corresponding man pages.

Depending on the version from which you upgraded your Cell Manager, see the corresponding table:

- After upgrading from Data Protector A.06.10, see "Upgrade from Data Protector A.06.10" (page 256).
- After upgrading from Data Protector A.06.11, see "Upgrade from Data Protector A.06.11" (page 261).
- After upgrading from Data Protector 6.20, see "Upgrade from Data Protector 6.20" (page 264).

Table 12 Upgrade from Data Protector A.06.10

Command	Affected options or arguments, notes	Status

`ob2install`	`veagent`
	`vmware`
	`chs_ls`
		NEW SOFTWARE COMPONENTS

	`saphana`	NEW SOFTWARE COMPONENT *(available with patch bundle set 7.03 and superseding updates)*
	`snapa`	OBSOLETE SOFTWARE COMPONENT
`omnib`	`-resume` `-ndmp_bkptype`	NEW OPTIONS
	`-storedrim *`	NEW OPTION *
	`-[no_]vss`	NEW/CHANGED OPTION

	`-veagent_list`
	`-e2010_list`
	`-mssharepoint_list`
		NEW INTEGRATIONS

	`-clp`	NEW OPTION COMBINATION
	`-copy`	UPDATED OPTION *(available with patch bundle set 7.01 and superseding updates)* This option can be specified also for backup using the Microsoft SQL Server integration.

Table 12 Upgrade from Data Protector A.06.10 *(continued)*

Command	Affected options or arguments, notes	Status
omnib2dinfo*	This command is available on systems with the User Interface component installed.	REDESIGNED COMMAND* This command was relocated from the Media Agent component.
omnicc	-encryption -enable -cert -key -trust -all -add_exception -remove_exception -list_exceptions -status -add_certificate -get_certificate -list_certificates -impersonation -create_userrestrictions_tmpl	NEW OPTIONS
	-import_vcd	NEW OPTION *(available with patch bundle set 7.01 and superseding updates)*
omnicreatedl	-va -lun_security	OBSOLETE OPTIONS
omnidb	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
	–detail	CHANGED OPTION
	–encryptioninfo –type verification	NEW OPTIONS
omnidbp4000	This command is available on Windows systems with the Data Protector User Interface component installed.	NEW COMMAND
omnidbsmis	-ompasswd -delete	NEW OPTION COMBINATION
	-reference -sync_check -exclude -include	NEW OPTIONS

Table 12 Upgrade from Data Protector A.06.10 *(continued)*

Command	Affected options or arguments, notes	Status
	-namespace -sync	OBSOLETE OPTIONS
omnidbva		OBSOLETE COMMAND
omnidbvss	-get session_persistent -all -details -save_metadata -disable session -enable session -mnttarget -readwrite -no_session_id -backhost -resolve	NEW OPTIONS
	-get disk -list disk -purge -export_metadata	OBSOLETE OPTIONS
omnidbxp	-user -add -username -password -user -check -host -user -update -username -password -user -list -user -remove	NEW OPTIONS AND OPTION COMBINATIONS
omnidbzdb	This command is available on systems with the Data Protector User Interface component installed.	NEW COMMAND *(available with patch bundle set 7.01 and superseding updates)*
omnihealthcheck	On Windows platform, the command was moved from the User Interface component to the Cell Manager component.	RELOCATED COMMAND
omniintconfig.pl	This command is available on systems with the Data Protector User Interface component installed.	NEW COMMAND
omniiso	-net -out -use_raw_object	NEW OPTIONS
	-iso	OBSOLETE OPTION Replaced by -out. Can be used for backward compatibility.
omniminit	-ams	NEW OPTION
	-init -pool -slot	CHANGED OPTIONS

Table 12 Upgrade from Data Protector A.06.10 *(continued)*

Command	Affected options or arguments, notes	Status
omnimm	-copy_to_mcf -import_from_mcf -output_directory -pool_prefix -no_pool_prefix -orig_pool -no_orig_pool -encryptioninfo -ams -show_locked_devs	NEW OPTIONS
omniobjcopy	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
	-restart -sourceprotect -targetprotect -no_auto_device _selection	NEW OPTIONS
	-protect -recycle -no_recycle	DEPRECATED OPTIONS
	-replication -replist	NEW OPTIONS *(available with patch bundle set 7.01 and superseding updates)*
omniobjverify	This command is available on systems with the Data Protector User Interface component installed.	NEW COMMAND
omniofflr	-rawdisk -section	NEW OPTIONS
omnir	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-appname	NEW OPTION New option for Lotus Notes/Domino Server restore.
	-resume -no_auto_device _selection	NEW OPTIONS
	-newinstance "None"	NEW OPTION VALUE

Table 12 Upgrade from Data Protector A.06.10 *(continued)*

Command	Affected options or arguments, notes	Status
		New option value for Data Protector VMware (Legacy) integration.
	-no_auto_dev	OBSOLETE OPTION Replaced by -no_auto_device_selection.
	-stopat -tail_log	NEW OPTIONS New options for Microsoft SQL Server restore.
	-copyback -switch -leave_source -no_leave_source -no_check_config	NEW OPTIONS New options for HP P6000 EVA Disk Array Family.
	-target Client	CHANGED OPTION Changed option for NDMP Server restore.
omnirpt	-verificationlist_sch -verificationlist_post -no_verificationlist	NEW OPTIONS
omnisetup.sh	veagent vmware chs_ls	NEW SOFTWARE COMPONENTS
	snapa	OBSOLETE SOFTWARE COMPONENT
	-bundleadd -bundlerem	NEW OPTIONS
omnisrdupdate	-use_raw_object	NEW OPTION
omniusb	This command is available on systems with the Data Protector Automatic Disaster Recovery component installed.	NEW COMMAND
sanconf	-mom	NEW OPTION
SharePoint_VSS_backup.ps1	This command is available on Windows systems with the Data Protector MS Volume Shadow Copy Integration component installed.	NEW COMMAND
util_cmd	veagent vmware	NEW INTEGRATIONS
	-encode	NEW OPTION
vepa_util.exe	This command is available on systems with the Data Protector Virtual Environment Integration component installed.	NEW COMMAND

Table 13 Upgrade from Data Protector A.06.11

Command	Affected options or arguments, notes	Status
`ob2install`	`veagent` `chs_ls`	NEW SOFTWARE COMPONENTS
	`saphana`	NEW SOFTWARE COMPONENT *(available with patch bundle set 7.03 and superseding updates)*
	`snapa`	OBSOLETE SOFTWARE COMPONENT
`omnib`	`-storedrim *`	NEW OPTION *
	`-clp`	NEW OPTION

	`-veagent_list`
	`-e2010_list`
	`-mssharepoint_list`
		NEW INTEGRATIONS

	`-copy`	UPDATED OPTION *(available with patch bundle set 7.01 and superseding updates)* This option can be specified also for backup using the Microsoft SQL Server integration.
`omnib2dinfo*`	This command is available on systems with the `User Interface` component installed.	REDESIGNED COMMAND* This command was relocated from the Media Agent component.

`omnicc`	`-encryption`
	`-enable`
	`-cert`
	`-key`
	`-trust`
	`-all`
	`-add_exception`
	`-remove_exception`
	`-list_exceptions`
	`-status`
	`-add_certificate`
	`-get_certificate`
	`-list_certificates`
	`-impersonation`
	`-create_userrestrictions_tmpl`
		NEW OPTIONS

	`-import_vcd`	NEW OPTION *(available with patch bundle set 7.01 and superseding updates)*

Table 13 Upgrade from Data Protector A.06.11 *(continued)*

Command	Affected options or arguments, notes	Status
omnicreatedl	-va -lun_security	OBSOLETE OPTIONS
omnidb	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
omnidbp4000	This command is available on Windows systems with the Data Protector User Interface component installed.	NEW COMMAND
omnidbsmis	-ompasswd -delete	NEW OPTION COMBINATION
	-reference -sync_check -exclude -include	NEW OPTIONS
	-namespace -sync	OBSOLETE OPTIONS
omnidbva		OBSOLETE COMMAND
omnidbxp	-user -add -username -password -user -check -host -user -update -username -password -user -list -user -remove	NEW OPTIONS AND OPTION COMBINATIONS
omnidbzdb	This command is available on systems with the Data Protector User Interface component installed.	NEW COMMAND *(available with patch bundle set 7.01 and superseding updates)*
omniiso	-out	NEW OPTIONS
	-net	
	-use_raw_object	
	-iso	OBSOLETE OPTION Replaced by -out. Can be used for backward compatibility.
omnimm	-show_locked_devs -all	NEW OPTIONS
omniobjcopy	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS

Table 13 Upgrade from Data Protector A.06.11 *(continued)*

Command	Affected options or arguments, notes	Status
	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
	-replication -replist	NEW OPTIONS *(available with patch bundle set 7.01 and superseding updates)*
omniobjverify	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
omniofflr	-rawdisk -section	NEW OPTIONS
omnir	-veagent -e2010 -mssharepoint	NEW INTEGRATIONS
	-copyback -switch -leave_source -no_leave_source -no_check_config	NEW OPTIONS New options for HP P6000 EVA Disk Array Family.
	-tail_log	NEW OPTION New option for Microsoft SQL Server restore.
omnirsh	-add -modify	NEW OPTIONS
omnisetup.sh	veagent chs_ls	NEW SOFTWARE COMPONENTS
	snapa	OBSOLETE SOFTWARE COMPONENT
	-bundleadd -bundlerem	NEW OPTIONS
omnisrdupdate	-use_raw_object	NEW OPTION
omniusb	This command is available on systems with the Data Protector Automatic Disaster Recovery component installed.	NEW COMMAND
SharePoint_VSS_backup.ps1	This command is available on Windows systems with the Data Protector MS Volume Shadow Copy Integration component installed.	NEW COMMAND

Table 13 Upgrade from Data Protector A.06.11 *(continued)*

Command	Affected options or arguments, notes	Status
util_cmd	veagent	NEW INTEGRATION
vepa_util.exe	This command is available on systems with the Data Protector Virtual Environment Integration component installed.	NEW COMMAND

Table 14 Upgrade from Data Protector 6.20

Command	Affected options or arguments, notes	Status
ob2install	saphana	NEW SOFTWARE COMPONENT *(available with patch bundle set 7.03 and superseding updates)*
omnib	-storedrim *	NEW OPTION *
	-copy	UPDATED OPTION *(available with patch bundle set 7.01 and superseding updates)* This option can be specified also for backup using the Microsoft SQL Server integration.
	-barmode	UPDATED OPTION *(available with patch bundle set 7.01 and superseding updates)* The value incr can be specified also for backup of Microsoft Hyper-V virtual machines using the Virtual Environment integration.
omnib2dinfo*	This command is available on systems with the User Interface component installed.	REDESIGNED COMMAND* This command was relocated from the Media Agent component.
omnicc	-import_vcd	NEW OPTION *(available with patch bundle set 7.01 and superseding updates)*
omnidb	-saphana	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
omnidbxp	-user -add -username -password -user -check -host -user -update -username -password -user -list -user -remove	NEW OPTIONS AND OPTION COMBINATIONS

Table 14 Upgrade from Data Protector 6.20 *(continued)*

Command	Affected options or arguments, notes	Status
`omnidbzdb`	This command is available on systems with the Data Protector `User Interface` component installed.	NEW COMMAND *(available with patch bundle set 7.01 and superseding updates)*

`omnidownload`	`-dev_info`
	`-list_devices`
	`-list_libraries -detail`
		UPDATED OPTIONS AND OPTION COMBINATIONS
		Updated options and option combinations for Backup to Disk devices.

`omniiso`	`-out`
	`-net`
	`-use_raw_object`
		NEW OPTIONS

	`-iso`	OBSOLETE OPTION Replaced by `-out`. Can be used for backward compatibility.
`omnimm`	`-delete_unprotected_media`	NEW OPTION New option for Backup to Disk devices.

	`-all`
	`-recycle`
	`-remove_slots`
		UPDATED OPTIONS
		Updated options for Backup to Disk devices.

`omniobjcopy`	`-saphana`	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
	`-replication` `-replist`	NEW OPTIONS *(available with patch bundle set 7.01 and superseding updates)*
`omniobjverify`	`-saphana`	NEW INTEGRATION *(available with patch bundle set 7.03 and superseding updates)*
`omniofflr`	`-rawdisk` `-section`	NEW OPTIONS
`omnir`	`-tail_log`	NEW OPTION New option for Microsoft SQL Server restore.
	`-deletebefore` `-skip`	UPDATED OPTIONS These options can be specified also for Microsoft Hyper-V restore using the Virtual Environment integration.

Table 14 Upgrade from Data Protector 6.20 *(continued)*

Command	Affected options or arguments, notes	Status
	-host/cluster -resourcePool -specificHost -fromSession -untilSession	NEW OPTIONS *(available with patch bundle set 7.01 and superseding updates)* New options for VMware vSphere using the Virtual Environment integration.
	-neworganization -virtual_datacenter_path -virtual_datacenter_uuid -vapp_path -vapp_uuid -vcenter_path -vcenter_uuid -network_name -network_uuid	NEW OPTIONS *(available with patch bundle set 7.01 and superseding updates)* New options for VMware vCloud Director using the Virtual Environment integration.
	-virtual-environment -method	UPDATED OPTIONS *(available with patch bundle set 7.01 and superseding updates)* These options can be specified also for VMware vCloud Director using the Virtual Environment integration.
	-targetstoragepath	NEW OPTION *(available with patch bundle set 7.01 and superseding updates)* New option for Microsoft Hyper-V using the Virtual Environment integration.
	-deleteafter * -keep_for_forensics * -new_name *	NEW OPTIONS * New options for VMware vSphere using the Virtual Environment integration.
	-network_name *	UPDATED OPTION * This option can be specified also for VMware vSphere using the Virtual Environment integration.
omnisetup.sh	-bundleadd -bundlerem	NEW OPTIONS
omnisrdupdate	-use_raw_object	NEW OPTION
vepa_util.exe	--list-organizations	NEW OPTION *(available with patch bundle set 7.01 and superseding updates)*

Table 14 Upgrade from Data Protector 6.20 *(continued)*

Command	Affected options or arguments, notes	Status
		New option for VMware vCloud Director using the Virtual Environment integration.

	`--check-config`
	`--config`
	`--configvm`
	`--virtual-environment`
		UPDATED OPTIONS
		(available with patch bundle set 7.01 and superseding updates)
		These options can be specified also for VMware vCloud Director using the Virtual Environment integration.

	`--show-incremental-flag`
	`--enable-incremental`
	`--disable-incremental`
	`--list-vms`
		NEW OPTIONS
		(available with patch bundle set 7.01 and superseding updates)
		New options for Microsoft Hyper-V using the Virtual Environment integration.

Glossary

A

access rights — *See* user rights.

ACSLS — *(StorageTek specific term)* The Automated Cartridge System Library Server (ACSLS) software that manages the Automated Cartridge System (ACS).

Active Directory — *(Windows specific term)* The directory service in a Windows network. It contains information about resources on the network and makes them accessible to users and applications. The directory services provide a consistent way to name, describe, locate, access and manage resources regardless of the physical system they reside on.

AES 256-bit encryption — Data Protector software encryption, based on the AES-CTR (Advanced Encryption Standard in Counter Mode) encryption algorithm that uses random keys of 256-bit length. The same key is used for both encryption and decryption. With AES 256-bit encryption, data is encrypted before it is transferred over a network and before it is written to media.

AML — *(ADIC/GRAU specific term)* Automated Mixed-Media library.

AMU — *(ADIC/GRAU specific term)* Archive Management Unit.

application agent — A component needed on a client to back up or restore online database integrations.
See also Disk Agent.

application system — *(ZDB specific term)* A system the application or database runs on. The application or database data is located on source volumes.
See also backup system and source volume.

archive logging — *(Lotus Domino Server specific term)* Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.

archived redo log — *(Oracle specific term)* Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to an archived log destination. This copy is the archived redo log. The presence or absence of an archived redo log is determined by the mode the database is using:

- ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A "hot" backup can be performed only when the database is running in this mode.
- NOARCHIVELOG - The filled online redo log files are not archived.

See also online redo log.

ASR set — A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\dr\asr` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), `Data_Protector_home\Config\Server\dr\asr` (other Windows systems), or `/etc/opt/omni/server/dr/asr` (UNIX systems) as well as on the backup medium. After a disaster occurs, the ASR archive file is extracted to diskettes which you need to perform ASR.

audit logs — Data files to which auditing information is stored.

audit report — User-readable output of auditing information created from data stored in audit log files.

auditing information — Data about every backup session that was performed over an extended, user-defined period for the whole Data Protector cell.

autochanger — *See* library.

autoloader — *See* library.

Automatic Storage Management (ASM) — *(Oracle specific term)* A filesystem and volume manager integrated into Oracle which manages Oracle database files. It eliminates complexity associated with data and disk management and optimizes performance by providing striping and mirroring capabilities.

automigration *(VLS specific term)* The functionality that allows data backups to be first made to the VLS' virtual tapes and then migrated to physical tapes (one virtual tape emulating one physical tape) without using an intermediate backup application.
See also Virtual Library System (VLS) and virtual tape.

auxiliary disk A bootable disk that has a minimal operating system with networking and Data Protector Disk Agent installed. It can be carried around and used to boot the target system in Phase 1 of Disk Delivery Disaster Recovery of UNIX clients.

B

BACKINT *(SAP R/3 specific term)* SAP R/3 backup programs can call the Data Protector backint interface program via an open interface, which enables them to communicate with Data Protector software. For backup and restore, SAP R/3 programs issue orders for the Data Protector backint interface.

backup API The Oracle interface between the Oracle backup/restore utility and the backup/restore media management layer. The interface defines a set of routines to allow the reading and writing of data to the backup media, the creation, searching and removing the backup files.

backup chain *See* restore chain.

backup device A device configured for use with Data Protector, which can write data to and read data from storage media. This can be, for example, a standalone DDS/DAT drive or a library.

backup generation One backup generation includes one full backup and all incremental backups until the next full backup.

backup ID An identifier of an integration object that equals the session ID of the backup of this object. The backup ID is preserved when an object is copied, exported, or imported.

backup object A backup unit that contains all items backed up from one disk volume (logical disk or mount point). The backed up items can be any number of files, directories, or the entire disk or mount point. Additionally, a backup object can be a database/application entity or a disk image.

A backup object is defined by:

- Client name: Hostname of the Data Protector client where the backup object resides.
- Mount point: For filesystem objects — the access point in a directory structure on the client where the backup object is located (drive on Windows and mount point on UNIX). For integration objects — backup stream identification, indicating the backed up database/application items.
- Description: For filesystem objects — uniquely defines objects with identical client name and mount point. For integration objects — displays the integration type (for example, SAP or Lotus).
- Type: Backup object type. For filesystem objects — filesystem type (for example, WinFS). For integration objects — "Bar".

backup owner Each backup object in the IDB has an owner. The default owner of a backup is the user who starts the backup session.

backup session A process that creates a copy of data on storage media. The activities are specified in a backup specification or an interactive session. All clients configured in one backup specification are backed up together in one backup session using the same backup type. The result of a backup session is a set of media, which was written to, also called the backup or media set.
See also backup specification, full backup, and incremental backup.

backup set A complete set of integration objects associated with a backup.

backup set *(Oracle specific term)* A logical grouping of backed up files that are created using the RMAN backup command. A backup set is a complete set of files associated with a backup. The files can be multiplexed to increase performance. A backup set contains either datafiles or archived logs, but not both together.

backup specification A list of objects to be backed up, together with a set of devices or drives to be used, backup options for all objects in the specification, and days and time that you want backups to be performed. The objects are entire disks/volumes or parts of them such as files, directories, or

even the Windows Registry for example. File selection lists such as include-lists and exclude-lists can be specified.

backup system *(ZDB specific term)* A system connected to a disk array together with one or multiple application systems. The backup system is typically connected to a disk array to create target volumes (a replica) and is used for mounting the target volumes (the replica).
See also application system, target volume, and replica.

backup types *See* incremental backup, differential backup, transaction backup, full backup, and delta backup.

backup view Data Protector provides different views for backup specifications:

By Type - according to the type of data available for backups/templates. Default view.

By Group - according to the group to which backup specifications/templates belong.

By Name - according to the name of backup specifications/templates.

By Manager - if you are running MoM, you can also set the Backup view according to the Cell Manager to which backup specifications/templates belong.

BC *(EMC Symmetrix specific term)* Business Continuance are processes that allow customers to access and manage instant copies of EMC Symmetrix standard devices.
See also BCV.

BC Process *(EMC Symmetrix specific term)* A protected storage environment solution that has defined specially configured EMC Symmetrix devices as mirrors or Business Continuance Volumes to protect data on EMC Symmetrix standard devices.
See also BCV.

BCV *(EMC Symmetrix specific term)* Business Continuance Volumes, or BCV devices, are dedicated SLDs that are pre-configured in the ICDA on which the business continuation operation runs. BCV devices are assigned separate SCSI addresses, differing from the addresses used by the SLDs they mirror. The BCV devices are used as splitable mirrors of the primary EMC Symmetrix SLDs that need to be protected.
See also BC and BC Process.

Boolean operators The Boolean operators for the full text search functionality of the Data Protector Help system are AND, OR, NOT, and NEAR. Used when searching, they enable you to define your query precisely by creating a relationship between search terms. If no operator is specified in a multi-word search, AND is used by default. For example, the query manual disaster recovery is equivalent to manual AND disaster AND recovery.

boot volume/disk/partition A volume/disk/partition with files required for the initial step of the boot process. Microsoft terminology defines the boot volume/disk/partition as a volume/disk/partition containing the operating system files.

BRARCHIVE *(SAP R/3 specific term)* An SAP R/3 backup tool that allows you to archive redo log files. BRARCHIVE also saves all the logs and profiles of the archiving process.
See also BRBACKUP and BRRESTORE.

BRBACKUP *(SAP R/3 specific term)* An SAP R/3 backup tool that allows an online or offline backup of the control file, of individual data files, or of all tablespaces and, if necessary, of the online redo log files.
See also BRARCHIVE and BRRESTORE.

BRRESTORE *(SAP R/3 specific term)* An SAP R/3 tool that can be used to restore files of the following type:

- Database data files, control files, and online redo log files saved with BRBACKUP
- Redo log files archived with BRARCHIVE
- Non-database files saved with BRBACKUP

You can specify files, tablespaces, complete backups, log sequence numbers of redo log files, or the session ID of the backup.
See also BRBACKUP and BRARCHIVE.

BSM The Data Protector Backup Session Manager controls the backup session. This process always runs on the Cell Manager system.

C

CAP
(StorageTek specific term) Cartridge Access Port is a port built into the door panel of a library. The purpose is to enter or eject media.

catalog protection
Defines how long information about backed up data (such as file names and file versions) is kept in the IDB.
See also data protection.

CDB
The Catalog Database is a part of the IDB that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. Depending on the selected logging level, it also contains file names and file versions. This part of the database is always local to the cell.
See also MMDB.

CDF file
(UNIX specific term) A Context Dependent File is a file consisting of several files grouped under the same pathname. The system ordinarily selects one of the files using the context of the process. This mechanism allows machine dependent executables, system data, and device files to work correctly from all hosts in a cluster while using the same pathname.

cell
A set of systems that are under the control of a Cell Manager. The cell typically represents the systems on a site or an organizational entity, which are connected to the same LAN or SAN. Central control is available to administer the backup and restore policies and tasks.

Cell Manager
The main system in the cell where the essential Data Protector software is installed and from which all backup and restore activities are managed. The GUI used for management tasks can be located on a different system. Each cell has one Cell Manager system.

centralized licensing
Data Protector allows you to configure centralized licensing for the whole enterprise environment consisting of several cells. All Data Protector licenses are installed and kept on the Enterprise Cell Manager system. You can then allocate licenses to specific cells to suit your needs.
See also MoM.

Centralized Media Management Database (CMMDB)
See CMMDB.

Certificate Server
A Windows Certificate Server can be installed and configured to provide certificates for clients. It provides customizable services for issuing and managing certificates for the enterprise. These services issue, revoke, and manage certificates employed in public key-based cryptography technologies.

Change Journal
(Windows specific term) A Windows filesystem feature that logs a record of each change as it occurs to the files and directories on a local NTFS volume.

Change Log Provider
(Windows specific term) A module that can be queried to determine which objects on a filesystem have been created, modified, or deleted.

channel
(Oracle specific term) An Oracle Recovery Manager resource allocation. Every allocated channel starts a new Oracle process, which performs backup, restore, and recovery actions. The type of channel allocated determines the type of media used:

- type 'disk'
- type 'sbt_tape'

If the specified channel is of type 'sbt_tape' and Oracle is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

circular logging
(Microsoft Exchange Server and Lotus Domino Server specific term) Circular logging is a Microsoft Exchange Server database and Lotus Domino Server database mode, in which the transaction log file contents are periodically overwritten after the corresponding data is committed to the database. Circular logging reduces disk storage space requirements.

client backup
A backup of all volumes (filesystems) mounted on a Data Protector client. What is actually backed up depends on how you select objects in a backup specification:

- If you select the check box next to the client system name, a single backup object of the `Client System` type is created. As a result, at the time of the backup, Data Protector first

detects all volumes that are mounted on the selected client and then backs them up. On Windows clients, `CONFIGURATION` is also backed up.

- If you individually select all volumes that are mounted on the client system, a separate backup object of the `Filesystem` type is created for each volume. As a result, at the time of the backup, only the selected volumes are backed up. Volumes that have been potentially mounted on the client after the backup specification was created are not backed up.

client or client system
Any system configured with any Data Protector functionality and configured in a cell.

cluster continuous replication
(Microsoft Exchange Server specific term) Cluster continuous replication (CCR) is a high availability solution that uses cluster management and failover options to create and maintain an exact copy (CCR copy) of a storage group. A storage group is replicated to a separate server. CCR removes any single point of failure in your Exchange back-end servers. You can perform backups using VSS on your passive Exchange Server node where a CCR copy is located and thus reducing the load on the active node.

A CCR copy is used for disaster recovery since you can switch to the CCR copy in a few seconds. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) like an ordinary storage group.

See also Exchange Replication Service and local continuous replication.

cluster-aware application
It is an application that supports the cluster Application Programming Interface. Each cluster-aware application declares its own critical resources (disk volumes (on Microsoft Cluster Server), volume groups (on MC/ServiceGuard), application services, IP names and addresses, and so on).

CMD script for Informix Server
(Informix Server specific term) A Windows CMD script that is created in INFORMIXDIR when an Informix Server database is configured. The CMD script is a set of system commands that export environment variables for Informix Server.

CMMDB
The Data Protector Centralized Media Management Database (CMMDB) is the result of merging MMDBs from several cells in the MoM environment. It allows you to share high-end devices and media across multiple cells in a MoM environment. One cell can control the robotics, serving the devices that are connected to systems in other cells. The CMMDB must reside on the Manager-of-Managers. A reliable network connection between the MoM cell and the other Data Protector cells is highly recommended
See also MoM.

COM+ Class Registration Database
(Windows specific term) The COM+ Class Registration Database and the Windows Registry store application attributes, class attributes, and computer-level attributes. This guarantees consistency among these attributes and provides common operation on top of these attributes.

command device
(HP P9000 XP Disk Array Family specific term) A dedicated volume in the disk array which acts as the interface between a management application and the disk array's storage system. It cannot be used for data storage and only accepts requests for operations that are then executed by the disk array.

Command View VLS
(VLS specific term) A web browser-based GUI that is used to configure, manage, and monitor the VLS through a LAN.
See also Virtual Library System (VLS).

command-line interface (CLI)
A set of DOS and UNIX like commands that you can use in shell scripts to perform Data Protector configuration, backup, restore, and management tasks.

concurrency
See Disk Agent concurrency.

container
(HP P6000 EVA Disk Array Family specific term) Space on a disk array, which is pre-allocated for later use as a standard snapshot, vsnap, or snapclone.

control file
(Oracle and SAP R/3 specific term) An Oracle data file that contains entries specifying the physical structure of the database. It provides database consistency information used for recovery.

copy set
(HP P6000 EVA Disk Array Family specific term) A pair that consists of the source volumes on a local P6000 EVA and their replica on a remote P6000 EVA.
See also source volume, replica, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

CRS
The Cell Request Server process (service), which runs on the Data Protector Cell Manager, and starts and controls the backup and restore sessions. The service is started as soon as Data Protector

is installed on the Cell Manager. On Windows systems, the CRS runs under the account of the user specified at installation time. On UNIX systems, it runs under the account `root`.

CSM The Data Protector Copy and Consolidation Session Manager process controls the object copy and object consolidation sessions and runs on the Cell Manager system.

D

data file *(Oracle and SAP R/3 specific term)* A physical file created by Oracle that contains data structures such as tables and indexes. A data file can only belong to one Oracle database.

data protection Defines how long the backed up data on media remains protected, that is, Data Protector will not overwrite it. When the protection expires, Data Protector will be able to reuse the media in one of the next backup sessions.
See also catalog protection.

data replication (DR) group *(HP P6000 EVA Disk Array Family specific term)* A logical grouping of HP P6000 EVA Disk Array Family virtual disks. It can contain up to eight copy sets provided they have common characteristics and share a common HP CA P6000 EVA log.
See also copy set.

data stream Sequence of data transferred over the communication channel.

Data_Protector_home A reference to the directory containing Data Protector program files (on Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012) or the directory containing Data Protector program files and data files (on other Windows operating systems). Its default path is `%ProgramFiles%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_program_data.

Data_Protector_program_data A reference to the directory containing Data Protector data files on Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012. Its default path is `%ProgramData%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_home.

database library A Data Protector set of routines that enables data transfer between Data Protector and a server of an online database integration, for example, Oracle Server.

database parallelism More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.

database server A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.

Dbobject *(Informix Server specific term)* An Informix Server physical database object. It can be a blobspace, dbspace, or logical log file.

DC directory The Detail Catalog (DC) directory contains DC binary files, which store information about file versions. It represents the DCBF part of the IDB, which occupies approximately 80% of the IDB. The default DC directory is called the `dcbf` directory and is located on the Cell Manager in the directory `Data_Protector_program_data\db40` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), `Data_Protector_home\db40` (other Windows systems), or `/var/opt/omni/server/db40` (UNIX systems). You can create more DC directories and use a custom location. Up to 50 DC directories are supported per cell. The default maximum size of a DC directory is 16 GB.

DCBF The Detail Catalog Binary Files (DCBF) part of the IDB stores information about file versions and attributes. It occupies approximately 80% of the IDB. One DC binary file is created for each Data Protector medium used for backup. Its maximum size is limited by the filesystem settings.

delta backup A delta backup is a backup containing all the changes made to the database from the last backup of any type.
See also backup types.

device A physical unit which contains either just a drive or a more complex unit such as a library.

device chain A device chain consists of several standalone devices configured for sequential use. When a medium in one device gets full, the backup automatically continues on a medium in the next device in the device chain.

device group *(EMC Symmetrix specific term)* A logical unit representing several EMC Symmetrix devices. A device cannot belong to more than a single device group. All devices in a device group must be on the same EMC Symmetrix unit. You can use a device group to identify and work with a subset of the available EMC Symmetrix devices.

device streaming A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes to write to the tape, and so on. In other words, if the data rate written to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.

DHCP server A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic IP address assignment and network configuration for DHCP clients.

differential backup An incremental backup that backs up changes made since the last full backup. To perform this type of backup, specify the Incr1 backup type.
See also incremental backup.

differential backup *(Microsoft SQL Server specific term)* A database backup that records only the data changes made to the database after the last full database backup.
See also backup types.

differential database backup A differential database backup records only those data changes made to the database after the last full database backup.

directory junction *(Windows specific term)* Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.

disaster recovery A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.

disaster recovery operating system *See* DR OS.

Disk Agent A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.

Disk Agent concurrency The number of Disk Agents that are allowed to send data to one Media Agent concurrently.

disk group *(Veritas Volume Manager specific term)* The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.

disk image backup A high-speed backup where Data Protector backs up files as bitmap images. A disk image backup does not track the files and directory structure stored on the disk, but stores a disk image structure on byte level. You can perform a disk image backup of either specific disk sections or a complete disk.

disk quota A concept to manage disk space consumption for all or a subset of users on a computer system. This concept is used by several operating system platforms.

disk staging The process of backing up data in several phases to improve the performance of backups and restores, reduce costs of storing the backed up data, and increase the data availability and accessibility for restore. The backup stages consist of backing up data to one media type first (for example disk) and later copying it to a different media type (for example tape).

distributed file media format A media format, available with the file library, which supports a space efficient type of synthetic backup called virtual full backup. Using this format is a prerequisite for virtual full backup.
See also virtual full backup.

Distributed File System (DFS) A service that connects file shares into a single namespace. The file shares can reside on the same or on different computers. DFS provides client access to the resources in a location-transparent manner.

DMZ The Demilitarized Zone (DMZ) is a network inserted as a "neutral zone" between a company's private network (intranet) and the outside public network (Internet). It prevents outside users from getting direct access to company servers in the intranet.

DNS server In the DNS client-server model, this is the server containing information about a portion of the DNS database that makes computer names available to client resolvers querying for name resolution across the Internet.

domain controller A server in a network that is responsible for user security and verifying passwords within a group of other servers.

DR image Data required for temporary disaster recovery operating system (DR OS) installation and configuration.

DR OS An operating system environment in which disaster recovery runs. It provides Data Protector with a basic runtime environment (disk, network, tape, and filesystem access). It has to be installed on disk or loaded into memory and configured before the Data Protector disaster recovery can be performed. DR OS can be either temporary or active. A temporary DR OS is used exclusively as a host environment for some other operating system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. An active DR OS not only hosts the Data Protector disaster recovery process but can also be a part of the restored system because it replaces its own configuration data with the original configuration data.

drive A physical unit that receives data from a computer system and can write it onto a magnetic medium (typically a tape drive). It can also read the data from the medium and send it to the computer system.

drive index A number that identifies the mechanical position of a drive inside a library device. This number is used by the robotic control to access a drive.

drive-based encryption Data Protector drive-based encryption uses the encryption functionality of the drive. While performing the backup, the drive encrypts both the data and the metadata that is written to the medium.

E

EMC Symmetrix Agent A Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

emergency boot file *(Informix Server specific term)* The Informix Server configuration file `ixbar.`*`server_id`* that resides in the directory *`INFORMIXDIR`*`/etc` (on Windows) or *`INFORMIXDIR`*`\etc` (on UNIX). *`INFORMIXDIR`* is the Informix Server home directory and *`server_id`* is the value of the `SERVERNUM` configuration parameter. Each line of the emergency boot file corresponds to one backup object.

encrypted control communication Data Protector secure communication between the clients in the Data Protector cell is based on Secure Socket Layer (SSL) that uses SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.

encryption key A 256-bit randomly generated number used by the Data Protector encryption algorithm to encode information during backups for which AES 256-bit software encryption or drive-based encryption has been specified. The same key is used for subsequent decryption of the information. Encryption keys for a Data Protector cell are stored in a central keystore on the Cell Manager.

encryption KeyID-StoreID Combined identifier used by the Data Protector Key Management Server to identify and administer encryption keys used by Data Protector. `KeyID` identifies the key within the keystore. `StoreID` identifies the keystore on the Cell Manager. If Data Protector has been upgraded from an earlier version with encryption functionality, there may several `StoreID`s used on the same Cell Manager.

enhanced incremental backup Conventional incremental backup backs up files that have changed since a previous backup, but has certain limitations in detection of changes. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up also renamed and moved files, as well as files with changes in attributes.

enterprise backup environment Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes all clients located in several Data Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept.
See also MoM.

Event Log (Data Protector Event Log) A central repository of all Data Protector-related notifications. By default, all notifications are sent to the Event Log. The events are logged on the Cell Manager into the file *Data_Protector_program_data*\log\server\Ob2EventLog.txt (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*\log\server\Ob2EventLog.txt (other Windows systems), or /var/opt/omni/server/log/Ob2EventLog.txt (UNIX systems). The Event Log is accessible only to users of the Data Protector Admin user group and to users who are granted the Data Protector Reporting and notifications user rights. You can view or delete all events in the Event Log.

Event Logs *(Windows specific term)* Files in which Windows logs all events, such as the starting or stopping of services and the logging on and off of users. Data Protector can back up Windows Event Logs as part of the Windows configuration backup.

Exchange Replication Service *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that represents storage groups that were replicated using either local continuous replication (LCR) or cluster continuous replication (CCR) technology.
See also cluster continuous replication and local continuous replication.

exchanger Also referred to as SCSI Exchanger.
See also library.

exporting media A process that removes all data about backup sessions, such as systems, objects, and file names, which reside on the media from the IDB. Information about the media and their relation to a pool is also removed from the IDB. The data on the media remains unchanged.
See also importing media.

Extensible Storage Engine (ESE) *(Microsoft Exchange Server specific term)* A database technology used as a storage system for information exchange in Microsoft Exchange Server.

F

failover Transferring of the most important cluster data, called group (on Windows) or package (on UNIX) from one cluster node to another. A failover can occur mostly because of software or hardware failures or maintenance on the primary node.

failover *(HP P6000 EVA Disk Array Family specific term)* An operation that reverses the roles of source and destination in HP Continuous Access + Business Copy (CA+BC) P6000 EVA configurations.
See also HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

FC bridge *See* Fibre Channel bridge.

Fibre Channel An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

Fibre Channel bridge A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries to a Fibre Channel environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.

file depot A file containing the data from a backup to a file library device.

file jukebox device A device residing on disk consisting of multiple slots used to store file media.

file library device A device which resides on a disk emulating a library with several media, hence containing multiple files, referred to as file depots.

File Replication Service (FRS) A Windows service that replicates the domain controller store logon scripts and group policies. FRS also enables replication of Distributed File System (DFS) shares between systems and allows any server to perform replication activity.

file tree walk *(Windows specific term)* The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

file version The same file can be backed up multiple times in case of full backups and incremental backups (if the file changed). If the log level ALL is selected for backup, Data Protector retains one entry in the IDB for the filename itself and one for each version (date/time) of the file.

filesystem The organization of files on a hard disk. A filesystem is backed up so that the file attributes and the file contents are stored on the backup media.

first-level mirror *(HP P9000 XP Disk Array Family specific term)* A mirror of an internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which can be further mirrored itself, producing second-level mirrors. For Data Protector zero downtime backup and instant recovery purposes, only first-level mirrors can be used.
See also primary volume and mirror unit (MU) number.

flash recovery area *(Oracle specific term)* A directory, filesystem, or Automatic Storage Management (ASM) disk group managed by Oracle that serves as a centralized storage area for files related to backup, restore, and database recovery (recovery files).
See also recovery files.

fnames.dat The `fnames.dat` files of the IDB contain information on the names of the backed up files. Typically, these files occupy about 20% of the IDB, if filenames are stored.

formatting A process that erases any data contained on a medium and prepares it for use with Data Protector. Information about media (medium ID, description, and location) is saved in the IDB as well as on the respective media (media header). Data Protector media with protected data are not formatted until the protection expires or the media are unprotected/recycled.

free pool An auxiliary source of media for use by media pools when they run out of media. The media pools must be configured to use free pools.

full backup A backup in which all selected objects are backed up, whether or not they have been recently modified.
See also backup types.

full database backup A backup of all data in a database, not only the data that has been changed after the last (full or incremental) backup of the database. A full database backup does not depend on any other backup.

full mailbox backup A full mailbox backup is a backup of the entire mailbox content.

full ZDB A ZDB-to-tape or ZDB-to-disk+tape session in which all selected objects are streamed to tape, even if there are no changes from the previous backup.
See also incremental ZDB.

G

global options file A file that allows you to customize Data Protector. It explains the global options, which cover various aspects of Data Protector, typically time-outs and limits, and affect the entire Data Protector cell. The file is located on the Cell Manager in the directory *`Data_Protector_program_data`*`\Config\Server\Options` (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *`Data_Protector_home`*`\Config\Server\Options` (other Windows systems), or `/etc/opt/omni/server/options` (HP-UX and Linux systems).

group *(Microsoft Cluster Server specific term)* A collection of resources (for example disk volumes, application services, IP names, and addresses) that are needed to run a specific cluster-aware applications.

GUI A graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. Besides the original Data Protector GUI that runs on Windows, Data Protector also provides a Java-based graphical user interface with the same look and feel, which runs on numerous platforms.

H

hard recovery *(Microsoft Exchange Server specific term)* A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.

heartbeat A cluster data set with a time stamp carrying information about the operational status of a particular cluster node. This data set or packet is distributed among all cluster nodes.

Hierarchical Storage Management (HSM) A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to less expensive optical platters. When needed, the data is migrated back to hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.

Holidays file A file that contains information about holidays. You can set different holidays by editing the Holidays file on the Cell Manager in the directory *Data_Protector_program_data*\Config\Server\holidays (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*\Config\Server\holidays (other Windows systems), or /etc/opt/omni/server/Holidays (UNIX systems).

hosting system A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.

HP Business Copy (BC) P6000 EVA *(HP P6000 EVA Disk Array Family specific term)* A local replication software solution that enables creation of point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the P6000 EVA firmware.
See also replica, source volume, snapshot, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

HP Business Copy (BC) P9000 XP *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of internal copies of LDEVs for various purposes, such as data duplication and backup. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system. For Data Protector zero downtime backup purposes, P-VOLs should be available to the application system, and one of the S-VOL sets should be available to the backup system.
See also LDEV, HP Continuous Access (CA) P9000 XP, Main Control Unit, application system, and backup system.

HP Command View (CV) EVA *(HP P6000 EVA Disk Array Family specific term)* The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, and mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed by a Web browser.
See also HP P6000 EVA SMI-S Agent and HP SMI-S P6000 EVA Array provider.

HP Continuous Access (CA) P9000 XP *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of remote copies of LDEVs for purposes such as data duplication, backup, and disaster recovery. HP CA P9000 XP operations involve main (primary) disk array units and remote (secondary) disk array units. The main disk array units are connected to the application system and contain primary volumes (P-VOLs), which store original data. The remote disk array units are connected to the backup system and contain secondary volumes (S-VOLs).
See also HP Business Copy (BC) P9000 XP, Main Control Unit, and LDEV.

HP Continuous Access + Business Copy (CA+BC) P6000 EVA *(HP P6000 EVA Disk Array Family specific term)* An HP P6000 EVA Disk Array Family configuration that enables creation and maintenance of copies (replicas) of the source volumes on a remote P6000 EVA, and later use of these copies as the source for local replication on this remote array.
See also HP Business Copy (BC) P6000 EVA, replica, and source volume.

HP P6000 EVA SMI-S Agent A Data Protector software module that executes all tasks required for the HP P6000 EVA Disk Array Family integration. With the P6000 EVA SMI-S Agent, the control over the array is established through HP SMI-S P6000 EVA Array provider, which directs communication between incoming requests and HP CV EVA.
See also HP Command View (CV) EVA and HP SMI-S P6000 EVA Array provider.

HP P9000 XP Agent
A Data Protector component that executes all tasks needed by the Data Protector HP P9000 XP Disk Array Family integration. It uses RAID Manager Library for communication with a P9000 XP Array storage system.
See also RAID Manager Library.

HP SMI-S P6000 EVA Array provider
An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the P6000 EVA SMI-S Agent, communicates with HP Command View EVA for information or method invocation, and returns standardized responses.
See also HP P6000 EVA SMI-S Agent and HP Command View (CV) EVA.

HP Operations Manager
HP Operations Manager provides powerful capabilities for operations management of a large number of systems and applications in a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for HP Operations Manager management servers on Windows, HP-UX, Solaris, and Linux. Earlier versions of HP Operations Manager were called IT/Operations, Operations Center, Vantage Point Operations, and OpenView Operations.

HP Operations Manager SMART Plug-In (SPI)
A fully integrated, out-of-the-box solution which "plugs into" HP Operations Manager, extending the managed domain. Through the Data Protector integration, which is implemented as an HP Operations Manager SMART Plug-In, a user can have an arbitrary number of Data Protector Cell Managers monitored as an extension to HP Operations Manager.

I

ICDA
(EMC Symmetrix specific term) EMC's Symmetrix Integrated Cached Disk Arrays (ICDA) is a disk array device that combines a set of physical disks, a number of FWD SCSI channels, an internal cache memory, and control and diagnostic software commonly referred to as the microcode.

IDB
The Data Protector Internal Database. IDB is an embedded database located on the Cell Manager and keeps information regarding which data was backed up, to which media it was backed up, how backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on.

IDB recovery file
An IDB file (obrindex.dat) with information about IDB backups, media, and devices used for the backup. This information can significantly simplify IDB recovery. It is recommended to relocate the file, together with IDB transaction logs, to a separate physical disk from other IDB directories, and, additionally, to make an additional copy of the file.

importing media
A process that re-reads all data about backup sessions which are on the medium back into the IDB. This then allows for fast and convenient access to the data on the media.
See also exporting media.

incremental (re)-establish
(EMC Symmetrix specific term) A BCV or SRDF control operation. In BCV control operations, an incremental establish causes the BCV device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired. In SRDF control operations, an incremental establish causes the target (R2) device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.

incremental backup
A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, which enables detailed control of restore chain length.
See also backup types.

incremental backup
(Microsoft Exchange Server specific term) A backup of the Microsoft Exchange Server data that has changed since the last full or incremental backup. With the incremental backup, only the transaction log files are backed up.
See also backup types.

incremental mailbox backup
An incremental mailbox backup backs up all the changes made to the mailbox after the last backup of any type.

incremental restore
(EMC Symmetrix specific term) A BCV or SRDF control operation. In BCV control operations, an incremental restore reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are updated with only the data that was written to

the BCV device during the time of the original pair split, and the data that was written to the standard device during the split is overwritten with data from the BCV mirror. In SRDF control operations, an incremental restore reassigns a target (R2) device as the next available mirror of the source (R1) device in the pair. However, the source (R1) devices are updated with only the data that was written to the target (R2) device during the time of the original pair split, and the data that was written to the source (R1) device during the split is overwritten with data from the target (R2) mirror.

incremental ZDB A filesystem ZDB-to-tape or ZDB-to-disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape.
See also full ZDB.

incremental1 mailbox backup An incremental1 mailbox backup backs up all the changes made to the mailbox after the last full backup.

Inet A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users.
See also Key Management Service and Site Replication Service.

Informix Server *(Informix Server specific term)* Refers to Informix Dynamic Server.

initializing *See* formatting.

Installation Server A computer system that holds a repository of the Data Protector installation packages for a specific architecture. The Installation Server is used for remote installation of Data Protector clients. In mixed environments at least two Installation Servers are needed: one for UNIX systems and one for Windows systems.

instant recovery *(ZDB specific term)* A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape session, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore from tape. Depending on the application or database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery.
See also replica, zero downtime backup (ZDB), ZDB to disk, and ZDB to disk+tape.

integration object A backup object of a Data Protector integration, such as Oracle or SAP DB.

Internet Information Services (IIS) *(Windows specific term)* Microsoft Internet Information Services is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

ISQL *(Sybase specific term)* A Sybase utility used to perform system administration tasks on Sybase SQL Server.

J

Java GUI Client The Java GUI Client is a component of the Java GUI that contains only user interface related functionalities (the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface) and requires connection to the Java GUI Server to function.

Java GUI Server The Java GUI Server is a component of the Java GUI that is installed on the Data Protector Cell Manager system. The Java GUI Server receives requests from the Java GUI Client, processes them and then sends the responses back to the Java GUI Client. The communication is done through Hypertext Transfer Protocol (HTTP) on port 5556.

jukebox *See* library.

jukebox device A device consisting of multiple slots used to store either optical or file media. When being used to store file media, the jukebox device is known as the “file jukebox device”.

K

Key Management Service
(Microsoft Exchange Server specific term) The Microsoft Exchange Server service that provides encryption functionality for enhanced security.
See also Information Store and Site Replication Service.

keychain
A tool that eliminates the supply of a passphrase manually when decrypting the private key. It needs to be installed and configured on the Installation Server if you perform remote installation using secure shell.

keystore
All encryption keys are centrally stored in the keystore on the Cell Manager and administered by the Key Management Server (KMS).

KMS
Key Management Server (KMS) is a centralized service that runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started as soon as Data Protector is installed on the Cell Manager.

L

LBO
(EMC Symmetrix specific term) A Logical Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as one entity and can only be restored as a whole.

LDEV
(HP P9000 XP Disk Array Family specific term) A logical partition of a physical disk of a disk array of the HP P9000 XP Disk Array Family. An LDEV is the entity that can be replicated using the split-mirror or snapshot functionality of such disk array.
See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and replica.

library
Also called autochanger, jukebox, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to media. The library can contain multiple drives.

lights-out operation or unattended operation
A backup or restore operation that takes place outside of normal business hours without an operator. This implies that no operator personnel is present to work with the backup application or service mount requests, for example.

LISTENER.ORA
(Oracle specific term) An Oracle configuration file that describes one or more Transparent Network Substrate (TNS) listeners on a server.

load balancing
By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery
Remote recovery is performed if all Media Agent hosts specified in the SRD file are accessible. If any of them fails, the disaster recovery process fails over to the local mode. This means that the target system is searched for locally attached devices. If only one device is found, it is automatically used. Otherwise, Data Protector prompts you to select the device, which will be used for restore.

local continuous replication
(Microsoft Exchange Server specific term) Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying.

An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal.

A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) as a normal storage group.

See also cluster continuous replication and Exchange Replication Service.

lock name You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script *(Informix Server UNIX specific term)* A script provided by ON-Bar that you can use to start backing up logical log files when Informix Server issues a logfull event alarm. The Informix Server `ALARMPROGRAM` configuration parameter defaults to the *`INFORMIXDIR`*`/etc/log_full.sh`, where *`INFORMIXDIR`* is the Informix Server home directory. If you do not want logical logs to be backed up continuously, set the `ALARMPROGRAM` configuration parameter to *`INFORMIXDIR`*`/etc/no_log.sh`.

logging level The logging level determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings influence the IDB growth, backup speed, and the convenience of browsing data for restore.

logical-log files This applies to online database backup. Logical-log files are files in which modified data is first stored before being flushed to disk. In the event of a failure, these logical-log files are used to roll forward all transactions that have been committed as well as roll back any transactions that have not been committed.

login ID *(Microsoft SQL Server specific term)* The name a user uses to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

login information to the Oracle Target Database *(Oracle and SAP R/3 specific term)* The format of the login information is *`user_name`*`/`*`password`*`@`*`service`*, where:

- *`user_name`* is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights.
- *`password`* must be the same as the password specified in the Oracle password file (`orapwd`), which is used for authentication of users performing database administration.
- *`service`* is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database *(Oracle specific term)* The format of the login information to the Recovery (Oracle) Catalog Database is *`user_name`*`/`*`password`*`@`*`service`*, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the Oracle target database. In this case, *`service`* is the name of the service to the Recovery Catalog Database, not the Oracle target database.

Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API *(Lotus Domino Server specific term)* An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

M

Magic Packet *See* Wake ONLAN.

mailbox *(Microsoft Exchange Server specific term)* The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

mailbox store *(Microsoft Exchange Server specific term)* A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text `.edb` file and a streaming native internet content `.stm` file.

Main Control Unit (MCU)
(HP P9000 XP Disk Array Family specific term) An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP or HP CA+BC P9000 XP configuration and acts as a master device.
See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

make_net_recovery
`make_net_recovery` is an Ignite-UX command, which allows you to create a recovery archive over the network onto the Ignite-UX server or any other specified system. The target system can be recovered across subnets after booting either from a bootable tape created by the Ignite-UX `make_boot_tape` command or the system boots directly from the Ignite-UX server. Booting directly from the Ignite-UX server can be automated with the Ignite-UX `bootsys` command or interactively specified on the boot console.

make_tape_recovery
`make_tape_recovery` is a command on Ignite-UX which creates a bootable recovery (installation) tape, customized for your system and enables you unattended disaster recovery by connecting the backup device directly to the target system and booting the target system from the bootable recovery tape. The backup device has to be locally connected to the client during the creation of the archive and recovery of the client.

Manager-of-Managers (MoM)
See MoM.

MAPI
(Microsoft Exchange Server specific term) The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

MCU
See Main Control Unit (MCU).

Media Agent
A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore or object verification session, a Media Agent locates data on the backup medium and sends it to the Disk Agent for processing. For a restore session, the Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

media allocation policy
Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.

media condition
The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of read and write errors with tape media. Media need to be replaced when they are marked as POOR.

media condition factors
The user-assigned age threshold and overwrite threshold used to determine the state of a medium.

media label
A user-defined identifier used to describe a medium.

media location
A user-defined physical location of a medium, such as "building 4" or "off-site storage".

media management session
A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.

media pool
A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

media set
The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.

media type
The physical type of media, such as DDS or DLT.

media usage policy
The media usage policy controls how new backups are added to the already used media. It can be `Appendable`, `Non-Appendable`, or `Appendable for incrementals only`.

medium ID
A unique identifier assigned to a medium by Data Protector.

merging
This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored.
See also overwrite.

Microsoft Exchange Server
A “client-server” messaging and a workgroup system that offers a transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

Microsoft Management Console (MMC)
(Windows specific term) An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.

Microsoft SQL Server
A database management system designed to meet the requirements of distributed "client-server" computing.

Microsoft Volume Shadow Copy Service (VSS)
A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets.
See also shadow copy, shadow copy provider, replica, and writer.

mirror *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)*
See target volume.

mirror rotation *(HP P9000 XP Disk Array Family specific term)*
See replica set rotation.

mirror unit (MU) number
(HP P9000 XP Disk Array Family specific term) A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family.
See also first-level mirror.

mirrorclone
(HP P6000 EVA Disk Array Family specific term) A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.

MMD
The Media Management Daemon process (service) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.

MMDB
The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells.
See also CMMDB and CDB.

MoM
Several cells can be grouped together and managed from a central cell. The management system of the central cell is the Manager-of-Managers (MoM). The cells are called MoM clients. The MoM enables you to configure and manage multiple cells from a central point.

mount point
The access point in a directory structure for a disk or logical volume, for example `/opt` or `d:`. On UNIX, the mount points are displayed using the `bdf` or `df` command.

mount request
A screen prompt that tells you to insert a specific medium into a device. Once you respond to the mount request by providing the required medium and confirm the mount request, the session continues.

MSM
The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.

multisnapping
(HP P6000 EVA Disk Array Family specific term) Simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot.
See also snapshot.

O

OBDR capable device A device that can emulate a CD-ROM drive loaded with a bootable disk and can thus be used as a backup or boot device for disaster recovery purposes.

obdrindex.dat *See* IDB recovery file.

object *See* backup object.

object consolidation The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.

object consolidation session A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.

object copy A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

object copy session A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.

object copying The process of copying selected object versions to a specific media set. You can select object versions from one or several backup sessions to be copied.

object ID *(Windows specific term)* The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

object mirror A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

object mirroring The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

object verification The process of verifying the data integrity of backup objects, from the Data Protector point of view, and the ability of Data Protector to deliver them to the required destination. The process can be used to provide a level of confidence in the ability to restore object versions created by backup, object copy, or object consolidation sessions.

object verification session A process that verifies the data integrity of specified backup objects or object versions and the ability of selected Data Protector network components to deliver them to a specified host. Object verification sessions can be run interactively, or as specified in automated post-backup, or scheduled specifications.

offline backup A backup during which an application database cannot be used by the application. In an offline backup session, the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the time period of the data replication process. For instance, for backup to tape, until streaming of data to the tape is finished. Normal database operation is resumed before potential post-backup operations are started.
See also zero downtime backup (ZDB) and online backup.

offline recovery Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Recovery of the Cell Manager is always offline.

offline redo log *See* archived redo log.

ON-Bar *(Informix Server specific term)* A backup and restore system for Informix Server. ON-Bar enables you to create a copy of your Informix Server data and later restore the data. The ON-Bar backup and restore system involves the following components:

- the `onbar` command
- Data Protector as the backup solution
- the XBSA interface
- ON-Bar catalog tables, which are used to back up dbobjects and track instances of dbobjects through multiple backups.

ONCONFIG *(Informix Server specific term)* An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, Informix Server uses the configuration values from the `onconfig` file in the directory *`INFORMIXDIR`*`\etc` (on Windows) or *`INFORMIXDIR`*`/etc/` (on UNIX).

online backup A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period of the data replication process. For instance, for backup to tape, until streaming of data to tape is finished. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. Normal database operation is resumed before potential post-backup operations are started.

In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored.

See also zero downtime backup (ZDB) and offline backup.

online recovery Online recovery is performed when Cell Manager is accessible. In this case, most of the Data Protector] functionalities are available (Cell Manager runs the session, restore sessions are logged in the IDB, you can monitor the restore progress using the GUI, and so on).

online redo log *(Oracle specific term)* Redo logs that have not been archived, but are either available to the instance for recording database activity or are filled and waiting to be archived or reused.
See also archived redo log.

Oracle Data Guard *(Oracle specific term)* Oracle Data Guard is Oracle's primary disaster recovery solution. Oracle Data Guard is able to maintain up to nine standby databases, each of which is a real-time copy of the production (primary) database, to protect against corruptions, data failures, human errors, and disasters. If a failure occurs on the production (primary) database, then a failover to one of the standby databases which becomes the new primary database is possible. In addition, planned downtime for maintenance can be reduced because the production processing can be moved from the current primary database to a standby database and back quickly.

Oracle instance *(Oracle specific term)* Each installation of an Oracle database on one or more systems. One computer system can have several instances of a database running.

ORACLE_SID *(Oracle specific term)* A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired *`ORACLE_SID`*. The *`ORACLE_SID`* is included in the CONNECT DATA parts of the connect descriptor in a `TNSNAMES.ORA` file and in the definition of the TNS listener in the `LISTENER.ORA` file.

original system The system configuration backed up by Data Protector before a computer disaster hits the system.

overwrite An option that defines one mode to resolve file conflicts during restore. All files are restored from a backup even if they are older than existing files.
See also merging.

ownership Backup ownership affects the ability of users to see and restore data. Each backup session and all the data backed up within it is assigned an owner. The owner can be the user that starts an interactive backup, the account under which the CRS process is running, or the user specified as the owner in the backup specification options.

If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.

If a modified backup specification is started by a user, the user is the owner unless the following is true:

- The user has the Switch Session Ownership user right.
- The backup session owner is explicitly defined in the backup specification, where the username, group or domain name, and the system name are specified.

If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.

If a backup is scheduled on a Windows Cell Manager, the session owner is the user specified during the installation, unless the above conditions are true.

When copying or consolidating objects, by default the owner is the user who starts the operation, unless a different owner is specified in the copy or consolidation specification.

P

P1S file P1S file contains information on how to format and partition all disks installed in the system during Enhanced Automated Disaster Recovery (EADR). It is created during full backup and is saved on backup medium and on Cell Manager into the directory *Data_Protector_program_data*\Config\Server\dr\p1s (Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012), *Data_Protector_home*\Config\Server\dr\p1s (other Windows systems), or /etc/opt/omni/server/dr/p1s (UNIX systems) with the filename recovery.p1s.

package *(MC/ServiceGuard and Veritas Cluster specific term)* A collection of resources (for example volume groups, application services, IP names, and addresses) that are needed to run a specific cluster-aware application.

pair status *(HP P9000 XP Disk Array Family specific term)* The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP P9000 XP Agent:

- PAIR – The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty.
- SUSPENDED – The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time.
- COPY – The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.

parallel restore Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism The concept of reading multiple data streams from an online database.

phase 0 of disaster recovery Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.

phase 1 of disaster recovery Installation and configuration of DR OS, establishing previous storage structure.

phase 2 of disaster recovery Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.

phase 3 of disaster recovery Restoration of user and application data.

physical device A physical unit that contains either a drive or a more complex unit such as a library.

post-exec A backup option that executes a command or script after the backup of an object or after the entire session completes. Post-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.
See also pre-exec.

pre- and post-exec commands Pre- and post-exec commands are used to perform additional action before and after a backup or restore session. They are not supplied by Data Protector. You need to create your own commands. They can be written as executables or batch files on Windows and as shell scripts on UNIX.

pre-exec A backup option that executes a command or script before the backup of an object or before the entire session is started. Pre-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.
See also post-exec.

prealloc list A subset of media in a media pool that specifies the order in which media are used for backup.

primary volume (P-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU).
See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection *See* data protection and also catalog protection.

public folder store *(Microsoft Exchange Server specific term)* The part of the Information Store that maintains information in public folders. A public folder store consists of a binary rich-text `.edb` file and a streaming native internet content `.stm` file.

public/private backed up data When configuring a backup, you can select whether the backed up data will be:

- public, that is visible (and accessible for restore) to all Data Protector users
- private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

R

RAID Redundant Array of Independent Disks.

RAID Manager Library *(HP P9000 XP Disk Array Family specific term)* A software library that is used for accessing the configuration, status, and performance measurement data of a P9000 XP Array storage system, and for invoking operations on the disk array. It translates function calls into sequences of low-level SCSI commands.
See also HP P9000 XP Agent.

RAID Manager P9000 XP *(HP P9000 XP Disk Array Family specific term)* A software application that provides a command-line interface to disk arrays of the HP P9000 XP Disk Array Family. It offers an extensive set of commands for reporting and controlling the status of a P9000 XP Array storage system, and for performing various operations on the disk array.

rawdisk backup *See* disk image backup.

RCU *See* Remote Control Unit (RCU).

RDBMS Relational Database Management System.

RDF1/RDF2 *(EMC Symmetrix specific term)* A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices.

RDS The Raima Database Server process (service) runs on the Data Protector Cell Manager and manages the IDB. The process is started when Data Protector is installed on the Cell Manager.

Recovery Catalog *(Oracle specific term)* A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about:

- The physical schema of the Oracle target database
- Data file and archived log backup sets
- Data file copies
- Archived Redo Logs
- Stored scripts

Recovery Catalog Database *(Oracle specific term)* An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

recovery files *(Oracle specific term)* Recovery files are Oracle specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces.
See also flash recovery area.

Recovery Manager (RMAN) *(Oracle specific term)* An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

RecoveryInfo When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume, and network configuration). This information is needed for disaster recovery.

recycle or unprotect A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.

redo log *(Oracle specific term)* Every Oracle database has a set of two or more redo log files. The set of redo log files for the database is known as the database's redo log. Oracle uses the redo log to record all changes made to data.

Remote Control Unit (RCU) *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.

Removable Storage Management Database *(Windows specific term)* A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications to access and share the same media resources.

reparse point *(Windows specific term)* A system-controlled attribute that can be associated with any directory or file. The value of a reparse attribute can have user-controlled data. The format of the data is understood by the application that stored the data and a filesystem filter that was installed to interpret the data and process such files. Whenever the filesystem encounters a file with a reparse point, it attempts to find the filesystem filter associated with the data format.

replica *(ZDB specific term)* An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware or software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror or snapclone), or a virtual copy (for example, a snapshot). From perspective of a basic operating system, the complete physical disk containing backup objects is replicated. However, if a volume manager is used on UNIX, the whole volume or disk group containing a backup object (logical volume) is replicated. If partitions are used on Windows, the whole physical volume containing the selected partition is replicated.
See also snapshot, snapshot creation, split mirror, and split mirror creation.

replica set *(ZDB specific term)* A group of replicas, all created using the same backup specification.
See also replica and replica set rotation.

replica set rotation *(ZDB specific term)* The use of a replica set for regular backup production: Each time the same backup specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set.
See also replica and replica set.

restore chain Backup images that are needed to restore a backed up object to the state it was in at the selected point in time. In general, a restore chain of an object consists of its full backup image and one or more related incremental backup images.

restore session A process that copies data from backup media to a client.

resync mode *(HP P9000 XP Disk Array Family VSS provider specific term)* One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL.
See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), mirror unit (MU) number, and replica set rotation.

RMAN *(Oracle specific term)* *See* Recovery Manager.

RSM The Data Protector Restore Session Manager controls restore and object verification sessions. This process always runs on the Cell Manager system.

RSM *(Windows specific term)* Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.

S

SAPDBA *(SAP R/3 specific term)* An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.

scanning A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device if someone has manually manipulated media without using Data Protector to eject or enter, for example.

Scheduler A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.

secondary volume (S-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration.
See also primary volume (P-VOL) and Main Control Unit (MCU).

session *See* backup session, media management session, and restore session.

session ID An identifier of a backup, restore, object copy, object consolidation, object verification, or media management session, consisting of the date when the session ran and a unique number.

session key This environment variable for the pre-exec and post-exec script is a Data Protector unique identification of any session, including preview sessions. The session key is not recorded in the database, and it is used for specifying options for the `omnimnt`, `omnistat`, and `omniabort` commands.

shadow copy *(Microsoft VSS specific term)* A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant.
See also Microsoft Volume Shadow Copy Service and replica.

shadow copy provider *(Microsoft VSS specific term)* An entity that performs the work on creating and representing the volume shadow copies. Providers own the shadow copy data and expose the shadow copies. Providers can be software (for example, system providers) or hardware (local disks, disk arrays).
See also shadow copy.

shadow copy set *(Microsoft VSS specific term)* A collection of shadow copies created at the same point in time.
See also shadow copy and replica set.

shared disks A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

SIBF The Serverless Integrations Binary Files (SIBF) is a part of the IDB that stores raw NDMP metadata. This data is necessary to perform restore of NDMP objects.

Site Replication Service *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server 2003 service that permits compatibility with Microsoft Exchange Server 5.5 by emulating the Exchange Server 5.5 directory service.
See also Information Store and Key Management Service.

slot A mechanical position in a library. Each slot can hold a medium, such as a DLT tape. Data Protector references each slot with a number. To read a medium, a robotic mechanism moves the medium from a slot into the drive.

smart copy *(VLS specific term)* A copy of the backed up data created from the virtual tape to the physical tape library. The smart copy process allows Data Protector to distinguish between the source and the target medium thus enabling media management.
See also Virtual Library System (VLS).

smart copy pool *(VLS specific term)* A pool that defines which destination library slots are available as smart copy targets for a specified source virtual library.
See also Virtual Library System (VLS) and smart copy.

SMB *See* split mirror backup.

SMBF The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, restore, object copy, object consolidation, object verification, and media management sessions. One binary file is created per session. The files are grouped by year and month.

SMI-S Agent (SMISA) *See* HP P6000 EVA SMI-S Agent.

snapshot *(HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP P10000 Storage Systems specific term)* A type of target volumes created using a specific replication technology. Depending on the disk array model and the chosen replication technique, a range of snapshot types with different characteristics is available. Basically, each snapshot may be either a virtual copy, still reliant upon the contents of the source volume, or an independent duplicate (clone) of the source volume.
See also replica and snapshot creation.

snapshot backup *See* ZDB to tape, ZDB to disk, and ZDB to disk+tape.

snapshot creation *(HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP P10000 Storage Systems specific term)* A replica creation process in which copies of the selected source volumes are created using storage virtualization technology. Such a replica is considered to be created at a particular point in time, and is immediately available for use. However, with certain snapshot types, a background data copying process continues to run on the disk array after the moment of the replica creation.
See also snapshot.

source (R1) device *(EMC Symmetrix specific term)* An EMC Symmetrix device that participates in SRDF operations with a target (R2) device. All writes to this device are mirrored to a target (R2) device in a remote EMC Symmetrix unit. An R1 device must be assigned to an RDF1 group type.
See also target (R2) device.

source volume *(ZDB specific term)* A storage volume containing data to be replicated.

sparse file A file that contains data with portions of empty blocks. Examples are: a matrix in which some or much of the data contains zeros, files from image applications, and high-speed databases. If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror *(EMC Symmetrix Disk Array and HP P9000 XP Disk Array Family specific term)* A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes.
See also replica and split mirror creation.

split mirror backup *(EMC Symmetrix specific term)* *See* ZDB to tape.

split mirror backup *(HP P9000 XP Disk Array Family specific term)* *See* ZDB to tape, ZDB to disk, and ZDB to disk+tape.

split mirror creation *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes.
See also split mirror.

split mirror restore *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards. Individual backup objects or complete sessions can be restored using this method.
See also ZDB to tape, ZDB to disk+tape, and replica.

sqlhosts file or registry *(Informix Server specific term)* An Informix Server connectivity information file (on UNIX) or registry (on Windows) that contains the names of each of the database servers and any aliases to which the clients on a host computer can connect.

SRD file *(disaster recovery specific term)* A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows or Linux system and stored on the Cell Manager. It contains system information required for installing and configuring the operating system on the target system in the case of a disaster.
See also target system.

SRDF *(EMC Symmetrix specific term)* The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.

SSE Agent (SSEA) *See* HP P9000 XP Agent.

sst.conf file The file `/usr/kernel/drv/sst.conf` is required on each Data Protector Solaris client to which a multi-drive library device is connected. It must contain an entry for the SCSI address of the robotic mechanism of each library device connected to the client.

st.conf file The file `/kernel/drv/st.conf` is required on each Data Protector Solaris client with a backup device connected. It must contain device information and a SCSI address for each backup drive connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

stackers Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

standalone file device A file device is a file in a specified directory to which you back up data.

Storage Group *(Microsoft Exchange Server specific term)* A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.

storage volume *(ZDB specific term)* An object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, filesystems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

StorageTek ACS library *(StorageTek specific term)* Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.

switchover *See* failover.

Sybase Backup Server API *(Sybase specific term)* An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

Sybase SQL Server *(Sybase specific term)* The server in the Sybase "client-server" architecture. Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

SYMA *See* EMC Symmetrix Agent.

synthetic backup A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

synthetic full backup The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

System Backup to Tape *(Oracle specific term)* An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases *(Sybase specific term)* The four system databases on a newly installed Sybase SQL Server are the:

- master database (master)
- temporary database (tempdb)
- system procedure database (sybsystemprocs)
- model database (model).

System Recovery Data file *See* SRD file.

System State *(Windows specific term)* The System State data comprises the Registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory services and the SYSVOL directory are also contained in the System State data. If the server is running the Cluster service, the System State data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

system volume/disk/partition A volume/disk/partition containing operating system files. Microsoft terminology defines the system volume/disk/partition as the volume/disk/partition containing files required for the initial step of the boot process.

SysVol *(Windows specific term)* A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

T

tablespace A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

tapeless backup *(ZDB specific term)* *See* ZDB to disk.

target (R2) device *(EMC Symmetrix specific term)* An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type.
See also source (R1) device.

target database *(Oracle specific term)* In RMAN, the target database is the database that you are backing up or restoring.

target system *(disaster recovery specific term)* A system after a computer disaster has occurred. The target system is typically in a non-bootable state and the goal of disaster recovery is to restore this system to the original system configuration. The difference between a faulty system and a target system is that a target system has all faulty hardware replaced.

target volume *(ZDB specific term)* A storage volume to which data is replicated.

Terminal Services *(Windows specific term)* Windows Terminal Services provide a multi-session environment that allows clients to access a virtual Windows desktop session and Windows-based programs running on the server.

thread *(Microsoft SQL Server specific term)* An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

TimeFinder *(EMC Symmetrix specific term)* A business continuation process that creates an instant copy of single or multiple Symmetrix Logical Devices (SLDs). The instant copy is created on specially preconfigured SLDs called BCVs and is accessible via a separate device address to the system(s).

TLU Tape Library Unit.

TNSNAMES.ORA *(Oracle and SAP R/3 specific term)* A network configuration file that contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

transaction A mechanism for ensuring that a set of actions is treated as a single unit of work. Databases use transactions to keep track of database changes.

transaction backup Transaction backups generally use fewer resources than database backups, so they can be created more frequently than database backups. By applying transaction backups, you can recover the database to a specific point in time prior to when a problem occurred.

transaction backup *(Sybase and SQL specific term)* A backup of the transaction log providing a record of changes made since the last full or transaction backup.

transaction log backup Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.

transaction log files Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.

transaction log table *(Sybase specific term)* A system table in which all changes to the database are automatically recorded.

transaction logs *(Data Protector specific term)* Keep track of IDB changes. The archiving of transaction logs should be enabled to prevent you from losing the transaction log files that are created after the last IDB backup and are necessary for IDB recovery.

transportable snapshot *(Microsoft VSS specific term)* A shadow copy that is created on the application system and can be presented to the backup system where a backup can be performed.
See also Microsoft Volume Shadow Copy Service (VSS).

TSANDS.CFG file *(Novell NetWare specific term)* A file that allows you to specify the names of containers where you want backups to begin. It is a text file located in the `SYS:SYSTEM\TSA` directory on the server where `TSANDS.NLM` is loaded.

U

UIProxy The Java GUI Server (`UIProxy` service) runs on the Data Protector Cell Manager. It is responsible for communication between the Java GUI Client and the Cell Manager, moreover, it performs business logic operations and sends only important information to the client. The service is started as soon as Data Protector is installed on the Cell Manager.

unattended operation *See* lights-out operation.

user account (Data Protector user account) You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

User Account Control (UAC) A security component in Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

user disk quotas NTFS quota-management support enables an enhanced tracking mechanism and control over disk space usage on shared storage volumes. Data Protector backs up user disk quotas on the whole system and for all configured users at a time.

user group Each Data Protector user is member of a User Group. Each User Group has a set of user rights that are given to every user in that User Group. The number of User Groups with their associated user rights can be defined as desired. Data Protector provides three default user groups: admin, operator, and user.

user profile *(Windows specific term)* Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.

user rights User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

user_restrictions file A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than *admin* and *operator*.

V

vaulting media The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

verify A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.

Virtual Controller Software (VCS) *(HP P6000 EVA Disk Array Family specific term)* The firmware that manages all aspects of storage system operation, including communication with HP Command View EVA through the HSV controllers.
See also HP Command View (CV) EVA.

Virtual Device Interface *(Microsoft SQL Server specific term)* This is a Microsoft SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk *(HP P6000 EVA Disk Array Family specific term)* A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array.
See also source volume and target volume.

virtual full backup An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

Virtual Library System (VLS) A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

virtual server A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

virtual tape *(VLS specific term)* An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs.
See also Virtual Library System (VLS) and Virtual Tape Library (VTL).

Virtual Tape Library (VTL) *(VLS specific term)* An emulated tape library that provides the functionality of traditional tape-based storage.
See also Virtual Library System (VLS).

VMware management client *(VMware (Legacy) integration specific term)* The client that Data Protector uses to communicate with VMware Virtual Infrastructure. This can be a VirtualCenter Server system (VirtualCenter environment) or an ESX Server system (standalone ESX Server environment).

volser *(ADIC and STK specific term)* A VOLume SERial number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

volume group A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volume mountpoint *(Windows specific term)* An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

Volume Shadow Copy Service *See* Microsoft Volume Shadow Copy Service (VSS).

VSS *See* Microsoft Volume Shadow Copy Service (VSS).

VSS compliant mode *(HP P9000 XP Disk Array Family VSS provider specific term)* One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching the disks.
See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

VxFS Veritas Journal Filesystem.

VxVM (Veritas Volume Manager) A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.

W

Wake ONLAN Remote power-up support for systems running in power-save mode from some other system on the same LAN.

Web reporting The Data Protector functionality that allows you to view reports on backup, object copy, and object consolidation status and Data Protector configuration using the Web interface.

wildcard character A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

Windows configuration backup Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.

Windows Registry A centralized database used by Windows to store configuration information for the operating system and the installed applications.

WINS server A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.

writer *(Microsoft VSS specific term)* A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.

X

XBSA interface *(Informix Server specific term)* ON-Bar and Data Protector communicate with each other through the X/Open Backup Services Application Programmer's Interface (XBSA).

Z

ZDB *See* zero downtime backup (ZDB).

ZDB database *(ZDB specific term)* A part of the IDB, storing ZDB-related information such as source volumes, replicas, and security information. The ZDB database is used in zero downtime backup, instant recovery, and split mirror restore sessions.
See also zero downtime backup (ZDB).

ZDB to disk *(ZDB specific term)* A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time. Multiple replicas, produced using the same backup specification at different times, can be kept in a replica set. A replica from ZDB to disk can be restored using the instant recovery process.
See also zero downtime backup (ZDB), ZDB to tape, ZDB to disk+tape, instant recovery, and replica set rotation.

ZDB to disk+tape *(ZDB specific term)* A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored using the instant recovery process, the standard Data Protector restore from tape, or with specific disk array families, split mirror restore.
See also zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.

ZDB to tape *(ZDB specific term)* A form of zero downtime backup where data in the replica produced is streamed to a backup medium, typically tape. Instant recovery is not possible from such a backup, so the replica need not be retained on the disk array after backup completion. The backed up data can be restored using standard Data Protector restore from tape. With specific disk array families, split mirror restore can also be used.
See also zero downtime backup (ZDB), ZDB to disk, ZDB to disk+tape, instant recovery, and replica.

zero downtime backup (ZDB) A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation.
See also ZDB to disk, ZDB to tape, ZDB to disk+tape, and instant recovery.

Index

D

J

K

L

T

U

V

W

Z