

HP OpenView Storage Data Protector Installation and Licensing Guide

Manual Edition: February 2006 (build label 249)



Manufacturing Part Number: B6960-90002

Release A.06.00

© Copyright Hewlett-Packard Development Company, L.P.2006.

Legal Notices

©Copyright 2004 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

UNIX® is a registered trademark of The Open Group.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

ARM® is a registered trademark of ARM Limited.

1. Overview of the Installation Procedure

In This Chapter	2
Overview of the Installation Procedure	3
The Concept of the Installation	6
Data Protector Installation DVD-ROMs	8
Choosing the Cell Manager System	10
Choosing the Data Protector User Interface System	12
The Data Protector Graphical User Interface	13

2. Installing Data Protector on Your Network

In This Chapter	16
Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS) . . .	17
Installing a UNIX or Linux Cell Manager	18
Installing a Windows Cell Manager	26
Installing Installation Servers	33
Installing Data Protector Clients	42
Remote Installation of the Data Protector Clients	45
Data Protector Components	54
Installing Windows Clients	58
Installing HP-UX Clients	64
Installing Solaris Clients	67
Installing Linux Clients	74
Installing AIX Clients	79
Installing Siemens Sinix Clients	81
Installing Tru64 Clients	83
Installing SCO Clients	85
Installing a Media Agent to Use the ADIC/GRAU Library or the StorageTek Library	87
Local Installation of the Novell NetWare Clients	96
Local Installation of OpenVMS Clients	103
Installing MPE/iX Clients	110
Local Installation of UNIX and Linux Clients	113
Installing the Data Protector Integration Clients	118
Local Installation	120
Remote Installation	121
Installing Cluster-Aware Integrations	121
Microsoft Exchange Server Clients	121
MS SQL Clients	122

Contents

Sybase Clients	122
Informix Server Clients	122
SAP R/3 Clients	123
SAP DB Clients	123
Oracle Clients	124
DB2 Clients	125
NNM Clients	125
NDMP Clients	126
MS Volume Shadow Copy Clients	126
Lotus Notes/Domino Server Clients	126
EMC Symmetrix Integration	127
HP StorageWorks XP Integration	130
HP StorageWorks Virtual Array Integration	136
HP StorageWorks Enterprise Virtual Array Integration	142
Installing Localized Data Protector User Interface	149
Installing Localized Data Protector User Interface on Windows Systems	149
Installing Localized Data Protector User Interface on UNIX Systems	151
Troubleshooting	152
Installing the Data Protector Single Server Edition	154
Limitations of SSE for Windows	154
Limitations of SSE for HP-UX and Solaris	154
Installing Data Protector Web Reporting	156
Installing Data Protector on MC/ServiceGuard	158
Installing a Cluster-Aware Cell Manager	158
Installing a Cluster-Aware Client	159
Installing Data Protector on Microsoft Cluster Server	160
Installing a Cluster-Aware Cell Manager	160
Installing a Cluster-Aware Client	168
Installing Data Protector Clients on a Veritas Cluster	171
Installing a Client	171
Installing Data Protector Clients on a Novell NetWare Cluster	172
Installing a Client	172

3. Maintaining the Installation

In This Chapter	176
Importing Clients to a Cell	177
Importing an Installation Server to a Cell	179
Importing a Cluster-Aware Client to a Cell	180

Microsoft Cluster Server	180
Other Clusters	181
Exporting Clients from a Cell	184
Security Considerations	187
Security Layers	187
Securing Clients	190
Strict Hostname Checking	197
Start Backup Specification User Right	199
Hiding the Contents of Backup Specifications	200
Host Trusts	200
Monitoring Security Events	201
Verifying Which Data Protector Patches Are Installed	203
Verifying Data Protector Patches Using the GUI	203
Verifying Data Protector Patches Using the CLI	204
Uninstalling Data Protector Software	205
Uninstalling a Data Protector Client	206
Uninstalling the Cell Manager and Installation Server	207
Manual Removal of Data Protector Software on UNIX	214
Changing Data Protector Software Components	216

4. Upgrading to Data Protector A.06.00

In This Chapter	222
Upgrade Overview	223
Upgrade Sequence	224
The Need to Convert File Names in the IDB	225
Upgrading from Data Protector A.05.x	226
Upgrading the UNIX Cell Manager and Installation Server	226
Upgrading the Windows Cell Manager and Installation Server	231
Checking Configuration Changes	235
Upgrading the Clients	237
Upgrading in a MoM Environment	249
Conversion of File Names in the IDB	250
IDB Conversion on a Windows Cell Manager	255
IDB Conversion on a UNIX Cell Manager	257
Upgrading from the Single Server Edition	259
Upgrading from Earlier Versions of SSE to Data Protector A.06.00 SSE	259
Upgrading from Data Protector A.06.00 SSE to Data Protector A.06.00	259
Upgrading from Windows NT to Newer Version of Windows	262

Contents

Upgrading from Solaris 7/8 to Solaris 9	263
Migrating from HP-UX 11.x to HP-UX 11.23	264
MoM Specifics	267
Installation Server Specifics	268
Upgrading the Cell Manager Configured on MC/ServiceGuard	269
Upgrading the Cell Manager Configured on Microsoft Cluster Server	273

5. Data Protector Licensing

In This Chapter	278
Introduction	279
License Checking and Reporting.	280
Cell Manager Related Licenses	280
Entity Based Licenses	281
Capacity Based Licenses	281
Capacity Based Licensing Examples	285
Producing a License Report on Demand	289
Which Licenses Are Available?	290
Password Considerations	292
Data Protector Passwords	293
Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility.	294
Other Ways of Obtaining and Installing Permanent Passwords	296
Verifying the Password	298
Finding the Number of Installed Licenses	299
Moving Licenses to Another Cell Manager System	299
Centralized Licensing.	301

6. Troubleshooting Installation

In This Chapter	304
Name Resolution Problems when Installing the Windows Cell Manager	305
Verifying DNS Connections Within Data Protector Cell.	306
Using the omnichck command	306
Troubleshooting Installation and Upgrade of Data Protector on Windows	309
Problems with Remote Installation of Windows Clients	309
Troubleshooting Installation of the Data Protector Cell Manager on Solaris	310
Troubleshooting Installation of UNIX Clients	311
Verifying Data Protector Client Installation	313
Troubleshooting Upgrade	314

Manual Upgrade Procedure	314
Using Log Files.	315
Local Installation	315
Remote Installation	316
Data Protector Log Files.	316
Creating Installation Execution Traces	318

A. Appendix A

In This Appendix	A-2
Data Protector A.06.00 Product Structure and Licenses.	A-3
Drive and Library Extensions	A-5
Functional Extensions	A-7
Single Server Editions	A-15
License Migration to Data Protector A.06.00 and A.05.10.	A-16
Support Contract Migration.	A-17
Data Protector Cell Configurations	A-19
Data Protector Licensing Forms	A-25

B. Appendix B

In This Appendix	B-2
Installing on HP-UX and Solaris Systems Using Native Tools.	B-3
Installing a Cell Manager on HP-UX Systems Using swinstall.	B-3
Installing the Cell Manager on Solaris Systems Using pkgadd.	B-5
Installing an Installation Server on HP-UX Systems	B-7
Installing an Installation Server on Solaris Systems Using pkgadd.	B-8
Installing the Clients	B-11
Upgrading on HP-UX and Solaris Systems Using Native Tools	B-12
Upgrading Data Protector on HP-UX Systems Using swinstall	B-12
Upgrading Data Protector on Solaris Systems Using pkgadd	B-13
Setting Up the TCP/IP Protocol on Windows Systems	B-15
Installing and Configuring the TCP/IP Protocol on Windows	B-16
Checking the TCP/IP Setup	B-19
Changing the Cell Manager Name	B-21
Changing the Default Port Number	B-23
Preparing a NIS Server	B-24
Using Tape and Robotics Drivers on Windows.	B-26
Creating Device Files (SCSI Addresses) on Windows	B-29
SCSI Robotics Configuration on HP-UX.	B-31

Contents

Creating Device Files on HP-UX	B-36
Setting a SCSI Controller's Parameters	B-39
Finding the Unused SCSI Addresses on HP-UX	B-40
Finding the Unused SCSI Target IDs on Solaris	B-42
Updating the Device and Driver Configuration on a Solaris System	B-43
Updating Configuration Files	B-43
Creating and Checking Device Files	B-46
Finding Unused SCSI Target IDs on a Windows System	B-48
Setting SCSI IDs on an HP StorageWorks 330fx Library	B-49
Connecting Backup Devices	B-50
Connecting an HP StorageWorks 24 Standalone Device	B-54
Connecting an HP StorageWorks DAT Autoloader	B-55
Connecting an HP StorageWorks DLT Library 28/48-Slot	B-57
Connecting a Seagate Viper 200 LTO Ultrium Tape Drive	B-61
Checking the General Media Agent Installation on Novell NetWare	B-64
Identifying the Storage Device.	B-64
Testing the General Media Agent Startup	B-64
Testing the HPUMA.NLM and the HPDEVBRA.NLM Startup	B-67
Installing Data Protector on Microsoft Cluster with Veritas Volume Manager	B-70
Configuration Files Path Changes in Data Protector A.06.00	B-71
Configuration Files on UNIX	B-71
Configuration Files on Windows	B-72
Command Line Changes After Upgrading to Data Protector A.06.00	B-74

C. Appendix C

Using CD-ROMs As the Installation Media	C-2
Data Protector Installation CD-ROMs	C-2
Additional Steps and Tasks When Installing Data Protector From CD-ROMs	C-5

Glossary

Index

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

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

Table 1

Edition History

Part Number	Manual Edition	Product
B6960-90079	May 2003	Data Protector Release A.05.10
B6960-90107	October 2004	Data Protector Release A.05.50
B6960-90002	April 2006	Data Protector Release A.06.00

Conventions

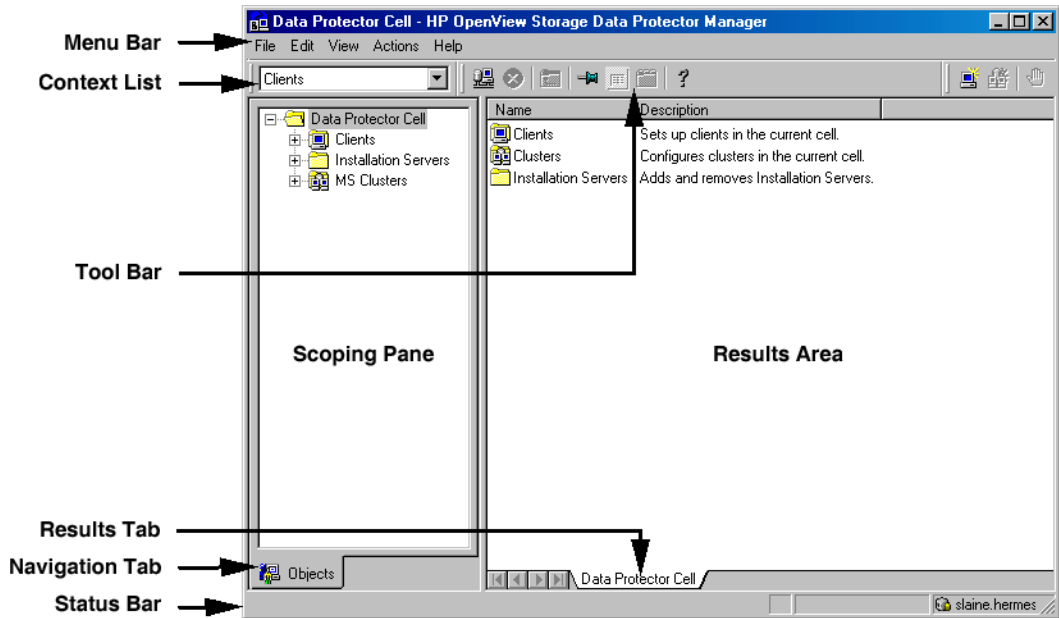
The following typographical conventions are used in this manual.

Table 2

Convention	Meaning	Example
<i>Italic</i>	Book or manual titles, and manual page names	Refer to the <i>HP OpenView Storage Data Protector Integration Guide</i> for more information.
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: rlogin <i>your_name</i> where you supply your login name.
Bold	New terms	The Data Protector Cell Manager is the main ...
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the grep command ...
	File and directory names	/usr/bin/X11
	Process names	Check to see if Data Protector Inet is running.
	Window/dialog box names	In the Backup Options dialog box...
	Text that you must enter	At the prompt, type: ls -l
Keycap	Keyboard keys	Press Return .

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface. Refer to the online Help for information about the Data Protector graphical user interface.

Figure 1 Data Protector Graphical User Interface



Contact Information

General Information

General information about Data Protector can be found at

<http://www.hp.com/go/dataprotector>

Technical Support

Technical support information can be found at the HP Electronic Support Centers at

<http://support.openview.hp.com/support.jsp>

<http://www.hp.com/support>

Information about the latest Data Protector patches can be found at

http://support.openview.hp.com/patches/patch_index.jsp

For information on the Data Protector required patches, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

HP does not support third-party hardware and software. Contact the respective vendor for support.

Documentation Feedback

Your comments on the documentation help us to understand and meet your needs. You can provide feedback at

http://ovweb.external.hp.com/lpe/doc_serv/

Training Information

For information on currently available HP OpenView training, see the HP OpenView World Wide Web site at

<http://www.openview.hp.com/training/>

Follow the links to obtain information about scheduled classes, training at customer sites, and class registration.

Data Protector Documentation

Data Protector documentation comes in the form of manuals and online Help.

Manuals

Data Protector manuals are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the *User Interface* component on Windows or the *OB2-DOCS* component on UNIX. Once installed, the manuals reside in the `<Data_Protector_home>\docs` directory on Windows and in the `/opt/omni/doc/C/` directory on UNIX. You can also find the manuals in PDF format at http://ovweb.external.hp.com/lpe/doc_serv/

HP OpenView Storage Data Protector Concepts Guide

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

HP OpenView Storage Data Protector Installation and Licensing Guide

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

HP OpenView Storage Data Protector Troubleshooting Guide

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

HP OpenView Storage Data Protector Disaster Recovery Guide

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

HP OpenView Storage Data Protector Integration Guide

This manual describes how to configure and use Data Protector to back up and restore various databases and applications. It is intended for backup administrators or operators. There are four versions of this manual:

- *HP OpenView Storage Data Protector Integration Guide for Microsoft Applications: SQL Server, Exchange Server, and Volume Shadow Copy Service*

This manual describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server 2000/2003, Microsoft SQL Server 7/2000/2005, and Volume Shadow Copy Service.

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

This manual describes the integrations of Data Protector with Oracle, SAP R3, and SAP DB.

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

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

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

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

HP OpenView Storage Data Protector Integration Guide for HP OpenView

This manual describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Information Portal, and HP OpenView Reporter. It is intended for backup administrators. It discusses how to use the OpenView applications for Data Protector service management.

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for UNIX

This manual describes how to monitor and manage the health and performance of the Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and HP OpenView Performance (OVP) on UNIX.

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for Windows

This manual describes how to monitor and manage the health and performance of the Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and HP OpenView Performance (OVP) on Windows.

There are two versions of the manual:

- for OVO 7.1x, 7.2x
- for OVO 7.5

HP OpenView Storage Data Protector Zero Downtime Backup Concepts Guide

This manual 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 OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide* and the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide

This manual describes how to configure and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility and TimeFinder, and HP StorageWorks Disk Array XP. 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 OpenView Storage Data Protector Zero Downtime Backup Integration Guide

This manual describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle, SAP R/3, Microsoft Exchange Server 2000/2003, and Microsoft

SQL Server 2000 databases. The manual also describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.

HP OpenView Storage Data Protector MPE/iX System User Guide

This manual describes how to configure MPE/iX clients and how to back up and restore MPE/iX data.

HP OpenView Storage Data Protector Media Operations User's Guide

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

HP OpenView Storage Data Protector Product Announcements, Software Notes, and References

This manual gives a description of new features of HP OpenView Storage Data Protector A.06.00. It also provides information on supported configurations (devices, platforms and online database integrations, SAN, and ZDB), required patches, and limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at http://www.openview.hp.com/products/datapro/spec_0001.html

There are also four other *Product Announcements, Software Notes and References*, which serve a similar purpose for the following:

- OVO UNIX integration
- OVO 7.1x/7.2x Windows integration
- OVO 7.5 Windows integration
- Media Operations

Online Help

Data Protector provides context-sensitive (F1) Help and Help Topics for Windows and UNIX platforms.

Documentation Map

Abbreviations

Abbreviations in the documentation map that follows are explained below. The manual titles are all preceded by the words “HP OpenView Storage Data Protector”

Abbreviation	Manual
CLI	Command Line Interface Reference Guide
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
Help	Online Help
IG-IBM	Integration Guide—IBM Applications
IG-MS	Integration Guide—Microsoft Applications
IG-O/S	Integration Guide—Oracle & SAP
IG-OV	Integration Guide—HP OpenView Service Information Portal/OpenView Reporter
IG-OVOU	Integration Guide—HP OpenView Operations, UNIX
IG-OVOW	Integration Guide—HP OpenView Operations 7.1x, 7.2x, Windows
IG-OVOW	Integration Guide—HP OpenView Operations 7.5, Windows
IG-Var	Integration Guide—Sybase, Network Node Manager & NDMP
Install	Installation and Licensing Guide
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide
PA	Product Announcements, Software Notes, and References

Abbreviation	Manual
Trouble	Troubleshooting Guide
ZDB Admin	ZDB Administrator's Guide
ZDB Concpt	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.

	Help	GS	Concepts				Integration Guides							ZDB			MO			MPE/iX	CLI		
			Install	Trouble	DR	PA	MS	O/S	IBM	Var	OV	OVOU	OVOW	Concept	Admin	IG	GS	User	PA				
Backup	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	
Disaster Recovery	X		X			X																	
Installation/Upgrade	X	X		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		
New features	X						X														X		
Planning strategy	X		X								X				X								
Procedures/Tasks	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			
Restore	X	X	X					X	X	X	X				X	X						X	
Support matrices							X																
Supported configurations															X								
Troubleshooting	X			X	X			X	X	X	X	X				X	X						

Integrations

Look in these manuals for details of the following integrations:

Integration	Guide
HP OpenView Operations (OVO)	IG-OVOU, IG-OVOW
HP OpenView Reporter (OVR)	IG-OV
HP OpenView Reporter Light	IG-OVOW
HP OpenView Service Information Portal (OVSIP)	IG-OV
HP StorageWorks Disk Array XP	all ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	all ZDB
HP StorageWorks Virtual Array (VA)	all ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX System	MPE/iX
Microsoft Exchange Servers	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Servers	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	all ZDB

In This Book

The *HP OpenView Storage Data Protector Installation and Licensing Guide* describes the installation of the Data Protector network product, the prerequisites that must be met before starting the installation procedure, upgrading and licensing.

Audience

The manual is intended for administrators who are 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 OpenView Storage Data Protector Concepts Guide*, which is recommended to fully understand the fundamentals and the model of Data Protector.

Organization

The manual is organized as follows:

- Chapter 1** “Overview of the Installation Procedure” on page 1.
- Chapter 2** “Installing Data Protector on Your Network” on page 15.
- Chapter 3** “Maintaining the Installation” on page 175.
- Chapter 4** “Upgrading to Data Protector A.06.00” on page 221.
- Chapter 5** “Data Protector Licensing” on page 277.
- Chapter 6** “Troubleshooting Installation” on page 303.
- Appendix A** “Appendix A” on page A-1.
- Appendix B** “Appendix B” on page B-1.
- Glossary** Definition of terms used in this manual.



1

Overview of the Installation Procedure

In This Chapter

This chapter provides an overview of the Data Protector installation procedure and introduces the installation concept. The Data Protector Cell Manager and Data Protector user interface are introduced.

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. 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 configuration of the cell.

The **Installation Server** (IS) is a computer or the Cell Manager component that contains Data Protector software repository used for remote client installations. This feature of Data Protector greatly eases the software installation process, particularly for remote clients.

A cell consists of one Cell Manager and usually many clients. A computer system becomes a Data Protector **client** as soon as you install one of the Data Protector software components on it. The client components installed on a system depend on the role of that system in your backup environment. The Data Protector components can be installed either locally on a single system, or distributed among many 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 that have disks to be backed up must have the Data Protector **Disk Agent** component 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. There are two Data Protector Media Agents: the **General Media Agent** and the **NDMP Media Agent**. The NDMP Media Agent is needed only on client systems controlling the backup of an NDMP server (on client systems controlling NDMP dedicated drives). In all other cases the two Media Agents are interchangeable.

Before you install Data Protector on your network, define the following:

- ✓ The system on which the Cell Manager will be installed. See the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for supported operating systems and versions.

Each cell can have only one Cell Manager. You cannot run Data Protector without having a Cell Manager installed.

- ✓ The systems that will be used to access 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 that will have backup devices 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 Server (IS) are available for remote software installation: one for UNIX clients and one for Windows clients. Each must be installed on the platform to which it relates.

The choice of Installation Server computer 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 on the same system (if both are for 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 Solaris system. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for the supported operating system versions.

IMPORTANT

When installing a Data Protector Cell Manager, Installation Server or 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.

When you have determined the roles of the systems in your future Data Protector cell, the installation procedure consists of these general steps:

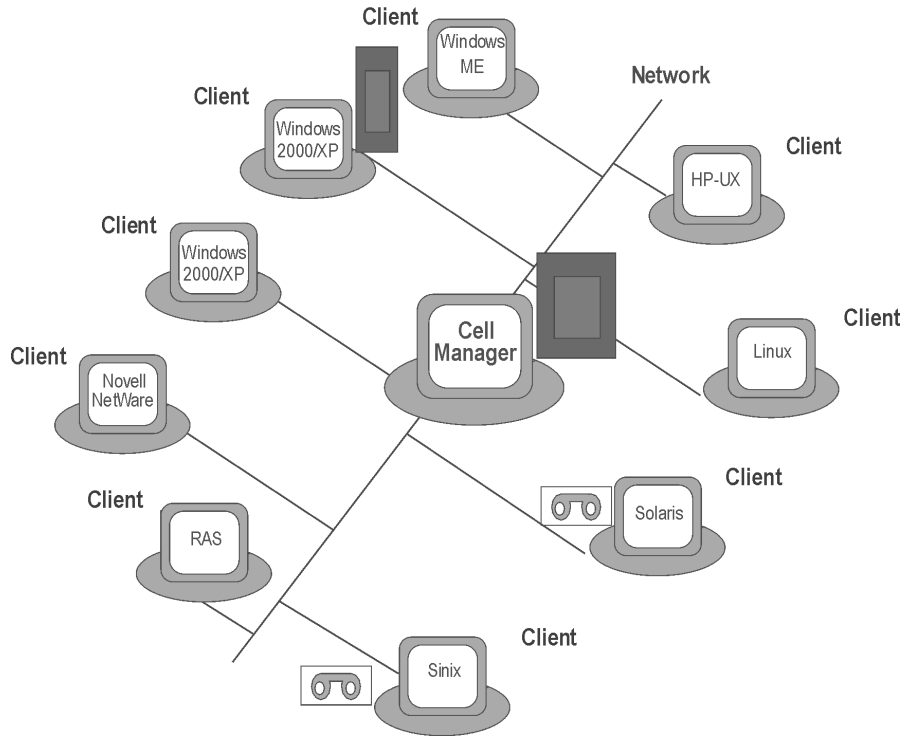
1. Checking the prerequisites for installation.
2. Installing the Data Protector Cell Manager.
3. Installing the Installation Server(s) and the User Interface.
4. Installing client systems either remotely (recommended option, where possible), or locally from the DVD-ROM.

NOTE

You cannot remotely install a Data Protector client on a Windows system after an Installation Server has been already 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, you must select all desired client components and the Installation Server component.

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

Figure 1-1 Data Protector Cell



The Concept of the Installation

Once you have installed the Data Protector Cell Manager, User Interface, and Installation Server(s) (at least one is needed for each platform, UNIX and Windows), you can distribute Data Protector software to clients on operating systems for which remote installation is supported. See the Figure 1-2 on page 8.

Every time you perform 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. Most likely you would install the User Interface on many systems so that you would be able to access the Cell Manager from different locations.

Client software can be distributed to any Windows system, except for Windows Me/XP HE, from an Installation Server for Windows.

Windows Me/XP HE client systems must be installed locally from the Data Protector DVD-ROM for Windows.

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

From an Installation Server for UNIX (for a list of supported platforms, refer to *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*), you can remotely install client software on HP-UX, Solaris, Sinix, Linux, AIX, and other supported UNIX operating systems.

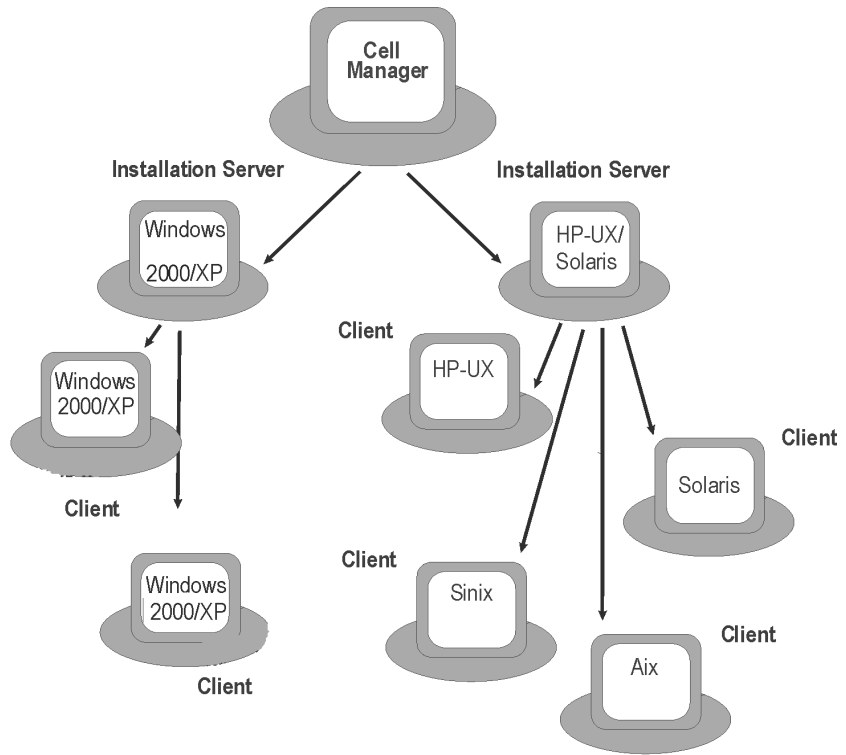
For UNIX operating systems for which remote installation is not supported, or if you do not install an Installation Server for UNIX, you can install UNIX clients locally, from the Data Protector UNIX installation DVD-ROM.

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

For further information on the available installation methods for the various Data Protector clients, refer to “Installing Data Protector Clients” on page 42.

For the procedure for installing UNIX clients locally, refer to “Local Installation of UNIX and Linux Clients” on page 113.

Figure 1-2 Data Protector Installation Concept



Data Protector Installation DVD-ROMs

Data Protector supports various operating systems on several processor architectures. As a consequence, 2 DVD-ROMs are required to cover all platforms. For details which components are found on which DVD-ROM, refer to “Data Protector DVD-ROM List” on page 9.

If you are installing Data Protector from CD-ROMs, see the TBD.

Table 1-1 Data Protector DVD-ROM List

DVD Num.	DVD-ROM Title	Contents
1	HP OpenView Storage Data Protector for UNIX	<ul style="list-style-type: none"> • Cell Manager and Installation Server for HP-UX (PA-RISC, IA64), Solaris, and Linux • Clients for other UNIX systems • Autopass • All English manuals in PDF format (in the DOCS directory) • OpenView Integration Packages • NAS8000 package
2	HP OpenView Storage Data Protector for Windows	<ul style="list-style-type: none"> • Cell Manager and Installation Server for Windows on 32-bit and 64-bit (AMD64/EM-64T) systems • All English manuals in PDF format (in the DOCS directory) • Novell Netware clients • OpenVMS clients • MPE clients • Open File Manager installation package • Product Demo for Windows platforms • Product information • Installation package for Media Operations

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.

Therefore, 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 Solaris platform. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details of the supported versions/releases of these platforms.

✓ 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 down, it is important to choose a very reliable system in your environment for the installation.

✓ Database growth and required disk space

Cell Manager holds the Data Protector Internal Database (IDB). 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 *estimate* is 2% of the disk space used by the backed up data. You can use the `IDB_capacity_planning.xls` table (located on the Data Protector installation medium) to estimate the size of the IDB.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information on planning and managing the size and growth of the database.

Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for requirements on sufficient disk space for the IDB.

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 find out the requirements that your future Cell Manager system must meet, refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17.

Choosing the Data Protector User Interface System

Data Protector provides the GUI and CLI for Windows, HP-UX, and Solaris 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 have several systems on which the user interface runs, and if the environment is a mixed one, on various platforms.

For instance, if you have a mixed UNIX network, and you have 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, due to performance reasons, it is recommended to install the Data Protector GUI interface on all systems that are to be used to control the Data Protector cell.

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

To use the Data Protector GUI functionality on those UNIX Cell Manager platforms where the Data Protector GUI is not supported, use the `omniusers` command to create a remote user account on the Cell Manager. You can then use the created user account on any other system with the Data Protector GUI installed to start the GUI and connect to the Cell Manager. Refer to the `omniusers` man page for details.

See the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details on supported operating system versions/releases for the user interface. For more information on local language support and the usage of non-ASCII characters in file names, refer to *HP OpenView Storage Data Protector Administrator's Guide*.

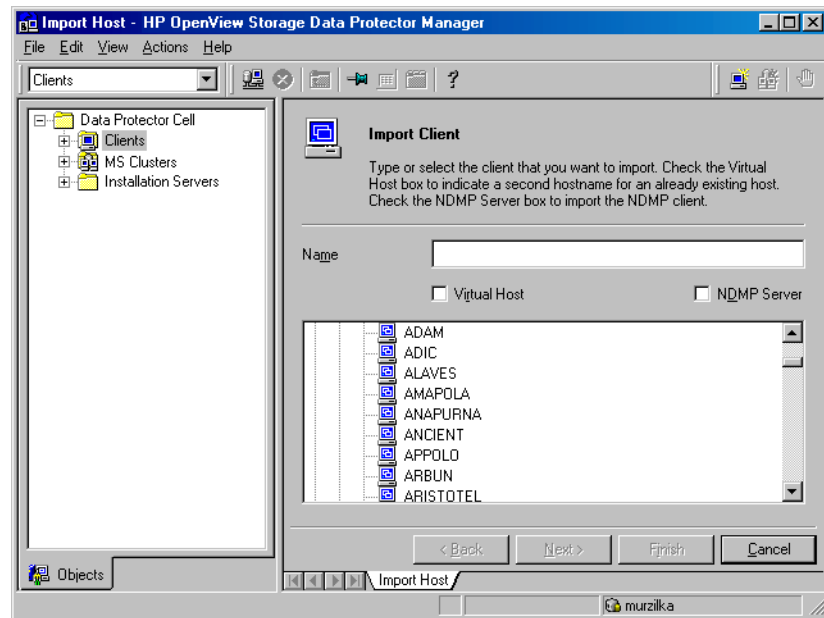
Once you have installed the user interface on a system in the cell, you can remotely access the Cell Manager from that system. You do not have to use the graphical user interface system on the Cell Manager.

The Data Protector Graphical User Interface

The Data Protector GUI is a powerful tool that provides easy access to the Data Protector functionality. The main window contains several views, such as Clients, Users, Devices & Media, Backup, Restore, Copy & Consolidation, 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, a user sees only installation specific messages displayed in the monitor window.

Figure 1-3 Data Protector Graphical User Interface



See also Figure 1 in the Preface, which defines the most important areas of the Data Protector GUI.

NOTE

On UNIX, specific local settings are required on the system where 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. Refer to *HP OpenView Storage Data Protector Administrator's Guide* for details.

2 **Installing Data Protector on Your Network**

In This Chapter

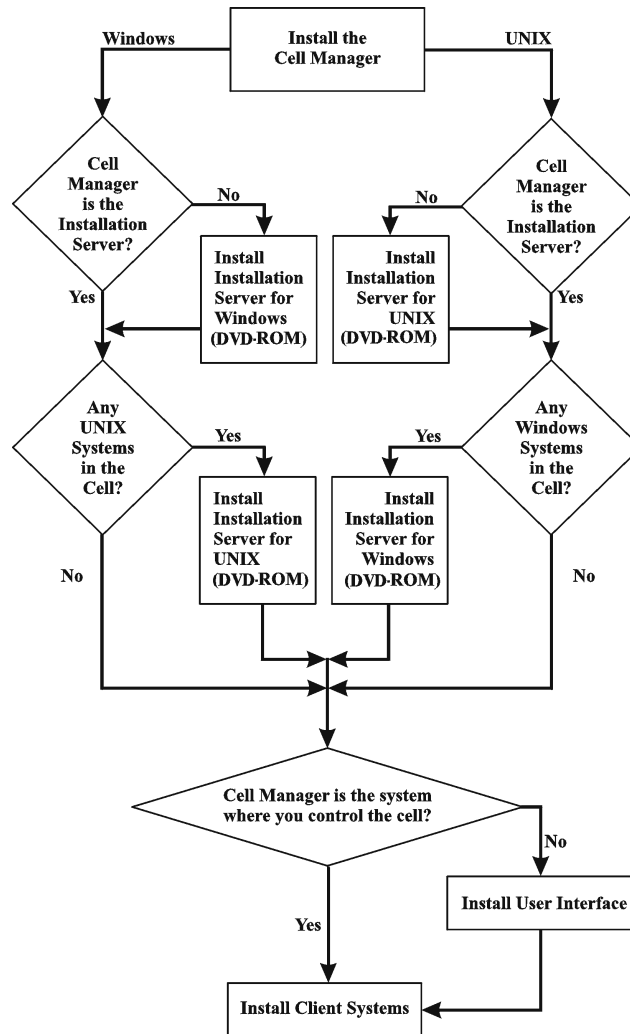
This chapter contains detailed instructions about:

- Installing the Data Protector Cell Manager (CM) and Installation Servers (IS). Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17.
- Installing the Data Protector clients. Refer to “Installing Data Protector Clients” on page 42.
- Installing the localized Data Protector user interface. Refer to “Installing Localized Data Protector User Interface” on page 149.
- Installing the Data Protector Single Server Edition. Refer to “Installing the Data Protector Single Server Edition” on page 154.
- Installing Data Protector Web Reporting. Refer to “Installing Data Protector Web Reporting” on page 156.
- Installing Data Protector on MC/ServiceGuard. Refer to “Installing Data Protector on MC/ServiceGuard” on page 158.
- Installing Data Protector on a Microsoft Cluster Server. Refer to “Installing Data Protector on Microsoft Cluster Server” on page 160.
- Installing Data Protector Clients on a Veritas Cluster. Refer to “Installing Data Protector Clients on a Veritas Cluster” on page 171.
- Installing Data Protector Clients on a Novell NetWare Cluster. Refer to “Installing Data Protector Clients on a Novell NetWare Cluster” on page 172.

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

Refer to the Figure 2-1 for the flow of installation procedure:

Figure 2-1 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.

NOTE

The procedures in this chapter for installing the Cell Manager, Installation Server, and for local installation of clients are written for DVD-ROM installation media. If you are using CD-ROM media, see also the TBD, where a list of CD-ROMS is provided together with the differences in the installation procedure.

Installing a UNIX or Linux Cell Manager

This section provides step-by-step instructions on how to install a UNIX or Linux Cell Manager. If you want to install the Windows Cell Manager only, refer to “Installing a Windows Cell Manager” on page 26.

Prerequisites

- The UNIX or Linux system that will become the Cell Manager must:
 - ✓ Have sufficient disk space for the Data Protector software. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details. You can overcome a shortage of space by installing to linked directories, but you should first refer to “The Installed Directory Structure on HP-UX, Solaris, and Linux” on page 22 and “Allocating More Disk Space for the Cell Manager Installation” on page 25.
 - ✓ Have sufficient disk space (about 2% of the planned data to be backed up) for the IDB. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details. Note that the current IDB design allows the database binary files to be relocated if growth in database size makes it necessary. See the online Help index: “IDB, calculating the size of”.

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

- ✓ Support long filenames. To find out if your file system supports long filenames use the `getconf NAME_MAX <directory>` command.
 - ✓ Have the `inetd` daemon up and running.
 - ✓ Have the port number 5555 (default) free. If this is not the case, refer to “Changing the Default Port Number” on page B-23.
 - ✓ 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. Refer to “Preparing a NIS Server” on page B-24.
 - ✓ The `ksh` shell installed.
- You will need `root` permissions on the target system.

NOTE

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

Cluster-Aware Cell Manager

Additional prerequisites and steps are required for installing a cluster-aware Cell Manager. Refer to “Installing a Cluster-Aware Cell Manager” on page 158.

Setting Kernel Parameters

On HP-UX, it is recommended to set the kernel parameter `maxdsiz` (Max Data Segment Size) to at least 134217728 bytes (128 MB), and the kernel parameter `semnu` (Number of Semaphore Undo Structures) to at least 256. After committing these changes, recompile the kernel and reboot the machine.

On Solaris, it is recommended to set the kernel parameter `shmsys:shminfo_shmmax` (maximum shared memory segment size (SHMMAX)) in `/etc/system` to at least 67108864 bytes (64 MB). After committing this change, reboot the machine.

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 running `omnisetup.sh -CM -IS`.

For a description of the `omnisetup.sh` command, refer to the README file located in the `<Mount_point>/LOCAL_INSTALL` directory on the DVD-ROM or to the *HP OpenView Storage 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, Solaris, or Linux system:

1. Insert and mount the UNIX installation DVD-ROM to a mount point.

For example:

```
mkdir /dvdrom
mount /dev/dsk/c0t0d0 /dvdrom
```

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

- To copy the `DP_DEPOT`, `AUTOPASS`, and `LOCAL_INSTALL` directories, where the installation files are stored, to your local disk, run:

```
mkdir <directory>
cp -r /dvdrom/<platform_dir>/DP_DEPOT <directory>
cp -r /dvdrom/<platform_dir>/AUTOPASS <directory>
cp -r /dvdrom/<platform_dir>/LOCAL_INSTALL <directory>
```

Where `<platform_dir>` is:

<code>hpux_ia</code>	HP-UX 11.23 on IA-64 systems
<code>hpux_pa</code>	HP-UX on PA-RISC systems
<code>linux_x86_64</code>	Linux systems on AMD64/EM64-T
<code>solaris</code>	Solaris systems

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

```
cp -r /dvdrom <dvd_image_dir>
```

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

2. Run the `omnisetup.sh` command.

To run this command from the DVD-ROM, type:

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

To start the installation from disk:

- If you have copied the `DP_DEPOT` directory to your local disk as `<directory>/DP_DEPOT`, go to the directory where the `omnisetup.sh` command is stored, and run:

```
./omnisetup.sh -source <directory> -CM
```

- If you have copied the whole DVD-ROM to `<dvd_image_dir>`, run the `omnisetup.sh` command with the `-CM` parameter:

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

3. **On HP-UX and Solaris**, `omnisetup.sh` prompts you to install or upgrade the HP OpenView 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, refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294. 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, AutoPass is not installed.

NOTE

If you installed the Cell Manager on Solaris 9, remotely install the Disk Agent on the Cell Manager using an Installation Server. This will replace the generic Solaris Disk Agent with the Solaris 9 Disk Agent. Refer to “Remote Installation of the Data Protector Clients” on page 45 or to the `ob2install` man page.

If you want install an Installation Server for UNIX on your Cell Manager, you can do it at this point. Refer to “Installing Installation Servers for UNIX” on page 34 for the required steps.

The Installed Directory Structure on HP-UX, Solaris, and Linux

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

IMPORTANT

If you want 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 must create the links before the installation and ensure that the destination directories exist.

Refer to “Allocating More Disk Space for the Cell Manager Installation” on page 25 for more information.

<code>/opt/omni/bin</code>	All commands
<code>/opt/omni/gui</code>	GUI items
<code>/opt/omni/gui/help</code>	Online Help files
<code>/opt/omni/lbin</code>	Data Protector internal commands
<code>/opt/omni/sbin</code>	Superuser commands
<code>/opt/omni/sbin/install</code>	Installation scripts
<code>/etc/opt/omni</code>	Configuration information
<code>/opt/omni/lib</code>	Shared libraries for compression, data encoding, and device handling
<code>/opt/omni/doc/C</code>	Online documentation (optional)
<code>/var/opt/omni/log and /var/opt/omni/server/log</code>	Log files
<code>/opt/omni/lib/nls/C</code>	Message catalog files
<code>/opt/omni/lib/man</code>	Man pages
<code>/var/opt/omni/tmp</code>	Temporary files

`/var/opt/omni/server/db40` IDB files. Refer to the online Help index: TBD for details.

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:

<code>/sbin/init.d/omni</code>	A script with startup and shutdown procedures.
<code>/sbin/rc1.d/K162omni</code>	A link to the <code>/sbin/init.d/omni</code> script that shuts down Data Protector.
<code>/sbin/rc2.d/S838omni</code>	A link to the <code>/sbin/init.d/omni</code> script that starts up Data Protector.
<code>/etc/rc.config.d/omni</code>	Contains an omni variable defining: omni=1.....Data Protector is automatically stopped and started at system reboot. This is the default option. omni=0.....Data Protector is not automatically stopped and started at system reboot.

Solaris:

<code>/etc/init.d/omni</code>	A script with startup and shutdown procedures.
<code>/etc/rc1.d/K09omni</code>	A link to the <code>/sbin/init.d/omni</code> script that shuts down Data Protector.
<code>/etc/rc2.d/S97omni</code>	A link to the <code>/sbin/init.d/omni</code> script that starts up Data Protector.

Linux:

TBD

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

HP-UX:

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

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

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

`/opt/omni/sbin/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. CRS starts and controls backup and restore sessions in the cell.

`/opt/omni/sbin/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. RDS manages the IDB.

`/opt/omni/sbin/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. MMD manages the device and media management operations.

Setting Environment Variables

The installation procedure for the UNIX and Linux Cell Manager described earlier also installs the Data Protector user interface.

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

Before using the user interface (either the graphical user interface or the command-line interface), you should add the following to your environment variables:

`/opt/omni/bin, /opt/omni/sbin and /opt/omni/sbin` to the `PATH` variable

`/opt/omni/lib/man` to the `MANPATH` variable

`/opt/omni/lib and /opt/omni/lib/arm` to the `LD_LIBRARY_PATH` variable

Before attempting to use the graphical user interface, please ensure that the `DISPLAY` variable and locale are set correctly.

NOTE

If you intend to use the Data Protector user interface to perform backups or restores across platforms, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for the limitations incurred and online Help index: TBD for information on how to customize language settings in the Data Protector GUI.

Allocating More Disk Space for the Cell Manager Installation

You need a considerable amount of disk space to install the UNIX or Linux 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). 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. Example procedures are shown below:

- If there is a disk with enough disk space mounted as `/data_protector`, create the following link for `/opt/omni`:

```
mkdir /data_protector/opt_omni
```

```
ln -s /data_protector/opt_omni /opt/omni
```

Repeat the same operation for any other directories you want to link, for example, `/var/opt/omni` and `/etc/opt/omni`.

- **On HP-UX**, if there is an unmounted filesystem `/dev/vgspare/lvol2` available, proceed as follows:

```
mkdir /opt/omni
```

```
mount /dev/vgspare/lvol2 /opt/omni
```

- **On Solaris**, if there is an unmounted filesystem `/dev/dsk/c0t0d0s0` available, proceed as follows:

```
mkdir /opt/omni
```

```
mount /dev/dsk/c0t0d0s0 /opt/omni
```

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, refer to “Installing Installation Servers for UNIX” on page 34.
2. Install an Installation Server for Windows, if you wish to remotely install software to Windows clients. Refer to “Installing an Installation Server for Windows” on page 37.
3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 42.

Installing a Windows Cell Manager

Prerequisites

The Windows system that will become your Cell Manager must meet the following requirements:

- ✓ Have a supported Windows operating systems installed. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details on supported operating systems for the Cell Manager.
- ✓ Have Microsoft Internet Explorer 5.0 or higher.
- ✓ Have sufficient disk space for the Data Protector Cell Manager software. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details.
- ✓ Have sufficient disk space (about 2% of the backed up data) for the IDB. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details.
- ✓ Have the port number 5555 (default) free. If this is not the case, refer to “Changing the Default Port Number” on page B-23.

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

- ✓ Have a static IP address for the system on which the Cell Manager is to 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. Refer to “Setting Up the TCP/IP Protocol on Windows Systems” on page B-15 for information on installation and configuration of the TCP/IP protocol.
- ✓ Have access to a DVD-ROM drive.

Microsoft Terminal Services Client

- ✓ If you want to install Data Protector on Windows through Microsoft Terminal Services Client, the system you want to install Data Protector on should have 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.

Recommendation

Check if you have Microsoft Installer (MSI) 2.0 prior to installing Data Protector A.06.00. If you have an older version of MSI, Data Protector setup will automatically upgrade it to version 2.0. In this case, Data Protector will display a note at the end of the upgrade, stating that MSI was upgraded. It is highly recommended to restart the system, if MSI was upgraded.

It is recommended that you upgrade your MSI to the version 2.0 before installing Data Protector A.06.00. Consult Microsoft Support for Microsoft Installer 2.0 prerequisites on the various Windows operating systems.

Cluster-Aware Cell Manager

Additional prerequisites and steps are required for installing a cluster-aware Cell Manager. Refer to “Installing a Cluster-Aware Cell Manager” on page 160.

Installation Procedure

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

1. Insert the Windows installation DVD-ROM and run:

32-bit systems: \Windows_other\i386\setup.exe

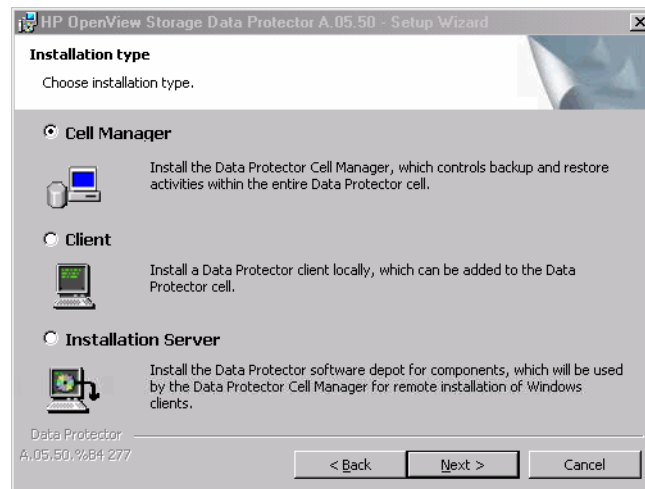
64-bit systems: \Windows_other\x8664\setup.exe

The Data Protector Setup Wizard is displayed.

2. Follow the Setup Wizard and carefully read the license agreement. Click Next to continue, if you accept the terms of the agreement.
3. In the Installation Type page, select Cell Manager and then click Next to install Data Protector Cell Manager software.

Figure 2-2

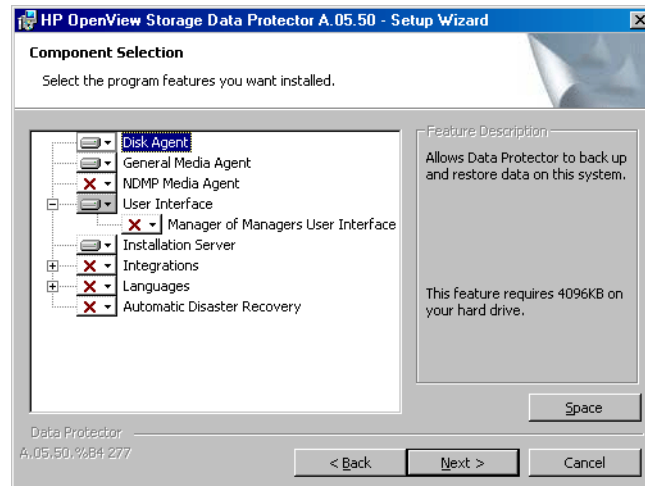
Selecting the Installation Type



4. Provide the username and password for the account under which the Data Protector services will run. Click Next to continue.
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. 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” on page 54.

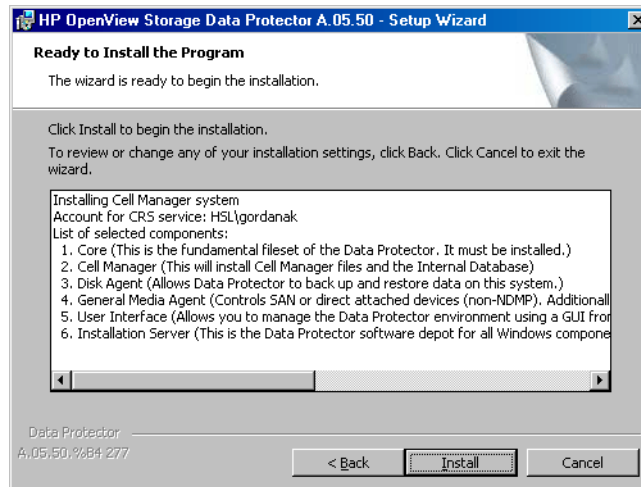
Figure 2-3 Selecting Software Components



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

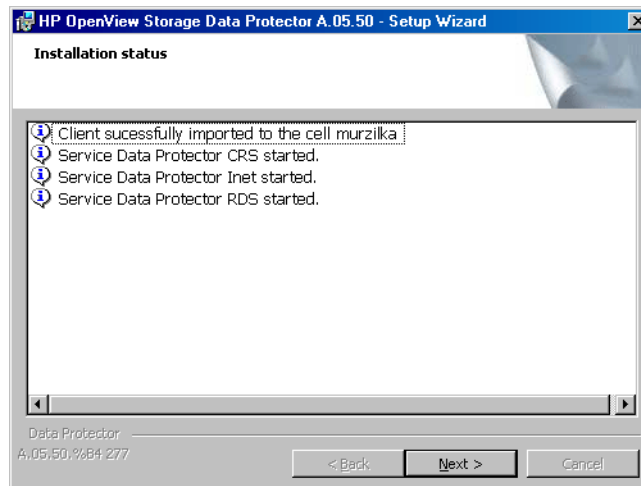
7. **Windows XP SP2 only:** If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the Initially, enable newly registered Data Protector binaries to open 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. Click Next.
8. The component summary list is displayed. Click Install to start installing the selected components. This may take several minutes.

Figure 2-4 Component Summary List



9. The Installation status page is displayed. Click Next.

Figure 2-5 Installation Status Page



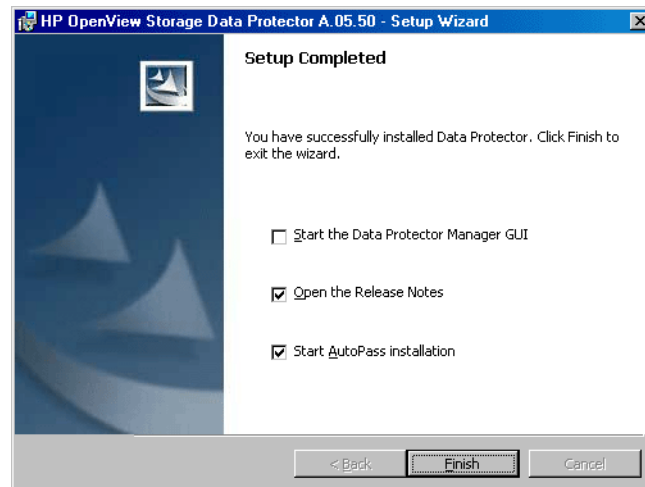
10. The Setup Wizard enables you to install or upgrade the HP OpenView AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294.

By default, the Start AutoPass installation or the Upgrade AutoPass installation option is selected. It is recommended to install the HP OpenView 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 OpenView Storage Data Protector Product Announcements, Software Notes, and References*, select Open the Product Announcements.

Figure 2-6 **Selecting AutoPass for Installation**



Click Finish.

After the Installation

As soon as the setup is finished, you have the Cell Manager files located in the `<Data_Protector_home>\bin` directory and the software depot for Windows located in the `<Data_Protector_home>\Depot` directory.

When the installation is finished, the following processes will be running on the Cell Manager system in the `<Data_Protector_home>\bin` directory:

<code>crs.exe</code>	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. CRS starts and controls backup and restore sessions in the cell.
<code>rds.exe</code>	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. RDS manages the IDB.
<code>omniinet.exe</code>	The Data Protector resident service that enables communication with Data Protector services on other systems on the network. The Data Protector Inet service must run on all systems in the Data Protector cell.

NOTE

If you intend to use the Data Protector user interface to perform backups or restores across platforms, refer to the *HP OpenView Storage 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. Refer to the operating system documentation for detailed steps.

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. Refer to the “Prerequisites” on page 26.

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. Refer to “Installing Installation Servers” on page 33. Skip this step if you do not need the Installation Server for UNIX.
2. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 42.

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. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details on supported operating systems for the Installation Server.

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

Prerequisites on UNIX

The UNIX system, which will become your future Installation Server, must meet the following requirements:

- ✓ Have HP-UX, Solaris, or Linux operating system installed. For details on supported operating systems for the Installation Server, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.
- ✓ Have the `inetd` daemon up and running.
- ✓ Have the port number 5555 (default) free. If this is not the case, refer to the “Changing the Default Port Number” on page B-23.
- ✓ 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. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details.
- ✓ Have a DVD-ROM drive.
- ✓ The Cell Manager in the Data Protector cell must be of the A.06.00 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/
```

you must 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 on an HP-UX, Solaris, or Linux system:

1. Insert and mount the UNIX installation DVD-ROM to a mount point.

For example:

```
mkdir /dvdrom
mount /dev/dsk/c0t0d0 /dvdrom
```

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

- To copy the DP_DEPOT, AUTOPASS, and LOCAL_INSTALL directories, where the installation files are stored, to your local disk, run:

```
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_ia	HP-UX 11.23 on IA-64 systems
hpux_pa	HP-UX on PA-RISC systems
linux_x86_64	Linux systems on AMD64/EM64-T
solaris	Solaris systems

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

```
cp -r /dvdrom <dvd_image_dir>
```

2. Run the omnisetup.sh command.

To run this command from the DVD-ROM, type:

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

To start the installation from disk:

- If you have copied the DP_DEPOT directory to your local disk as *<directory>/DP_DEPOT*, go to the directory where the omnisetup.sh command is stored, and run:

```
./omnisetup.sh -source <directory> -IS
```

- If you have copied the whole DVD-ROM to *<dvd_image_dir>*, run the omnisetup.sh command with the -IS parameter:

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

For a description of the `omnisetup.sh` command, refer to the `README` file located in the `<Mount_point>/` directory on the DVD-ROM or to the *HP OpenView Storage 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 you must use `swinstall` (for HP-UX), `pkgadd` (for Solaris) or `rpm` (for Linux). Refer to Appendix B , “Installing on HP-UX and Solaris Systems Using Native Tools,” on page B-3.

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.

NOTE

If you install the User Interface component (either the graphical user interface or the command-line interface), you should update your environment variables before using it. Refer to “Setting Environment Variables” on page 24 for more information.

If you intend to use the Data Protector user interface to perform backups or restores across platforms, refer to the *HP OpenView Storage 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. Refer to “Importing an Installation Server to a Cell” on page 179.

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 push-packets. This can be used from the CLI to check the available push-packets. For this file to be kept up to date, you should export and re-import an Installation Server whenever push-packets 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. Refer to “Installing an Installation Server for Windows” on page 37.
3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 42.

Installing an Installation Server for Windows**Prerequisites on Windows**

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

- ✓ Have one of the supported Windows operating systems installed. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details on supported operating systems for the Installation Server.
- ✓ Have Microsoft Internet Explorer 5.0 or higher.
- ✓ Have enough disk space for the complete Data Protector software depot. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details.
- ✓ 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. Refer to “Setting Up the TCP/IP Protocol on Windows Systems” on page B-15 for information on the installation and configuration of the TCP/IP protocol.

Limitation 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.

Recommendation Check if you have Microsoft Installer (MSI) 2.0 prior to installing Data Protector A.06.00. If you have an older version of MSI, Data Protector setup will automatically upgrade it to version 2.0. In this case, Data Protector will display a note at the end of the upgrade, stating that MSI was upgraded. It is highly recommended to restart the system, if MSI was upgraded. Consult Microsoft Support about the MSI 2.0 prerequisites for various Windows operating systems.

It is recommended that you upgrade your MSI to the version 2.0 before installing Data Protector A.06.00. Consult Microsoft Support for Microsoft Installer 2.0 prerequisites on the various Windows operating systems.

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. Refer to “Installing Windows Clients” on page 58.

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

1. Insert the Windows installation DVD-ROM and run
32-bit systems: \Windows_other\i386\setup.exe

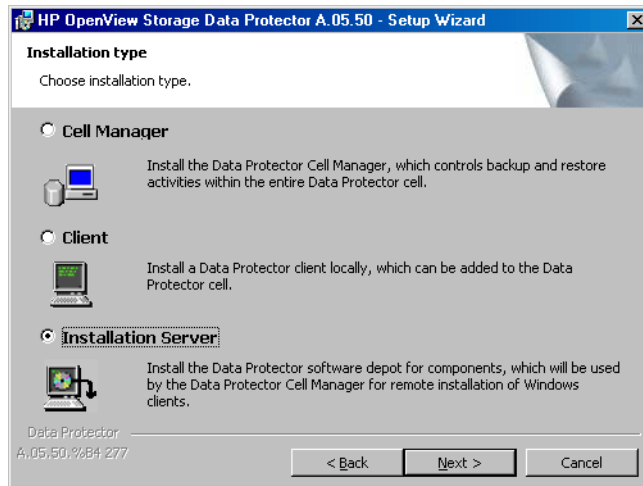
64-bit systems: \Windows_other\x8664\setup.exe

The Data Protector Setup Wizard is displayed.

2. Follow the Setup Wizard and carefully read the license agreement.

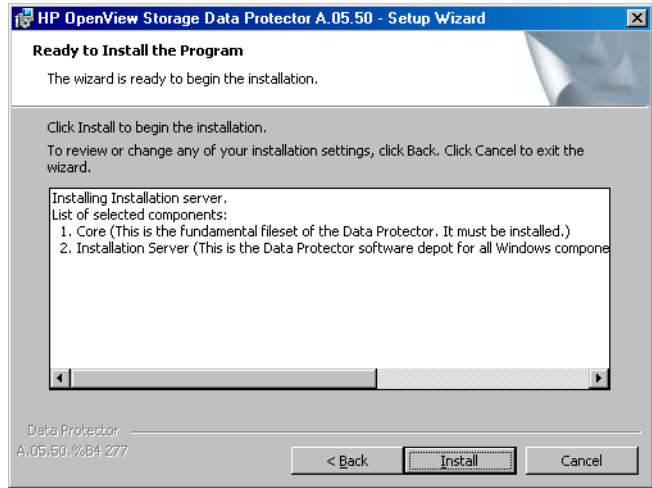
- Click **Next** to continue, if you accept the terms of the agreement.
3. In the **Installation Type** page, select **Installation Server** and then click **Next** to install Data Protector software depot.

Figure 2-7 **Selecting the Installation Type**



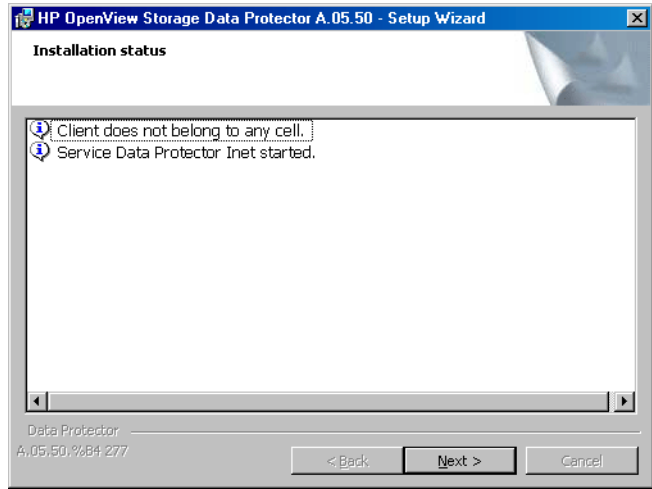
4. Click **Next** to install Data Protector on the default folder.
Otherwise, click **Change** to open the **Change Current Destination Folder** window and enter a new path.
5. **Windows XP SP2 only:** If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page 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.
Click **Next**.
6. The component summary list is displayed. Click **Install** to start installing the selected components. This may take several minutes.

Figure 2-8 Component Selection Summary Page



7. The Installation status page is displayed. Click Next.

Figure 2-9 Installation Status Page



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

8. To view the *HP OpenView Storage 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 `<Data_Protector_home>\Depot` directory, which 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 (i.e. not on the Cell Manager) you must manually add (import) the system to the Data Protector cell. Refer to “Importing an Installation Server to a Cell” on page 179.
2. Install an Installation Server for UNIX on HP-UX, Solaris, or Linux if you have a mixed backup environment. Refer to “Installing Installation Servers for UNIX” on page 34.
3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 42.

Installing Data Protector Clients

You can install 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, refer to “Data Protector Installation DVD-ROMs” on page 8.

After you have installed the Data Protector clients and eventually imported them into the Data Protector cell, it is highly recommended to verify the installation and to protect clients from unwarranted access. For procedure on verifying the client installation, refer to “Verifying Data Protector Client Installation” on page 313. For more information on security protection, refer to “Security Considerations” on page 187.

Table 2-1 lists Data Protector client systems with references to detailed descriptions. Table 2-2 lists

Table 2-1

Installing Data Protector Client Systems

Client System	Installation Type & Reference
Windows	Remote and local installation; see “Installing Windows Clients” on page 58.
HP-UX	Remote and local installation; see “Installing HP-UX Clients” on page 64.
AIX	Remote and local installation; see “Installing AIX Clients” on page 79.
Solaris	Remote and local installation; see “Installing Solaris Clients” on page 67.
Tru64	Remote and local installation; see “Installing Tru64 Clients” on page 83.
Siemens Sinix	Remote and local installation; see “Installing Siemens Sinix Clients” on page 81.
SCO	Remote and local installation; see “Installing SCO Clients” on page 85.

Table 2-1 **Installing Data Protector Client Systems**

Client System	Installation Type & Reference
Linux	Remote and local installation; see “Installing Linux Clients” on page 74.
DAS Client	Remote and local installation; see “Installing a Media Agent to Use the ADIC/GRAU Library or the StorageTek Library” on page 87.
ACS Client	Remote and local installation; see “Installing a Media Agent to Use the ADIC/GRAU Library or the StorageTek Library” on page 87.
Novell NetWare	Local installation; see “Local Installation of the Novell NetWare Clients” on page 96.
OpenVMS	Local installation; see “Local Installation of OpenVMS Clients” on page 103.
MPE/iX	Local installation; see “Installing MPE/iX Clients” on page 110.
Other UNIX clients	Local installation; see “Local Installation of UNIX and Linux Clients” on page 113.

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, MS Exchange 2000/2003 Integration

Installing Data Protector Clients

component for backing up the Microsoft Exchange Server database, Oracle Integration component for backing up an Oracle database, and so on). Refer to Table 2-2 for the references.

Table 2-2 **Installing Integrations**

Application	Reference
Microsoft Exchange Server	See “Microsoft Exchange Server Clients” on page 121.
Microsoft SQL Server	See “MS SQL Clients” on page 122.
Sybase	See “Sybase Clients” on page 122.
Informix Server	See “Informix Server Clients” on page 122.
SAP R/3	See “SAP R/3 Clients” on page 123.
SAP DB	See “SAP DB Clients” on page 123.
Oracle	See “Oracle Clients” on page 124.
IBM DB2 UDB	See “DB2 Clients” on page 125.
NNM	See “NNM Clients” on page 125.
NDMP	See “NDMP Clients” on page 126.
Microsoft Volume Shadow Copy	See “MS Volume Shadow Copy Clients” on page 126.
Lotus Domino Server	See “Lotus Notes/Domino Server Clients” on page 126.
EMC Symmetrix	See “EMC Symmetrix Integration” on page 127.
HP StorageWorks XP	See “HP StorageWorks XP Integration” on page 130.
HP StorageWorks Virtual Array	See “HP StorageWorks Virtual Array Integration” on page 136.
HP StorageWorks Enterprise Virtual Array	See “HP StorageWorks Enterprise Virtual Array Integration” on page 142.

Table 2-3 Other Installations

Installation	Reference
Localized User Interface	See “Installing Localized Data Protector User Interface” on page 149.
Web Reporting	See “Installing Data Protector Web Reporting” on page 156.
MC/ServiceGuard	See “Installing Data Protector on MC/ServiceGuard” on page 158.
Microsoft Cluster Server	See “Installing Data Protector on Microsoft Cluster Server” on page 160.
Veritas Cluster Server	See “Installing Data Protector Clients on a Veritas Cluster” on page 171
Novell NetWare Cluster	See “Installing Data Protector Clients on a Novell NetWare Cluster” on page 172

Remote Installation of the Data Protector Clients

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

Prerequisites

- For prerequisites and recommendations on the installation, refer to the section that describes the installation procedure for that particular client. The references are listed in Table 2-1 on page 42 and in Table 2-2 on page 44.
- Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for the information on supported platforms, Data Protector components, and for disk space requirements.
- At this point, you should have the Cell Manager and the Installation Server(s) installed on your network.

NOTE

The Installation Server for Windows must reside in a shared directory so that it is visible throughout the network.

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

- To use secure shell installation, install and set up OpenSSH on the client and Installation Server, and keychain on the Installation Server only. See “Remote Installation Using Secure Shell” on page 51 for instructions.

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.

Adding Clients to the Cell

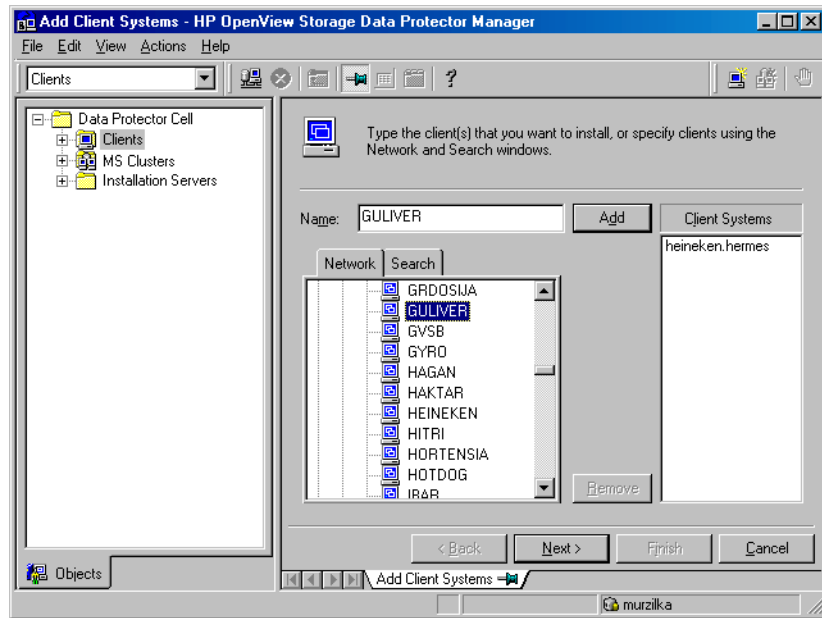
To distribute the Data Protector software to the clients that are not in the Data Protector cell yet, proceed as follows:

1. Start the Data Protector graphical user interface:
 - On Windows: Select Start->Programs->HP OpenView Storage Data Protector->Data Protector Manager.
 - On HP-UX (or Solaris: Enter `/opt/omni/bin/xomni` in the command line.

Refer to the online Help for details on the Data Protector graphical user interface.

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 Figure 2-10. Click Next.

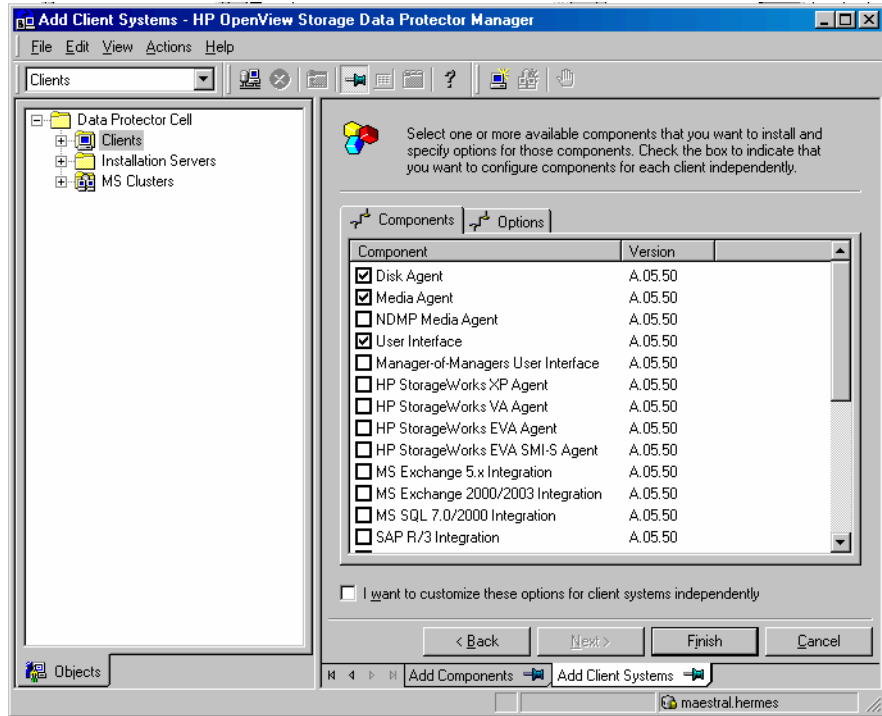
Figure 2-10 **Selecting the Client(s)**



6. Select the Data Protector components you want to install as shown in Figure 2-11. Note that you can select only one type of Media Agent. See “Data Protector Components” on page 54.

Figure 2-11

Selecting the Components (TBD - to be replaced because of EVAA
obsolescence)



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.

As soon as a system has the Data Protector software installed and is added to the Data Protector cell, it becomes the 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, refer to the online 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” on page 303.

Adding Components to the 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” on page 216.

MC/ServiceGuard Clients

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

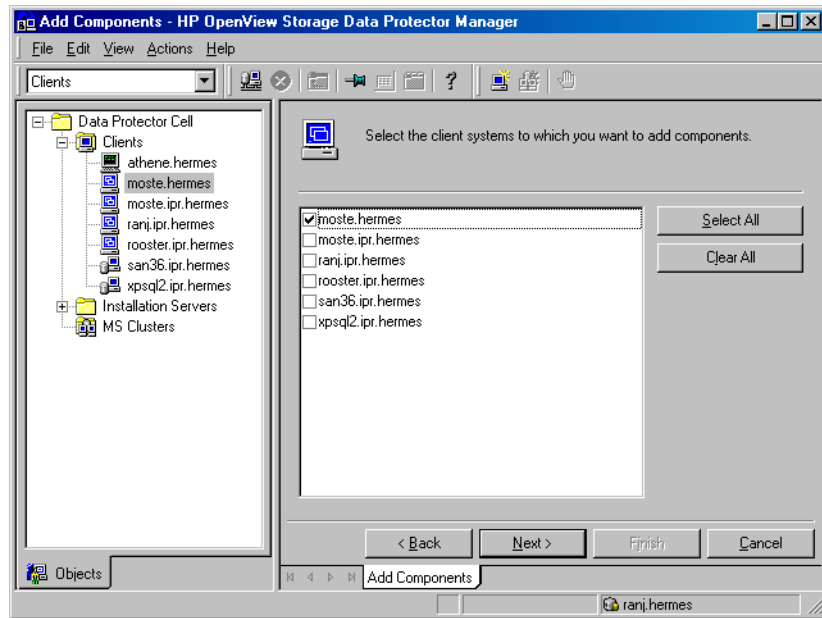
Prerequisite

The corresponding Installation Server must be available.

To distribute the Data Protector software to the 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 Figure 2-12. Click **Next**.

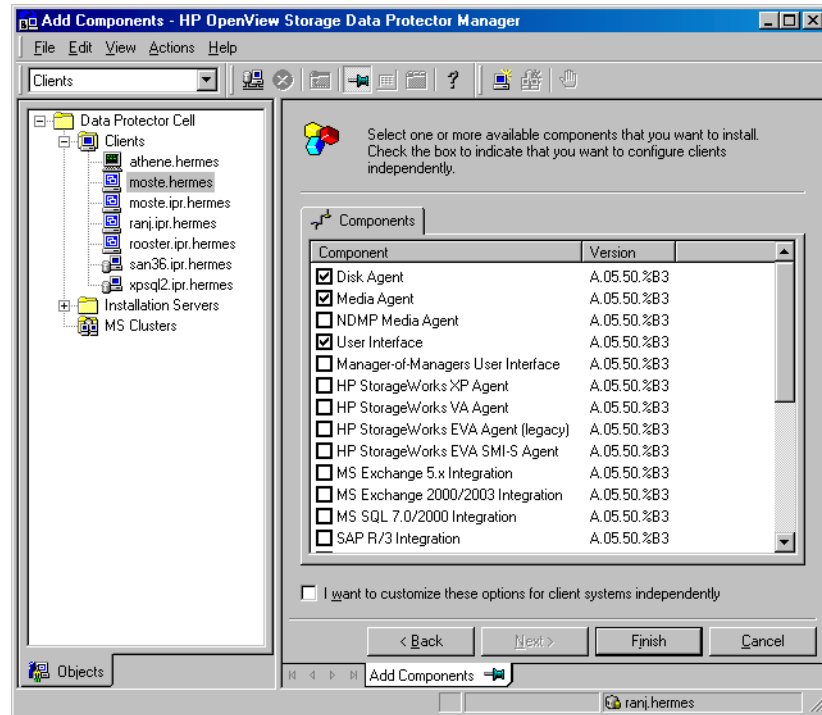
Figure 2-12 **Selecting the Client(s)**



5. Select the Data Protector components you want to install as shown in Figure 2-13. Note that you can select only one type of Media Agent. See “Data Protector Components” on page 54.

Figure 2-13

Selecting the Components (TBD - to be replaced because of EVAA obsolescence)



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.

Remote Installation Using Secure Shell

Secure shell installation method helps you protect your client and Installation Server by installing the 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.

See the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for information on platforms on which secure shell installation is supported.

Prerequisites

- Install OpenSSH and keychain on the Installation Server.
- Install OpenSSH on the client.
- Enable the `OB2_SSH_ENABLED` omnirc variable (`/opt/omni/.omnirc`) on the Installation Server. For more information on omnirc variables, see the *HP OpenView Storage Data Protector Troubleshooting Guide*.

Setting Up OpenSSH

OpenSSH is an open source implementation of the secure shell protocol. To set up OpenSSH:

1. Download `openssh` from <http://www.openssh.org> and install it (preferably, under `/opt`) on both Data Protector client and Installation Server. Alternately, on HP-UX, you can use 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.

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 directory of the root user.

To set an SSH protocol version (SSH1 or SSH2), edit the following files by modifying the `protocol` parameter:

- a. ***On the Installation Server:***

`<ssh_install_folder>/ssh/etc/ssh_config`. This file will be used by the `ssh` command.

b. ***On the client:***

`<ssh_install_folder>/ssh/etc/sshd_config`. This command will be used by the `ssh` daemon (`sshd`).

Note that these two files must be in synch.

NOTE

The default SSH protocol version is SSH2.

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

```
<ssh_install_folder>/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>
```

Note that `<client_host>` must be a fully qualified DNS name, for example:

```
ssh root@client1.company.com
```

6. On the Installation Server, set the `OB2_SSH_ENABLED` variable to 1.

**Setting Up
Keychain**

Keychain is a tool eliminating the supply of a pass phrase manually when decrypting the private key. To set up keychain:

1. Download keychain from <http://www.gentoo.org/proj/en/keychain/index.xml> on the Installation Server.

2. Add the following two lines to the `<$HOME>/.profile` file:

```
<keychain_install_folder>/keychain-<keychain_version>/keychain <$HOME>/.ssh/<private_key>
```

```
. <$HOME>/.keychain/'hostname' -sh
```

3. On the Installation Server, set the `OB2_ENCRYPT_PVT_KEY_omnirc` variable to 1 if you want to generate an encrypted private key. When this variable is set, Data Protector uses keychain and stores the key with encryption.

NOTE

If secure shell installation cannot be performed because the execution of its command fails, a warning will be issued to this effect. However, the installation will continue using the standard Data Protector remote installation method.

Data Protector Components

For the latest information on the supported platforms, visit the HP OpenView Storage Data Protector home page at http://www.openview.hp.com/products/datapro/spec_0001.html

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

User Interface

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

NOTE

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

Manager-of-Managers (MoM)
User Interface

The Manager-of-Managers (MoM) User Interface includes the Data Protector graphical user interface, and the command-line interface. The software is needed to access the Data Protector Manager-of-Managers functionality and control the multi-cell environment.

Disk Agent	The Disk Agent component must be installed on clients that have disks that will be backed up with Data Protector.
General Media Agent	The General Media Agent component must be installed on clients that have backup devices connected or have access to a library robotics and will be managed by Data Protector.
Automatic Disaster Recovery	The Automatic Disaster Recovery component must be installed on clients for which you want to enable recovery using an automatic disaster recovery method; and on the system where the DR CD ISO image for Enhanced Disaster Recovery 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 clients 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 clients that have an SAP DB database that will be backed up using Data Protector.
Oracle Integration	The Oracle Integration component must be installed on clients that have an Oracle database that will be backed up with Data Protector.
DB2 Integration	The DB2 Integration component must be installed on all clients that have a DB2 Server that will be backed up with Data Protector.
Sybase Integration	The Sybase Integration component must be installed on clients that have a Sybase database that will be backed up with Data Protector.

Installing Data Protector Clients

Informix Integration	The Informix Integration component must be installed on clients that have an Informix Server database that will be backed up 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 StorageWorks XP Agent	The HP StorageWorks XP Agent component must be installed on the application and backup system to integrate HP StorageWorks XP with Data Protector.
HP StorageWorks VA Agent	The HP StorageWorks VA Agent component must be installed on the application and backup system to integrate HP StorageWorks Virtual Array with Data Protector.
HP StorageWorks EVA SMI-S Agent	The HP StorageWorks EVA SMI-S Agent component must be installed on the application and the backup system to integrate HP StorageWorks Enterprise Virtual Array with Data Protector.
MS SQL 7.0/2000 Integration	The SQL 7.0/2000 Integration component must be installed on the systems that have an MS SQL database which will be backed up with Data Protector.
MS Exchange 2000/2003 Integration	The MS Exchange 2000/2003 Integration component must be installed on clients that have an Microsoft Exchange Server database that will be backed up with Data Protector.
Cluster Server	The Cluster Server component must be installed on all Data Protector cluster-aware clients.

HP OpenView NNM Backup Integration	The NNM Integration component must be installed on all clients 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 clients that are backing up data to NDMP dedicated drives through an NDMP server.
Lotus Integration	The Lotus Integration component must be installed on all clients in the cell that have a Lotus Notes/Domino Server database 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 2003 systems where you want to run backups coordinated by Volume Shadow Copy service.
French Language Support	The French Language Support component must be installed on clients where you want to use the Data Protector User Interface localized into French.
Japanese Language Support	The Japanese Language Support component must be installed on clients where you want to use the Data Protector User Interface localized into Japanese.

NOTE

You cannot install the General Media Agent and the NDMP Media Agent on the same client.

Installing Windows Clients

For details on supported platforms, processors, and components for a particular Windows operating system, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Prerequisites

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

- ✓ Have Microsoft Internet Explorer 5.0 or higher.
- ✓ Have sufficient disk space for the Data Protector client software. Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details.
- ✓ 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. Refer to “Setting Up the TCP/IP Protocol on Windows Systems” on page B-15 for information on installation and configuration of the TCP/IP protocol.

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 Me/XP HE, Data Protector clients can only be installed locally.

Recommendation

On each Windows client, check if you have Microsoft Installer (MSI) 2.0 prior to installing Data Protector A.06.00. If you have an older version of MSI, Data Protector setup will automatically upgrade it to version 2.0. In this case, Data Protector will display a note at the end of the upgrade, stating that MSI was upgraded. It is highly recommended to restart the client system, if MSI was upgraded. Consult Microsoft Support for Microsoft Installer 2.0 prerequisites on the various Windows operating systems.

If you start the Data Protector installation with an older version of the MSI, Data Protector setup will upgrade it to version 2.0. However, the system must be rebooted for the changes to take effect. After the computer is rebooted, restart the installation.

Automatic Disaster Recovery

The Automatic Disaster Recovery component must be installed on clients for which you want to enable recovery using an automatic disaster recovery method, and on the system where the DR CD ISO image for Enhanced Disaster Recovery will be prepared.

Cluster-Aware Clients

Additional prerequisites are required for installing cluster-aware clients. Refer to “Installing a Cluster-Aware Client” on page 168 for more details.

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” on page 54.

Remote Installation

You can remotely install Windows clients as soon as you have the Cell Manager and Installation Server for Windows installed on your network. Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17 for instructions.

You can distribute the Windows client software from the Installation Server for Windows using the Data Protector graphical user interface. For the step-by-step procedure, refer to “Remote Installation of the Data Protector Clients” on page 45.

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

Local Installation

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

1. Insert the DVD-ROM and run:

32 bit processors: \Windows_other\i386\setup.exe

AMD-64/EM-64T processors: \Windows_other\x8664\setup.exe

Itanium processors: \Windows_other\ia64\setup.exe.

2. In the Installation Type page, select Client. For Itanium clients, the type is selected automatically.
3. Enter the name of the Cell Manager. Refer to Figure 2-14.

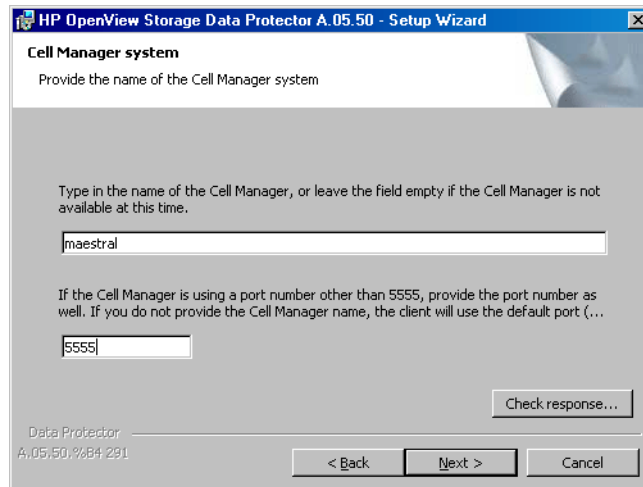
Installing Data Protector on Your Network

Installing Data Protector Clients

If your Cell Manager uses a different port than 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 2-14 Choosing the Cell Manager



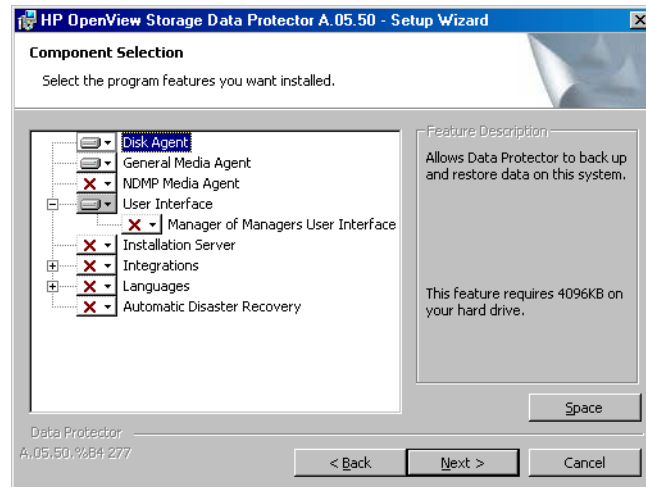
4. Click Next to install Data Protector on the default folder.
Otherwise, click Change to open the Change Current Destination Folder page and enter the path.
5. Select the Data Protector components that you want to install.
For information on other Data Protector components, refer to “Data Protector Components” on page 54.
Click Next.
6. **Windows XP SP2 only:** 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.

Click Next.

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

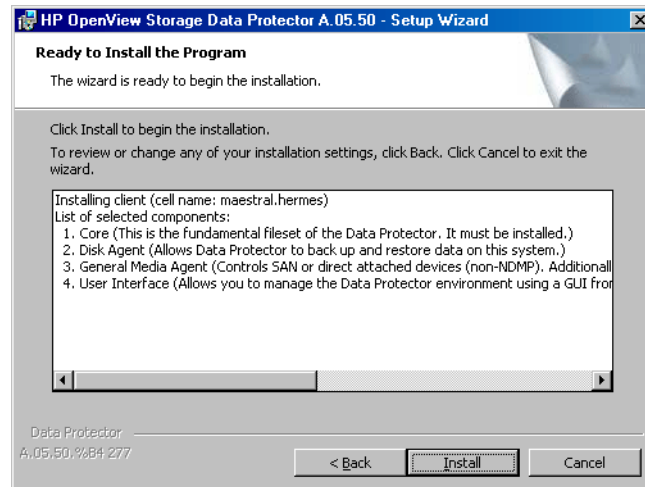
Figure 2-15 Component Selection Summary Page



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

Figure 2-16

Installation Summary Page



9. To start using Data Protector immediately after setup, select Launch Data Protector Manager.

To view the *HP OpenView Storage 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. Refer to “Finding Unused SCSI Target IDs on a Windows System” on page B-48.
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, refer to the documentation that comes with the device.

Also see

http://www.openview.hp.com/products/datapro/spec_0001.html for information about supported devices.

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.

You should 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, refer to “Using Tape and Robotics Drivers on Windows” on page B-26. For more information on creating a device filename, refer to “Creating Device Files (SCSI Addresses) on Windows” on page B-29.

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. Refer to the online Help index: TBD for information on configuration tasks.

Installing HP-UX Clients

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

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, refer to the *HP OpenView Storage 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, see “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17 for instructions.
- To install an HP-UX client, you will need either *root* access or an account with *root* capabilities.

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. See “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

After the local installation, the client system has to be manually imported into the cell. See also “Importing Clients to a Cell” on page 177.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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.

Cluster-Aware Clients

Additional prerequisites and steps are required for installing cluster-aware clients. Refer to “Installing a Cluster-Aware Client” on page 159 for more details.

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. Refer to “SCSI Robotics Configuration on HP-UX” on page B-31 for instructions on how to build the kernel manually.

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 Figure 2-17. 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.

Installing Data Protector Clients

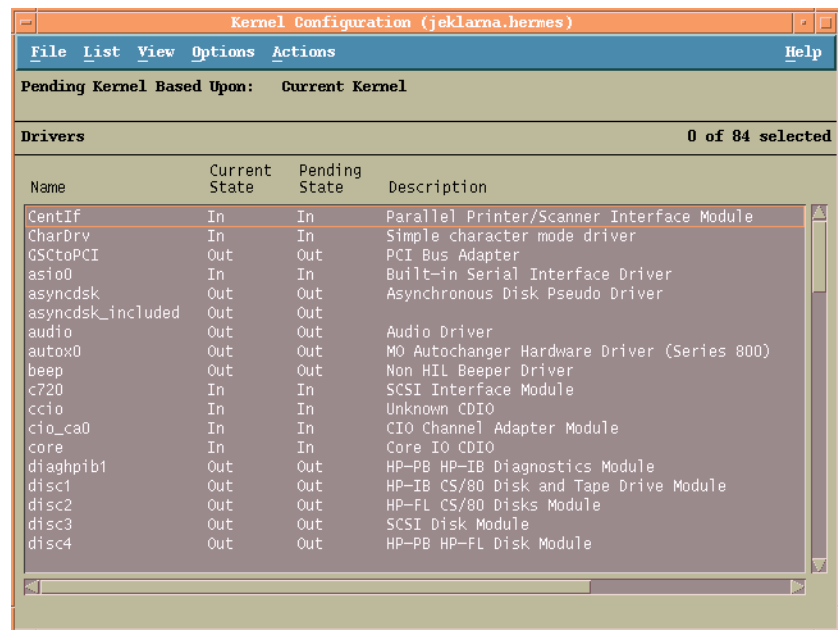
If you have connected a Quantum DLT 4000 device to an HP-UX 11.00 system, we recommend using `tape2` rather than the `stape` driver.

- 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.

Refer to “SCSI Robotics Configuration on HP-UX” on page B-31 for details.

Figure 2-17

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:

- 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.

- b. 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.
Refer to “Finding the Unused SCSI Addresses on HP-UX” on page B-40 for more information.
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, refer to the documentation that comes with the device.

Refer to

http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices.

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. Refer to “Creating Device Files on HP-UX” on page B-36.

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

Installing Solaris Clients

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

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage 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. Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17 for instructions.
- To install a Solaris client, you will need either *root* access or an account with *root* capabilities.

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. Refer to “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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. Refer to “Setting Environment Variables” on page 24 for more information.

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

If you want 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 must create the links before the installation and ensure that the destination directories exist.

Cluster-Aware Clients

Additional prerequisites are required for installing cluster-aware clients. Refer to “Installing a Client” on page 171 for more details.

Post-Installation Configuration**Configuration Files**

Once you have a Media Agent component installed on the client system, you have to check your configuration files (`/kernel/drv/st.conf`), depending on the device type you will be using.

- For Exabyte devices (8 mm), no changes to the `/kernel/drv/st.conf` file are necessary.
- 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.

Installing Data Protector Clients

- 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 the SCSI Exchanger devices on Solaris using the SCSI Pass-Through driver, you have to install the SCSI Pass-Through driver first, then you 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:

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

64 bit Solaris:

```
$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. Install the driver on the system by entering the following command:

```
add_drv sst
```

4. 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:

```
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 install the SCSI device, follow the steps:

- a. Edit `/kernel/drv/st.conf` to set up the device's drive parameters in order to use the assigned SCSI ports (refer to the appropriate device's documentation).

The following example will show the setup of the ADIC-VLS DLT device with the SCSI port 5 assigned to the SCSI tape drive and the SCSI port 4 assigned to the ADIC SCSI control device (picker):

Example

```
tape-config-list = "DEC      DLT2000", "ADIC
DLTDlib", "ADIC2000-data";
ADIC2000-data =
1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;name="st" class=
"scsi"
target=5 lun=0;
name="st" class= "scsi"
target=4 lun=0;
```

The data displayed in the example above must be in the `/kernel/drv/st.conf` file.

- b. Edit `/usr/kernel/drv/sst.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 drive to the `/usr/kernel/drv/sst.conf` file:

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

When you have modified the `/kernel/drv/st.conf` file and the `/usr/kernel/drv/sst.conf` file, 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.openview.hp.com/products/datapro/spec_0001.html 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 reboot your system. Load a cleaning tape manually, when Data Protector issues a request for it.

3. Switch your computer back on and interrupt the boot process by pressing the Stop-A key. 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.

4. 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 systems, (especially in case of Solaris 64-bit), links to the SCSI control device (picker) are not always created automatically. In this case, create symbolic links. For example:

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

Make sure you use Berkeley-style device files, in this case, `/dev/rmt/0hb` (not `/dev/rmt/0h`) for the exchanger 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, refer to the online Help index: TBD for more information about configuring backup devices, media pools, or other configuration tasks.

Installing Linux Clients

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

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" on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage 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)” on page 17 for instructions.

NOTE

Data Protector uses the default port number 5555. Therefore, this particular port number should not be used by another program. Some versions of Linux 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 Port Number” on page B-23.

HP ServiceGuard Cluster TBD

With HP 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.

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. See “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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

Troubleshooting

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:

Installing Data Protector Clients

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. Kill 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:

```
<my_installation_server> 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, refer to “Local Installation of UNIX and Linux Clients” on page 113.

Kernel Configuration

The following procedure explains how to check and build your kernel configuration:

1. Log in as a root user, then in the `/usr/src/linux` directory run the `make menuconfig` command.
2. Select `SCSI Support` and press `Enter`. Then select the following options: `SCSI support`, `SCSI tape support`, `SCSI generic support` and optionally `Probe all LUNS on each SCSI device`.

If the items are already included in kernel, exit without saving changes. You can continue by connecting a backup device to your system. Refer to “Connecting a Backup Device to the Linux System” on page 78.

3. If you made changes, save the configuration and do the following:
 - a. Run the `make dep` command.

This command builds the tree of dependencies in the kernel sources. These dependencies could be affected by the options you chose when configuring the kernel.

- b. Run the `make clean` command to purge files left from previous builds of the kernel.
 - c. Run the `make bzImage` command. After it is completed, run the `make modules` command.
4. To install the kernel to the `/boot` directory on an Intel-based system, copy the new `bzImage` to the `/boot` directory as follows:
 - a. Run the following command:

```
cp /usr/src/linux/arch/i386/boot/bzImage/boot/newkernel
```
 - b. Run the `make modules_install` command to install the modules in the `/lib/modules` directory.

Installing Data Protector Clients

c. Edit `/etc/lilo.conf` and add the following:

```
image = /boot/newkernel  
label = new  
read-only
```

d. Run the `/sbin/lilo` command to update LILO.

At the next reboot, select the kernel 'new' in LILO and to load the new kernel. If everything is working correctly, move the kernel 'new' to the first position in the `lilo.conf` file so it will boot every time by default.

More information about kernel and SCSI configuration can be found in kernel source directory `/usr/src/linux/Documentation/`.

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, refer to the documentation that comes with the device.

Refer to

http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices.

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 RedHat Linux, 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, run:

```
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, refer to the online Help index:TBD for information about configuring backup devices and media pools, or other configuration tasks.

Installing AIX Clients

AIX clients can be installed locally from the UNIX installation DVD-ROM, or remotely using the Installation Server for UNIX.

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Installing Data Protector Clients

- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17 for instructions.

IMPORTANT

Before installing the Disk Agent component on an AIX system, check that the portmapper is up and running. In the `/etc/rc.tcpip` file, there must be the line that starts the portmapper:

```
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 notification.

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. See “Local Installation of UNIX and Linux Clients” on page 113 and for instructions.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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 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.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices.

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, refer to the online Help index: TBD for information on configuring backup devices, media pools, or on other Data Protector configuration tasks.

Installing Siemens Sinix Clients

Siemens Sinix clients can be installed locally by using the UNIX installation DVD-ROM, or remotely using the Installation Server for UNIX.

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage 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)” on page 17 for instructions.

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. See “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

Remote Installation

You install the Sinix 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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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 Siemens Sinix System

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

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

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices and the documentation that comes with the device.

Check that no other device is using the same SCSI address as the one selected for your backup device.

2. Switch your computer back on and wait until the boot process is completed.
3. Select the appropriate device file name from the `/dev` directory.

You can obtain the list of devices with the `autoconf -l` command. Use the tape device (for example, `ios0/stape006`) that was reported in the output of this command to get the special device filename that Data Protector can use (for example, `/dev/ios0/rstape006nv`).

NOTE

The special device files are located in the `/dev` directory, so you must add the `/dev` path in front of the device name.

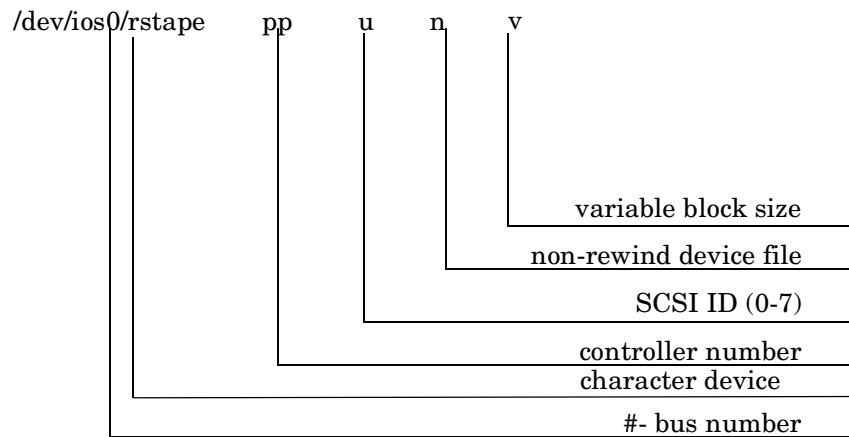
Since Data Protector can use only a character device, the letter `r` is added in front of the `stape006`.

Data Protector can handle a tape device if it is opened as non-rewindable and with variable block size; therefore you must add letters `n` and `v` as suffixes.

The `/dev/ios0/rstape006nv` device filename is explained in Figure 2-18.

Figure 2-18

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 Siemens Sinix client system, refer to the online Help index: TBD for information about configuring backup devices and media pools, or other configuration tasks.

Installing Tru64 Clients

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

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage 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)” on page 17 for instructions.

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. See “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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 locally or remotely 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” on page 180.

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.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices.

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, refer to the online Help index: TBD for information on configuring backup devices, media pools, or on other Data Protector configuration tasks.

Installing SCO Clients

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

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, refer to the *HP OpenView Storage 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)” on page 17 for instructions.

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. See “Local Installation of UNIX and Linux Clients” on page 113 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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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/m SCSI` file. This file shows the currently connected SCSI devices.

See http://www.openview.hp.com/products/datapro/spec_0001.html/ 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.

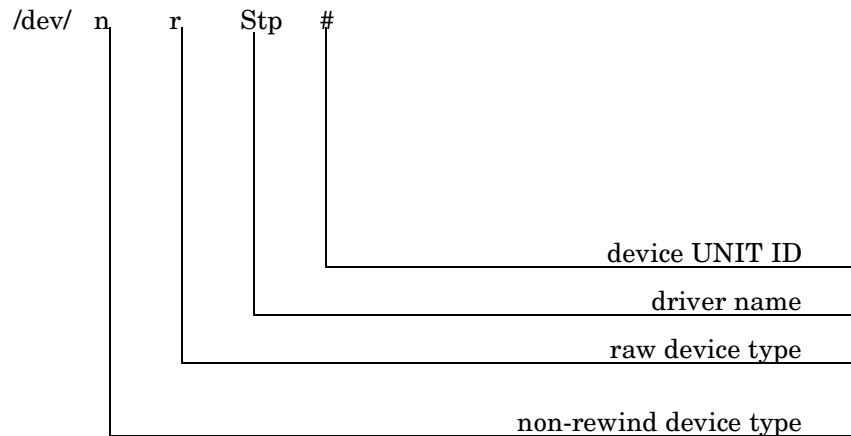
5. After you have configured the device and restarted the system, check in the `/etc/conf/cf.d/m SCSI` file if your device was connected properly.
6. Select the appropriate device filename from the `/dev` directory.

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 Figure 2-19.

CAUTION

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

Figure 2-19 **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, refer to the online Help index: TBD for information about configuring backup devices and media pools or other configuration tasks.

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. See Chapter 5, “Data Protector Licensing,” on page 277 for more information.

Connecting Library Drives

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

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported ADIC/GRAU or STK libraries.

See “Installing HP-UX Clients” on page 64 for information about how to physically attach a backup device to the system. Also see the documentation that comes with the ADIC/GRAU or StorageTek library.

See “Installing Windows Clients” on page 58 for information on how to physically attach a backup device to a supported Windows system. Also see 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, /opt/omni/.omnirc file on HP-UX and Solaris, or /usr/omni/omnirc file on AIX) and set the following variables:

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. Refer to the *AMU Reference Manual* for information on how to check what type of allocation policy is used.

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` variable 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, please 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)” on page 17 in this chapter.
- ✓ 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” on page 67.

Installing Data Protector Clients

- 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” on page 62.

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 of the Data Protector Clients” on page 45 in this chapter.
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 rebooting 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:

- **On Windows:** `<Data_Protector_home>\bin\devbra -dev`
- **On HP-UX:** `/opt/omni/1bin/devbra -dev`
- **On AIX:** `/usr/omni/bin/devbra -dev`

You should 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, refer to the online Help index: TBD 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)” on page 17.
- ✓ The following information must be obtained before you start installing a Media Agent software:
 - The `<hostname>` of the host where ACSLS is running.

Installing Data Protector Clients

- 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” on page 67.

- 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, refer to “Connecting a Backup Device to Windows Systems” on page 62.

- ✓ 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 of the Data Protector Clients” on page 45 in this chapter.
2. Start the ACS `ssi` daemon for every ACS client:

- On HP-UX and Solaris ACS clients, run the following command:

```
/opt/omni/acs/ssi.sh start <ACS_LS_hostname>
```

- On Windows ACS clients, install the `LibAttach` service. Refer to the ACS documentation for details. 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 reboot as well.

- On AIX ACS clients, 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 or Solaris 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`

You should 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, refer to the online Help index: TBD for information about additional configuration tasks, such as configuring backup devices and media pools.

Local Installation of the 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 5.x or later. For information on Data Protector components, refer to “Data Protector Components” on page 54.

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

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, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

✓ Make sure the TCP/IP transport protocol is installed and functional.

✓ Set the `TIMEZONE` variable on your Novell NetWare server:

On a NetWare 5.x, and 6.x system, the `TIMEZONE` variable is automatically set during the NetWare installation process. It is not necessary to reload the `CLIB.NLM`.

Refer to the *Supervising the Network* manual for more information on the `SET TIMEZONE` command.

✓ 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. Refer to “Installing a Client” on page 172 for more details.

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.

Installing Data Protector Clients

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
- TSAxxx.NLM (TSA500.NLM (Novell NetWare 5.1), TSA600.NLM (Novell NetWare 6.0), TSAFS.NLM (Novell NetWare 6.x))
- TSANDS.NLM

NOTE

TSAFS.NLM and TSA600.NLM both work on Novell NetWare 6.x. However, since the Novell engineering does not support TSA600.NLM anymore, it is recommended to start using TSAFS.NLM on your NetWare 6.x server instead of TSA600.NLM.

Tests showed that the functionality of Data Protector changes according to the module loaded. Therefore, a prerequisite for proper operation of Data Protector A.06.00 on Novell NetWare 6.0 is to have both modules (TSA600 and TSAFS) loaded.

The Data Protector NetWare client installation script has been changed to load both, TSA600.NLM and TSAFS.NLM, on NetWare 6.0 server.

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=HSL
```

- 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=HSL 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. Refer to the online Help index: TBD for instructions about additional configuration tasks.

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. See the *Adaptec Driver User's Guide* for the list of available options and calculation of the slot number.

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 StorageWorks Tape 12000e 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” on page B-64.

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. Refer to the online Help index: TBD for information on additional configuration tasks.

Local Installation of 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 7.3-1/IA64 8.2. You can also install the Oracle Integration component on systems running OpenVMS 7.3-1 or above. For information on Data Protector components, refer to “Data Protector Components” on page 54.

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

Prerequisites

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

- ✓ Make sure the TCP/IP transport protocol is installed and running.

Installing Data Protector Clients

- ✓ 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 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 CD and execute the program `DPVMSKIT.EXE` found in the OpenVMS directory on the CD. The PCSI installation file will be extracted to your default directory, or the destination provided.

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 A06.00-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, User Interface, and Oracle Integration (Alpha systems only) will be installed. You also may 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 AXPVMS DP A6.00-xx: HP AXPVMS Data Protector V6.00  
Copyright 2006 Hewlett-Packard Development Company, L.P.
```


Do you want the defaults for all options? [YES] NO
Do you wish to install a disk agent for this client node?
[YES] YES
Do you wish to install a media agent for this client node?
[YES] YES
Do you wish to install the command language interface
(CLI)? [YES] YES
Do you want to review the options? [NO] YES

HP AXPVMS DP A6.00-xx: HP OpenVMS Alpha Data Protector
V6.00 [Installed]

Do you wish to install a disk agent for this client node?:
YES

Do you wish to install a media agent for this client
node?: YES

Do you wish to install the command language interface
(CLI)? : YES

Are you satisfied with these options? [YES] YES

The default 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.

Installing Data Protector Clients

- 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:SYSHUTDOWN.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” on page 177.

An account with the name OMNIADMIN was 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.

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.

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 '*'.

If you want to include all versions of the file in a backup, you must 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 online Help index: TBD.

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
```

See the *HP OpenView Storage Data Protector Command Line Interface Reference* for a description of the available CLI commands.

Oracle Integration

After you installed the Oracle integration and configured it as described in the *HP OpenView Storage 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 A.06.00
```

Installing Data Protector Clients

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?

Refer to the online Help index: TBD for information on additional
configuration tasks.

Installing MPE/iX Clients

Refer to the *HP OpenView Storage Data Protector MPE/iX System User
Guide* for detailed information. If the documentation package is installed
on your system (on HP-UX, Solaris, or Windows), the guide is available
as `MPE_user.pdf` in `<Data_Protector_home>\Docs` (on Windows),
`/opt/omni/doc/C/` (on UNIX), or on the Data Protector Windows
installation DVD-ROM in the `docs` directory.

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” on page 54.

Refer to the *HP OpenView Storage Data Protector Product
Announcements, Software Notes, and References* for information about
supported devices, MPE/iX platform versions, and Data Protector
components.

Prerequisites

Before you install Data Protector on the MPE/iX platform, check the
following:

- ✓ TurboStore/iX or TurboStore/iX 7x24 True-Online is installed on your
computer.
- ✓ The TCP/IP protocol is installed and configured.
- ✓ The name resolving mechanism (DNS or host files) is enabled.
- ✓ For disk space requirements refer to the *HP OpenView Storage Data
Protector Product Announcements, Software Notes, and References*.

Installation

To install Data Protector on the MPE/iX server, proceed as follows:

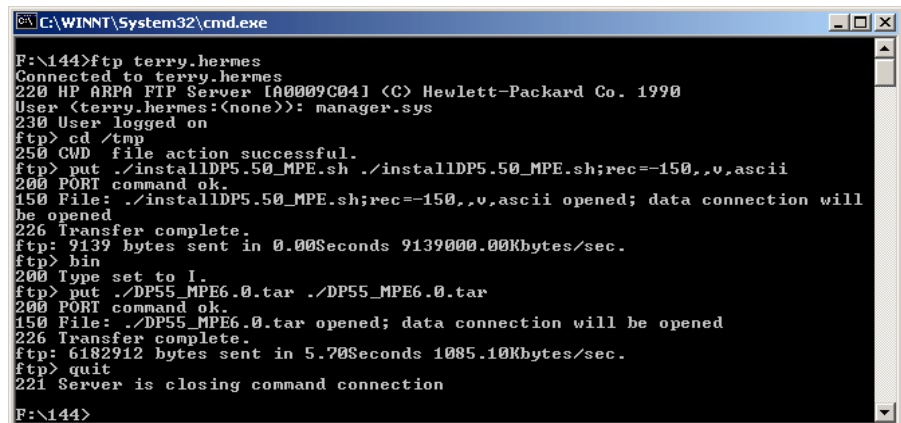
1. Transfer `installDP6.00_MPE.sh` and the `DP60_MPE6.5.tar`
package, or `DP60_MPE7.0.tar` package (depending on the MPE/iX OS
version) to the `/tmp` directory, using the `ftp` utility. See Example 2-1
on page 111.

It is important that you transfer the `installDP6.60_MPE.sh` file with the following characteristics:

- Record size: `-150`
- Block factor: `-empty`
- Variable length of the records of the file: `v`
- Type of coded records: `ASCII`

Example 2-1

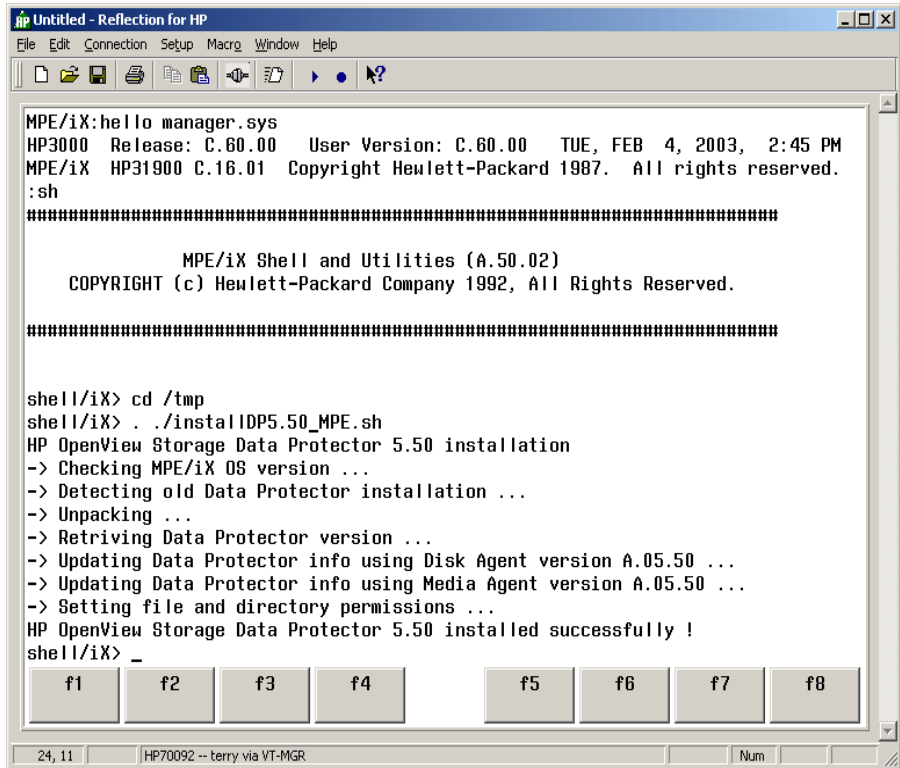
Transfer of the `installDP6.00_MPE.sh` script and `DP60_MPE6.5.tar` package TBD



```
C:\WINNT\System32\cmd.exe
F:\144>ftp terry.hermes
Connected to terry.hermes
220 HP ARPA FTP Server [a0009c041 (C) Hewlett-Packard Co. 1990]
User (terry.hermes:(none)): manager.sys
230 User logged on
ftp> cd /tmp
250 CWD file action successful.
ftp> put ./installDP5.50_MPE.sh ./installDP5.50_MPE.sh;rec=-150,,v,ascii
200 PORT command ok.
150 File: ./installDP5.50_MPE.sh;rec=-150,,v,ascii opened; data connection will
be opened
226 Transfer complete.
ftp> 9139 bytes sent in 0.00Seconds 9139000.00Kbytes/sec.
ftp> bin
200 Type set to I.
ftp> put ./DP55_MPE6.0.tar ./DP55_MPE6.0.tar
200 PORT command ok.
150 File: ./DP55_MPE6.0.tar opened; data connection will be opened
226 Transfer complete.
ftp> 6182912 bytes sent in 5.70Seconds 1085.10Kbytes/sec.
ftp> quit
221 Server is closing command connection
F:\144>
```

2. Log in to the target system and start the unpacking process, as shown in the following example:

Example 2-2 **Unpacking process on target system TBD**



After this operation, the files are located in the `/usr/omni` directory.

NOTE

Use `EDIT/3000` (invoked with the editor command) to change the files below. Refer to *EDIT/3000 Reference Manual* for more information.

3. Add the following line to the `DCNF.NET.SYS` file:

```
omni stream tcp nowait MANAGER.SYS /usr/omni/bin/inet
inet -log /tmp/inet.log
```

4. Add the following line to the `SERVICES.NET.SYS` file:

```
omni 5555/tcp #Data Protector inet
```


- Restart `inetd` to update the configuration with the new settings.

Refer to the *Configuring and Managing MPE/iX Internet Services* manual for more information.

- To check if the Data Protector Inet is running, telnet port 5555 from a different system:

```
telnet <hostname> 5555
```

You will get a message from Data Protector. If there is no response in 10 seconds, check the `INETDCNF.NET.SYS` and `SERVICES.NET.SYS` files.

- Import the system to the Data Protector cell. For the procedure, refer to “Importing Clients to a Cell” on page 177.
- When the client system is successfully imported, add the `MANAGER.SYS` user to the Data Protector Admin user group.

For more information on MPE/iX clients, refer to the *HP OpenView Storage Data Protector MPE/iX System User Guide*, which is located on the Windows installation DVD-ROM at `\Docs\MPE_user.pdf`.

Local Installation of UNIX and Linux Clients

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.

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” on page 54.

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.
- You must have root permissions on every target system.

Limitation

Only the `ksh` shell is supported.

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 clients locally:

1. Insert and mount the UNIX installation DVD-ROM.
2. From the `<Mount_Point>/LOCAL_INSTALL` directory run 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 CD 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 does not reside on the Cell Manager, 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.

However, to upgrade the client components residing on the Cell Manager, run the `omnisetup.sh` command with the `-install <component_list>` parameter after the Cell Manager upgrade has been completed.

- `<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, if you do not specify the `-install` parameter, 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” on page 54.

Table 2-4 Data Protector Component Codes

Component Code	Component
cc	User Interface
momgui	MoM User Interface
da	Disk Agent
ma	General Media Agent
ndmp	NDMP Media Agent
informix	Informix Integration
lotus	Lotus Integration
oracle	Oracle Integration
ov	HP OpenView Network Node Manager
omnist	OmniStorage Integration
sybase	Sybase Integration
sap	SAP R/3 Integration
sapdb	SAP DB Integration
db2	DB2 Integration
emc	EMC Symmetrix Agent

Table 2-4 Data Protector Component Codes

Component Code	Component
ssea	HP StorageWorks Disk Array XP Agent
snapa	HP StorageWorks VA Agent
evaa	HP StorageWorks EVA Agent (legacy)
smisa	HP StorageWorks EVA SMIS-S Agent
fra_ls	French Language Support
jpn_ls	Japanese Language Support

Example

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

```
./omnisetup.sh -server anapola.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

If you want to copy the installation DVD-ROM to your computer and run the installation/upgrade of UNIX or Linux clients from the hard disk, copy at least the DP_DEPOT directory and the LOCAL_INSTALL/omnisetup.sh command. For example, if you copy installation packages to /var/dp60, DP_DEPOT must be a subdirectory of /var/dp60:

```
# pwd  
/var/dp60
```

```
# ls
DP_DEPOT
omnisetup.sh
```

After you have copied this to the hard disk, you can run:

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

Note, that the `-source` option is required. For example:

```
./omnisetup.sh -source /var/dp60
```

What's Next?

If during the installation, you have not specified the name of the Cell Manager, 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, refer to “Importing Clients to a Cell” on page 177. Refer to the online Help index: TBD for information on additional configuration tasks.

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 or Microsoft Exchange, with Data Protector. Data Protector ZDB integrations are software components that allow you to run a ZDB using ZDB disk arrays, such as HP StorageWorks Enterprise Virtual Array.

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 2000/2003 Integration component for backing up the MS Exchange database, HP StorageWorks EVA SMI-S Agent component for a ZDB on HP StorageWorks Enterprise Virtual Array, and so on).

Prerequisites

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.
- You need a license to use the Data Protector integration with a database application (except for the VSS integration). For information about licensing, see “HP OpenView Storage Data Protector On-line Extension” on page A-7.
- At this point, you should have the Cell Manager and Installation Server (optionally, for remote installation) already installed on your network. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17 for instructions.

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” on page 54.

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 MS 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 disk image and filesystem ZDB.
 - 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 locally from the appropriate Windows or HP-UX Installation Server installation DVD-ROM, or remotely using the Installation Server for Windows or for UNIX.

For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

For additional information on specific integration clients, refer to the corresponding sections below:

- Microsoft Exchange Server Clients
- MS SQL Clients
- Sybase Clients
- Informix Server Clients

- SAP R/3 Clients
- SAP DB Clients
- Oracle Clients
- DB2 Clients
- NNM Clients
- NDMP Clients
- MS Volume Shadow Copy Clients
- Lotus Notes/Domino Server Clients
- EMC Symmetrix Integration
- HP StorageWorks XP Integration
- HP StorageWorks Virtual Array Integration
- HP StorageWorks Enterprise Virtual Array Integration

When you have finished installing Data Protector integration software to Data Protector integration clients as described in the listed sections, refer to the *HP OpenView Storage Data Protector Integration Guide*, *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*, or to the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide* to configure Data Protector integration clients.

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 UNIX installation DVD-ROM depending on the platform you install a client to. See “Installing Windows Clients” on page 58 or “Local Installation of UNIX and Linux Clients” on page 113 for instructions.

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 also “Importing Clients to a Cell” on page 177.

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, refer to “Remote Installation of the Data Protector Clients” on page 45.

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

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 StorageWorks 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” on page 158.
- “Installing Data Protector on Microsoft Cluster Server” on page 160.
- “Installing Data Protector Clients on a Veritas Cluster” on page 171.
- “Installing Data Protector Clients on a Novell NetWare Cluster” on page 172.

For more information on clustering, refer to the online Help index: TBD and *HP OpenView Storage Data Protector Concepts Guide*.

What’s Next?

When the installation has been completed, refer to the *HP OpenView Storage Data Protector Integration Guide* for information on configuring the integration.

Microsoft Exchange Server Clients

It is assumed that your Microsoft Exchange Server is up and running.

To be able to back up the Microsoft Exchange Server database or individual mailboxes, you need to select the MS Exchange 2000/2003 Integration component during the installation procedure.

The Microsoft Exchange Single Mailbox integration agent will be installed as part of the Data Protector Microsoft Exchange Server integration package.

MS SQL 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 7.0/2000 Integration component during the installation procedure.

Sybase 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, etc.) that *cannot* be backed up using ON-Bar.

SAP R/3 Clients

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
 - Install this component if you intend to use the Oracle Recovery Manager to back up and restore the SAP R/3 database files.
- Disk Agent
 - Data Protector requires a Disk Agent to be installed on Backup Servers (clients with filesystem data to be backed up).

SAP DB Clients

It is assumed that your SAP DB Server is up and running.

To be able to back up the SAP DB 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 DB database
- Disk Agent - to be able to run a non-integrated offline backup of an SAP DB database

Oracle 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.

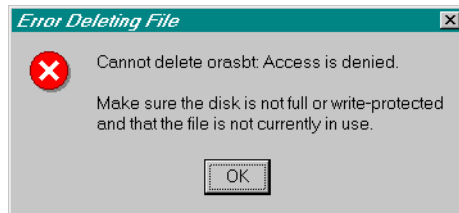
Once the setup has finished, you must start Oracle services and verify that the `<Drive_Label>:\<%SystemRoot%\system32\orasbt.dll` Data Protector Database Library is loaded:

1. In the Windows Explorer switch to the `<DriveLabel>:\<%SystemRoot%\system32` directory and right-click `orasbt.dll`.
2. Select Properties and click the Version tab from the `orasbt.dll` Properties window. In the Description field, you must see the file described as a part of the Data Protector integration.

To verify that `orasbt.dll` is loaded properly, make a copy of the file and then try to delete the original. You should receive a message that the file is currently in use.

Checking the orasbt.dll

Figure 2-20 **Error Message**



OpenVMS

On OpenVMS, after you installed the Oracle integration and configured it as described in the *HP OpenView Storage 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 A.06.00
```

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.

DB2 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.

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 OpenView 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 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.

MS Volume Shadow Copy Clients

Prerequisite

MS Volume Shadow Copy integration is supported on Windows Server 2003 operating system.

To be able to perform shadow copy backups of the VSS-aware writers, you need to select the MS Volume Shadow Copy Integration component during the installation procedure.

If you want to perform VSS transportable backups, Windows Advanced Server 2003 is required. Install the following components on the backup system: MS Volume Shadow Copy Integration and General Media Agent.

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.

EMC Symmetrix Integration

To integrate EMC Symmetrix with Data Protector, install the following Data Protector software components on the application and backup systems:

- EMC Symmetrix Agent (SYMA)
- 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.

Installing in a Cluster

You can install the EMC Symmetrix integration in a cluster environment. For the supported cluster configurations and specific installation requirements, refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with Other Applications

If you want 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 on non-mirrored disks:

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 software
- ✓ SQL*Plus

Oracle server and SQL*NET V2 or NET8 are minimum installation requirements.

- 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.

See the Oracle documentation for information on how to install the Oracle recovery catalog database on the application system on non-mirrored disks. Leave the recovery catalog unregistered.

2. Install the following Data Protector software components:

- EMC Symmetrix Agent - on both the application and backup systems.
- Oracle Integration - if you use the backup set ZDB method, install this component on both the application and backup systems; if you use the proxy-copy ZDB method, install it on the application system only.

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
- The database on the application system can be installed on disk images, logical volumes, or filesystems. The Oracle datafiles *must* be located on disk array source volumes.

The Oracle control file, archive redo log files, and online redo log files do not have to reside on disk array source volumes.

- The user `ora<ORACLE_SID>` with primary group `dba` must be created on the application system.

The UNIX user `<ORACLE_SID>adm` must be created on the application system 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. Refer to the SAP R/3 documentation for more information.

`<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`

Installing Data Protector on Your Network

Installing the Data Protector Integration Clients

```
<SAPDATA_HOME>/saptrace  
/usr/sap/<ORACLE_SID>/SYS/exe/run
```

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 `PROD`, then the permissions inside the directory `/usr/sap/<ORACLE_SID>/SYS/exe/run` should look like:

```
-rwsr-xr-x  1 oraprod dba 4598276 Apr 17  1998 brarchive  
-rwsr-xr-x  1 oraprod dba 4750020 Apr 17  1998 brbackup  
-rwsr-xr-x  1 oraprod dba 4286707 Apr 17  1998 brconnect  
-rwsr-xr-x  1 prodadm sapsys 430467 Apr 17  1998 brrestore  
-rwsr-xr-x  1 oraprod dba 188629 Apr 17  1998 brtools  
-rwsr-xr-x  1 oraprod dba 6081400 May  8  1998 sapdba.
```

Installation Procedure

Perform the following installation tasks:

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components:
 - EMC Symmetrix Agent - on both the application and backup systems
 - SAP R/3 Integration - on the application system only
 - Disk Agent - on both the application and backup systems

HP StorageWorks XP Integration

To integrate HP StorageWorks XP with Data Protector, install the following Data Protector software components to the application and backup systems:

- HP StorageWorks 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 disk image and filesystem ZDB.

Installing in a Cluster

You can install the HP StorageWorks XP integration in a cluster environment. For the supported cluster configurations and specific installation requirements, refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with Other Applications

If you want to install the HP StorageWorks XP 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 StorageWorks XP integration with Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server.

HP StorageWorks XP Integration with Oracle

Prerequisites

- The following software must be installed and configured on the application system source volumes:
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 software
 - ✓ SQL*Plus

Oracle server and SQL*NET V2 or NET8 are minimum installation requirements.

- The Oracle database files on the application system must be installed on HP StorageWorks Disk Array XP LDEVs that are mirrored to the backup system.

Depending on the location of the Oracle control file, online redo log files, and Oracle9i/10g SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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 variables. For more information, see the *HP OpenView Storage 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.

See the Oracle documentation for information on how to install the Oracle recovery catalog database on the application system on non-mirrored disks. Leave the recovery catalog unregistered.

2. Install the following Data Protector software components:

- HP StorageWorks XP Agent - on both the application and backup systems
- Oracle Integration - if you want to use the backup set ZDB method, install this component on both the application and backup systems; if you want to use the proxy-copy ZDB method, install it on the application system only.

HP StorageWorks XP Integration with SAP R/3

Prerequisites

- The following Oracle software must be installed and configured on the disk array source volumes:
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 software
 - ✓ SQL*Plus

Oracle server and SQL*NET V2 or NET8 are minimum installation requirements.

- The database on the application systems can be installed on disk images, logical volumes, or filesystems. The Oracle datafiles *must* reside on disk array source volumes.

Depending on the location of the Oracle control file, online redo log files, and Oracle9i/10g SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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 variables. For more

information, see the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

The Oracle archive redo log files do not have to reside on source volumes.

- The user ora<ORACLE_SID> with primary group dba must be created on the application system.

On UNIX systems, the UNIX user <ORACLE_SID>adm must be created on the application system 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. See the SAP R/3 documentation for more information.

<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)
BRTOOLS (Windows systems)

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 PROD, then the permissions inside the directory `/usr/sap/<ORACLE_SID>/SYS/exe/run` should look like:

```
-rwsr-xr-x 1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x 1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x 1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x 1 prodadm sapsys 430467 Apr 17 1998
brrestore
-rwsr-xr-x 1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x 1 oraprod dba 6081400 May 8 1998 sapdba.
```

Windows Systems

On Windows systems, the `SAPMNT` share must be created on the application system and must contain the `<SAPDATA_HOME>` subdirectory.

Installation Procedure

Perform the following installation tasks:

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the Data Protector integration software.

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.

Install the following Data Protector software components:

- HP StorageWorks XP Agent - on both the application and backup systems
- SAP R/3 Integration - on the application system only
- Disk Agent - on both the application and backup systems

HP StorageWorks XP Integration with Microsoft Exchange Server

Prerequisite

The Microsoft Exchange Server database must be installed on the application system on the HP StorageWorks Disk Array XP volumes (LDEVs), which are mirrored to the backup system. The mirroring can be BC or CA 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 StorageWorks XP Agent - on both the application and the backup system
- MS Exchange 2000/2003 Integration - on the application system only

HP StorageWorks XP 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 StorageWorks XP Agent
- MS SQL 7.0/2000 Integration

HP StorageWorks Virtual Array Integration

To integrate HP StorageWorks VA with Data Protector, install the following Data Protector software components to the application and backup systems:

- HP StorageWorks VA 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 disk image and filesystem ZDB.

Installing in a Cluster

You can install the HP StorageWorks VA integration in a cluster environment. For the supported cluster configurations and specific installation requirements, refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with Other Applications

If you want to install the HP StorageWorks VA 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 StorageWorks VA integration with Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server.

HP StorageWorks VA Integration with Oracle

Prerequisites

- The following software must be installed and configured on the application system source volumes and on the backup system for the backup set ZDB method:

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8/9 software
- ✓ 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.

Oracle server and SQL*NET V2 or NET8/9 are minimum installation requirements.

- The Oracle database files used by the application system must be installed on the source volumes that will be replicated using the VA Agent (SNAPA).

Depending on the location of the Oracle control file, online redo log files, and Oracle9i/10g SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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_OLF, and ZDB_ORA_NO_CHECKCONF_IR omnicirc variables. For more information, see the *HP OpenView Storage 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.

Refer to Oracle documentation for information on how to install the Oracle recovery catalog database on the application system. Leave the recovery catalog unregistered.

2. Install the following Data Protector software components:

- HP StorageWorks VA Agent - on both the application and backup systems
- Oracle Integration - if you want to use the backup set ZDB method, install this component on both the application and backup systems; if you want to use the proxy-copy ZDB method, install it on the application system only.

HP StorageWorks VA Integration with SAP R/3

Prerequisites

- The following Oracle software must be installed on the application system source volumes:

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 software
- ✓ SQL*Plus

Oracle server and SQL*NET V2 or NET8 are minimum installation requirements.

- The Oracle datafiles used by the application system must be installed on source volumes that will be replicated using the VA agent (SNAPA).

Depending on the location of the Oracle control file, online redo log files, and Oracle9i/10g SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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 variables. For more information, see the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

The Oracle archive redo log files do not have to reside on source volumes.

- The user `ora<ORACLE_SID>` with primary group `dba` must be created on the application system.

On UNIX systems, the UNIX user `<ORACLE_SID>adm` must be created on the application system 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. Refer to the SAP R/3 documentation for more information.

Installing Data Protector on Your Network

Installing the Data Protector Integration Clients

<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)
BRTOOLS (Windows systems)

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 PROD, then the permissions inside the directory /usr/sap/<ORACLE_SID>/SYS/exe/run should look like:

```
-rwsr-xr-x  1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x  1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x  1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x  1 prodadm sapsys 430467 Apr 17 1998
brrestore
-rwsr-xr-x  1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x  1 oraprod dba 6081400 May 8 1998 sapdba.
```

Windows Systems On Windows systems, the `SAPMNT` share must be created on the application system and must contain the `<SAPDATA_HOME>` subdirectory.

Installation Procedure Perform the following installation tasks:

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the Data Protector integration software.

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.

Install the following Data Protector software components:

- HP StorageWorks VA Agent - on both the application and backup systems
- SAP R/3 Integration - on the application system only
- Disk Agent - on both the application and backup systems

HP StorageWorks VA 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 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 StorageWorks VA Agent - on both the application and the backup system
- MS Exchange 2000/2003 Integration - on the application system only

HP StorageWorks VA 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 StorageWorks VA Agent
- MS SQL 7.0/2000 Integration

HP StorageWorks Enterprise Virtual Array Integration

To integrate HP StorageWorks EVA with Data Protector, install the following Data Protector software components to the application and backup systems:

- HP StorageWorks 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 disk image and filesystem ZDB.

Installing in a Cluster You can install the HP StorageWorks EVA integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*.

Integrating with Other Applications If you want to install the HP StorageWorks EVA 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 StorageWorks EVA integration with Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server.

HP StorageWorks EVA Integration with Oracle

Prerequisites

- The following Oracle software must be installed on the application system source volumes:

- ✓ Oracle Enterprise Server (RDBMS)
- ✓ Oracle Net8 software
- ✓ SQL*Plus

Oracle server and SQL*NET V2 or NET8 are minimum installation requirements.

- 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 Oracle9i/10g SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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 variables. For more information, see the *HP OpenView Storage 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.
See the Oracle documentation for information on how to install the Oracle recovery catalog database on the application system. Leave the recovery catalog unregistered.
2. Install the following Data Protector software components:
 - HP StorageWorks EVA SMI-S Agent on both the application and backup systems
 - Oracle Integration - if you want to use the backup set ZDB method, install this component on both the application and backup systems; if you want to use the proxy-copy ZDB method, install it on the application system only.

HP StorageWorks EVA Integration with SAP R/3

Prerequisites

- The following Oracle software must be installed on the application system source volumes.
 - ✓ Oracle Enterprise Server (RDBMS)
 - ✓ Oracle Net8 software
 - ✓ SQL*PlusRDBMS and SQL*NET V2 or NET8 are minimum installation requirements.
- 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 Oracle9i/10g SPFILE, the following two options are possible:
 - Oracle control file, online redo log files, and Oracle9i/10g 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 Oracle9i/10g 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 omnic variables. For more information, see the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

The Oracle archive redo log files do not have to reside on source volumes.

- The user ora<ORACLE_SID> with primary group dba must be created on the application system.

On UNIX systems, the UNIX user <ORACLE_SID>adm must be created on the application system 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. Refer to the SAP R/3 documentation for more information.

<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

Installing Data Protector on Your Network

Installing the Data Protector Integration Clients

```
<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)
BRTOOLS (Windows systems)
```

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 `PROD`, then the permissions inside the directory `/usr/sap/<ORACLE_SID>/SYS/exe/run` should look like:

```
-rwsr-xr-x  1 oraprod dba 4598276 Apr 17 1998 brarchive
-rwsr-xr-x  1 oraprod dba 4750020 Apr 17 1998 brbackup
-rwsr-xr-x  1 oraprod dba 4286707 Apr 17 1998 brconnect
-rwsr-xr-x  1 prodadm sapsys 430467 Apr 17 1998
brrestore
-rwsr-xr-x  1 oraprod dba 188629 Apr 17 1998 brtools
-rwsr-xr-x  1 oraprod dba 6081400 May 8 1998 sapdba.
```

Windows Systems

On Windows systems, the `SAPMNT` share must be created on the application system and must contain the `<SAPDATA_HOME>` subdirectory.

Installation Procedure

Perform the following installation tasks:

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the Data Protector integration software.

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.

Install the following Data Protector software components:

- HP StorageWorks EVA SMI-S Agent on both the application and backup systems
- SAP R/3 Integration - on the application system only
- Disk Agent - on both the application and backup systems

HP StorageWorks EVA 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 StorageWorks EVA SMI-S Agent on both the application and backup systems
- MS Exchange 2000/2003 Integration - on the application system only

HP StorageWorks EVA Integration with MS SQL

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 StorageWorks EVA SMI-S Agent on both the application and backup systems
- MS SQL 7.0/2000 Integration

Installing Localized Data Protector User Interface

Data Protector A.06.00 provides a localized Data Protector user interface on Windows and UNIX systems. This consists of the localized Data Protector GUI and CLI. Localized online Help and printed documentation is also provided. For more information on which Data Protector manuals are localized, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

NOTE

By default, during the Data Protector installation, the English language support is installed. When you install an additional language support, the localized Data Protector user interface is started according to the locale environment set on the system.

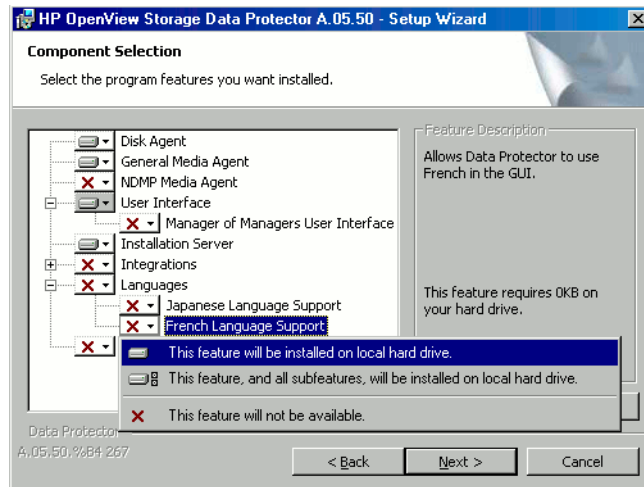
Installing Localized Data Protector User Interface on Windows Systems

Local Installation

To install the localized Data Protector user interface on Windows systems, select the appropriate language support (French or Japanese) in the Custom Setup page of the Setup wizard, as shown on Figure 2-21.

For the local installation procedure, refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17.

Figure 2-21 **Selecting Language Support at Setup**

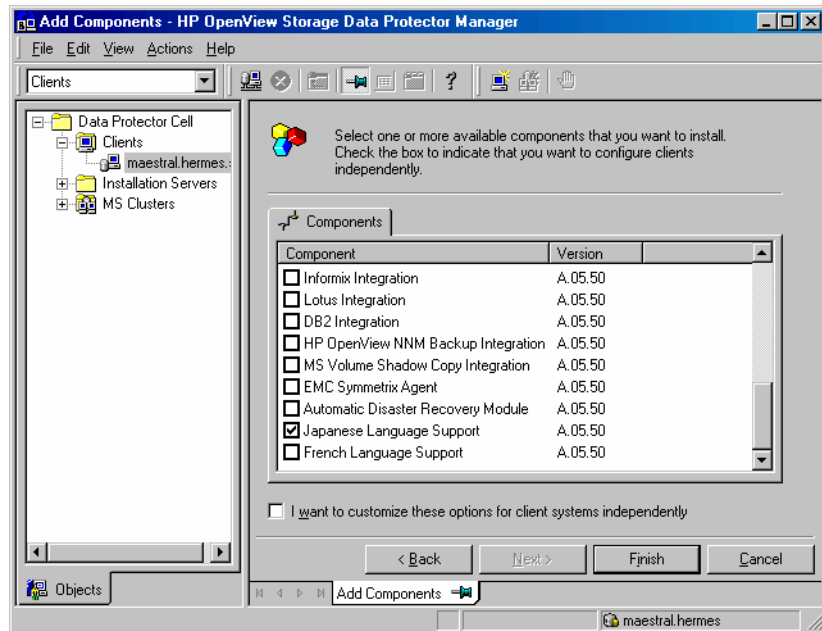


Remote Installation

When distributing the Data Protector language support remotely using the Installation Server, select the appropriate language support in the Component Selection page of the Add Components wizard, as shown on Figure 2-22.

For the procedure on how to remotely add the Data Protector software components to clients, refer to “Remote Installation of the Data Protector Clients” on page 45.

Figure 2-22 Installing Language Support Remotely



Installing Localized Data Protector User Interface on UNIX Systems

Local Installation You can install the Japanese or French language support locally only on a Data Protector client using the `omnisetup.sh` command. Specify the `jpn_ls` or `fra_ls` software components depending on the language support you need. For the detailed procedure, refer to “Local Installation of UNIX and Linux Clients” on page 113.

If you are using the `swinstall` or `pkgadd` utility to install the Data Protector Cell Manager or Installation Server, you can only install the English language support. If you want the localized Data Protector user interface to reside on the same system with the Cell Manager or Installation Server, you need to install the additional language support remotely.

Remote Installation

When distributing the Data Protector language support remotely using the Installation Server, select the appropriate language support in the Component Selection page of the Add Components wizard, as shown on Figure 2-22.

For the procedure on how to remotely add the Data Protector software components to clients, refer to “Remote Installation of the Data Protector Clients” on page 45.

Troubleshooting

If the English Data Protector user interface is started after you installed a different language support, verify the following:

1. Check that the following files exist:

For French Language Support:

- On Windows: `<Data_Protector_home>\bin\OmniFra.dll`
- On HP-UX: `/opt/omni/lib/nls/fr.iso88591/omni.cat`
- On Solaris: `/opt/omni/lib/nls/fr.ISO8859-1/omni.cat`

For Japanese Language Support:

- On Windows: `<Data_Protector_home>\bin\OmniJpn.dll`
- On HP-UX: `/opt/omni/lib/nls/ja.eucJP/omni.cat` and `/opt/omni/lib/nls/ja.SJIS/omni.cat`
- On Solaris: `/opt/omni/lib/nls/ja.eucJP/omni.cat` and `/opt/omni/lib/nls/ja.PCK/omni.cat`

2. Check the locale environment settings on your system:

- On Windows: In the Windows Control Panel, click Regional Options and check that you have an appropriate language selected in locale and language settings.
- On UNIX: 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; 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 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 and Solaris 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)” on page 17.

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, please refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Limitations of SSE for HP-UX and Solaris

- 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, please refer to the *HP OpenView Storage 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, refer to “Data Protector Passwords” on page 293.

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, refer to the *HP OpenView Storage 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, refer to the online Help index: TBD.

What's Next?

When the installation has been completed, refer to the online Help index: TBD 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. For details on supported operating system versions, refer to the *HP OpenView Storage 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 the “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17.

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. Refer to the online Help index: TBD for more information on configuring MC/ServiceGuard with Data Protector.

Installing a Cluster-Aware Client

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 HP-UX client. Refer to “Installing HP-UX Clients” on page 64 for detailed instructions.

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” on page 180.

Refer to the online Help index: TBD for more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks.

Installing Data Protector on Microsoft Cluster Server

For supported operating systems for Microsoft Cluster Server integration, refer to the *HP OpenView Storage 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 the cluster-aware Cell Manager, make sure that you do not have resources with the following names on the cluster:

OBVS_MCRS,OBVS_VELOCIS,OmniBack_Share

If they exist and you are performing a new installation (not an upgrade), delete or rename these resources, because Data Protector uses those names for the Data Protector virtual server.

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.

To properly install and configure Data Protector in a Microsoft Cluster Server environment, you must provide an account with the appropriate user rights:

- ✓ Administrator rights on the Cell Manager
- ✓ Cluster Administrator rights within the cluster
- ✓ Password Never Expires
- ✓ Logon as a service
- ✓ User Cannot Change Password
- ✓ All logon hours are allowed

NOTE

When you are installing a Data Protector Cell Manager as cluster-aware in a Microsoft Cluster environment, the Data Protector User Account must be a domain user account, which has all of the above mentioned user rights.

TIP

An account with administrator rights on all the cluster systems is required for a Cluster Server installation. It is recommended that you use this account to install Data Protector as well. Invalid user rights may result in Data Protector services running in the standard, instead of the cluster-aware, mode.

Before you start installing the Cell Manager software on a cluster, check the requirements:

- ✓ A cluster must be installed properly with all of its functionality. For example, you must be able to move groups from one to another node as many times as needed, with no problems with shared disk(s).
- ✓ At least one group in the cluster should have a *<File Share>* resource defined. Data Protector will install its database components on this *<File Share>* resource. Refer to the cluster specific documentation in order to define *<File Share>* resource. Note that the file share name of the *<File Share>* resource cannot be OmniBack.
- ✓ If the virtual server does not exist in the same group as the *<File Share>* resource group, a new virtual server must be created using a free registered IP address and associating a network name with it.
- ✓ The *<File Share>* resource where Data Protector is to be installed must have the IP Address, Network Name, and Physical Disk set among the *<File Share>* dependencies. This is necessary to ensure that Data Protector cluster group will be able to run on any node independently of any other group.
- ✓ Ensure that only the cluster administrator has access to the *<File Share>* resource and that he has full access to it.
- ✓ Each system of the cluster should be up and running properly.

- ✓ If a system in the cluster has the Data Protector software installed, you need to uninstall it prior to the setup. The upgrade option is supported only if the already installed Data Protector software is the Cell Manager which was installed in a cluster-aware mode.
- ✓ Data Protector must be installed on the same location (drive and pathname) on all cluster nodes. Ensure that these locations are free.
- ✓ Other MSI based installations must *not* be running on other cluster nodes.

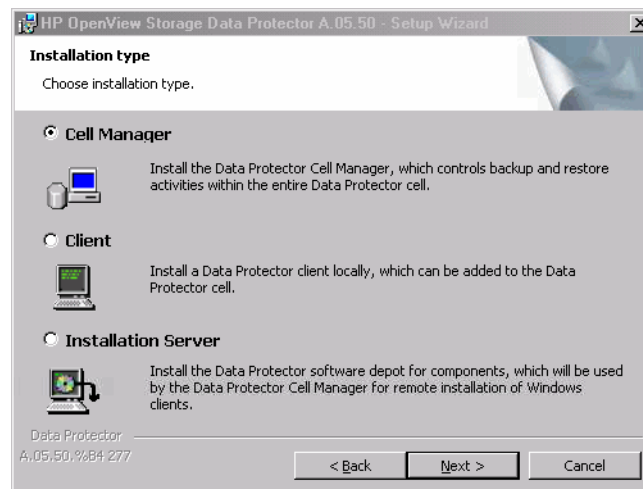
Local Installation

The Data Protector cluster-aware Cell Manager software must be installed locally, from the DVD-ROM. This can be done as follows:

1. From the installation DVD-ROM, run `\Windows_other\i386\setup.exe`. The Data Protector Setup Wizard displays.
2. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
3. In the Installation Type page, select **Cell Manager** and then click **Next** to install Data Protector Cell Manager software.

Figure 2-23

Selecting the Installation Type



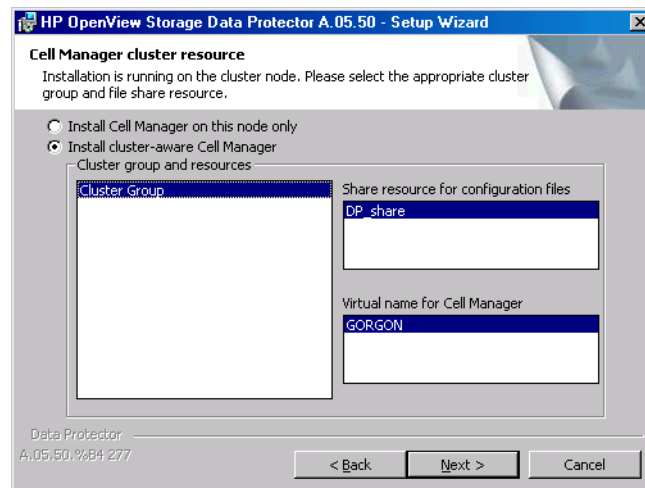
4. Setup automatically detects that it is running in a cluster environment. Select **Install cluster-aware Cell Manager** to enable a cluster setup.

Select the cluster group, the virtual hostname, and the cluster *<File Share>* resource on which Data Protector shared files and the database will reside.

NOTE

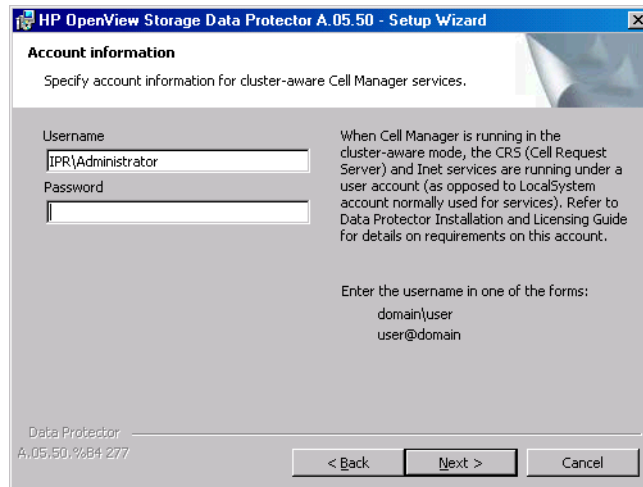
If you select **Install Cell Manager** on this node only, the Cell Manager will *not* be cluster aware. Refer to “Installing a Windows Cell Manager” on page 26.

Figure 2-24 **Selecting the Cluster Resource**



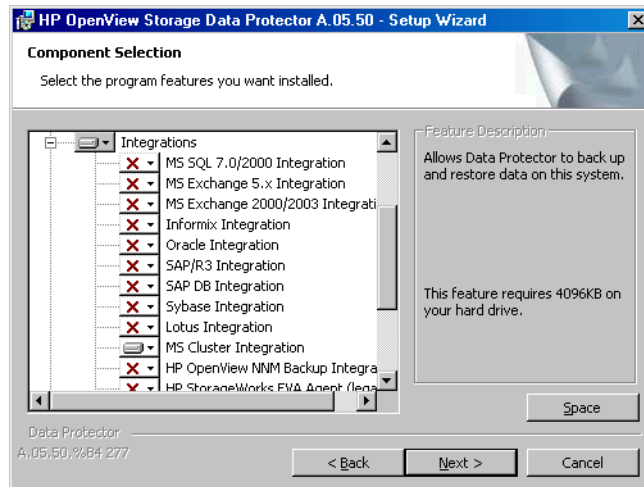
5. Enter the username and password for the account that will be used to start Data Protector services.

Figure 2-25 **Entering the Account Information**



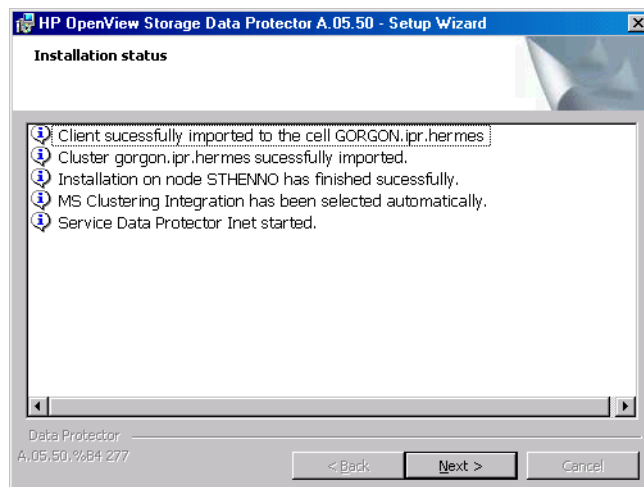
6. Click **Next** to install Data Protector on the default folder.
Otherwise, click **Change** to open the **Change Current Destination Folder** window and enter a new path.
7. In the **Component Selection** window, select the components you want to install on all cluster nodes and cluster virtual servers. Click **Next**.
The **MS Cluster Integration** component is selected automatically.
The selected components will be installed on all the cluster nodes.

Figure 2-26 Component Selection Page



8. The component selection summary page is displayed. Click **Install**.
9. The **Installation** setup page is displayed. Click **Next**.

Figure 2-27 Installation Status Page



10. To start Data Protector immediately after install, select Start the Data Protector Manager GUI.

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

To install or upgrade the HP OpenView AutoPass utility, select the Start AutoPass installation or the Upgrade AutoPass installation option.

It is *not* recommended to install the HP OpenView AutoPass utility in Microsoft 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.

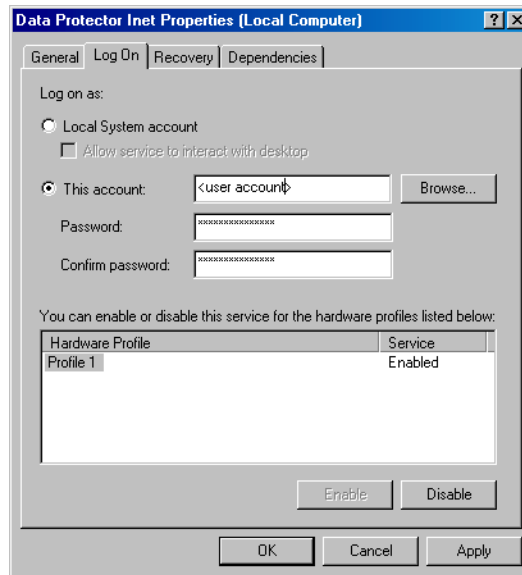
Click Finish to complete the installation.

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 Figure 2-28 on page 167.

Figure 2-28 **Data Protector User Account**



2. Switch to the `<Data_Protector_home>\bin` directory and run the following command:

```
omnirsh <host> INFO_CLUS
```

where `<host>` is the name of the cluster virtual server. 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`. You should see the newly installed systems listed in the Results Area.

Installing a Cluster-Aware Client

Prerequisites

Before you install a cluster-aware Data Protector client, the following prerequisites must be fulfilled:

- ✓ A cluster must be installed properly with all of its functionality on all cluster nodes. For example, you must be able to move groups from one to another node as many times as needed, with no problems with shared disk(s).
- ✓ Each system of the cluster should be up and running properly.
- ✓ TBD If Oracle8 is installed on cluster nodes, stop Oracle8 database services (recommendation) on the cluster nodes.

Local Installation

The Data Protector cluster-aware 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.

The cluster Administrator account is required to perform the installation. Apart from that, the cluster client setup is the same as for the Windows client setup. The Cluster Integration component, which is selected by default during the installation, must be installed in addition to Data Protector client components, such as Disk Agents and Media Agents.

See “Installing Windows Clients” on page 58 for information on how to locally install a Data Protector Windows client system. Note that during the installation, Data Protector reports that a cluster was detected.

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 TBD Oracle8 resource group.

NOTE

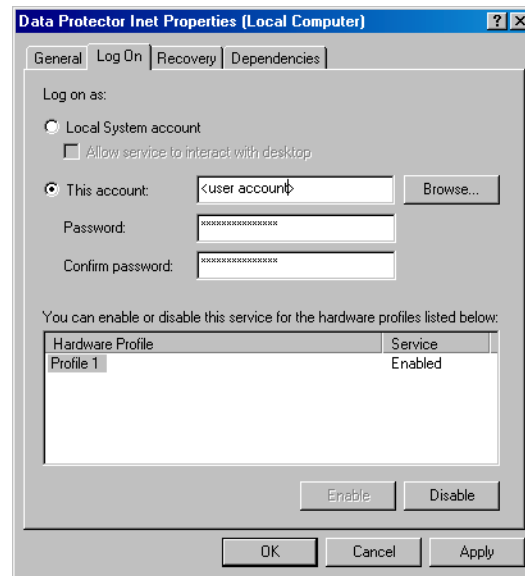
You can import a cluster-aware client to the Data Protector cell that is managed using either the standard Cell Manager or the cluster-aware Cell Manager.

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 Figure 2-28 on page 167.

Figure 2-29 Data Protector User Account



2. Switch to the `<Data_Protector_home>\bin` directory.
3. Run the following command:

```
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. See “Installing Data Protector on Microsoft Cluster with Veritas Volume Manager” on page B-70, for the additional steps to be performed.

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” on page 180.

Refer to the online Help index: TBD for more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks.

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.

Note that if you want 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 a Client

The installation procedure is standard procedure for installing Data Protector on a Solaris client system. Refer to “Installing Solaris Clients” on page 67 for detailed instructions.

What’s Next?

When the installation has been completed:

- If you want to back up the virtual server, you must import it into the cell.
- If you want to back up the physical nodes, you must also import them into the cell.

See “Importing a Cluster-Aware Client to a Cell” on page 180.

Refer to the online Help index: TBD for more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks.

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 refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Note that if you want 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 a Client

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 /override=question
```

The modified unload script for every virtual server is:

```
nss /pooldeactivate=FIRST /override=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, refer to 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 `nmlArray = Array("SMDR", "TSA600", "TSAPROXY")` (or `nmlArray = Array("SMDR", "TSAFS /NoCluster")`) line in the `Sub Main()` section to:

```
— nmlArray = Array("SMDR", "TSA600 /cluster=off",  
  "TSAPROXY") if you have TSA600 installed.
```

```
— nmlArray = 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. Refer to “Local Installation of the Novell NetWare Clients” on page 96 for detailed instructions.

What’s Next?

When the installation has been completed:

- If you want to back up the physical nodes, you must also import them into the cell.
- If you want to back up the virtual server (shared cluster volumes), you must import it into the cell.

See “Importing a Cluster-Aware Client to a Cell” on page 180.

Refer to the online Help index: TBD for more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks.

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. Refer to “Importing Clients to a Cell” on page 177.
- How to import an Installation Server to a cell using the graphical user interface. Refer to “Importing an Installation Server to a Cell” on page 179.
- How to import clusters/virtual servers using the graphical user interface. Refer to “Importing a Cluster-Aware Client to a Cell” on page 180.
- How to export clients using the graphical user interface. Refer to “Exporting Clients from a Cell” on page 184.
- How to ensure security using the graphical user interface. Refer to “Security Considerations” on page 187.
- How to verify which Data Protector patches are installed. Refer to “Verifying Which Data Protector Patches Are Installed” on page 203.
- How to uninstall the Data Protector software. Refer to “Uninstalling Data Protector Software” on page 205.
- How to add or remove Data Protector software components. Refer to “Changing Data Protector Software Components” on page 216.

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, OpenVMS, and Windows XP Home Edition, 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, refer to “Exporting Clients from a Cell” on page 184.

IMPORTANT

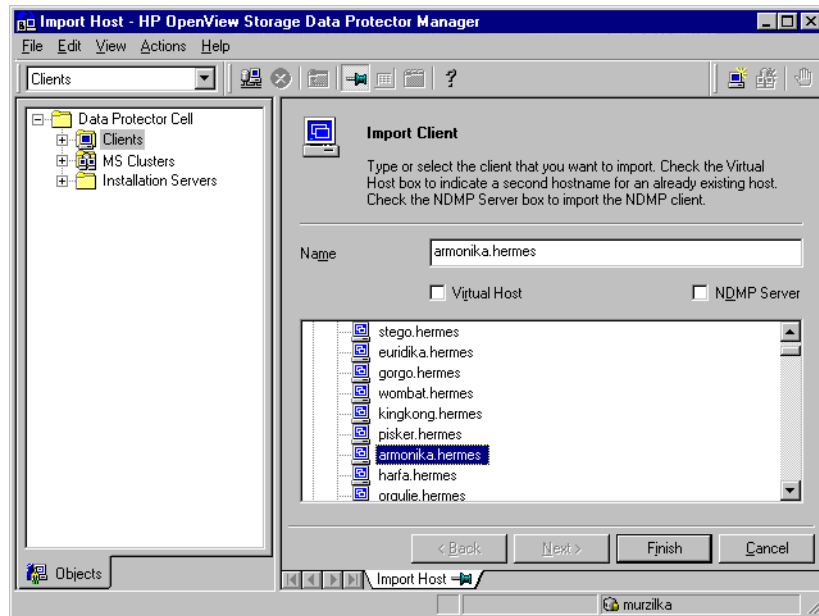
After you have installed Data Protector clients and imported them to a cell, it is highly recommended to protect the clients from access by unwanted cell authorities. Refer to “Securing Clients” on page 190.

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 Figure 3-1.

Figure 3-1 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 OpenVMS client, type the TCP/IP name of the OpenVMS client in the `Name` text box.

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, i.e., it is not installed on a Cell Manager.

In this case, it will not be possible to remotely (push) 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 Figure 3-1 on page 178.
3. Follow the wizard to add a system to the cell. Refer to online Help for details.

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

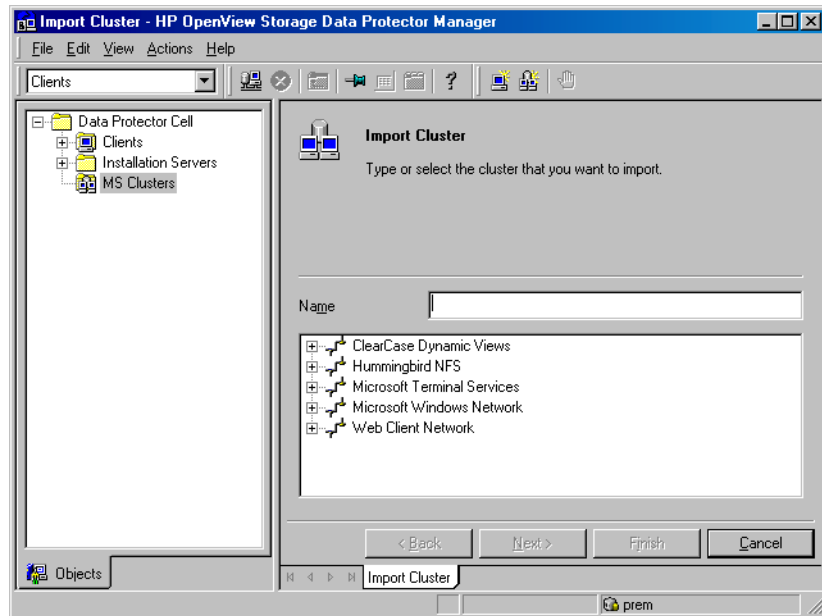
- Data Protector must be installed on all cluster nodes.
- All cluster packages must be running within the cluster.

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 Figure 3-2.

Figure 3-2 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

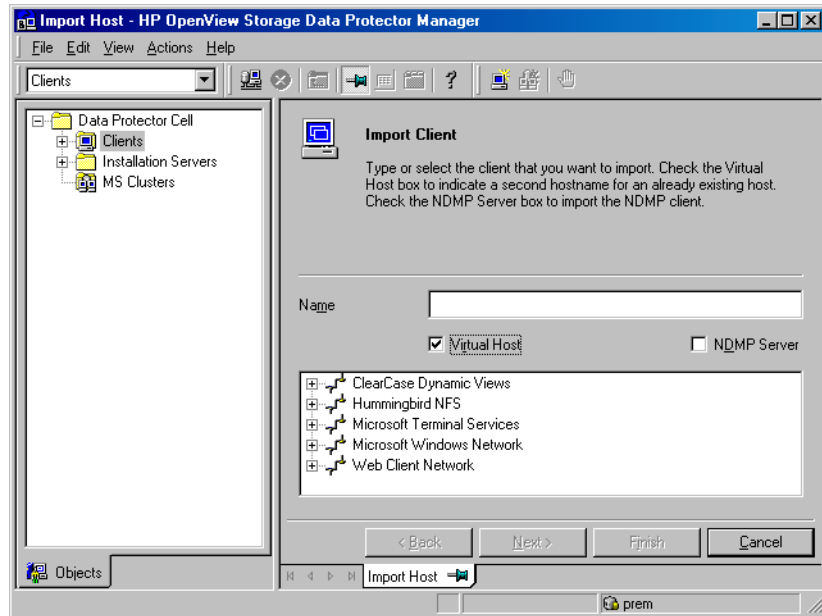
To import a MC/ServiceGuard, Veritas, Tru64 Cluster, or Novell NetWare Cluster Services client to the Data Protector cell, proceed as follows:

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 Figure 3-3.

4. Click Finish to import the virtual server.

Figure 3-3 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” on page 177.

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 fix problems caused by insufficient licenses

By exporting a client from a cell, the license becomes available to some other system.

Prerequisites

Before you export a client, check the following:

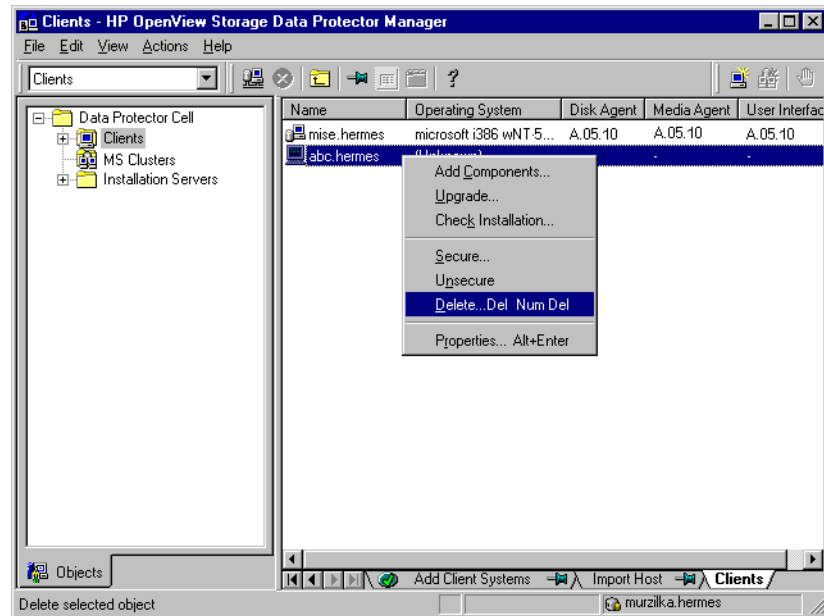
- ✓ All the occurrences of the client have been removed from backup specifications. Otherwise, Data Protector will try to back up unknown clients and this part of the backup specification will fail. Refer to online Help for instructions on how to modify backup specifications.
- ✓ The client does not have any connected and configured backup devices. Once the system is exported, Data Protector can no longer use its backup devices 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 Figure 3-4 on page 185.

Figure 3-4 Exporting a Client System



3. You will be asked if 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 a Data Protector client using the Installation Server which is installed on the same system as the client you would like to export.

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**.

Maintaining the Installation
Exporting Clients from a Cell

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. There are also some changes in the default behavior compared to the previous releases of Data Protector. See “Start Backup Specification User Right” on page 199.

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, refer to “Securing Clients” on page 190.

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. The 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 rights.

- 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” on page 199.
- 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.
- The configuration of users is connected with user validation (see “Strict Hostname Checking” on page 197). Enhanced validation can be worthless without careful user configuration and vice versa - even the most careful user configuration can be worked around without the enhanced validation.
- It is important that there are no “weak” user specifications in the Data Protector user list. Note that 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.

See also the *HP OpenView Storage Data Protector Administrator's Guide* for details on 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. Refer to “Strict Hostname Checking” on page 197 and “Securing Clients” on page 190.

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, or media copying, data is transferred via network. If sufficient separation from the untrusted network cannot be achieved with network segmentation, one must use locally attached devices or a custom encoding library.

Refer also to the *HP OpenView Storage Data Protector Concepts Guide* for other security related aspects.

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 also “Client Security” on page 187.

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

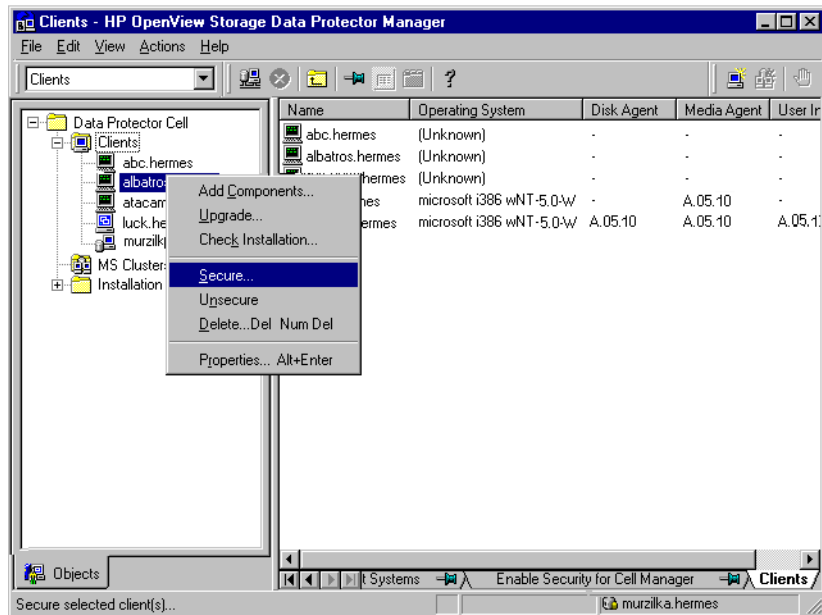
If an Installation Server residing on a system other than the Cell Manager is not added to the list of allowed clients, it will not have access to a secured client. In this case, the operations dependent on the Installation Server (such as checking installation, adding components and removing clients) 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:

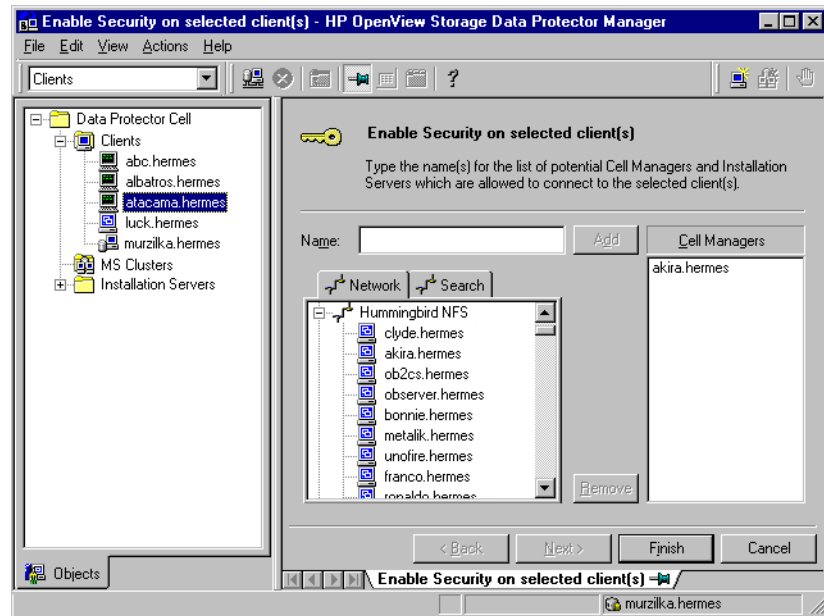
1. In the Context List, click `Clients`.
2. In the Scoping Pane, expand `Clients`, right-click the client(s) you want to secure, and click `Secure`. See Figure 3-5.

Figure 3-5 **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` (on Windows GUI only) or `Search` tabs. Click `Add` to add each system to the list. See Figure 3-6.

Figure 3-6 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:

- On Windows: `<Data_Protector_home>\log`
- On HP-UX, Solaris, and Linux: `/var/opt/omni/log`
- On other UNIX systems: `/usr/omni/log`

To secure all clients in the cell, perform the following steps in the Data Protector GUI:

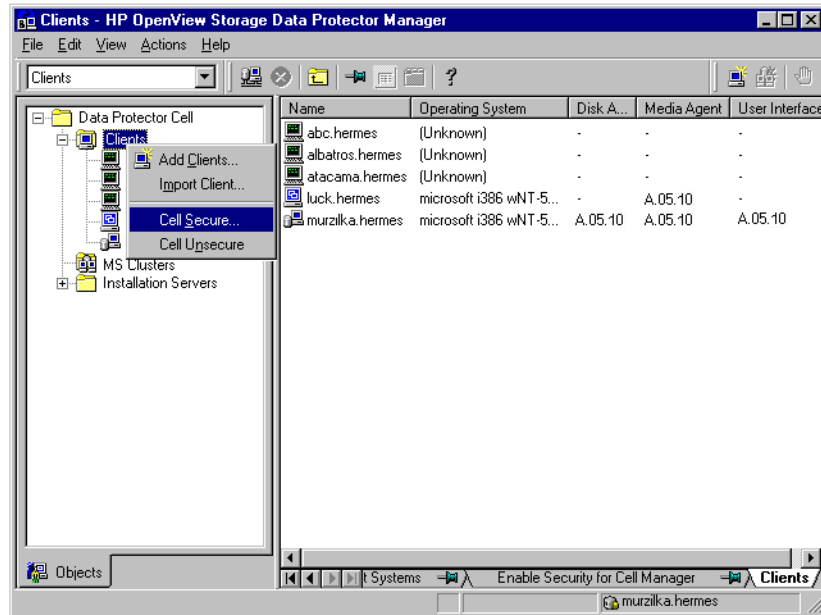
1. In the Context List, click **Clients**.

Maintaining the Installation

Security Considerations

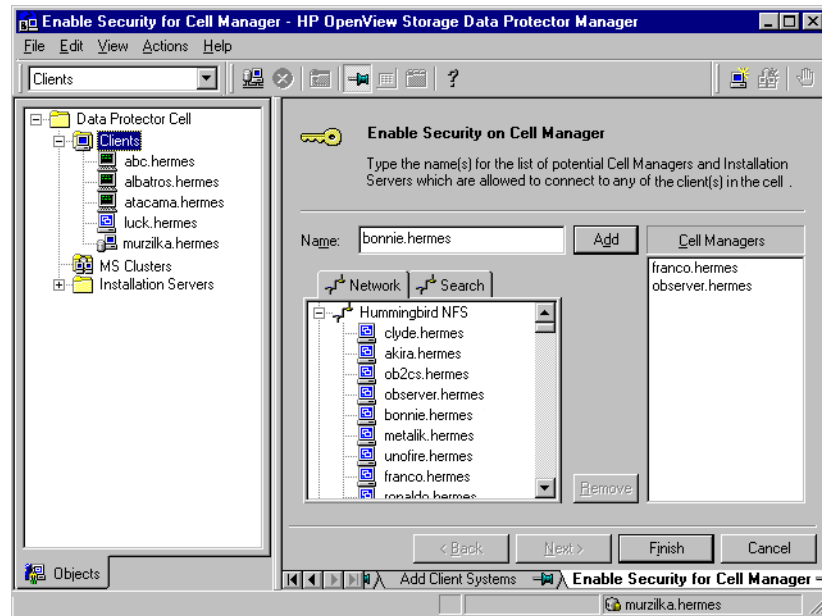
2. In the Scoping Pane, right-click Clients and click Cell Secure. See Figure 3-7.

Figure 3-7 **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 Figure 3-8.

Figure 3-8 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:

- On Windows: `<Data_Protector_home>\log`
- On HP-UX, Solaris, and Linux: `/var/opt/omni/log`
- On other UNIX 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

If you want 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).

If you want 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 directories:

- On Windows: `<Data_Protector_home>\Config\client`
- On HP-UX, Solaris, and Linux: `/etc/opt/omni/client`
- On other UNIX 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” (i.e. 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, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.
- 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, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Enabling the Feature

To enable the strict hostname checking, set the StrictSecurityFlags flags 0x0003 in the global options file.

For more information about the global options file, refer to the online Help index keyword “global options file”.

Start Backup Specification User Right

For general information about the Data Protector users and user rights, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

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 about the global options file, refer to the online Help index keyword “global options file”.

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, refer to the online Help index keyword “global options file”.

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, create the `/etc/opt/omni/server/cell/host_trusts` file on a UNIX or Linux Cell Manager or `<Data_Protector_home>\Config\Server\cell\host_trusts` file on a Windows Cell Manager.

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:

- On Windows: `<Data_Protector_home>\log`
- On HP-UX, Solaris, or Linux: `/var/opt/omni/log`

Maintaining the Installation
Security Considerations

- On other UNIX systems: `/usr/omni/log`

**Cell Manager
Security Events**

Cell Manager security events are logged in the `security.log` file:

- On a Windows Cell Manager:
`<Data_Protector_home>\log\server`
- On a UNIX Cell Manager: `/var/opt/omni/server/log`

Verifying Which Data Protector Patches Are Installed

You can verify which Data Protector patches are installed on each system in the cell.

Limitations

Below are the limitations for patch verification:

- Patch verification can be used only on Data Protector clients that have Data Protector A.05.10 or later installed. If the command encounters a client with an older Data Protector version, an error message is returned.
- Patch verification can check which patches are installed only on members that belong to the same cell.

Prerequisite

To use this functionality, you should have the User Interface component installed.

NOTE

After you install a site-specific patch, it will always be listed in the patch report, even if it has been included into later patches.

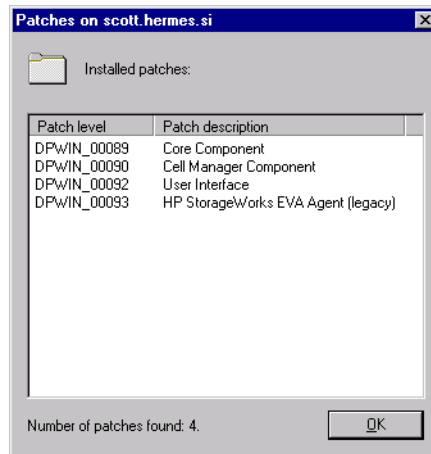
To verify which Data Protector patches are installed on a particular system in a cell, use the Data Protector GUI or CLI.

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 3-9 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, run the `omnicheck -patches -host hostname` command from the following directory:

- On Windows: `<Data_Protector_home>\bin`
- On UNIX or Linux: `/opt/omni/bin`

where *hostname* is the name of the system to be verified.

Refer to the `omnicheck` man page for more information on the `omnicheck` command.

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 means removing all Data Protector software components from the system, including *all* references to this system from the IDB on the Cell Manager computer.

If you have some other data in the folder where Data Protector is installed, make sure you saved this data to the other 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” on page 206.
2. Uninstalling Data Protector Cell Manager and Installation Server. See “Uninstalling the Cell Manager and Installation Server” on page 207.

You can also uninstall Data Protector software components without uninstalling the Cell Manager or client. See “Changing Data Protector Software Components” on page 216

You can also manually remove the Data Protector software. See “Manual Removal of Data Protector Software on UNIX” on page 214.

Prerequisites

Before you uninstall the Data Protector software from a computer, check the following:

- ✓ Make sure that all references 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. Refer to online Help for instructions on how to modify backup specifications.
- ✓ Make sure that no backup devices are connected and configured on the system that you want to uninstall. Once the system is uninstalled, backup devices connected to the system are no longer accessible to 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 if 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.

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. Refer to “Uninstalling the Cell Manager and Installation Server” on page 207.

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).

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” on page 184.

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 Solaris systems.

Uninstalling from Windows System

Uninstalling on a MS Cluster Server System

If you have installed HP OpenView AutoPass utility together with Data Protector on a Microsoft Cluster Server 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 OpenView AutoPass or not, and if you want to remove the Data Protector configuration data or not, different actions apply.

IMPORTANT

If you choose to leave the Data Protector configuration data on the system, and later install Data Protector Cell Manager A.05.00 to this system, during upgrade of such Cell Manager to the latest version the configuration data will not be upgraded.

To avoid this problem, optionally back up the Internal Database first, and make a choice that will remove the configuration data.

Proceed as follows:

- If AutoPass utility was installed together with Data Protector:
Select HP OpenView Storage Data Protector A.06.00 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.
 - If AutoPass has not been installed:
 - To uninstall Data Protector and leave the Data Protector configuration data on the system, select HP OpenView Storage Data Protector A.06.00 and click Remove.
 - To uninstall Data Protector and remove the Data Protector configuration data, select HP OpenView Storage Data Protector A.06.00, 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 windows to refresh the list of installed programs and components.

Uninstalling from HP-UX System

IMPORTANT

If you leave the Data Protector configuration data on the system after the uninstallation, and you later install Data Protector A.05.00, A.05.10 or A.05.50 Cell Manager to this system, during upgrade of such Cell Manager to the latest version the configuration data will not be upgraded.

To avoid this problem, optionally back up the Internal Database before the uninstallation, and after the uninstallation remove the remaining Data Protector directories from your system.

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` command from the `/opt/omni/sbin` directory.
2. Type 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 -9 <process_ID>` command before you proceed with uninstalling.

3. Run `/usr/sbin/swremove DATA-PROTECTOR` to uninstall Data Protector software.
4. The HP OpenView 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 refer to “Manual Removal of Data Protector Software on UNIX” on page 214.

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.

Maintaining the Installation

Uninstalling Data Protector Software

For example:

```
cmhaltpkg ob2c1
```

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 OpenView AutoPass utility by running the `/usr/sbin/swremove HPOVLIC` command as the user root.

10. Unmount 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
```

Maintaining the Installation

Uninstalling Data Protector Software

8. You can remove the HP OpenView AutoPass utility by running the `/usr/sbin/swremove HPOVLIC` command as the user root.

9. Unmount 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 Solaris Systems

Cell Manager

The Cell Manager for Solaris is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `pkgrm` utility.

IMPORTANT

If you leave the Data Protector configuration data on the system after the uninstallation, and you later install Data Protector A.05.00, A.05.10 or A.05.50 Cell Manager to this system, during upgrade of such Cell Manager to the latest version the configuration data will not be upgraded.

To avoid this problem, optionally back up the Internal Database before the uninstallation, and 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 `pkginfo | grep OB2` command to list all the Data Protector packages installed on the Cell Manager.

The packages associated with the Cell Manager are as follows:

OB2-CORE	Data Protector Core software
OB2-C-IS	Installation Server software
OB2-CS	Cell Manager software

OB2-CC Cell Console software, containing the graphical user interface and the command-line interface

If Data Protector clients or an Installation Server are also installed on the system, other packages will also be listed.

NOTE

If you wish to leave any other Data Protector components installed, you must leave the OB2-CORE package installed, since it is a dependency for other packages.

3. In reverse order to the sequence in which they were installed, remove the packages mentioned in the previous step using the `pkgrm <package name>` command and follow the prompts.
4. The HP OpenView AutoPass utility is not removed during a Data Protector uninstallation. You can manually remove it by running the following commands as the user root:

```
swremove HPOvLic  
swremove HPOvLicJ
```

Installation Server The Installation Server for UNIX on Solaris is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `pkgrm` 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 `pkginfo | grep OB2` command to list all the Data Protector packages installed on the Installation Server system.

The packages associated with the Installation Server are as follows:

OB2-CORE	Data Protector Core software
OB2-C-IS	Installation Server Core software
OB2-SOLUX	Disk Agent, Media Agent and GUI packets for remote Solaris systems
OB2-OTHUX	Disk Agent and Media Agent packets for remote non-Solaris UNIX systems

If other Data Protector components are installed on the system, other packages will also be listed.

NOTE

If you wish to leave any other Data Protector components installed, you must leave the OB2-CORE package installed, since it is a dependency for other packages.

3. In reverse order to the sequence in which they were installed, remove the packages mentioned in the previous step using the `pkgrm <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, refer to “Exporting Clients from a Cell” on page 184.

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
```

**Other UNIX
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, and Solaris systems. For the list of supported Data Protector components for a particular operating system, refer to the *HP OpenView Storage 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 refer to “Remote Installation of the Data Protector Clients” on page 45.

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 OpenView Storage Data Protector A.06.00** 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 CD-ROM, on each cluster node. After that, the virtual server hostname has to be manually imported to the Data Protector cell using the graphical user interface.

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 3-1 Data Protector Software Component Dependencies on HP-UX

Components	Depend on
OMNI-MOMGUI	OMNI-CC
OMNI-CC, OMNI-CORE-IS	OMNI-CORE
OMNI-CS	OMNI-CORE, OMNI-CC
OMNI-INTEG, OMNI-DA, OMNI-MA or OMNI-NDMP	OMNI-CORE
OMNI-NDMP-P	OMNI-CORE-IS
OMNI-INF-P, OMNI-SYB-P, OMNI-ORA-P, OMNI-OR8-P, OMNI-SAP-P, OMNI-SAPDB-P, OMNI-DB2-P, OMNI-EMC-P, OMNI-SSEA-P, OMNI-SNAPA-P, OMNI-SMISA-P	OMNI-INTEG OMNI-CORE-IS
OMNI-HPUX-P, OMNI-OTHUX-P, OMNI-OMNIST	OMNI-CORE-IS
OMNI-LOTUS-P, OMNI-OV-P	OMNI-CORE-IS

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. Refer to the *HP OpenView Storage 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 3-2 Data Protector Software Component Dependencies on Solaris

Components	Depend on
OB2-MOMGUI	OB2-CC
OB2-CC, OB2-C-IS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
OB2-INTGP, OB2-DA, OB2-MA or OB2-NDMPP	OB2-CORE
OB2-SOLUX	OB2-C-IS
OB2-INFP, OB2-SYBP, OB2-OR8P, OB2-SAPP, OB2-SAPDP, OB2-DB2P, OB2-SSEAP, OB2-SMISAP	OB2-INTGP OB2-C-IS
OB2-OTHUX, OB2-OSTP, OB2-LOTP, OB2-OVP	OB2-C-IS

Procedure

Perform the following procedure to remove Data Protector software components from the Solaris systems:

1. Make sure you have terminated all Data Protector sessions and exited the GUI.
2. Enter the command `pkginfo | grep OB2` to list all the Data Protector packages installed.
3. In reverse order to the sequence in which they were installed, remove the packages mentioned in the previous step using the `pkgrm <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 uninstalled 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 running the following command on a system in the cell with the Cell Console installed:

```
/opt/omni/bin/omnicc -update_host <HostName>
```

Maintaining the Installation
Changing Data Protector Software Components



| 4

**Upgrading to Data Protector
A.06.00**

In This Chapter

This chapter includes the instructions on performing the following upgrade tasks:

- How to upgrade from Data Protector release A.05.00, A.05.10, or A.05.50 to Data Protector A.06.00.
Refer to “Upgrading from Data Protector A.05.x” on page 226.
- How to upgrade from the Data Protector Single Server Edition.
Refer to “Upgrading from the Single Server Edition” on page 259.
- How to upgrade from Windows NT to Windows 2000/XP.
Refer to “Upgrading from Windows NT to Newer Version of Windows” on page 262.
- How to migrate your existing Cell Manager from an HP-UX 11.x system for PA-RISC architecture to HP-UX 11.23 for IA-64 architecture. Refer to “Migrating from HP-UX 11.x to HP-UX 11.23” on page 264.
- How to upgrade the existing product version to Data Protector A.06.00 in the MC/ServiceGuard environment. Refer to “Upgrading the Cell Manager Configured on MC/ServiceGuard” on page 269.
- How to upgrade the existing product version to Data Protector A.06.00 in the Microsoft Cluster Server environment. Refer to “Upgrading the Cell Manager Configured on Microsoft Cluster Server” on page 273.

Upgrade Overview

Before You Begin Before upgrading an existing product version to Data Protector A.06.00, consider the following:

- Refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for information about supported and discontinued platforms and versions.
- After the upgrade, the Cell Manager, Installation Server and all clients must have the same Data Protector version installed.
- 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.05.00, Data Protector A.05.10, or Data Protector A.05.50, it can be used with Data Protector A.06.00.

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, refer to Chapter 5, “Data Protector Licensing,” on page 277.

Prerequisite

- Perform a backup of the existing Cell Manager system and the internal database (IDB).

Limitations

- The upgrade to Data Protector A.06.00 is only supported for Data Protector A.05.00, Data Protector A.05.10, and A.05.50.
- Changing the Cell Manager platform is not supported in the A.06.00 release of Data Protector. Upgrades are only supported on the same Cell Manager platform (HP-UX to HP-UX, Solaris to Solaris, and Windows to Windows).
- The restore from Microsoft Exchange Server single mailbox backups created with Data Protector version A.05.00 is not possible after the upgrade to Data Protector A.06.00. However, you can restore the existing backups to a .pst file using a filesystem restore.
- If you are upgrading to Data Protector A.06.00 on Windows and you have the version of Microsoft Installer (MSI) older than 2.0, the Data Protector setup will automatically upgrade it to version 2.0. In this

Upgrade Overview

case, Data Protector will display a note at the end of the upgrade, stating that MSI was upgraded. It is highly recommended to restart the system, if MSI was upgraded. Consult Microsoft Support about the MSI 2.0 prerequisites for various Windows operating systems.

To find out the version of MSI on your system, right-click the file `c:\winnt\system32\msi.dll` in Explorer and select Properties. In the Properties dialog box, select Version.

Upgrade Sequence

To upgrade your cell from the earlier versions of the product to Data Protector A.06.00, proceed as follows:

1. Upgrade the Cell Manager and Installation Server to Data Protector A.06.00. 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.

For some specific cell configurations, the file names in the IDB need to be converted after the upgrade of the Cell Manager has been performed. You will be prompted in such case. Refer to Table 4-1 on page 251 and Table 4-2 on page 252.

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. For Data Protector A.05.00 and A.05.10 MA clients, certain limitations apply. Refer to Table 4-1 on page 251 and Table 4-2 on page 252.
5. TBD Upgrade the clients that have the filesystem Disk Agent (DA) installed within the next two weeks.

For information on impact of DA version on backup and restore before and after the IDB file name conversion, refer to “Conversion of File Names in the IDB” on page 250.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.06.00, 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 A.06.00 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.

The Need to Convert File Names in the IDB

Data Protector versions A.05.50 and A.06.00 have improved handling and display of file names created with different locales on different platforms. This requires a conversion of the existing file names in the IDB for some specific cell configurations in case you are upgrading from Data Protector A.05.00 or A.05.10.

The conversion is performed on the:

- UNIX Cell Manager as a part of post-upgrade backups of Windows clients.
- Windows Cell Manager as a background process after the upgrade of the Cell Manager.

You will be prompted, if it is needed to perform the IDB conversion.

UNIX

On a UNIX Cell Manager, the IDB conversion is performed as a part of the post-upgrade backups of Windows clients until

- the period for conversion expires, or
- a full backup of all Windows clients in the cell has been performed. This step is very important and must be done.

For file name conversion performance related figures refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Windows

On a Windows Cell Manager, the IDB conversion can be postponed, however, certain limitations apply until it is performed.

More detailed information regarding the file name conversion in the IDB on Windows and UNIX Cell Managers can be found in “Conversion of File Names in the IDB” on page 250

Upgrading from Data Protector A.05.x

The Data Protector A.05.x release versions can be directly upgraded to Data Protector A.06.00 for UNIX and Windows platforms.

Licenses

The existing Data Protector A.05.x licenses are fully compatible and valid for use with Data Protector A.06.00. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 277.

Before You Begin

Before you begin with the upgrade, refer to “Upgrade Overview” on page 223 for information on limitations and the upgrade sequence.

Upgrading the UNIX Cell Manager and Installation Server

Prerequisites

- Stop all Data Protector services using the `/opt/omni/sbin/omnisv -stop` command.
- On Solaris, if you have any old patches installed, uninstall them before the upgrade.
- The Korn Shell (`ksh`) must be installed.
- You must have `root` permissions to perform the upgrade.

If the HP-UX or Solaris Installation Server is installed together with the Cell Manager, it is upgraded automatically when the `omnisetup.sh` command is run.

If the HP-UX or Solaris Installation Server is installed on a separate system, refer to “Upgrading an Installation Server” on page 229.

Upgrading a Cell Manager

The HP-UX or Solaris Cell Manager is upgraded automatically when the `omnisetup.sh` command is run.

On HP-UX, this command directly upgrades the existing package set using the `swinstall` utility. On Solaris, this command removes the existing package set using the `pkgrm` utility and installs new packages using the `pkgadd` 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 reimport the upgraded Installation Server. For details, refer to “Importing an Installation Server to a Cell” on page 179.

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” on page 269.

Setting Kernel Parameters

On HP-UX systems, it is recommended that you set the kernel parameter `maxdsiz` (Max Data Segment Size) to at least 134217728 bytes (128 MB), and the kernel parameter `semnu` (Number of Semaphore Undo Structures) to at least 256. After you commit these changes, recompile the kernel and reboot the machine.

On Solaris systems, it is recommended that you set the kernel parameter `shmsys:shminfo_shmmax` (maximum shared memory segment size (SHMMAX)) in `/etc/system` to at least 67108864 bytes (64 MB). After you commit this change, reboot the machine.

Upgrade Procedure To upgrade the HP-UX or Solaris Cell Manager to Data Protector A.06.00, follow the procedure described below:

1. Insert and mount the UNIX installation DVD-ROM to a mount point. For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

For example:

```
mkdir /dvdrom
mount /dev/c0d0t0 /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:

<code>hpux_ia</code>	HP-UX 11.23 on IA-64 systems
<code>hpux_pa</code>	HP-UX on PA-RISC systems
<code>solaris</code>	Solaris systems

- Copy the whole DVD-ROM to your local disk:

```
cp -r /dvdrom <dvd_image_dir>
```

2. Run the `omnisetup.sh` command.

To run this command from the DVD-ROM, execute:

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

To start the installation from disk, run:

- If you have copied the `DP_DEPOT` directory to your local disk as `<directory>/DP_DEPOT`, go to the directory where the `omnisetup.sh` command is stored, and run:
- If you have copied the whole DVD-ROM to `<dvd_image_dir>`, run the `omnisetup.sh` command without any parameters:

```
./omnisetup.sh -source <directory>
```

```
cd <dvd_image_dir>/LOCAL_INSTALL
./omnisetup.sh
```

3. `omnisetup.sh` prompts you to install or upgrade the HP OpenView 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, refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294. 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.05.x version of Data Protector is detected, the upgrade procedure is automatically started. If you want 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, refer to “Installing a UNIX or Linux Cell Manager” on page 18 and “Installing Installation Servers for UNIX” on page 34.

4. If you are upgrading from Data Protector A.05.00 or A.05.10 and have Windows clients in the cell, you will be informed that conversion of file names in the IDB will be performed. The IDB conversion is necessary to correctly handle file names with international characters. Refer to “Conversion of File Names in the IDB” on page 250 for details.

As soon as the procedure is completed, you can start using Data Protector.

For the description of the `omnisetup.sh` command, refer to the `README` file located in the `<Mount_point>/LOCAL_INSTALL` directory on the DVD-ROM or *HP OpenView Storage 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. Refer to “Checking Configuration Changes” on page 235.

Upgrading an Installation Server

The HP-UX or Solaris Installation Server is upgraded automatically when the `omnisetup.sh` command is run.

On HP-UX, this command directly upgrades the existing package set using the `swinstall` utility. On Solaris, this command removes the existing package set using the `pkgrm` utility and installs new packages using the `pkgadd` 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 reimport the upgraded Installation Server. For details, refer to “Importing an Installation Server to a Cell” on page 179.

IMPORTANT

You cannot upgrade the Installation Server unless you upgraded the Cell Manager first.

Upgrade Procedure

To upgrade the HP-UX or Solaris Installation Server to Data Protector A.06.00, follow the procedure described below:

1. Insert and mount the UNIX installation DVD-ROM to a mount point. For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

For example:

```
mkdir /dvdrom  
mount /dev/c0d0t0 /dvdrom
```

Optionally, to install Data Protector from a depot on the disk, perform the following:

- To copy the DP_DEPOT, AUTOPASS, 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 11.23 on IA-64 systems
hpux_pa	HP-UX on PA-RISC systems
solaris	Solaris systems

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

```
cp -r /dvdrom <dvd_image_dir>
```

2. Run the omnisetup.sh command.

To run this command from the DVD-ROM, execute:

```
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 directory to your local disk as *<directory>/DP_DEPOT*, go to the directory where the omnisetup.sh command is stored, and run:

```
./omnisetup.sh -source <directory>
```

- If you have copied the whole DVD-ROM to `<dvd_image_dir>`, run 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, refer to the `README` file located in the `<Mount_point>/LOCAL_INSTALL` directory on the DVD-ROM or *HP OpenView Storage 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. Refer to “Checking Configuration Changes” on page 235.

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 obsoleted components). The existing package set is removed and the new package set is 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

Reimport the upgraded Installation Server after the installation procedure has finished. For details, refer to “Importing an Installation Server to a Cell” on page 179.

NOTE

If you want to upgrade your Windows operating system from Windows NT to a newer version of Windows, you should first upgrade the operating system and then upgrade the previous version of the product to Data Protector A.06.00. For details, refer to “Upgrading from Windows NT to Newer Version of Windows” on page 262.

MS Cluster Server

The upgrade procedure for the Cell Manager, running in the MS Cluster Server environment, is different from the upgrade procedure for the Cell Manager not configured for use with MS Cluster Server. The detailed steps you need to follow are described in “Upgrading the Cell Manager Configured on Microsoft Cluster Server” on page 273.

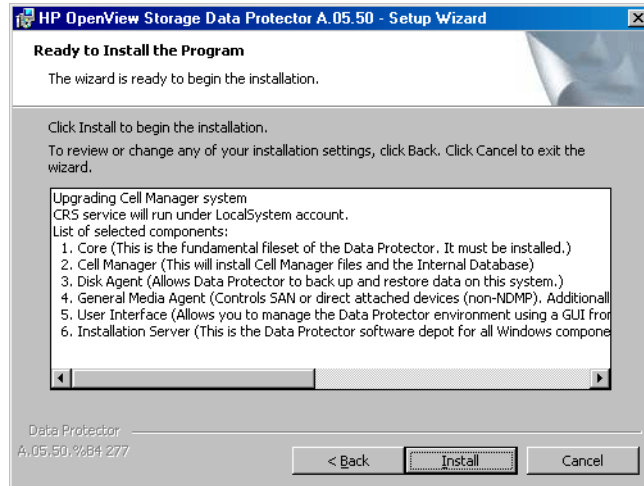
Upgrade Procedure

To upgrade the Windows Cell Manager and Installation Server to Data Protector A.06.00, 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, refer to the next step of the wizard. Click `Next`.
3. **Windows XP SP2 only:** 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.

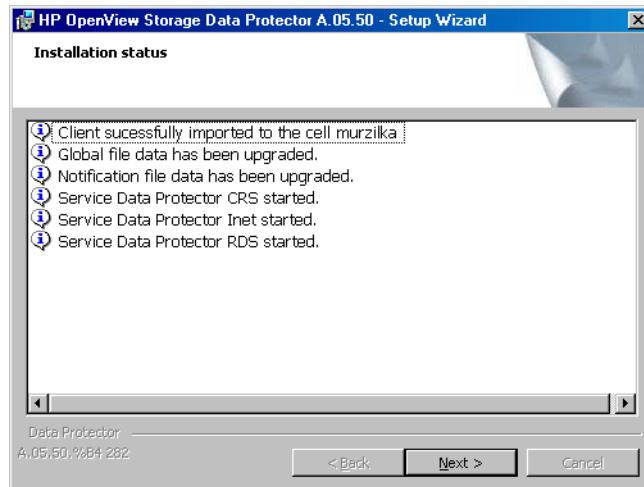
Click `Next`.
4. The component summary list is displayed. Click `Install` to perform the upgrade.

Figure 4-1 Component Selection Summary Page TBD



5. The Installation status page is displayed. Click Next.

Figure 4-2 Installation Status Page TBD



6. If you have UNIX clients in the cell, the IDB Conversion page will be displayed. Refer to “Conversion of File Names in the IDB” on page 250.

7. This step is performed only for Cell Manager upgrade. If Installation Server installed on a client other than the Cell Manager being upgraded, this step does not occur.

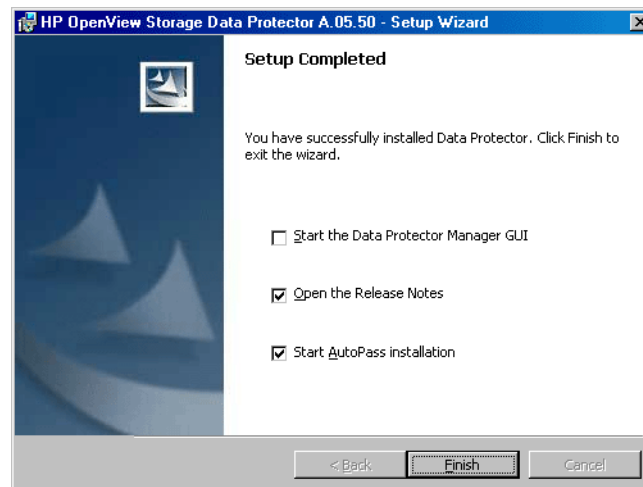
The Setup Wizard enables you to install or upgrade the HP OpenView AutoPass utility if you want to download and install passwords for the purchased licenses directly through the internet from the HP password delivery center web server. For more information on the AutoPass utility, refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294.

By default, the Start AutoPass installation or the Upgrade AutoPass installation option is selected. It is recommended to install the HP OpenView 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 OpenView Storage Data Protector Product Announcements, Software Notes, and References*, select Open the Product Announcements.

Figure 4-3 **Selecting AutoPass for Installation**



8. 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:

- The Data Protector IDB will be converted if you have UNIX clients in the cell to enable correct handling of non-ASCII characters in file names in the Data Protector. Refer to “Conversion of File Names in the IDB” on page 250 for details about IDB conversion.
- Check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 235.

Checking Configuration Changes

Global Options File

During the upgrade, the contents of the *old* global options file residing in the `/etc/opt/omni/server/options` directory on UNIX Cell Manager, or in the `<Data_Protector_home>\Config\server\Options` directory on Windows Cell Manager, are merged with the contents of the *new* global options file on the Cell Manager:

- `/opt/omni/newconfig/etc/opt/omni/server/options` - UNIX Cell Manager
- `<Data_Protector_home>\NewConfig\Server\Options` - Windows Cell Manager

The *merged* file, which is named `global`, resides in the `/etc/opt/omni/server/options` directory on UNIX Cell Manager, or in the `<Data_Protector_home>\Config\server\Options` directory on Windows Cell Manager, and is used by the upgraded version of the product. The *old* global options file is renamed to `global.1`, `global.2`, etc., depending on the number of upgrades performed.

The following applies when the merged file is created:

- Global options file variables that were active (uncommented) in the old file remain active in the merged file. The following comment, stating that the value of the variable was copied from the old file, is added to the merged file:

```
<variable>=<value>
# Data Protector A.06.00
# This value was automatically copied from previous version.
```

- Global options file variables, not used anymore, are commented (made inactive) in the merged file and added the following comment stating that the variable is no longer in use:

```
# <variable>=<value>
# Data Protector A.06.00
# This value is no longer in use.
```

- Variables with values, not supported anymore, are commented (made inactive) in the merged file. The following comment is added, containing a template (<variable_template>) and stating the previous value of this variable:

```
# <variable>=<variable_template>
# Data Protector A.06.00
# This variable cannot be transferred automatically.
# The previous setting was:
# <variable>=<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.

The description of new options is in the merged global options file: /etc/opt/omni/server/options/global on UNIX Cell Manager and <Data_Protector_home>\config\server\options\global on Windows Cell Manager. The section “Global Options File” in the *HP OpenView Storage Data Protector Troubleshooting Guide* shows you how to use global options.

Manual Steps

The following list summarizes the steps to be performed 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, refer to “Using Omnirc Options” in the *HP OpenView Storage Data Protector Troubleshooting Guide*.

- Command line

Refer to “Command Line Changes After Upgrading to Data Protector A.06.00” on page B-74 for a list of commands that have been changed or provided with extended functionality. You have to check and modify the scripts that use the old commands. Refer to the corresponding man pages for usage synopsis.

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. Refer to “Upgrading the Clients” on page 237.

Upgrading the Clients

Upgrade Sequence

For information about the sequence in which the client upgrade is performed, refer to “Upgrade Overview” on page 223.

Upgrading Clients Remotely

For the procedure on how to upgrade the clients using the Installation Server, refer to “Remote Installation of the Data Protector Clients” on page 45. 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, refer to “Installing Windows Clients” on page 58. To upgrade UNIX clients locally, refer to “Local Installation of UNIX and Linux Clients” on page 113. For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

Novell NetWare

After upgrading any Novell NetWare 5.x or 6.x client, you need to perform some additional steps that will enable you to perform any backup and restore of the NDS/eDirectory database. Refer to “Local Installation of the Novell NetWare Clients” on page 96 for details.

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 push 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 and manually transfer the settings to the new file.

Upgrading Clients Configured on 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 running:

```
omnicc -export_host <virtual_hostname>
```

2. Reimport the virtual host by running:

```
omnicc -import_host <virtual_hostname> -virtual
```

Upgrading Clients with Integrations

If you are upgrading a Data Protector client that has the integration installed (such as Oracle, SAP R/3, Informix Server, Sybase, Microsoft Exchange Server, HP StorageWorks Disk Array XP, EMC Symmetrix, etc.), follow the steps described in sections below to successfully perform the upgrade:

- For instructions on how to upgrade the Oracle integration, refer to “Upgrading the Oracle Integration” on page 239.
- For instructions on how to upgrade the SAP R/3 integration, refer to “Upgrading the SAP R/3 Integration” on page 241.
- For instructions on how to upgrade the Informix Server integration, refer to “Upgrading the Informix Server Integration on UNIX Systems” on page 241 and “Upgrading the Informix Server Integration on Windows Systems” on page 243.

- For instructions on how to upgrade the Sybase integration, refer to “Upgrading the Sybase Integration on UNIX Systems” on page 244 and “Upgrading the Sybase Integration on Windows Systems” on page 245.
- For instructions on how to upgrade the MS SQL integration in a ZDB environment, refer to “Upgrading the MS SQL Integration in a ZDB Environment” on page 250.
- For instructions on how to upgrade MS Exchange, MS SQL, HP StorageWorks Disk Array XP, EMC Symmetrix, etc., refer to “Upgrading Other Integrations” on page 248.

Upgrading the Oracle Integration

The clients that have the Oracle integration installed are upgraded either locally by running the `omnisetup.sh -install oracle8` command on UNIX systems and the `setup.exe` command on Windows systems, or remotely by pushing 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.

New Templates After Upgrading If you are upgrading from Data Protector A.05.00 or A.05.10, the Oracle templates are replaced with newer versions. The new templates are located in the following directory:

```
/opt/omni/newconfig/etc/opt/omni/server/dltemplates/lists/oracle8 (on UNIX systems) or  
<Data_Protector_home>\NewConfig\server\dltemplates\lists\oracle8 (on Windows systems).
```

To use the new templates, copy them after the upgrade to Data Protector A.06.00 to the `/etc/opt/omni/server/dltemplates/lists\oracle8` (on UNIX systems) or

```
<Data_Protector_home>\Config\server\dltemplates\lists\oracle8 (on Windows systems) directory. If you wish to keep the old templates, save them under another name.
```

ZDB Method Configuration Depending on whether the Oracle instance configuration file contains the `<ORACLE_DBID>` parameter or not, the ZDB method configuration file is set for Data Protector A.06.00 as follows:

- If the Oracle instance configuration file contains the `<ORACLE_DBID>` parameter (in Data Protector A.05.10 and A.05.50), the ZDB method configuration file is created for each database instance *during the upgrade*.
- If the Oracle instance configuration file *does not* contain the `<ORACLE_DBID>` parameter (Data Protector A.05.00), the ZDB method configuration file is created for each instance *during the first backup session*.

The Oracle ZDB method is not changed during the upgrade. For information on how to switch between the proxy-copy and backup set ZDB methods, refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

Oracle ZDB Upgrade If you are upgrading from Data Protector A.05.00 or A.05.10, the Oracle ZDB backup specifications are automatically upgraded at the end of a standard Oracle integration upgrade procedure.

The following steps are performed during a backup specification upgrade:

- The `OB2DMAP` and `OB2SMB` parameters are added to the *first* `RMAN ALLOCATE CHANNEL` command. The `OB2DMAP` parameter is set to the number of channels that were allocated before the upgrade. For example, with an `RMAN` script with 4 allocated channels, the `OB2DMAP` parameter will be set to 4.
- All `ALLOCATE CHANNEL` commands except the first one are removed from the scripts.
- If instant recovery is enabled, the `TABLESPACE` or `DATAFILES` backup objects are changed to `DATABASE` to allow only backups of the whole database.
- If the proxy copy backup method was used, all `RELEASE CHANNEL` commands are removed except the one referring to the first `ALOCATE CHANNEL` command.

Refer to the *HP OpenView Storage Data Protector Integration Guide for Oracle and SAP* or *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide* for more details.

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` variables. Refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

Upgrading the SAP R/3 Integration

The clients that have the SAP R/3 integration installed are upgraded either locally by running the `omnisetup.sh -install sap` command on UNIX systems and the `setup.exe` command on Windows systems, or remotely by pushing 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.

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` variables. Refer to the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

Upgrading the Informix Server Integration on UNIX Systems

When upgrading the Informix Server integration from Data Protector A.05.00 and A.05.10 to Data Protector A.06.00, there are, depending on the environment, three upgrade procedures:

Procedure 1

If the Informix Server client *does not reside* on the same system as the Cell Manager and it *is not configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are automatically moved from a Data Protector Informix Server client to the Cell Manager during the upgrade. No reconfiguration of the Informix Server databases is needed after the upgrade.

Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.

Procedure 2

If the Informix Server client *does not reside* on the same system as the Cell Manager and it *is configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are automatically moved from the Data Protector Informix Server client to the Cell Manager during the upgrade. After the upgrade, the Informix Server databases must be reconfigured.

1. Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.
2. Configure the Informix Server databases using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Configure the Informix Server databases using the virtual hostname of Informix Server.

Procedure 3

If the Informix Server client *resides* on the same system as a *cluster-aware Cell Manager* and it *is either configured or not configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are not automatically moved from the Data Protector Informix Server client to the Cell Manager during the upgrade. After the upgrade, the Informix Server databases must be reconfigured.

1. Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.

2. Configure the Informix Server databases using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Upgrading the Informix Server Integration on Windows Systems

When upgrading the Informix Server integration from Data Protector A.05.00 and A.05.10 to Data Protector A.06.00, there are, depending on the environment, three upgrade procedures:

Procedure 1

If the Informix Server client *does not reside* on the same system as the Cell Manager and it *is not configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are automatically moved from the Data Protector Informix Server client to the Cell Manager during the upgrade. No reconfiguration of the Informix Server databases is needed after the upgrade.

Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.

Procedure 2

If the Informix Server client *does not reside* on the same system as the Cell Manager and it *is configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are automatically moved from the Data Protector Informix Server client to the Cell Manager during the upgrade. After the upgrade, the Informix Server databases must be reconfigured.

1. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.
2. Configure the Informix Server databases using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Configure the Informix Server databases using the virtual hostname of Informix Server.

Procedure 3

If the Informix Server client *resides* on the same system as a *cluster-aware Cell Manager* and it *is either configured or not configured* as a Data Protector cluster aware client, the Data Protector Informix Server configuration parameters are not automatically moved from the

Data Protector Informix Server client to the Cell Manager during the upgrade. After the upgrade, the Informix Server databases must be reconfigured.

1. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Informix Server integration agent to the client using the Data Protector GUI.
2. Configure the Informix Server databases using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Upgrading the Sybase Integration on UNIX Systems

When upgrading the Sybase integration from Data Protector A.05.00 and A.05.10 to Data Protector A.06.00, there are, depending on the environment, three upgrade procedures:

Procedure 1

If the Sybase client *does not reside* on the same system as the Cell Manager and it *is not configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. No reconfiguration of the Sybase Server is needed after the upgrade.

Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.

Procedure 2

If the Sybase client *does not reside* on the same system as the Cell Manager and it *is configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. After the upgrade, the Sybase Server must be reconfigured.

1. Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.
2. Configure the Sybase client using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Configure the Sybase Server using the virtual hostname of the Sybase Server.

Procedure 3

If the Sybase client *resides* on the same system as a *cluster-aware Cell Manager* and it *is either configured or not configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are not automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. After the upgrade, the Sybase Server must be reconfigured.

1. Upgrade the client either locally by running the `omnisetup.sh` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.
2. Configure the Sybase Server using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

If the Sybase Server is configured as a Data Protector cluster aware client, configure it using the virtual hostname of the Sybase Server.

If the Sybase Server is not configured as a Data Protector cluster aware client, configure it using the hostname of the Sybase Server.

Upgrading the Sybase Integration on Windows Systems

When upgrading the Sybase integration from Data Protector A.05.00 and A.05.10 to Data Protector A.06.00, there are, depending on the environment, three upgrade procedures:

Procedure 1

If the Sybase client *does not reside* on the same system as the Cell Manager and it *is not configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. No reconfiguration of the Sybase Server is needed after the upgrade.

Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.

Procedure 2

If the Sybase client *does not reside* on the same system as the Cell Manager and it *is configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. After the upgrade, the Sybase Server must be reconfigured.

1. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.
2. Configure the Sybase client using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

Configure the Sybase Server using the virtual hostname of the Sybase SQL Server.

Procedure 3

If the Sybase client *resides* on the same system as a *cluster-aware Cell Manager* and it is *either configured or not configured* as a Data Protector cluster aware client, the Data Protector Sybase configuration parameters are not automatically moved from the Data Protector Sybase client to the Cell Manager during the upgrade. After the upgrade, the Sybase Server must be reconfigured.

1. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the Sybase integration agent to the client using the Data Protector GUI.
2. Configure the Sybase client using the Data Protector GUI or CLI as described in the *HP OpenView Storage Data Protector Integration Guide*.

If the Sybase Server is configured as a Data Protector cluster aware client, configure it using the virtual hostname of the Sybase Server.

If the Sybase Server is not configured as a Data Protector cluster aware client, configure it using the hostname of the Sybase Server.

Upgrading the HP StorageWorks EVA Integration

When and Why This Upgrade Is Needed

Upgrading the HP StorageWorks EVA Integration consists of upgrading from the HP StorageWorks EVA Agent (legacy) to the HP StorageWorks EVA SMI-S Agent. This upgrade is needed if you upgraded the Command View (CV) EVA software to version 3.2, and, subsequently, upgraded the EVA VCS firmware to version 3.02x. If you did *not* upgrade CV and VCS, skip this section and follow the general upgrade instructions described in “Upgrading the Clients” on page 237.

Upgrade from the EVA Agent (legacy) to the SMI-S Agent is a very important step, since the EVA Agent (legacy), used with previous versions of CV and VCS, is not compatible with the newer versions listed

above. Successful completion of the upgrade procedure results in upgrading the backup specifications created by the EVA Agent (legacy) and transferring the information on the backup sessions from the EVADB to the SMISDB to enable their restore by the SMI-S Agent.

For detailed information on the supported versions/releases of the dependent products, as well as for a list of the platforms on which the SMI-S Agent is supported, refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References*.

Prerequisites

- Install HP OpenView Storage Operations Manager (the HP StorageWorks SMI-S EVA provider part) starting with v1.1.
- Check that you have the CV EVA software starting with v3.2 and the EVA VCS firmware starting with v3.02x. Lower versions of CV EVA and EVA VCS are not supported with the EVA SMI-S Agent.
- Make sure there are no running EVA backups. The upgrade procedure may cause the backup to fail; in this case, no session information about will appear in the SMIDB and the restore will not be possible.

NOTE

The EVA SMI-S Agent cannot coexist with the EVA Agent (legacy) on one client. Therefore, the installation of the SMISA package checks if the EVAA package is installed, and removes it if it is detected on the system.

Upgrade Procedure

To upgrade from the HP StorageWorks EVA Agent (legacy) to the HP StorageWorks EVA SMI-S Agent, carry out the steps described below:

1. On the application system, run the `omnisetup.sh -install smisa` command on UNIX systems or the `setup.exe` command on Windows systems if you perform a local upgrade. If you upgrade remotely, push the EVA SMI-S Agent to the client using the Add Components GUI wizard and selecting HP StorageWorks EVA SMI-S Agent.

The pre-exec script checks if the EVAA package exists on the system. If the package is detected, the information about it is removed from the Cell Manager.

Along with uninstallation of the EVAA package, the information on the EVA backup sessions (replicas) created by the EVA Agent (legacy) is transferred from the EVADB to the SMISDB. It means that after the upgrade, you will be able to restore the backup sessions created by the EVA Agent (legacy) using the SMI-S Agent.

NOTE

For a particular client, the information is transferred from the EVADB to the SMISDB only in case this client was involved in a backup session as the application system.

2. Perform this step only if you upgrade in cluster environments; otherwise, skip it.

After the SMISA package installation has been finished on cluster nodes, run the `upgrade_cfg_from_evaa <virtual_server_name>` command on any node of the cluster that represents the application system. Note that to successfully execute this command, you need to be a member of either `Admin` or `Operator` user group.

IMPORTANT

Make sure you provide the cluster virtual hostname when running the `upgrade_cfg_from_evaa` command, and not the name of any other system configured in your cell. Executing this command for a system, which is working with the EVA Agent (legacy), might result in a loss of data.

3. After you have upgraded the application system, you need to upgrade the backup system as well. The scheduled backup specifications will not work until both the application and the backup systems are successfully upgraded.

Upgrading Other Integrations

If the Data Protector client has the MS Exchange, MS SQL, HP StorageWorks Disk Array XP, EMC Symmetrix or some other integration installed, upgrade such client either locally using the `omnisetup.sh -install <component_list>` command on UNIX systems and the `setup.exe` command on Windows systems, or remotely using the Data Protector GUI. For a list of the Data Protector component codes, refer to “Local Installation of UNIX and Linux Clients” on page 113. 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 limitation:

- After upgrading the MoM Manager/CMMDB Server, you cannot perform a *restore* of a Data Protector A.05.x filesystem or integration from the Data Protector A.06.00 MoM GUI. Therefore, use either the old MoM GUI for restore or upgrade the clients.

You can perform filesystem and integration *backup* of Data Protector A.05.x clients from the Data Protector A.06.00 MoM GUI.

To upgrade your MoM environment to Data Protector A.06.00, proceed as follows:

1. Upgrade the MoM Manager/CMMDB Server to Data Protector A.06.00.

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, refer to “Upgrading the UNIX Cell Manager and Installation Server” on page 226 and “Upgrading the Windows Cell Manager and Installation Server” on page 231.

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 A.06.00 MoM GUI.

Conversion of File Names in the IDB

Data Protector A.05.50 and A.06.00 have improved handling and display of file names created with different locales on different platforms. This requires a conversion of the existing file names in the IDB for some specific cell configurations if you are upgrading from Data Protector A.05.00 or A.05.10. If you are upgrading from A.05.50, no conversion is needed.

The conversion of file names in the IDB must be performed. Otherwise, the browsing and restore selection of file names containing non-ASCII characters depend on many factors. The probability of undesirable results is thus high.

The conversion is performed:

- On the UNIX Cell Manager as a part of post-upgrade backups of Windows clients.
- On the Windows Cell Manager as a background process after the upgrade of the Cell Manager.

You will be prompted, if it is needed to perform the IDB conversion.

Table 4-1 on page 251 (for Windows Cell Manager) and Table 4-2 on page 252 describe the impact of file name conversion on the Cell Manager if you are upgrading from Data Protector A.05.00 or A.05.10.

Table 4-1 File Name Conversion Impact on a Windows Cell Manager

	UNIX and Other Clients	Windows Clients
Needs IDB conversion	Yes. ¹	No.
Backup before the conversion, client not upgraded	Problematic. ² Any client with non-ASCII characters in backup specifications (trees, exclude lists, etc.) must be upgraded to Data Protector A.06.00. Data Protector logs all such clients in the Data Protector Event Log during upgrade to help you prioritize your upgrade tasks.	No problems.
Backup before the conversion, client upgraded to A.06.00	No problems. If a client is being backed up while the conversion is running and IDB data for this particular client is being converted, the backup will switch to No log mode for this session.	No problems.
Display of files for restore before the conversion, selecting non-ASCII file names/trees for restore	Problematic. ³ The correct display (and selection for restore) of non-ASCII characters in the Data Protector GUI is impossible until the file names in the IDB for this client are converted.	No problems.

Table 4-1 File Name Conversion Impact on a Windows Cell Manager

	UNIX and Other Clients	Windows Clients
Backup after the conversion	No problems. The client must be upgraded to Data Protector A.06.00.	No problems.
Display and restore of files after the conversion	No problems. The client must be upgraded to Data Protector A.06.00.	No problems.
Disk Agent compatibility (earlier versions) ⁴	Data Protector A.05.00 = No, A.05.10 = No, A.05.50 = YES ⁴ .	Data Protector A.05.00 = YES ⁴ , A.05.10 = YES ⁴ , A.05.50 = YES ⁴ .

Table 4-2 File Name Conversion Impact on a UNIX Cell Manager

	UNIX and Other Clients	Windows Clients
Needs IDB conversion	No.	Yes. ¹

Table 4-2 File Name Conversion Impact on a UNIX Cell Manager

	UNIX and Other Clients	Windows Clients
Backup during the conversion period, client not upgraded	No problems.	Problematic. ² Any client with non-ASCII characters in backup specifications (trees, exclude lists, etc.) must be upgraded to Data Protector A.06.00. Data Protector logs all such clients in the Data Protector Event Log to help you prioritize your upgrade tasks.
Backup during the conversion period, client upgraded to A.06.00	No problems.	No problems. Note that backing up Windows clients during the conversion period is required. IDB data for each client is automatically converted while the client is being backed up. You need to perform a full backup to convert all file names stored in the IDB for this client.
Display of files for restore before the conversion, selecting non-ASCII file names/trees for restore	No problems.	Problematic. ³ The correct display (and selection for restore) of non-ASCII characters in the Data Protector GUI is impossible unless a full backup is performed after the upgrade of the Cell Manager.
Backup after the conversion period	No problems.	No problems. The client must be upgraded to Data Protector A.06.00.

Table 4-2 File Name Conversion Impact on a UNIX Cell Manager

	UNIX and Other Clients	Windows Clients
Display and restore of files after the conversion	No problems.	No problems. The client must be upgraded to Data Protector A.06.00.
Disk Agent compatibility (earlier versions) ⁴	Data Protector A.05.00 = YES ⁴ A.05.10 = YES ⁴ , A.05.50.= YES ⁴	Data Protector A.05.00 = No, A.05.10 = No, A.05.50 = YES ⁴

1. If the file name conversion is not performed, the number of file names in the Catalog Database (CDB) part of IDB will grow for the amount of file names with non-ASCII characters in file names being backed up. Files and directories that require conversion but have not been converted yet, cannot be selected for restore. You can restore them only by restoring a parent tree containing only ASCII characters to a temporary location.
2. Restrictions do not apply if file names (trees) in the backup specification contain only ASCII characters. If so, all files and directories within a tree are backed up and their names are stored in the IDB correctly even if file names (trees) contain non-ASCII characters.
3. Restrictions do not apply if the file name (tree) you are restoring contains only ASCII characters. Otherwise, you can restore them by restoring a parent tree containing only ASCII characters to a temporary location. All files and directories within such parent tree will be restored with their original file names (even if they are not displayed correctly in the Data Protector GUI) provided that they are restored to the original platform.

4. TBD Filesystem Disk Agent compatibility with the Data Protector A.06.00 Cell Manager. The support for Disk Agent from earlier versions is limited to 2 weeks. During this period, you should upgrade all clients in the cell.

Remarks

- Regardless of file name handling issues, when a file is backed up and restored, the original byte sequence of the file body is retained.
- File names consisting of 7 bit ASCII characters only are fully supported for all combinations of platforms for all components involved (Cell Manager, client, GUI). For non-ASCII characters in file names, specific setup and configuration is required for proper handling of file names.

IDB conversion can take quite some time and system resources to complete, depending on the size of the filename part of the IDB and your cell configuration. However, this will not affect the success of your backups or restores.

IDB Conversion on a Windows Cell Manager

Introduction

This section applies only for Windows Cell Managers that have non-Windows clients in the cell and are being upgraded from Data Protector A.05.00 or A.05.10. If you are upgrading from A.05.50, no conversion is needed.

IDB conversion will take some time, depending on the size of the IDB and the configuration of your cell, but it does not affect the success of your backups or restores. The conversion is performed as a background process in a single run for all non-Windows clients in the cell, while Data Protector is fully operational. It first converts all data for one client before proceeding with conversion of the next client's data. After it is finished, IDB conversion is complete and does not need to be performed again.

If the filenames do not include non-ASCII characters, the IDB conversion will still be run, but nothing will be changed in the IDB.

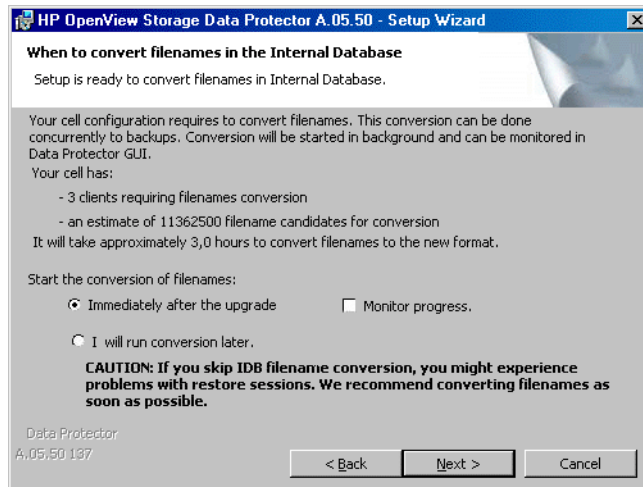
IDB conversion will not affect the IDB size.

How IDB Conversion Is Performed

After the upgrade of Data Protector is finished, the Data Protector Setup Wizard offers you conversion of filenames in the IDB.

Figure 4-4

IDB Conversion After Upgrade TBD



You are given a rough estimate of how long the IDB conversion will take to finish. The estimate is based on the number of non-Windows clients in the cell and the number of their files stored in the IDB.

If you postpone the conversion to later, you will have to run the IDB conversion manually using the `omnidbupgrade` command. Refer to *HP OpenView Storage Data Protector Command Line Interface Reference* for details.

NOTE

It is recommended to perform IDB conversion and to upgrade the Disk Agents on clients as soon as possible.

You can check the status of the IDB conversion (data for which clients has already been converted) in the Data Protector GUI in the Monitor Context.

Backup During Conversion

Backups during IDB filename conversion are possible, because the conversion runs in the background, while Data Protector is fully operational.

If the client's data in the IDB is being converted during the backup of this client then the backup is done using the `No Log` option (and hence no information about backed up files and directories is logged to the IDB for this client in this session).

Restore During Conversion

Restore *during* the conversion of file names is possible. However, only restores of entire objects or selections of directories/files from non-Windows systems, containing 7-bit ASCII characters, are safe.

If files or directories you have selected for restore to a specific client contain non-ASCII characters (and originate from a non-Windows platform), wait for the IDB conversion of that client's data to finish. The Disk Agent on that client must be upgraded prior to the restore.

Backup and Restore After IDB Conversion

After the whole IDB has been converted and all Disk Agents on all clients in the cell have been upgraded to A.06.00 version, backup and restore will operate normally.

IDB Conversion on a UNIX Cell Manager

Introduction

This section applies only for UNIX Cell Managers with Windows clients in the cell are being upgraded from Data Protector A.05.00 or A.05.10. If you are upgrading from A.05.50, no conversion is needed..

IDB conversion takes some time, depending on the size of the IDB and the configuration of your cell, but it will not affect the success of your backups or restores. The conversion is being performed as a background process during backups of Windows clients in the cell for a specific period. After a full backup of all filesystem backup objects of all Windows clients in the cell is performed, IDB conversion is complete and does not need to be performed again.

The conversion of filenames in the IDB during backups will by default run for one month, which is defined by the `ConvertFilenamesInIDBDuringBackup` global option. See the *HP OpenView Storage Data Protector Troubleshooting Guide* for details on how to edit the global options file.

Impact on performance

The conversion of file names in the IDB has impact on performance. While the conversion is running (the `ConvertFilenamesInIDBDuringBackup` global option is enabled), a backup of a Windows client is slower until the first full backup of the

client is performed. Please refer to the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for detailed information.

Limitations

Consider the following limitations:

- It is possible that a file, backed up with the previous version of Data Protector and stored in the IDB using the old encoding, has been deleted from the client before the IDB conversion. In this case, the filename will not be converted in the IDB. The same situation occurs if no backups have been performed during the conversion period (defined by the `ConvertFileNamesInIDBDuringBackup` global option). This makes the restore of such file more difficult if it uses non-ASCII characters in the filename. See the *HP OpenView Storage Data Protector Troubleshooting Guide* for a workaround.
- For other limitations, refer to Table 4-2 on page 252.

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 A.06.00 Single Server Edition. For details, refer to “Upgrading from Earlier Versions of SSE to Data Protector A.06.00 SSE” on page 259.
- From Data Protector A.06.00 Single Server Edition to Data Protector A.06.00. For details, refer to “Upgrading from Data Protector A.06.00 SSE to Data Protector A.06.00” on page 259.

Upgrading from Earlier Versions of SSE to Data Protector A.06.00 SSE

The upgrade procedure from earlier versions of SSE to Data Protector A.06.00 SSE is the same as the upgrade procedure from earlier versions of Data Protector to Data Protector A.06.00. For the information, refer to “Upgrading from Data Protector A.05.x” on page 226.

Upgrading from Data Protector A.06.00 SSE to Data Protector A.06.00

Licenses

You need to have a license to perform the upgrade from Data Protector A.06.00 Single Server Edition to Data Protector A.06.00. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 277.

The upgrade from Data Protector A.06.00 Single Server Edition to Data Protector A.06.00 is offered for two possible scenarios:

- If you have the Data Protector Single Server Edition installed on one system (Cell Manager) only. Refer to “Upgrading the Cell Manager” on page 260.
- If you have the Data Protector Single Server Edition installed on multiple systems and you want to merge these cells. Refer to “Upgrading from Multiple Installations” on page 260.

NOTE

If you want 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 A.06.00, refer to “Upgrading from Data Protector A.05.x” on page 226.

Upgrading the Cell Manager

To upgrade the Single Server Edition Cell Manager, do the following:

1. Remove the Single Server Edition license:
 - on Windows:
`del <Data_Protector_home>\Config\server\Cell\lic.dat`
 - on UNIX:
`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. Refer to “Choosing the Cell Manager System” on page 10.
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. Refer to “Uninstalling Data Protector Software” on page 205.
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. See the online Help index: TBD for the information about importing media and details about the `List from media restore`.

Upgrading from Windows NT to Newer Version of Windows

If you have the Cell Manager installed on the Windows NT system, you must upgrade the operating system to a newer version, as Windows NT is not supported by Data Protector A.06.00 as a Cell Manager platform.

If you want to upgrade your operating system from Windows NT to a newer version of Windows, you have to consider the impact of this upgrade on Data Protector.

If you have Data Protector A.05.00 or A.05.10 Cell Manager installed on Windows NT, and you want to upgrade it to Data Protector A.06.00, perform the upgrade in the following sequence:

1. Upgrade the operating system from Windows NT to a newer version of Windows. For more information, refer to Windows documentation.
2. Upgrade the Data Protector A.05.00 or A.05.10 Cell Manager to Data Protector A.06.00. For the procedure, refer to “Upgrading from Data Protector A.05.x” on page 226.

Upgrading from Solaris 7/8 to Solaris 9

If you have Data Protector A.06.00 Disk Agent (DA) installed on Solaris 7/8, and you want to upgrade the operating system to Solaris 9, consider the impact of this upgrade on Data Protector. It is recommended to replace the generic Solaris DA installed on the system with the Solaris 9 DA to ensure proper operation of Data Protector and enable advanced backup options for Solaris 9, such as backup of extended attributes.

Perform the upgrade in the following sequence:

1. Upgrade the operating system from Solaris 7/8 to Solaris 9. For more information, refer to Solaris documentation.
2. Remotely install the Disk Agent on the upgraded system using an Installation Server. This will replace the generic Solaris Disk Agent with Solaris 9 Disk Agent. Refer to “Remote Installation of the Data Protector Clients” on page 45 or to `ob2install` man page.

Migrating from HP-UX 11.x to HP-UX 11.23

This section describes the procedure for migrating your existing Cell Manager from a PA-RISC architecture based HP-UX 11.x system to an HP-UX 11.23 system for the Intel Itanium 2 (IA-64) architecture.

Limitations

See the *HP OpenView Storage Data Protector Product Announcements, Software Notes, and References* for details on supported operating system versions, platforms, processors and Data Protector components as well as required patches, general limitations, and installation requirements.

- The migration is supported only from the Data Protector A.06.00 Cell Manager on a PA-RISC based HP-UX 11.x system.
- For the supported combinations of MoM configurations, refer to “MoM Specifics” on page 267.

Recommendation

- It is recommended to perform the conversion of file names in the IDB prior to migration. Refer to “Conversion of File Names in the IDB” on page 250.

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. Refer to “License Migration to Data Protector A.06.00 and A.05.10” on page A-16 for details.

NOTE

GUI is not supported on HP-UX 11.23. However, you can use the `omniusers` command to create a remote user account on the new Cell Manager. You can then use this user account on any system with the Data Protector GUI installed to start the GUI and connect to the new Cell Manager. Refer to the `omniusers` man page.

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. Refer to “Installing HP-UX Clients” on page 64.

2. Run 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, refer to “Securing Clients” on page 190 and “Host Trusts” on page 200.

3. Back up the IDB. Refer to the online Help index keyword “IDB backup”.
4. Restore the IDB to a temporary location on the IA-64 system. Refer to online Help index keyword “IDB restore”.
5. Uninstall the Data Protector client from the IA-64 system. Refer to “Uninstalling a Data Protector Client” on page 206.
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). Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 17.
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. Refer to “Changing the Default Port Number” on page 23.
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. Refer to online Help index keyword “IDB restore”.

If the old Cell Manager was cluster-aware, comment out the `SHARED_DISK_ROOT` and `CS_SERVICE_HOSTNAME` variables 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:
 - If you want to configure a standalone IA-64 Cell Manager:
 - a. Run the `omnimigrate.pl -configure` command. Refer to the `omnimigrate.pl` man page.
 - If you want to configure a cluster-aware IA-64 Cell Manager:
 - a. Run the `omnimigrate -configure_idb` command to configure the IDB from the old Cell Manager for use on the new Cell Manager. Refer to the `omnimigrate.pl` man page.
 - b. Run the `omnimigrate -configure_cm` command to reconfigure the configuration data transferred from the old Cell Manager for use on the new Cell Manager. Refer to the `omnimigrate.pl` man page.
 - c. Export the old virtual server from the cell by running the `omnicc -export_host <Old_CM_Name>`.
 - d. Configure the primary and secondary Cell Manager. Refer to the online Help index keyword "MC/ServiceGuard integration configuring".
 - e. Run 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. Refer to "Changing Data Protector Software Components" on page 216.

10. Configure the licenses on the new Cell Manager. Refer to “Data Protector A.06.00 Product Structure and Licenses” on page A-3.
11. Create a remote user account on the new Cell Manager and use the newly created user account on any other system with the Data Protector GUI installed to start the GUI and connect to the Cell Manager. Refer to the `omniusers` man page for details.
12. Additional steps are required if the following is true:
 - Your cell is a part of the MoM environment. Refer to “MoM Specifics” on page 267
 - Your cell works across a firewall. Reconfigure all firewall related settings on the new Cell Manager. Refer to online Help index keyword “firewall environments”.
 - You want to have an Installation Server on your new Cell Manager. Refer to “Installation Server Specifics” on page 268.

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. Refer to the online Help index keyword “client systems exporting”.
2. Add the MoM administrator to the users list on the new Cell Manager. Refer to the online Help index keyword “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.

NOTE

GUI is not supported on HP-UX 11.23. However, you can use `omniusers` command to create a remote user account on the new Cell Manager. You can then use this user account on any system with the Data Protector MoM GUI installed to start the MoM GUI and connect to the new Cell Manager. Refer to the `omniusers` man page.

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.

If you want 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. Refer to the online Help index keyword “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 A.06.00 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.05.00, Data Protector A.05.10, or Data Protector A.05.50 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 OmniBack II/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 A.06.00. See “Upgrading the UNIX Cell Manager and Installation

Server” on page 226.

5. Stop the Data Protector services if they are running:

```
/opt/omni/sbin/omnisv -stop
```

6. Unmount 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 A.06.00. Follow the steps described in “Upgrading the UNIX Cell Manager and Installation Server” on page 226.

4. Rename the `csfailover.sh` and `mafailover.ksh` startup scripts in the `/etc/opt/omni/server/sg` directory (for example, to `csfailover_DP51.sh` and `mafailover_DP51.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.

NOTE

The default paths of some configuration, log and (on UNIX) database files has been changed in Data Protector A.06.00. Some of the files are now split in the server and client directory. Refer to “Configuration Files on UNIX” on page B-71.

5. Stop the Data Protector services if they are running:

```
/opt/omni/sbin/omnisv -stop
```

6. Unmount 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`. Run:

```
/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
```

3. Reimport the virtual host:

```
omnicc -import_host <virtual_hostname> -virtual
```

4. Change the Cell Manager name in the IDB:

```
omnidbutil -change_cell_name
```

5. 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. Refer to “Security Considerations” on page 187 for information on how to secure a cell.

Upgrading the Cell Manager Configured on Microsoft Cluster Server

The upgrade of Data Protector A.05.00, A.05.10, or A.05.50 Cell Manager to Data Protector A.06.00 on Microsoft Cluster Server (MSCS) is performed locally, from the Windows installation DVD-ROM.

NOTE

It is recommended that all cluster nodes have MSI 2.0 installed.

To perform the upgrade, proceed as follows:

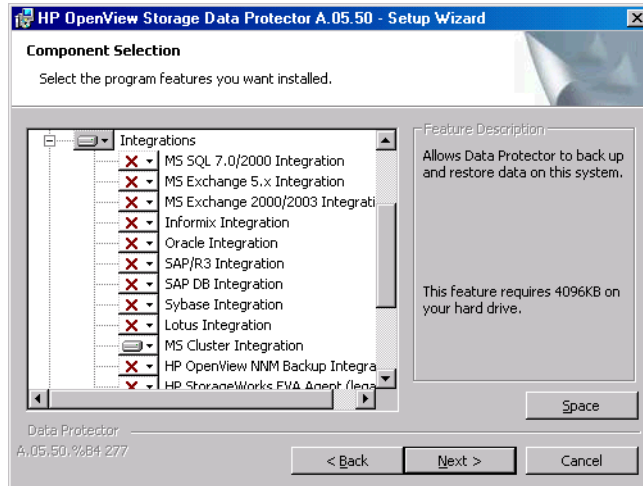
1. Insert the Windows installation DVD-ROM and run `\Windows_other\i386\setup.exe`. It is recommended to start the setup on the currently active virtual server node.

Setup automatically detects the old version of the product and prompts you to upgrade it to Data Protector A.06.00.

Click **Next** to continue.

2. Data Protector automatically selects the components that were installed.

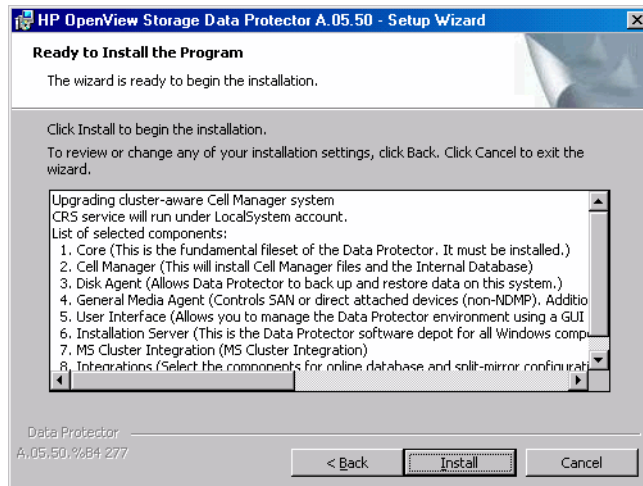
Figure 4-5 Selecting the Components TBD



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.

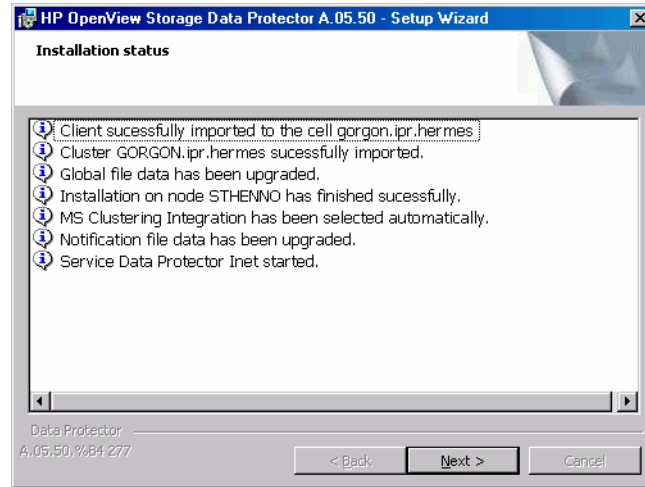
Figure 4-6 Component Selection Summary Page TBD



- The Installation status page is displayed. Click Next.

Figure 4-7

Installation Status Page TBD



- If you have UNIX clients in the cell, the IDB Conversion page will be displayed. Refer to “Conversion of File Names in the IDB” on page 250.
- To start using Data Protector immediately after setup, select Start the Data Protector Manager GUI.

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

It is *not* recommended to install the HP OpenView AutoPass utility in Microsoft 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.

Click Finish.

NOTE

If you are upgrading cluster-aware clients, first upgrade every cluster node separately, and then reimport the virtual server. The remote upgrade is not supported.

5 Data Protector Licensing

In This Chapter

This chapter contains information about how Data Protector licenses are checked and reported, and about how to obtain and install Data Protector passwords.

Introduction

The Data Protector A.06.00 product structure and licensing consists of three main categories:

1. The Starter Packs

Starter packs - management system (Cell Manager) is supported on HP-UX, Windows and Solaris. A starter pack license is obligatory.

2. Additional tape drive licenses and libraries.

3. Data Protector Functional Extensions.

The functional extensions licenses are required once per instance (system, or terabyte) for on-line backup of databases and applications, the Manager-of-Managers functionality, for open file backup, direct backup, instant recovery, NDMP, Zero Downtime Backup (ZDB), advanced backup to disk and media operations.

NOTE

The UNIX product licenses operate on the UNIX, Windows and Novell NetWare platforms, providing the functionality regardless of the platform, while the Windows product licenses operate on the Windows, Novell NetWare and Linux platforms only.

Passwords are bound to the Cell Manager and are valid for the entire Data Protector cell. Clients do not require any license for filesystem or disk image backups.

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. For more information on Data Protector checking and maintenance mechanism, refer to *HP OpenView Storage Data Protector Administrator's Guide*.
- 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, refer to *HP OpenView Storage Data Protector Administrator's Guide*.
- 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:

- Cell Manager & Single Drive
- Starter packs
- Manager-of-Managers Extension
- Single Server Edition

When a certain Data Protector component, such as the Cell Manager or the Manager-of-Managers 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.
- Library extension for one library with unlimited slots
- Drive extension for UNIX / NAS / SAN and Drive extension for Windows / NetWare / Linux (Intel)
- On-line extension for one UNIX system and On-line extension for one Windows / Linux system

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 three 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:

- Zero Downtime Backup (ZDB) for 1 TB HP StorageWorks XP
- Zero Downtime Backup for EMC Symmetrix for 1 TB
- Zero Downtime Backup for HP StorageWorks enterprise virtual array and HP StorageWorks virtual array for 1 TB
- Instant Recovery for HP StorageWorks disk array XP for 1 TB
- Instant Recovery for HP StorageWorks enterprise virtual array and HP StorageWorks virtual array for 1 TB
- Direct Backup for HP StorageWorks disk array XP for 1 TB
- Direct Backup for HP StorageWorks virtual array for 1 TB
- Direct Backup using NDMP for 1 TB

- Advanced backup to disk for the File Library device and for virtual tape libraries

The advanced backup to disk and virtual tape library capacity based licence is treated differently than other licenses in this group. See “The Advanced Backup to Disk License” on page 284.

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 number 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 or direct 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.

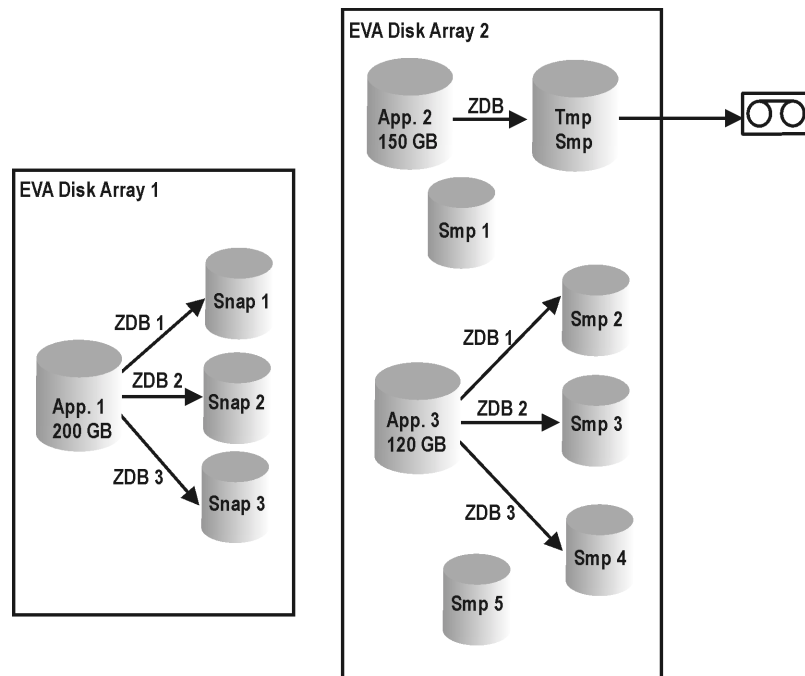
Used Capacity Calculation

The used capacity calculation calculates the licensed capacity of each disk array type 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 session has been run that includes instant recovery or direct backup, the original unit’s total capacity is calculated both for ZDB used capacity per disk array, and in addition, that used for instant recovery or direct backup capacity per disk array.

For example, imagine a scenario where there are two 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 snapshots 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 snapshots are rotated for instant recovery.

Figure 5-1 Used Capacity Calculation Scenario



The calculation for ZDB used capacity counts all disks used in backup sessions in the last twenty-four hours $200 \text{ GB (App.1)} + 150 \text{ GB (App.2)} + 120 \text{ GB (App.3)} = 470 \text{ GB}$.

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 $200 \text{ GB (App.1)} + 120 \text{ GB (App.3)} = 320 \text{ GB}$.

The Advanced Backup to Disk License

The advanced backup to disk license is used if the destination device for the backup or object copy is

- an *advanced file device*
- a *virtual tape library*.

When the advanced backup to disk license is checked, the amount of used space on all media configured in devices that use the advanced backup to disk license (advanced file devices and virtual tape libraries) is compared to the number of licenses installed.

One advanced backup to disk license is required for each 1 TB of backed up data on all advanced file device media and virtual tape library media. For virtual tape libraries, a compression ratio of 2:1 is assumed. That means that you can back up to 2 TB of data with one single advanced backup to disk license.

If an advanced file device or virtual tape library medium is exported from the IDB, the data on such a medium is not counted for this license anymore. Importing a medium (if the data has not been overwritten) causes the data on the imported medium to be counted for the advanced backup to disk license again.

At the start of the backup or object copy, the amount of disk space already occupied by previous backup or object copy sessions is calculated. If the number is smaller than or equal to the amount of licensed backup to disk space, then the backup will start and complete, regardless of how much data is being backed up (potentially exceeding the amount of disk space). If the limit has already been exceeded by previous backup sessions, the backup session will start, but a warning will be issued that the license limit has been exceeded.

To calculate the disk space consumed by the backup to disk in the cell, Data Protector calculates the sum of the sizes of all media created with backups to advanced file libraries and virtual tape libraries in the cell.

The advanced backup to disk license does not involve checking the number of backup devices, drives and slots, it checks only the amount of data on the advanced file device media and virtual tape library as kept in the IDB.

NOTE

By default, Data Protector treats virtual tape library devices as ordinary libraries (such as SCSI II libraries). To utilize the advanced backup to disk licenses, the device must be marked as a virtual tape library during the device configuration. See the online Help index: “virtual tape library”.

Capacity Based Licensing Examples

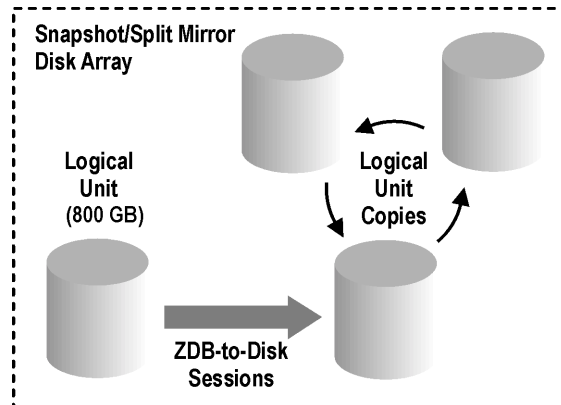
This section provides examples of how capacity based licensing is calculated.

Example 1

Figure 5-2 on page 285 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 5-2

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:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 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 the situation shown in Figure 5-2 on page 285.

Example 2

Figure 5-3 on page 286 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:

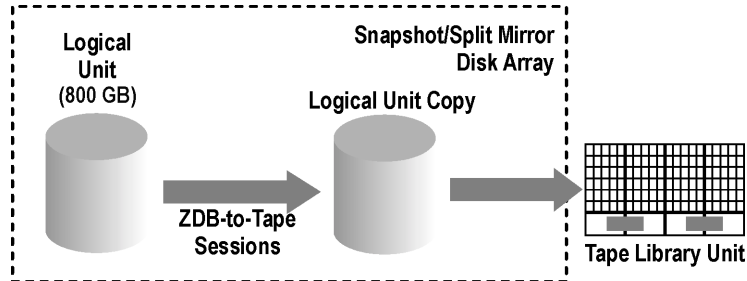
One 800 GB logical unit is used for ZDB-to-disk sessions:

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 5-3

ZDB-to-Tape Sessions



Example 3

Figure 5-4 on page 287 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:

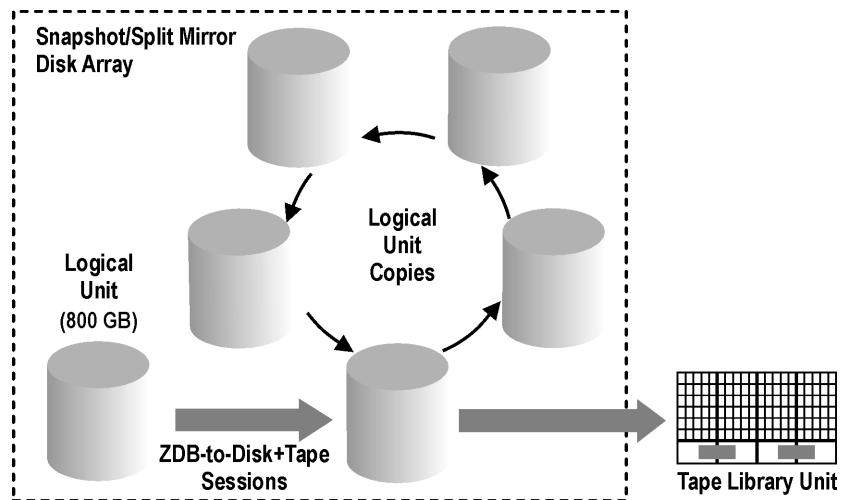
1 x 800 GB = 0.8 TB for the “Zero Downtime Backup for 1 TB” license.

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:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$ 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 5-4 ZDB-to-Disk+Tape Sessions



Example 4 Figure 5-5 on page 288 shows a situation where data from one 800 GB logical unit is backed up 4 times a day in a direct backup session. Three split mirror or snapshot copies (replicas) created during the direct backup session 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 direct backup sessions:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$ for the “Direct Backup for 1 TB” license.

The same 800 GB logical unit is used for ZDB-to-disk+tape sessions and is therefore subject of another license:

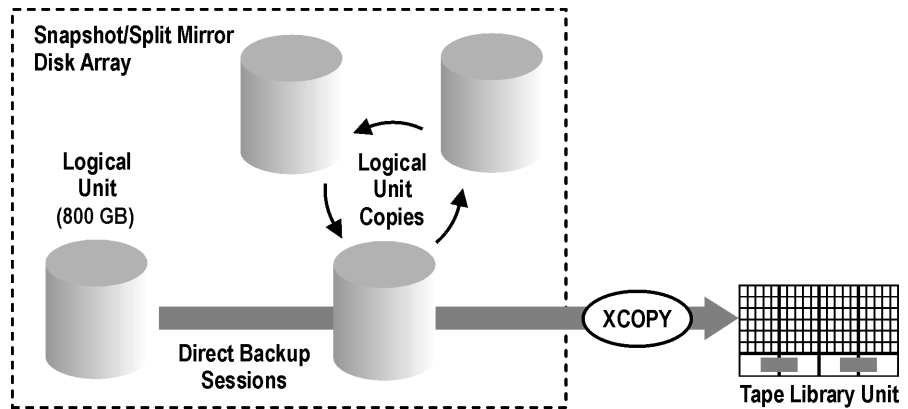
$1 \times 800 \text{ GB} = 0.8 \text{ TB}$ for the “Zero Downtime Backup for 1 TB” license.

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:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$ for the “Instant Recovery for 1 TB” license.

One “Direct Backup for 1 TB” license, one “Zero Downtime Backup for 1 TB” license and one “Instant Recovery for 1 TB” license are sufficient for the situation shown in Figure 5-5 on page 288.

Figure 5-5 Direct Backup Sessions



Example 5

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:

$1 \times 200 \text{ GB} + 1 \times 500 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 1.12 \text{ TB}$ 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:

$1 \times 200 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 0.62 \text{ TB}$ for the “Instant Recovery for 1 TB” license.

One 300 GB logical unit is used in direct backup sessions:

$1 \times 300 \text{ GB} = 0.3 \text{ TB}$ for the “Zero Downtime Backup for 1 TB” license.

One “Direct Backup for 1 TB” license, two “Zero Downtime Backup for 1 TB” licenses and one “Instant Recovery for 1 TB” license are sufficient if all four examples in figures 5-2 to 5-6 are configured in a cell.

Producing a License Report on Demand

To produce a license report, the Data Protector `omnicc` command is to be used. Enter the following command:

```
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.

If the `-detail` option is specified, a detailed report is produced. The following information is returned for every license in the cell: license name, licenses installed, licenses used and licenses required.

Refer to the `omnicc` man page for more information. 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, enter the following command:

```
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.

Which Licenses Are Available?

The following table shows the licenses available in this product. For details of each product number please refer to Appendix A of this guide.

Figure 5-6 The HP OpenView Storage Data Protector Product Structure

HP OpenView Storage Data Protector 6.0 product structure 

1. starter packs (obligatory)		all platforms	Windows	Linux	HP-UX	Solaris
LTU & DVDs	1x management system	B6960LA	B6961AA	B6961DA	B6951AA	B6951DA
Starter Pack manuals - printed						
LTU only	1x management system	B6960MA	B6961BA	B6961CA	B6951BA	B6951CA
DVDs set	Includes 2 DVDs	B6960MB				
CDs set (DVDs suggested)	Includes 15 CDs					
2. drive & library extensions		all platforms	Windows, NetWare, Linux		SAN, UNIX, NAS	
drive LTU	1x drive		B6963AA		B6953AA	
library LTU	1x 61-250/unlimited slots 1x upgr. to unlimited slots	B6957BA/B6958BA B6958CA				
3. functional extensions		all platforms	Windows & Linux		UNIX	
functional extensions manuals - printed		B6960EA				
on-line backup LTU	1x system		B6965BA		B6955BA	
manager-of-mgrs. LTU	1x system		B6966AA		B6956AA	
adv. backup to disk LTU	1x TB/10x TB/100x TB	B7038AA/ BA/CA				
open file backup LTU	1x enterprise server	BA155AA				
	1x 1-server/1x10-servers	BA153AA/BA				
	5x workstations	BA154AA				
	CD only	BA152AA				
media operations LTU	1x2,000/10,000 media	B7100AA/B7101AA				
	1x unlimited media	B7102AA				
	CD only/manuals only	B7129AA/B7128AA				
		NDMP				
ZDB LTU	1x TB /10x TB		HP XP	HP EVA	EMC	
instant recovery LTU	1x TB /10x TB		B7023CA/ DA	B7025CA/ DA	B6959CA/ DA	
direct backup LTU	1x TB /10x TB		B7026CA/ DA	B7028AA/ DA		
		B7022BA/ DA	B7027AA/ DA			
single server edition			Windows	HP-UX	Solaris	
LTU & media / LTU only			B7030AA/BA	B7020AA/BA	B7020DA/CA	
migration to starter pack			B7031AA	B7021AA	B7021DA	

NEW SKUs with Data Protector 6.0

Data Protector leverages the product numbers of its predecessor, OmniBack II, for easy migration to Data Protector. This is why existing OmniBack II A.03.x licenses remain valid after the migration. Some license types have been replaced by new license types and are no longer

available for purchase. Refer to “Data Protector A.06.00 Product Structure and Licenses” on page A-3 for more information about available licenses.

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.
- 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.
- 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 IP addresses.

NOTE

If you intend 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 (and you do not use the MoM functionality), you must contact the *HP Password Delivery Center (PDC)* in order to update the licenses. See “Other Ways of Obtaining and Installing Permanent Passwords” on page 296 for information about contacting the *HP Password Delivery Center*.

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. Please refer to your support contact or to the HP Licensing site at: <http://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://webware.hp.com> where passwords can be generated, moved, and so on.

The recommended way of obtaining passwords is by using the *HP OpenView AutoPass utility*, which can be installed during the Cell Manager installation process. Refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294 for instructions on how to obtain passwords using the HP OpenView AutoPass utility after it has been installed during the Cell Manager installation process.

Refer to “Other Ways of Obtaining and Installing Permanent Passwords” on page 296 for instructions on how to obtain and install a password by means other than *HP OpenView AutoPass utility*.

Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility

The HP OpenView AutoPass utility lets you install passwords for your HP OpenView products’ purchased licenses directly through the internet from the HP password delivery center web server. Refer to the *HP OpenView AutoPass Licensing Guide* for more information on the HP OpenView AutoPass utility.

Prerequisites and Limitations

To obtain and install permanent passwords using the HP OpenView AutoPass utility, the following conditions must be fulfilled:

- The HP OpenView AutoPass utility must have been installed during the Cell Manager installation using the Data Protector `omnisetup.sh` script (UNIX systems) or during the Cell Manager installation (Windows systems).
- It is *not* recommended to install the HP OpenView AutoPass utility in Microsoft Cluster, because it will be installed only on one node and not on all nodes.
- On MC/ServiceGuard, the HP OpenView AutoPass utility must be installed on 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.

For additional prerequisites and limitations, refer to the *HP OpenView AutoPass Licensing Guide*.

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. Refer to the *HP OpenView AutoPass Licensing Guide* to see what information is required.
2. Order the password online using the *HP OpenView AutoPass utility*. To start the *HP OpenView AutoPass utility*, run the following 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).

```
/opt/omni/sbin/omniinstlic (UNIX Cell Manager) or  
<Data_Protector_home>\bin\omniinstlic (Windows Cell  
Manager)
```

For more information on the `omniinstlic` command refer to its man page.

3. Follow the *HP OpenView AutoPass utility* wizard and enter the required information.

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. To verify the installed passwords, refer to “Verifying the Password” on page 298 for instructions.

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” on page A-25 to find the location of the forms and get instructions on how to fill them out.
2. See “Data Protector A.06.00 Product Structure and Licenses” on page A-3 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 (refer to 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 distribution media:

- On Windows:
 <Data_Protector_home>\Docs\license_forms.txt
- On Windows CD-ROM:
 <Disk_Label>:\Docs\license_forms.txt
- On UNIX: /opt/omni/doc/C/license_forms_UNIX

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

The following is the procedure to install a permanent password that the *HP Password Delivery Center (HP PDC)* has sent to you:

Prerequisites

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:

```
4PXV EG9S B6WS 2VX3 5967 XEZK AAA9 MQJB "Product: B6963AA"
```

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 Windows:
`<Data_Protector_home>\Config\server\Cell\lic.dat`
- On UNIX: `/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. Run the following command:
 - On Windows:
`<Data_Protector_home>\bin\omnicc -install_license <password>`
 - On UNIX:
`/opt/omni/bin/omnicc -install_license <password>`

The `<password>` string must be entered exactly as it appears on the *Password Certificate*.

You can also append the password to the following file:

- On Windows:
`<Data_Protector_home>\config\server\cell\lic.dat`
- On UNIX: `/etc/opt/omni/server/cell/lic.dat`

If the file does not exist, create it with an editor, such as `vi` or Notepad. Refer to step 3 in the procedure for the graphical user interface for an example of a password.

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 Manager:

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:

- On Windows:
`<Data_Protector_home>\bin\omnicc -password_info`
- On UNIX: `/opt/omni/bin/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. Run the following command:
 - On Windows: `<Data_Protector_home>\bin\omnicc -query`
 - On UNIX: `/opt/omni/bin/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*. If you want to move licenses for products, which can no longer be purchased, then please use the *License Move Forms* delivered with the previous version of the product. Refer to “Data Protector Licensing Forms” on page A-25.

On the form, you must specify the number of licenses you want to move from the existing Cell Manager.

2. Delete the following file:
 - On Windows:
`<Data_Protector_home>\config\server\cell\lic.dat`
 - On UNIX: `/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, refer to the Data Protector online 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, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

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 for 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, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

| 6 Troubleshooting Installation

In This Chapter

This chapter contains information specific to installation related problems. For general troubleshooting information, see the *HP OpenView Storage Data Protector Troubleshooting Guide*.

This chapter includes information on:

- “Name Resolution Problems when Installing the Windows Cell Manager” on page 305
- “Verifying DNS Connections Within Data Protector Cell” on page 306
- “Troubleshooting Installation and Upgrade of Data Protector on Windows” on page 309
- “Troubleshooting Installation of the Data Protector Cell Manager on Solaris” on page 310
- “Troubleshooting Installation of UNIX Clients” on page 311
- “Verifying Data Protector Client Installation” on page 313
- “Troubleshooting Upgrade” on page 314
- “Using Log Files” on page 315
- “Creating Installation Execution Traces” on page 318

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. For information, see the “Troubleshooting Networking and Communication” chapter of the *HP OpenView Storage Data Protector Troubleshooting Guide*.

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 “Setting Up the TCP/IP Protocol on Windows Systems” on page B-15.

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 vice versa
- Media Agent to any other member of the cell and vice versa

Using the `omnicheck` command

Limitations

- The command verifies connections among the cell members only; it does not verify DNS connections in general.
- It can be used only on Data Protector clients that have Data Protector A.05.10 or later installed. If the command encounters a client with an older Data Protector version, an error message is returned and the command resumes operation on the next client.

The `omnicheck` command resides on the Cell Manager in the following directory:

Windows: `<Data_Protector_home>\bin`

UNIX: `/opt/omni/bin`

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 vice versa, run:

```
omnicheck -dns [-verbose]
```

- To check that a particular Data Protector client resolves DNS connections to every Data Protector client in the cell properly and vice versa, run:

```
omnicheck -dns -host <client> [-verbose]
```

where <client> is the name Data Protector client checked.

- To check all possible DNS connections in the cell, run:

```
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.

See the omnicheck man page for more information.

Table 6-1 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 OpenView Storage Data Protector Troubleshooting Guide*.

Table 6-1

Return Messages

Return Message	Meaning
<i>client_1</i> cannot connect to <i>client_2</i>	Timeout connecting to <i>client_2</i> .
<i>client_1</i> connects to <i>client_2</i> , but connected system presents itself as <i>client_3</i>	The <%SystemRoot%>\System32\drivers\etc\hosts (Windows systems) or /etc/hosts (UNIX systems) file on the <i>client_1</i> is not correctly configured or the hostname of the <i>client_2</i> does not match its DNS name.

Table 6-1 **Return Messages**

Return Message	Meaning
<i>client_1</i> failed to connect to <i>client_2</i>	<i>client_2</i> is either unreachable (e.g. disconnected) or the <%SystemRoot%>\System32\drivers\etc\hosts (Windows systems) or /etc/hosts (UNIX systems) file on the <i>client_1</i> is not correctly configured.
checking connection between <i>client_1</i> and <i>client_2</i>	
all checks completed successfully.	
<i>number_of_failed_checks</i> checks failed.	
<i>client</i> is not a member of the cell.	
<i>client</i> contacted, but is apparently an older version. Hostname is not checked.	

Troubleshooting Installation and Upgrade of Data Protector on Windows

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 A.06.00, 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.

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 II 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 OmniBack II share.

Troubleshooting Installation of the Data Protector Cell Manager on Solaris

Problem

Unable to make temporary directory

During the installation of the Cell Manager on Solaris, a temporary directory cannot be created and the installation fails with the following error message:

```
Processing package instance <OB2-CORE> from  
</tmp/DP_A0510_158_SUN78.pkg>  
  
pkgadd: ERROR: unable to make temporary directory  
<>//tmp/old//installR.a0j3>
```

Action

Manually create the missing temporary directory in the location provided in the error message and restart the installation procedure.

For example, if you get the above error message, create the following directory: `//tmp/old//installR.a0j3`.

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 biggest package being installed. 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 OpenView Storage 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

Omniinet 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 and Solaris: `ps -ef | grep inetd`

Linux: `ps -ef | grep xinetd`

To start the service, run:

HP-UX: `/usr/sbin/inetd`

Solaris: `/usr/sbin/inetd -s`

Linux: `rcxinetd start`

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 and MPE 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.

See online Help for details.

If your installation has not succeeded, see “Using Log Files” on page 315.

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 OmniBack II/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” on page 203.

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
```

Manual Upgrade Procedure

Normally, you upgrade Data Protector A.05.00, Data Protector A.05.10, or Data Protector A.05.50 on UNIX Cell Manager and Installation Server by running the `omnisetup.sh` command, which performs an automated upgrade procedure. However, you can also perform the upgrade manually. See “Upgrading on HP-UX and Solaris Systems Using Native Tools” on page 12.

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:

On HP-UX Cell Manager:

- /var/adm/sw/swinstall.log
- /var/adm/sw/swagent.log (for more details)

On Solaris Cell Manager:

/var/opt/omni/log/debug.log

On Linux Cell Manager: TBD

/var/opt/omni/log/debug.log

On Windows clients (on the system where the setup is running):

- <Temp>\OB2SetupLauncher.log
- <System_disk>:\<Temp>\OB2_Setup_ui_<Date>_<Time>.txt
- <Temp>\OB2DBG_<did>__setup_<Host><Debug_no>.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.
- <Host> is the name of the host where the trace file is created.

— `<Debug_no>` is a number generated by Data Protector.

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 a remote installation, check the following log files:

On UNIX Installation Server:

`/var/opt/omni/log/IS_install.log`

On Windows clients (only on the remote client system):

- `<Temp>\INSTALL_SERVICE*.*`
 - `<System_disk>:\<Temp>\OB2_Setup_exe_<Date>_<Time>.txt`
- where `<Temp>` is a directory specified in the `TEMP` environment variable.

In case the setup log files are not created, run the remote installation with the debug option. See “Creating Installation Execution Traces” on page 318.

Data Protector Log Files

The Data Protector log files listed below are located in:

Windows: `<Data_Protector_home>\log`

HP-UX, Solaris, and Linux: `/var/opt/omni/log` and
`/var/opt/omni/server/log`

Other UNIX: `/usr/omni/log`

Novell NetWare: `SYS:\USR\OMNI\LOG`

The following log files are important for troubleshooting installation:

<code>debug.log</code>	Contains unexpected conditions. While some can be meaningful to you, the information is mainly used by the support organization.
<code>inet.log</code>	Contains requests made to the Data Protector <code>inet</code> 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 (UNIX only) This log is created during upgrade and contains traces of the upgrade process.

For more log files, see the *HP OpenView Storage 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 OpenView Storage Data Protector Troubleshooting Guide*.

Windows:

For debugging remote installation on a Windows system, run the Data Protector GUI with the debug option:

```
Manager -debug 1-99 <Debug_postfix>
```

Once the session is finished/aborted, collect the debug output from the following locations:

- On the Installation Server system:

```
<Data_Protector_home>\tmp\OB2DBG_<did>__BM_  
<Installation_Server><Debug_no><Debug_postfix>
```

- On the remote system:

```
<System_disk>:\<Temp>\OB2DBG_<did>__INSTALL_SERVICE<Host_  
name><Debug_no><Debug_postfix>
```

UNIX:

For debugging the installation on a UNIX system, run the Data Protector GUI with the debug option:

```
xomni -debug 1-99 <Debug_postfix>
```

or

```
xomniadmin -debug 1-99 <Debug_postfix>
```

Once the session is finished/aborted, collect the debug output from the Installation Server system's `tmp` directory.



A **Appendix A**

In This Appendix

This Appendix provides a description of the Data Protector A.06.00 product structure and Data Protector licensing forms.

Data Protector A.06.00 Product Structure and Licenses

Data Protector builds upon the product structure of its predecessor, OmniBack II, in order to make the upgrade process easier. Data Protector also includes new *License Categories (Licenses-to-use, or LTUs)* and *Product Numbers* for new functionality. Data Protector licensing has a Starter Pack license as the starting point. Backup drives connected to the system, and the functionality used in the Data Protector cell, such as online backups, zero downtime backup integrations, the Manager-of-Managers, and so on has separate licenses.

This section explains the *Product Numbers* and types of licenses offered by Data Protector A.06.00 Cell Manager.

NOTE


The licenses delivered for the UNIX products can be applied either to UNIX, Windows, Novell Netware or Linux.

Data Protector A.06.00 Cell Manager software is available for the HP-UX, Solaris and Windows platforms. Disk agents are supplied free for all major platforms which are supported as disk agents,

For a product overview, see Figure A-1 on page A-4.

Figure A-1 on page A-4 provides an overview of the available Data Protector A.06.00 product structure.

Figure A-1 HP OpenView Storage Data Protector Product Structure

HP OpenView Storage Data Protector 6.0 product structure 

1. starter packs (obligatory)		all platforms	Windows	Linux	HP-UX	Solaris
LTU & DVDs	1x management system	B6960LA	B6961AA	B6961DA	B6951AA	B6951DA
Starter Pack manuals - printed						
LTU only	1x management system		B6961BA	B6961CA	B6951BA	B6951CA
DVDs set	Includes 2 DVDs	B6960MA				
CDs set (DVDs suggested)	Includes 15 CDs	B6960MB				
2. drive & library extensions		all platforms	Windows, NetWare, Linux		SAN, UNIX, NAS	
drive LTU	1x drive	B6957BA/B6958BA	B6963AA		B6953AA	
library LTU	1x 61-250/unlimited slots 1x upgr. to unlimited slots		B6958CA			
3. functional extensions		all platforms	Windows & Linux		UNIX	
functional extensions manuals - printed		B6960EA				
on-line backup LTU	1x system	B7038AA/ BA/CA	B6965BA		B6955BA	
manager-of-mgrs. LTU	1x system		B6966AA		B6956AA	
adv. backup to disk LTU	1x TB/10x TB/100x TB	BA153AA/BA				
open file backup LTU	1x enterprise server					
	1x 1-server/1x10-servers					
	5x workstations	BA154AA				
	CD only	BA152AA				
media operations LTU	1x2,000/10,000 media	B7100AA/B7101AA				
	1x unlimited media	B7102AA				
	CD only/manuals only	B7129AA/B7128AA				
		NDMP				
ZDB LTU	1x TB /10x TB	B7022BA/ DA	HP XP	HP EVA	EMC	
instant recovery LTU	1x TB /10x TB		B7023CA/ DA	B7025CA/ DA	B6959CA/ DA	
direct backup LTU	1x TB /10x TB		B7026CA/ DA	B7028AA/ DA		
			B7027AA/ DA			
single server edition			Windows	HP-UX	Solaris	
LTU & media / LTU only			B7030AA/BA	B7020AA/BA	B7020DA/CA	
migration to starter pack			B7031AA	B7021AA	B7021DA	

NEW SKUs with Data Protector 6.0

Drive and Library Extensions

HP OpenView Storage Data Protector Drive Extension for UNIX, NAS, SAN

B6953AA

B6963AA

This product includes the license-to-use (LTU) for one additional backup drive directly attached to a UNIX system, a NAS device, used in a SAN, or used for serverless backup.

Drives attached to HP MPE systems and OpenVMS systems require this license.

A backup drive can be a tape drive, a logical drive on disk (backup to disk using a file device), or Magneto Optical. The drive can be accessed and managed locally or via the network from a system with any Cell Manager license.

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.

IMPORTANT

For releases prior to Data Protector A.05.10, drive licenses were defined as “concurrently used” drive licenses. The underlying concept is that the customer does not pay for all configured drives, but for all drives used in parallel at any point in time (for any operation such as backup, restore, disaster recovery, format, verify, tape copy, object copy, mirror, scan,...). This concept is still the same with Data Protector A.05.10 and A.05.50. However, in the past the number of configured drives varied greatly from the number of drives used at the same time (for example, embedded drives in each server). Today, most customers share their drives in the network (SAN or LAN). The effect of this is that there is no longer a de facto difference between configured drives and concurrently used drives. Therefore, you should buy as many licenses as you have configured drives, otherwise it will not be possible to use them all at the same time.

Please note that even though Data Protector does enforce some license schemes, with the current release it does not enforce the complete license structure. For example, Data Protector does not enforce the read operation from a drive, to make sure that in disaster recovery situations, you do not need to deal with missing license keys.

The license description is the legally binding document, not the product enforcement, and/or the license reporting.

This LTU is also required for:

- NAS systems managed via NDMP (for example, Network Appliance Filers and EMC Celerra File Servers), or NAS systems requiring a Data Protector proprietary Device Server (Media Agent), (for example, HP Storage Works NAS 8000). NAS systems powered by Windows, NetWare or standard Linux which can run a standard Data Protector Device Server (Media Agent) only require Data Protector drive extensions for Windows, Netware, Linux (B6963AA).

It can also be used for single drives attached to Windows, NetWare, and Linux systems. However, in the case where the drive is not used in a SAN, it is cheaper to use LTU B6963AA.

HP OpenView Storage Data Protector Drive Extension for Windows, Novell NetWare, Linux (Intel)

B6963AA

This product includes the license-to-use (LTU) for one additional backup drive used directly attached to a Windows, NetWare or Linux (Intel) system. A backup drive can be a tape drive, a logical drive on disk (backup to disk using a file device), or Magneto Optical. The drive can be accessed and managed locally or via the network from a system with any Cell Manager license.

This license is valid for drives attached to NAS devices powered by Windows, NetWare or Linux, which can run a standard Data Protector Device Server (Media Agent).

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.

IMPORTANT

For releases prior to Data Protector A.05.10, drive licenses were defined as “concurrently used” drive licenses. The underlying concept is that the customer does not pay for all configured drives, but for all drives used in parallel at any point in time (for any operation such as backup, restore, disaster recovery, format, verify, tape copy, object copy, mirror, scan,...). This concept is still the same with Data Protector A.05.10 and A.05.50.

However, in the past the number of configured drives varied greatly from the number of drives used at the same time (for example, embedded drives in each server). Today, most customers share their drives in the network (SAN or LAN). The effect of this is that there is no longer a de facto difference between configured drives and concurrently used drives. Therefore, you should buy as many licenses as you have configured drives, otherwise it will not be possible to use them all at the same time.

Please note that even though Data Protector does enforce some license schemes, with the current release it does not enforce the complete license structure. For example, Data Protector does not enforce the read operation from a drive, to make sure that in disaster recovery situations, you do not need to deal with missing license keys.

The license description is the legally binding document, not the product enforcement, and/or the license reporting.

Drive licenses cannot be shared between multiple cells.

NOTE

This license-to-use is not sufficient for storage resource sharing in a SAN (Storage Area Network). B6952AA is required where multiple systems share backup drives in a SAN. A fibre channel point-to-point connection is not considered a SAN.

For details of supported drives please see the Data Protector support matrices:

http://www.openview.hp.com/products/datapro/spec_0001.html

Functional Extensions

HP OpenView Storage Data Protector On-line Extension

B6955BA	for UNIX
B6965BA	for Windows/Linux

These products include the license-to-use (LTU) to perform on-line backup of databases and applications running on the specified platform.

- If a system runs multiple partitions, this LTU is required for each partition.

- In a cluster environment, each system participating in the cluster requires a license-to-use. For releases prior to Data Protector 5.5 just one LTU was required for fail over (active/stand by). As from the Data Protector 5.5 release, all systems in a cluster require an LTU.
- As from the release of Data Protector 5.1 on-line backup licenses are required for Zero Downtime Backup (ZDB).
- As from the release of Data Protector 5.1, the Windows 2003 file system snapshot feature VSS (Volume Shadow copy Service) is supported at not extra charge. however on-line backup of databases, which are not part of the operating system, require this on-line backup extension. System configuration backup does not require the on-line backup extension.
- This LTU is required for MS Exchange Single Mailbox backup.

This LTU is not required for HP OpenView Network Node Manager on-line backup.

For supported databases please refer to the Data Protector support matrices at:

http://www.openview.hp.com/products/datapro/spec_0001.html

HP OpenView Storage Data Protector Open File Backup

BA153AA	1 server
BA153BA	10 servers
BA154AA	5 workstations
BA155AA	1 enterprise server
BA152AA	Media

This product contains the Licenses-to-use (LTU) for open file backup of applications, databases and e-mail files (for example, “.pst” - Microsoft Outlook files) running on specified servers that are not covered by the Data Protector integration matrix.

The Licenses-to-Use (LTU) for 1 server and 10 servers supports Windows NT 4.0 Server, Windows 2000 Server and Windows 2003 Server.

The License-to-Use (LTU) for 5 workstations supports Windows NT/2000/XP workstations.

The License-to-Use (LTU) for 1 enterprise server supports 1 Windows NT Server 4.0 Enterprise Edition, Windows 2000 Advanced Server, Windows 2003 Enterprise Server, Microsoft Cluster Server, Netware 4.x, 5.x LFS only, NetWare 6.0 LFS, NSS and Netware 6.5 LFS and NSS.

The media is included in the Data Protector starter packs. It can also be ordered separately via BA152AA (which includes the open file backup software).

HP OpenView Storage Data Protector Manager-of-Managers Extension

B6956AA	for UNIX
B6966AA	for Windows

Includes the license-to-use required for each Data Protector management server (Cell Manager), running on the specified platform to be part of a Manager-of-Managers environment.

This license is required to share tape libraries between multiple Data Protector cells. It is an ideal solution for central backup management of branch offices.

B6956AA can be used for a Windows management server (Cell Manager). However, ordering B6966AA is more affordable.

HP OpenView Storage Data Protector Library Extensions

B6957BA with 61-250 slots

B6958BA with unlimited slots

This product contains the License-to-use (LTU) for managing tape libraries with the specified number of slots. The license is required once per library.

This license is required once for each library per cell.

STK silos using ACSLS and GRAU/EMASS library systems using DAS require the license B6958BA.

If a tape library is shared between multiple Data Protector cells, an LTU for a Manager-of-Managers extension is required.

This product contains the License-to-use (LTU) for managing tape libraries with no slot limitation.

STK silos using ACSLS and GRAU/EMASS library systems using DAS require the license B6958BA.

For details of supported libraries please refer to the Data Protector support matrices under:

http://www.openview.hp.com/products/datapro/spec_0001.html

HP OpenView Storage Data Protector Media Operations Extension

B7100AA	Entry Level
B7101AA	Enterprise
B7102AA	Unlimited
B7128AA	Manuals
B7129AA	Media

The Entry Level includes the License-to-use (LTU) for 2000 media, one management server and unlimited clients.

The Enterprise Level includes the License-to-use (LTU) for 10000 media, one management server and unlimited clients.

The unlimited media includes the License-to-use (LTU) for unlimited media, one management server and unlimited clients.

Media refers to the total number of tape media to be tracked in the Data Protector Media Operations internal database. The entry level and enterprise level licenses can be used in any combination to match the customer's total number of tape media to be tracked.

The Data Protector Media Operations CD is included in the Data Protector starter packs, but it can also be ordered separately via B7129AA.

The Data Protector Media Operations manuals are included in the Data Protector Functional Extensions manuals pack, but they can be ordered separately via B7128AA.

HP OpenView Storage Data Protector Advanced Backup to Disk Extension

B7038AA

This product contains the License-to-use (LTU) for one terabyte (TB) of backup to disk storage.

Used backup disk storage is the space occupied by protected backups.

Used capacity differs from raw capacity in that the RAID overhead is excluded. This means the RAID configuration does not need to be considered.

The backup to disk storage cannot be distributed over multiple disk arrays and systems.

This extension does not require any drive and library LTU. Drive and library licenses are required for file devices, but not for advanced backup to disk. Similarly, advanced backup to disk cannot be licenses with drive and library licenses.

It does not matter whether the backup to disk functionality is being run on Windows or Unix.

“Advanced Backup to Disk” is a combination of many features: “file library”, “object copy”, “backup mirroring”, “automated media copy” etc.

Some examples of the way this license would work are as follows:

One backup disk array with a total raw capacity of 2.5 TB, fully configured for advanced backup to disk requires 3 X B7038AA. It does not matter how much backup data resides on the disk.

One backup disk array with a total raw capacity of 2.5 TB, fully configured in RAID 1 (mirroring) has only a logical volume capacity of 1.25 TB and would only require 2 X B7038AA if fully configured for advanced backup to disk.

Two backup disk arrays with a logical capacity of 2.5 TB each, each fully configured for advanced backup to disk require 5 X B7038AA.

Ten blade servers with 0.75 TB logical capacity each, fully configured for advanced backup to disk require 8 X B7038AA.

HP OpenView Storage Data Protector Zero Downtime Backup (ZDB) Extension

B7023CA	for HP StorageWorks Disk Array XP
B7025CA	for HP StorageWorks Virtual Array and StorageWorks Enterprise Virtual Array
B6959CA	for EMC Symmetrix

These products include the license-to-use for up to one terabyte (TB) of used disk space capacity of the specified disk array type protected by zero downtime backup (ZDB) and utilizing:

- HP Business Copy XP/EVA/VA and/or
- HP Continuous Access XP or
- EMC TimeFinder and/or
- EMC SRDF

NOTE

If performing Zero Downtime Backup (ZDB), an On-line extension LTU is also required in addition to the relevant ZDB extension LTU. Refer to “HP OpenView Storage Data Protector On-line Extension” on page A-7.

Used disk space capacity is the total capacity of all primary volumes on the disk array type being used for Zero Downtime Backup or instant recovery (i.e. Primary means the original production data volumes). This amount represents the total usable capacity of these volumes matching with their configured LDEV sizes. Data Protector does not require licenses for the capacity consumed by the secondary volumes, mirrors, snapshots that are used for protection.

- Excludes RAID overhead. This means the RAID configuration does not have to be considered.

As from Data Protector 5.1 the on-line backup LTU (B6955BA, B6865BA) is required. Customers with existing ZDB installations can continue to use them without the on-line backup extension for each application server. Further extensions require the on-line backup extension.

As from Data Protector 5.1 the Windows 2003 file system snapshot feature VSS (Volume Shadow copy Service) is supported at no extra charge. However, backup via a hardware provider requires this ZDB extension. For example, file system snapshot, MS Exchange Server, MS SQL Server backup via an HP disk array provider.

HP OpenView Storage Data Protector Instant Recovery Extension

B7026CA for HP StorageWorks Disk Array XP

B7028AA for HP StorageWorks Virtual Array and StorageWorks Enterprise Virtual Array

These products include the license-to-use (LTU) for up to one terabyte (TB) of used disk space capacity, required for the instant recovery of the specified disk array type utilizing instant recovery. Data Protector instant recovery permits recovery of terabytes of data from one or multiple recovery disks in minutes; rather than recovery from tape, which could take hours.

Used disk space capacity is the total capacity of all volumes on the disk array types that are used for Zero Downtime Backup (ZDB) or instant recovery (i.e. Primary means the original production data volumes). This amount represents the total usable capacity of these volumes corresponding with their configured LDEV sizes. Data Protector does not require licenses for the capacity consumed by the secondary volumes, mirrors, snapshots that are used for protection.

- Excludes RAID overhead. This means the RAID configuration does not need to be considered.
- Requires a matching quantity of Data Protector ZDB LTUs.

HP OpenView Storage Data Protector Direct Backup Extension

B7027AA for HP StorageWorks Disk Array XP

Includes the license-to-use (LTUs) to perform direct backup with HP StorageWorks disk array XP. Required once for each terabyte (TB) of used source disk space needed for Direct (serverless) backup.

Requires a matching quantity of Data Protector ZDB LTUs and On-line backup LTUs.

HP OpenView Storage Data Protector Direct Backup Using NDMP

B7022BA

This product contains the License-to-use (LTU) to perform the backup of up to one terabyte (TB) on 1 NDMP Server.

This license is required once per terabyte (TB) of used disk space for each filer being backed up via NDMP (e.g., Network Appliance Filer or EMC Celerra File Server).

Used disk space capacity is the total capacity of all volumes of the filer being backed up via NDMP. This amount represents the total usable capacity of these volumes matching with their configured LDEV sizes.

HP OpenView Storage Data Protector Manuals: Functional Extensions

B6960EA	English
B6960EJ	Japanese

Includes the manuals for the Data Protector Functional Extensions:

- *HP OpenView Storage Data Protector Integration Guide for Microsoft Applications: SQL Server, Exchange Server, and Volume Shadow Copy Service*
- *HP OpenView Storage Data Protector Integration Guide for Oracle and SAP*
- *HP OpenView Storage Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes / Domino*
- *HP OpenView Storage Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol*
- *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*
- *HP OpenView Storage Data Protector Zero Downtime Backup Concepts Guide*
- *HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide*
- *HP OpenView Storage Data Protector Media Operations User's Guide*
- *HP OpenView Storage Data Protector Integration Guide for HP OpenView*
- *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for UNIX*
- *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for Windows*

Note: LTUs for the functional extensions have separate product numbers

All manuals are available electronically in Acrobat PDF format on your system, if you have installed the documentation packet.

Single Server Editions

HP OpenView Storage Data Protector Single Server Edition

LTU, Media, and Manuals

B7020AA	HP-UX - English
B7020AJ	HP-UX - Japanese
B7020DA	Solaris - English
B7020DJ	Solaris - Japanese
B7030AA	Windows - English
B7030AJ	Windows - Japanese

LTU Only

B7020BA	HP-UX
B7020CA	Solaris
B7030BA	Windows

Migration to Starter Pack

B7021AA	HP-UX
B7021DA	Solaris
B7031AA	Windows

The license-to-use (LTU) in the single server edition can be used to backup one single server on the specified platform with an unlimited number of UNIX and/or Windows workstations, one backup drive. Additionally, this edition can manage one autochanger/library with up to 10 slots.

To obtain the following functionality the Single Server Edition has to be migrated to the Starter Pack:

- additional backup clients (agents) on any platform
- additional backup drives
- the ability to manage autoloaders/libraries with more than 10 slots
- systems disaster recovery
- sophisticated reporting (in the Data Protector GUI and via the web)
- SAN support (with the management server for HP-UX, Solaris)
- service-centric management through integrations into OpenView

To order the migration LTU, a single server edition LTU is required.

NOTE

The Single Server Edition for Windows can manage only Windows workstations.

Once migrated, additional drives as well as further additional functionality can be ordered via LTUs.

To order the migration LTU a single server edition LTU is required.

Migration to the Starter Packs

B7021AA	HP-UX
B7021DA	Solaris
B7031AA	Windows

These products contain the License-to-use (LTU) to migrate from the Single Server Edition to the HP OpenView Storage Data Protector Cell Manager Single Drive.

This upgrade is available only if you already have the Single Server license. Order it to obtain the following functionalities: more Server clients, Cluster support, additional backup drives, online backup, Manager-of-Managers, autochanger with more than 10 slots and, in the case of the Single Server Edition Windows only, UNIX and Novell NetWare clients.

License Migration to Data Protector A.06.00 and A.05.10

Migration from previous versions of Data Protector is as follows:

Data Protector A.05.x

Migrate directly to Data Protector A.06.00. No license migration is required or any other kind of migration. Data Protector A.05.x customers on support contract will receive Data Protector A.06.00 for free. Once they upgrade their environment to Data Protector, the functionality that they were using with A.05.x will be available with Data Protector A.06.00 at no additional cost. They only need to purchase new licenses if they want to acquire new functional extensions provided with Data Protector.

Support Contract Migration

No license (password) migration is required when updating to Data Protector A.06.00. However, support contracts should reflect the appropriate Data Protector A.06.00 product numbers as they get updated.

For example, if a customer had 1 B7023BA (ZDB for XP) LTU in OmniBack II A.04.00, and migrates to Data Protector A.06.00, this line item on the support contract should be changed to 3 B7023CA LTUs.

The following migration table indicates how to migrate OmniBack II A.03.x support products to OmniBack II A.04.x support products and OmniBack II A.04.x support products to Data Protector A.05.x support products.

Table A-1 Support Contract Migration Table 1

OmniBack II A.03.5x support products associated with	Product short description	OmniBack II A.04.x support product(s) associated with	Product short description
Multi-Drive Server migration to Single Drives			
B6952AA	Cell Manager Multi-Drive Server for HP-UX	1*B6951AA + 5*B6953AA	1* Cell Manager Single Drive for HP-UX + 5 * Single Drive UNIX
B6962AA	1*Cell Manager Multi-Drive Server for NT/2000	1*B6961AA + 3*B6963AA	1*Cell Manager Single Drive for NT/2000 + 3 * Single Drive NT/2000
B6954AA	Multi-Drive Server for HP-UX	6*B6953AA	6* Single Drive UNIX
B6964AA	Multi-Drive Server for NT/2000	4*B6963AA	4* Single Drive NT/2000
Functional Extensions			
B6955AA	On-line backup UNIX	B6955BA	
B6965AA	On-line backup NT/2000	B6965BA	
B6957AA	61 to 250 slots libraries UNIX	B6957BA	
B6967AA	61 to 250 slots libraries NT/2000	B6957BA	
B6958AA	Unlimited slot libraries UNIX	B6958BA	
B6968AA	Unlimited slot libraries NT/2000	B6958BA	
B7023AA	Split Mirror XP	B7023BA	
B6959AA	Split Mirror EMC Symmetrix	B6959BA	

Table A-2 Support Contract Migration Table 2

OmniBack II A.04.00 support products associated with	Product short description	OmniBack II A.04.10 and Data Protector A.05.x support product(s) associated with	Product short description
Functional Extensions			
B7023BA	Split Mirror XP	3*B7023CA	3*Split Mirror XP
B6959BA	Split Mirror EMC Symmetrix	3*B6959CA	3*Split Mirror EMC Symmetrix
B7024AA	Serverless Backup EMC	3*B7024BA	3*Serverless Backup EMC

Table A-3 Support Contract Migration Table 3

OmniBack II A.04.10 support products associated with	Product short description	Data Protector A.05.x support product(s) associated with	Product short description
Functional Extensions			
B7022AA	NDMP backup	X*B7022BA	X*Direct backup using NDMP

Data Protector Cell Configurations

The following figures show some Data Protector cell configurations and the corresponding licenses that are needed.

Figure A-2 **Single Server Backup**

1 × B7020AA: Single Server Edition for HP-UX



Figure A-3 **Cell Manager - Single Drive for HP-UX, Including up to 60 Slot Single Drive Autochangers**

1 × B6951AA: Starter pack for HP-UX



Figure A-4 Mixed Environment

1 × B6951AA: Starter pack for HP-UX
 11 × B6953AA: Drive extension for UNIX, NAS, SAN
 4 × B6963AA: Drive extension for Windows, NetWare, Linux (Intel)

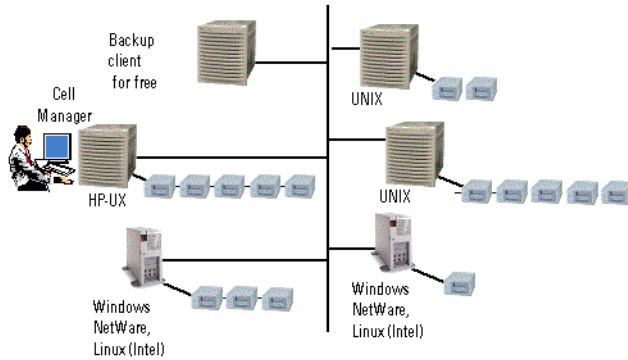


Figure A-5 Online Backup

1 × B6951AA: Starter pack for HP-UX
 2 × B6953AA: Drive extension for UNIX, NAS, SAN
 3 × B6963AA: Drive extension for Windows, NetWare, Linux (Intel)
 3 × B6955BA: On-line extension for UNIX
 3 × B6965BA: On-line extension for Windows

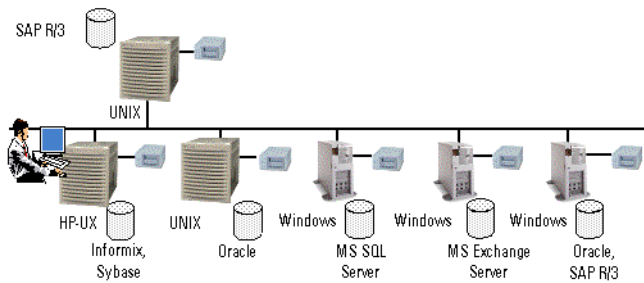


Figure A-6 Application Online Backup

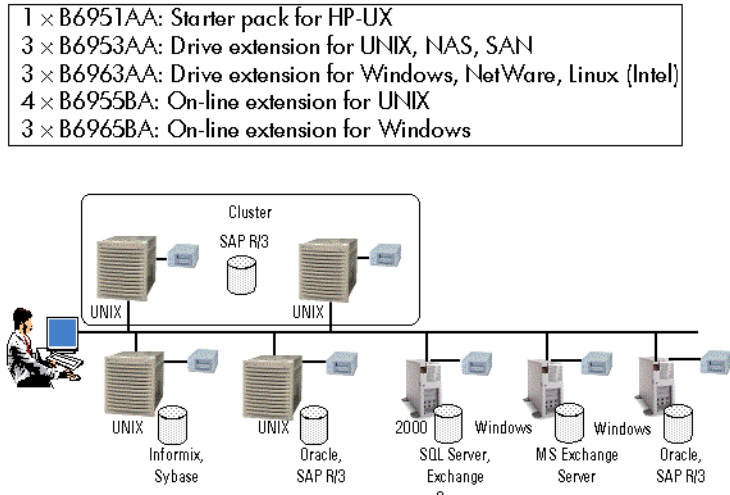


Figure A-7 61 - 250 Slot Libraries - example 1

- 1 × B6961AA: Starter pack for Windows
 7 × B6963AA: Drive extension for Windows, NetWare, Linux (Intel)
 4 × B6953AA: Drive extension for UNIX, NAS, SAN
 1 × B6957BA: Library extension with 61 - 250 slots
 1 × B6958BA: Library extension with unlimited slots

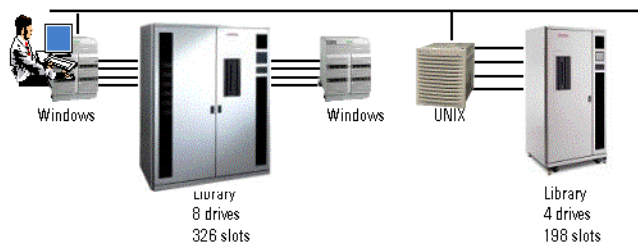


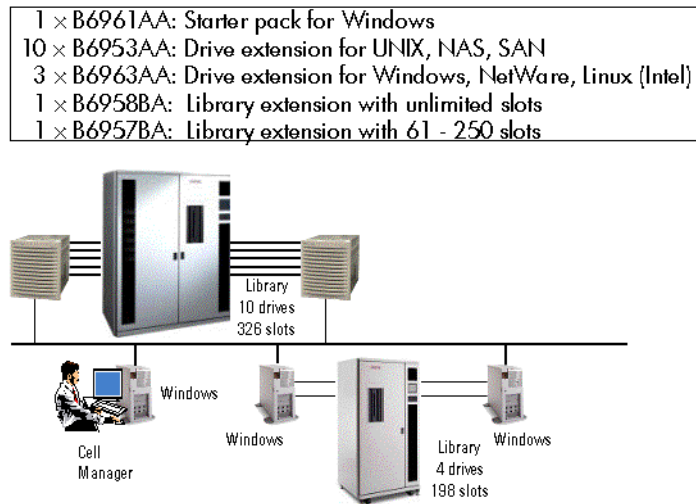
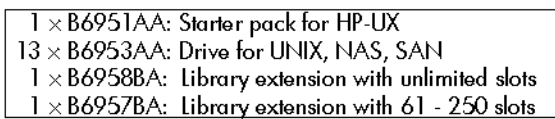
Figure A-8 61 - 250 Slot Libraries - example 2**Figure A-9 61 - 250 Slot Libraries - example 3**

Figure A-10 Zero Downtime Backup

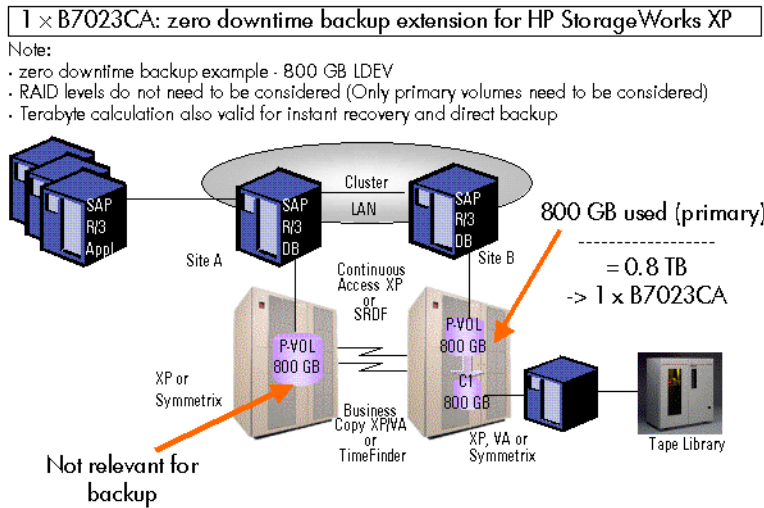
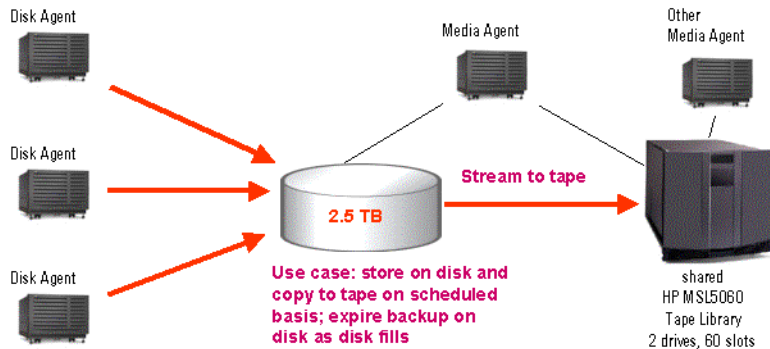


Figure A-11 Advanced Backup to Disk

3 x B7038AA: Advanced backup to disk extension
 2 x B6951AA: Drive extension for UNIX, NAS, SAN



Data Protector Licensing Forms

This chapter discusses Data Protector Licensing forms. Fill them out to order permanent passwords using one of the following methods:

- Use the HP OpenView AutoPass utility to obtain and install permanent passwords directly through the internet from the HP password delivery center web server. Refer to “Obtaining and Installing Permanent Passwords Using the HP OpenView AutoPass Utility” on page 294 for more information. This is the recommended method.
- Print the electronic version of the license forms that are included in the following files on the Cell Manager system and the distribution media:

HP-UX or Solaris /opt/omni/doc/C/license_forms_UNIX

Windows CD-ROM <Disk_Label>:Docs\license_forms.txt

or use the electronic files to “copy” and “paste” your message to the *Password Delivery Center (PDC)*.

- Order permanent passwords using the online *Password Delivery Center* site at <http://www.webware.hp.com>.

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.

Appendix A
Data Protector Licensing Forms

New Cell Manager	Enter the required information about your New Cell Manager.
Order Number	Enter the <i>Order Number</i> printed on the <i>Entitlement Certificate</i> . The <i>Order Number</i> is required to verify that you are entitled to request a permanent password.
IP Address	<p>This field defines for which system the <i>Password Delivery Center</i> will generate the passwords. In case you want to use centralized licensing (MoM environments only) then this system must be the MoM Manager system.</p> <p>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.</p> <p>If you have Data Protector in a MC/ServiceGuard or MS Cluster environment, enter the IP address of your virtual server. See the <i>HP OpenView Storage Data Protector Administrator's Guide</i> for more information on clusters.</p>
<i>The Password Delivery Center</i> Fax Numbers	Refer to the <i>Entitlement Certificate</i> , shipped with your product for contact information.
Product License Type	In the fields next to the <i>Product Numbers</i> , 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 <i>Order Number</i> .



B **Appendix B**

In This Appendix

This Appendix provides some additional information about tasks that are beyond the scope of this manual but strongly influence the installation procedure.

Examples are given of system and device setup and configuration for Windows, HP-UX and Solaris systems.

Installing on HP-UX and Solaris Systems Using Native Tools

NOTE

The native installation procedures on HP-UX and Solaris are only documented if you intend to install an Installation Server with a limited set of packages. It is recommended to install Data Protector using `omnisetup.sh`.

Installing a Cell Manager on HP-UX Systems Using `swinstall`

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

1. Insert and mount the UNIX installation DVD-ROM and run the `/usr/sbin/swinstall` utility.

For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

2. In the Specify Source window, select Network Directory/CDROM, and then enter:

- On a PA-RISC based HP-UX:

`<Mountpoint>/hpux_pa/DP_DEPOT/DP_A0600_UX11x.sd_depot`

- On a IA-64 based HP-UX:

`<Mountpoint>/hpux_ia/DP_DEPOT/DP_A0600_UXia64.sd_depot`

in the Source Depot Path. Then, click OK to open the SD Install - Software Selection window.

3. In the list of available software packages 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 subproducts are included in the product:

OB2-CM

Cell Manager software

OB2-DOCS

Data Protector documentation subproduct that includes Data Protector manuals in the PDF format.

4. Right-click DATA-PROTECTOR, and then click Mark for Install to install the whole software.

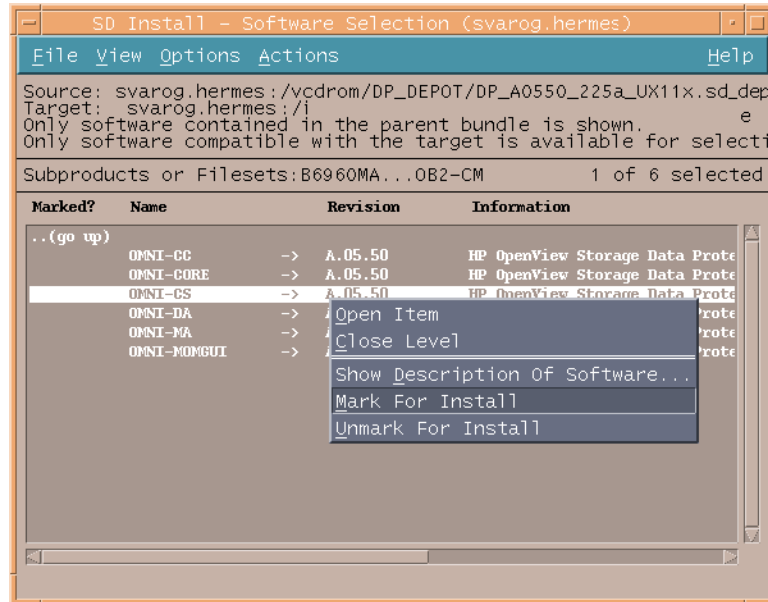
In case you do not need all subproducts, double-click DATA-PROTECTOR and then right-click an item from the list. Click Unmark for Install to exclude the package or Mark for Install to select it for installation.

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. Refer to Figure B-1.

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.

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.

Figure B-1 SD Install - Software Selection Window**NOTE**

If you want 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 Solaris Systems Using pkgadd

Follow the procedure below to install the Cell Manager on a Solaris system:

1. Insert the UNIX installation DVD-ROM.
2. Change to the main `<package_source>` directory, i.e. the directory that contains the installation depot file (in this case `<Mount_point>/solaris/DP_DEPOT`).

The following sub-product packages related to Cell Manager installation are included in the product:

OB2-CORE Data Protector Core software.

OB2-CC	Cell Console software. This contains the graphical user interface and 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.
and optionally:	
OB2-MA or OB2-NDMPP	The General Media Agent (OB2-MA) or the NDMP Media Agent (OB2-NDMPP) software. This is required if you want to attach a backup device to the Cell Manager.
OB2-DOCS	Data Protector online manuals.
OB2-INTGP	Data Protector Core Integrations software. This component is necessary if you want to install integrations.

3. Use the `pkgadd` facility to install the above packages.

IMPORTANT

The sub-product packages on Solaris are dependent on each other. You should install the packages in the order in which they are listed above.

Run the following command to install each package:

```
pkgadd -d DP_A0600_SUN8.pkg <package_name>
```

4. Restart the Data Protector services:

```
/opt/omni/sbin/omnisv stop
```

```
/opt/omni/sbin/omnisv start
```

NOTE

If you installed the Cell Manager on Solaris 9, remotely install the Disk Agent on the Cell Manager using an Installation Server. This will replace the generic Solaris Disk Agent with the Solaris 9 Disk Agent. Refer to “Remote Installation of the Data Protector Clients” on page 45 or to the `ob2install` man page.

Installing an Installation Server on HP-UX Systems

1. Insert and mount the UNIX installation DVD-ROM. For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.
2. At the command line, type `/usr/sbin/swinstall` to run the installation program.
3. In the Specify Source window, select `NetworkPath/CDROM`, and then in the Source Depot Path text box, enter:
 - On a PA-RISC based HP-UX:
`<Mount_point>/hpux_pa/DP_DEPOT/DP_A0600_UX11x_IS.sd_depot.`
 - On a IA-64 based HP-UX:
`<Mount_point>/hpux_ia/DP_DEPOT/DP_A0600_UXia64_IS.sd_depot.`

Then open the SD Install - Software selection window.

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 UNIX installation DVD-ROM.

Installing an Installation Server on Solaris Systems Using pkgadd

Local Installation on Solaris

To install the Installation Server for UNIX on a Solaris system:

1. Insert the UNIX installation DVD-ROM.
2. Change to the main `<package_source>` directory, that is the directory that contains the installation depot file (in this case `<Mount_point>/solaris/DP_DEPOT`).

The following sub-product packages 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-C-IS	Installation Server Core software.
OB2-SOLUX	Disk Agent, Media Agent, and GUI push packets for remote Solaris systems.
OB2-OTHUX	Disk Agent and Media Agent push packets for remote non-Solaris 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 graphical user interface and the command-line interface.
--------	---

OB2-INTGP Data Protector Core Integrations software. This component is necessary if you want to install integrations.

3. Use the `pkgadd` facility to install the above packages.

IMPORTANT

The sub-product packages on Solaris are dependent on each other. You should install the packages in the order in which they are listed above.

Run the following command to install each package:

```
pkgadd -d DP_A0600_SUN8_IS.pkg <package_name>
```

NOTE

The `pkgadd` facility can only be run locally, not remotely.

4. Once you have installed these components, use `pkgadd` to install the push packets for all the integration packages that you will want to install remotely. For instance:

OB2-SAPP	SAP Integration component.
OB2-INFP	Informix Integration component.
OB2-SYBP	Sybase Integration component.
OB2-OR8P	Oracle Integration component.
OB2-DB2P	DB2 Integration component.
OB2-EMCP	EMC Symmetrix Integration component.
OB2-SNAPP	HP StorageWorks Virtual Array.
OB2-EVAAP	HP StorageWorks Enterprise Virtual Array.
OB2-SSEAP	HP StorageWorks Disk Array XP.

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 UNIX installation DVD-ROM.

IMPORTANT

If you want 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 must create the links before the installation and ensure that the destination directories exist.

NOTE

If you install the User Interface component (either the graphical user interface or the command-line interface), you should update your environment variables before using it. Refer to “Setting Environment Variables” on page 24 for more information.

If you intend to use the Data Protector user interface to perform backups or restores across platforms, refer to the *HP OpenView Storage 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. Now you should perform the following tasks:

1. If you have set up an independent Installation Server (i.e. not on the Cell Manager) you must manually add (import) the system to the Data Protector cell. Refer to “Importing an Installation Server to a Cell” on page 179.

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 push-packets. This can be used

from the CLI to check the available push-packets. For this file to be kept up to date, you should export and re-import an Installation Server whenever push-packets 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. Refer to “Installing an Installation Server for Windows” on page 37.
3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 42.

Installing the Clients

The clients are not installed during a Cell Manager Installation Server installation. The clients must be installed either by using `omnisetup.sh` or by pushing the installation components from the Data Protector GUI. For detailed information on how to install the clients, refer to “Installing Data Protector Clients” on page 42.

Upgrading on HP-UX and Solaris Systems Using Native Tools

Upgrading Data Protector on HP-UX Systems Using `swinstall`

An upgrade of a Cell Manager must be performed from UNIX installation DVD-ROM.

For the list of Data Protector installation DVD-ROMs, refer to “Data Protector Installation DVD-ROMs” on page 8.

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 pushing the installation components from the Installation Server. For details refer to “Local Installation of UNIX and Linux Clients” on page 113 or “Remote Installation of the Data Protector Clients” on page 45.

Upgrade Procedure

To upgrade Data Protector A.05.00, A.05.10, or A.05.50 to Data Protector A.06.00, using `swinstall`, proceed as follows:

1. Log in as `root` and shut down the OmniBack II/Data Protector services on the Cell Manager by running the `/opt/omni/sbin/omnisv -stop` command.

Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no OmniBack II/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`” on page B-3 or/and “Installing an Installation Server on HP-UX Systems” on page B-7.

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 Solaris Systems Using `pkgadd`

To upgrade the Solaris 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 pushing the installation components from the Installation Server. For details refer to “Local Installation of UNIX and Linux Clients” on page 113 or “Remote Installation of the Data Protector Clients” on page 45.

Upgrade Procedure

To upgrade Data Protector A.05.00 or A.05.10 to Data Protector A.05.50, using `pkgadd`, proceed as follows:

1. Log in as `root` and shut down the OmniBack II/Data Protector services on the Cell Manager by running the `/opt/omni/sbin/omnisv -stop` command.

Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no OmniBack II/Data Protector services listed after executing the `ps -ef | grep omni` command.

2. Uninstall Data Protector using `pkgrm`.

The configuration files and the database are preserved during this procedure.

3. Run the `pkginfo` 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 UNIX installation DVD-ROM and use `pkgadd` to install the Cell Manager. For detailed steps, refer to “Installing the Cell Manager on Solaris Systems Using `pkgadd`” on page B-5.

If you are upgrading an Installation Server, insert and mount the UNIX installation DVD-ROM and install the Installation Server. For detailed steps, refer to “Installing an Installation Server on Solaris Systems Using `pkgadd`” on page B-8.

NOTE

If you upgraded the Cell Manager on Solaris 9, remotely install the Disk Agent on the Cell Manager after upgrade is complete, using an Installation Server. This will replace the generic Solaris Disk Agent with the Solaris 9 Disk Agent. Refer to “Remote Installation of the Data Protector Clients” on page 45 or to the `ob2install` man page.

Setting Up the TCP/IP Protocol on Windows Systems

IMPORTANT

Only the Microsoft implementation of the TCP/IP protocol is supported.

Data Protector uses the TCP/IP protocol for network communications and must be installed and configured on every client in the cell.

Entering a command using the Data Protector user interface establishes a connection to the Cell Manager through the TCP/IP protocol.

The TCP/IP protocol is a group of related protocols and utilities used for network communications. It consists of the TCP (Transmission Control Protocol) and the IP (Internet Protocol).

The TCP/IP software is installed on a hard disk, and each computer that uses this protocol must have the following addresses, usually assigned by the network administrator:

- The `IP address` for each network adapter card installed on the computer. This is a 32-bit number, usually displayed in the dotted quad or dotted decimal format.
- The `Subnet mask` for each network adapter card installed on the computer, which, combined with `IP address`, identifies the Network ID and the host ID. The `Subnet mask` is displayed in the same format as the `IP address`.
- The `Default Gateway address` is required for the default local gateway (IP router) to enable Internet access.

Prerequisites

Before installing the TCP/IP protocol on a Windows computers, you need to know the following:

- There are different configuration options, depending on the type of Windows software installed on your computer.

A Windows Server computer can be configured as a Dynamic Host Configuration Protocol (DHCP) server, a Windows Internet Name Service (WINS) server, or a Domain Name System (DNS) server, among others. See the Windows online Help for details.

- You can configure the TCP/IP protocol automatically using DHCP as long as you have the DHCP server installed on your network.

The TCP/IP protocol must be configured manually if there is no DHCP server available on your network or if you configure the TCP/IP protocol on the DHCP server computer. See the Windows online Help for details.

- If you configure the TCP/IP manually, make sure that you are logged on as a member of the Administrator group for the local computer. To prevent duplicate addresses, make sure that all values are obtained from your network administrator. In addition to the IP address, Subnet mask, and Default gateway mentioned above, you need to obtain:
 - ✓ The name of your DNS domain and the IP addresses of the DNS servers, if you will be using DNS services.
 - ✓ The IP addresses for WINS servers if there are WINS servers available on your network.

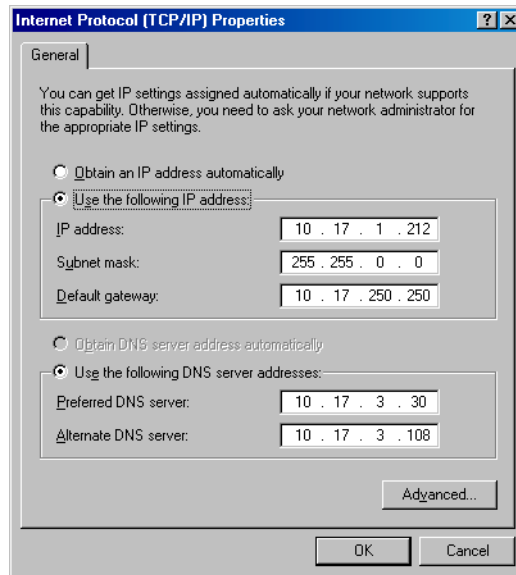
Installing and Configuring the TCP/IP Protocol on Windows

The TCP/IP protocol on Windows systems is installed during the installation of the operating system.

To check the current TCP/IP settings on Windows 2000 system, proceed as follows:

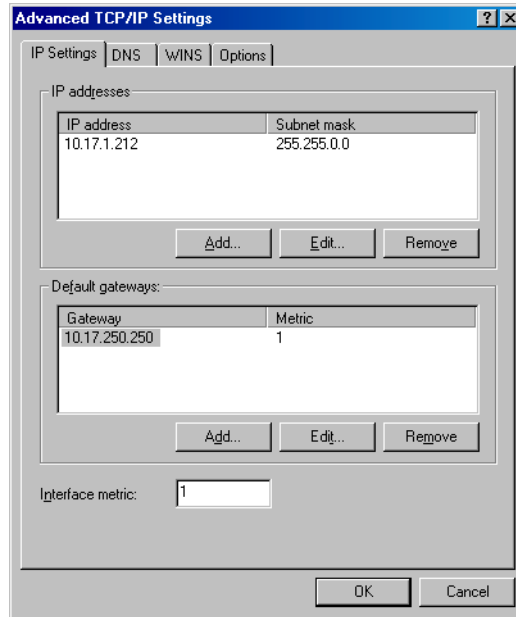
1. In the Windows Control Panel, double-click Network and Dial-up Connections, and then Local Area Connection.
2. Click Properties, select Internet Protocol (TCP/IP) and then click Properties. You can then edit IP settings.

Figure B-2 **The TCP/IP Properties Window on Windows**



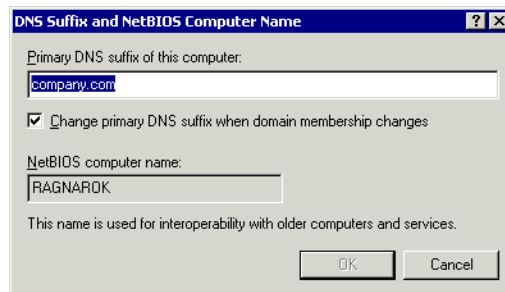
To edit advanced settings, click Advanced.

Figure B-3 **Advanced TCP/IP Settings on Windows**



DNS Suffix To configure the DNS suffix on a Windows 2000 system, right-click the My Computer icon on the desktop and then select Properties, Network Identification, Properties, More. The new DNS settings will take effect after the system is rebooted.

Figure B-4 **The DNS Suffix and NetBIOS Computer Name on Windows**



Checking the TCP/IP Setup

An important aspect of the TCP/IP configuration process is the setup of a hostname resolution mechanism.

- If using hosts files, located in the `<%SystemRoot%\system32\drivers\etc` folder, each system in the cell must be able to resolve the address of the Cell Manager, and of all systems with Media Agents and backup devices. The Cell Manager must be able to resolve the names of all systems in the cell.
- If using DNS, make sure the local DNS server is properly configured and specified in the IP settings for each system in the cell.

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig` utilities to verify that the TCP/IP setup is correct. If you have changed the TCP/IP settings, restart the computer first.

1. At the command line, type `ipconfig /all` to display 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 `kesukozi`, and the domain name was `campo.com`, you would enter: `ping kesukozi.campo.com`.

If this does not work, refer to “Installing and Configuring the TCP/IP Protocol on Windows” on page B-16, for steps required to access the TCP/IP Properties window. Here, verify that the domain name 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 that, 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 can not be installed properly.

Also note that the Windows computer name must be the same as the hostname. Otherwise, Data Protector setup reports a warning.

To check the hostname, refer to “Installing and Configuring the TCP/IP Protocol on Windows” on page B-16 for steps required to access the TCP/IP Properties window.

-
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 that by running the `omnicheck -dns` command from the `<Data_Protector_home>\bin` directory. Failed checks and the total number of failed checks are listed.

For detailed information on the `omnicheck` command, refer to the *HP OpenView Storage Data Protector Command Line Interface Reference*.

MS Proxy

If the MS Proxy is installed, the port number 5555 is occupied and the Data Protector services fail. Solve the problem as follows:

1. Create a file, named `wspcfg.ini`, in the `<Data_Protector_home>\bin` directory.
2. Add the following lines to the file:

```
[OmniInet]
Disable=1
```

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, refer to “Exporting Clients from a Cell” on page 184. After you have changed the hostname, import the clients back to the cell. For the procedure, refer to the “Importing Clients to a Cell” on page 177.

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

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 running:

```
/opt/omni/sbin/omnidbutil -change_cell_name [old_host]
```

On Windows

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
```

Appendix B

Changing the Cell Manager Name

2. Change the Cell Manager name in the following registry key:
 \\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\
 OpenView\OmniBack II\Site\CellServer

Changing the Default Port Number

The Data Protector `Inet` service (process), which starts other processes needed for backup and restore, should use the same port number on each system within the cell.

By default, Data Protector uses the port number 5555. Therefore, you should view the `/etc/services` file on UNIX systems or run the `netstat -a` command on Windows to verify that this particular port number is not used by another program. If the port number 5555 is already in use by another program, you must change this value to an unused port number.

UNIX

These are the steps to change the port number on a UNIX system:

1. Open the `/etc/services` file in an editor. By default, this file should contain the entry:

```
omni 5555/tcp # DATA-PROTECTOR
```

Change the 5555 entry to an unused port number.

2. Restart the `Inet` service by killing the process concerned using the `kill -HUP <inetd_pid>` command. To determine the process ID (`inetd_pid`), type `ps -ef`.

Windows

These are the steps to change the port number on a Windows systems:

1. From the command line, run `Regedit.exe` to open the Registry editor.
2. Expand `HKEY_LOCAL_MACHINE`, `Software`, `Hewlett-Packard`, `OpenView`, `OmniBack II`, and select `Common`.
3. Double-click `InetPort` to open the `Edit String` dialog box. In the `Value data` text box, enter an unused port number. The same must be done in the `Parameters` subfolder of the `Common` folder.
4. In the Windows Control Panel, go to `Administrative Tools`, `Services`, then select the `Data Protector Inet` service, and restart the service (click the `Restart` icon on the toolbar).

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 Port Number” on page B-23.

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/sbin/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
```

Using Tape and Robotics Drivers on Windows

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:

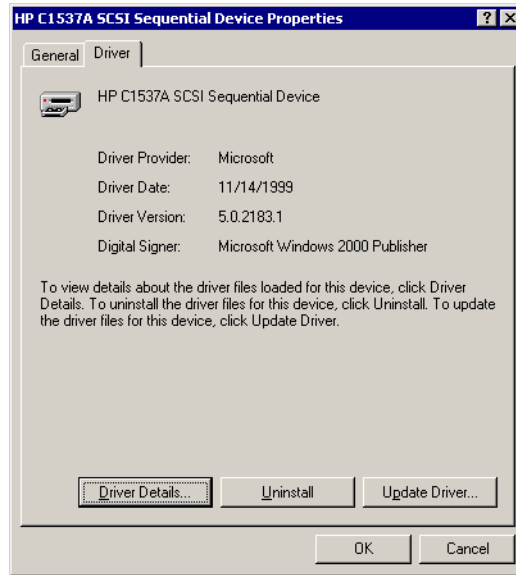
<http://www.microsoft.com/whdc/hcl/default.mspx>

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 Driver tab and click Update Driver. See Figure B-5 on page B-27. 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.

Figure B-5 **Driver Properties**



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`).

Refer to “Creating Device Files (SCSI Addresses) on Windows” on page B-29 for details.

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.

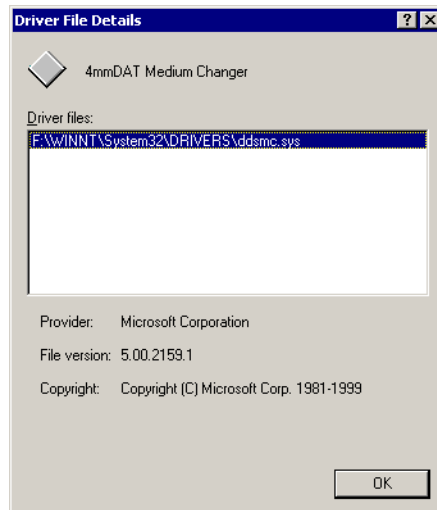
An HP 1557A tape library using the 4mm DDS tapes is used in the example below. Proceed as follows to disable the automatically loaded robotics driver (`ddsmc.sys`) on a Windows system:

1. In the Windows Control Panel, double-click Administrative Tools.

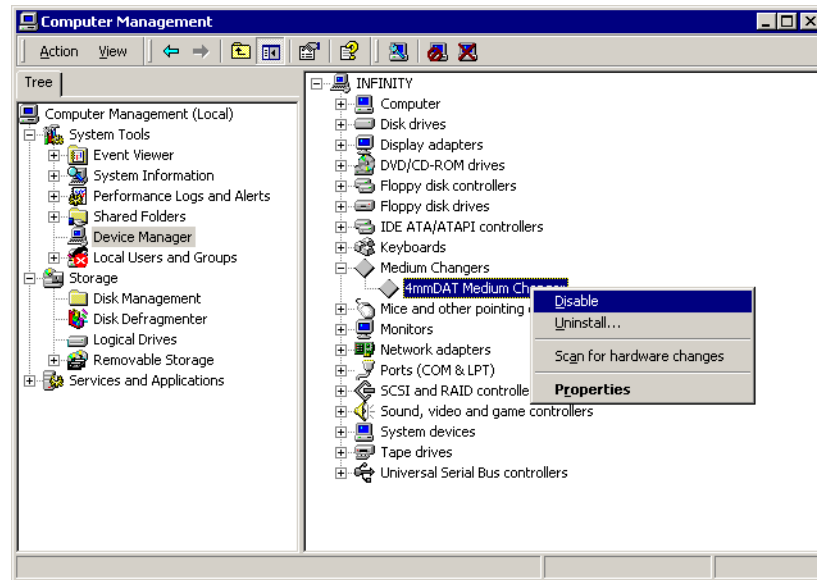
2. In the Administrative Tools window, double-click the Computer Management. Click Device Manager.
3. In the Results Area of the Device Manager window, expand Medium Changers.
4. To check which driver is currently loaded, right-click the 4mm DDS Medium Changer and then Properties.

Select Driver tab and click Driver details. In this case, the following window will display:

Figure B-6 Medium Changer Properties



To disable the native robotics driver, right-click the 4mm DDS Medium Changer and then select Disable.

Figure B-7 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

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.

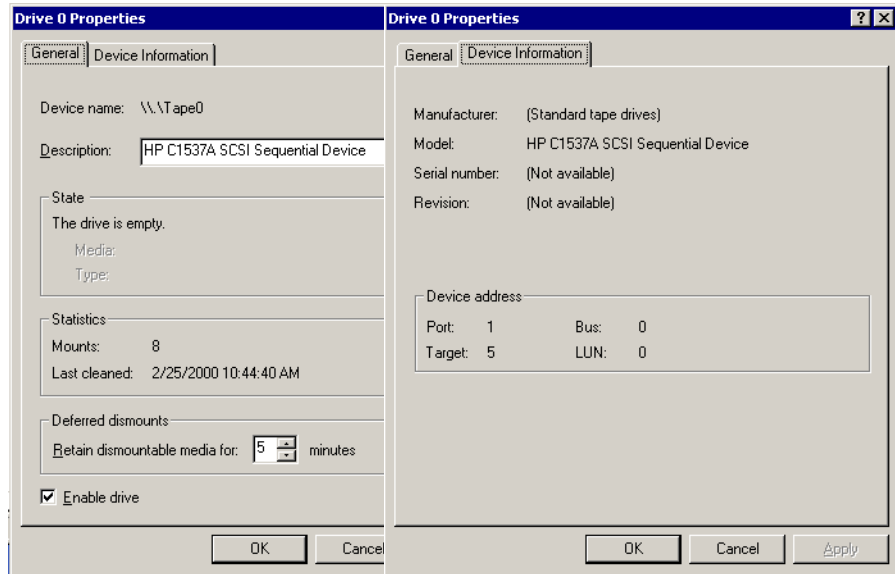
Windows Using the Native Tape Driver

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.

- 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 Figure B-8 on page B-30.

Figure B-8 Tape Drive Properties



The file name for the tape drive in Figure B-8 on page B-30 is created as follows:

Native Tape Driver Used Tape0 or Tape0:0:5:0

Native Tape Driver NOT Used scsi1:0:5:0

Magneto-Optical Devices

If you connect a magneto-optical device to a Windows system, a drive letter is assigned to the device after you reboot 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

On the 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 StorageWorks 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 B-9 SCSI Controlled Devices

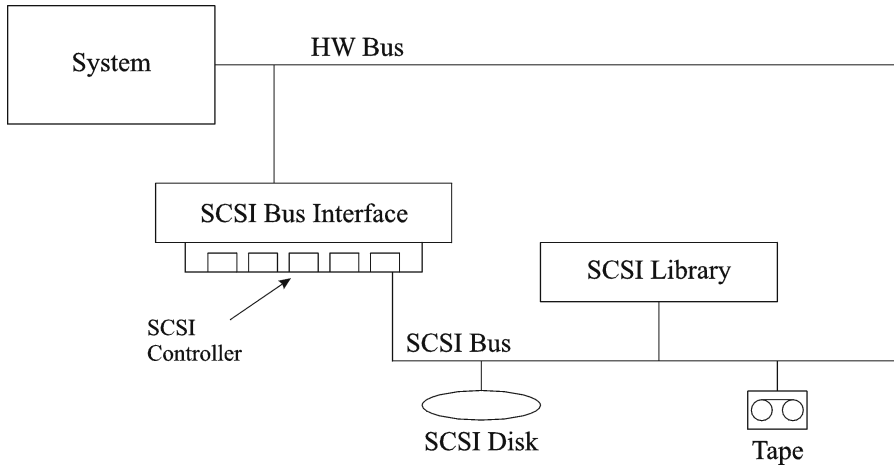
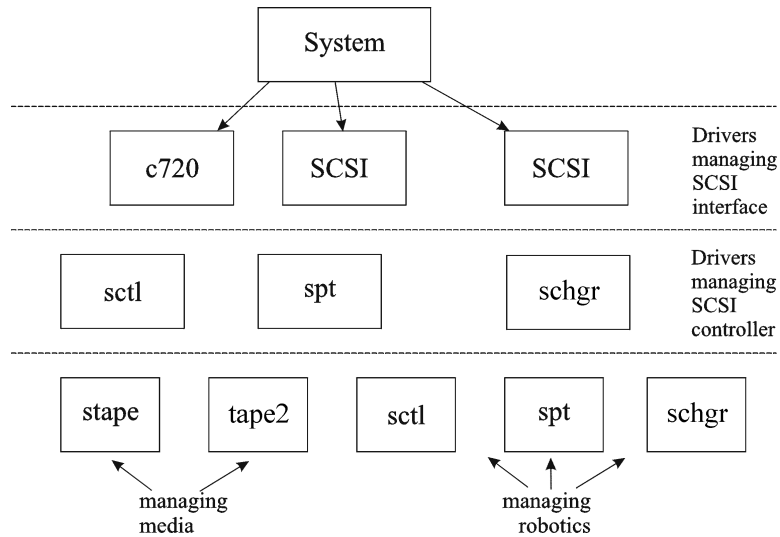


Figure B-10 Managing Devices



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” on page 64 in Chapter 2.

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 B-11 **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           unknown     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 Figure B-11 on page B-33, 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 B-12 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        scsil   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
lammux    0  56        lammux0 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 Figure B-12 on page B-34, 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 StorageWorks 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/sbin/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 Driver> system
```

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 StorageWorks 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. Reboot the system from the new kernel by entering the following command:

```
shutdown -r 0
```

9. Once you have rebooted the system, verify the changes you have made using the `/usr/sbin/ioscan -f` command.

Creating Device Files on HP-UX

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 StorageWorks 12000e library device connected to an HP-UX 11.00 system. The device file for the tape drive has already been created automatically after the reboot of the system, while the device file for the control device must be created manually.

In Figure B-12 on page B-34, you can see the output of the `ioscan -f` command on the selected HP-UX system.

Figure B-13

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 GD-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 StorageWorks 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 Figure B-13 on page B-36) 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:

```
0xIIITL00
```

I I -> 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 `sct1`, 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

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, 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 Figure B-14 on page B-40, there is the output of the `/usr/sbin/ioscan -f` command on an HP-UX 11.x system.

Figure B-14

The Output of `ioscan -f` 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        scsil1  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 Figure B-14 on page B-40 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 StorageWorks 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

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. Refer to the next section for instructions on updating the configuration files.

Updating the Device and Driver Configuration on a Solaris System

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 StorageWorks 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 StorageWorks 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. Reboot 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 reboot 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 a Windows System

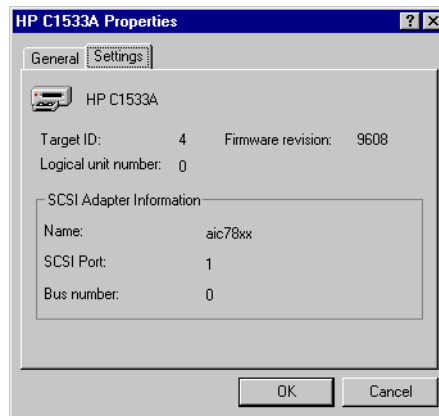
Follow the steps below to determine the unused SCSI Target IDs (SCSI Addresses) on a Windows system:

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 Figure B-15 on page B-48.

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 B-15

Device Settings



Setting SCSI IDs on an HP StorageWorks 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 StorageWorks 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, etc.

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, 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 of the Data Protector Clients” on page 45.
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” on page B-40. For Solaris systems, see “Finding the Unused SCSI Target IDs on Solaris” on page B-42. For a Windows system, see “Finding Unused SCSI Target IDs on a Windows System” on page B-48.

- ✓ 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” on page 65.

If you need to configure a SCSI Pass-Through Driver, see “SCSI Robotics Configuration on HP-UX” on page B-31.

- ✓ 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 a Solaris System” on page B-43. 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” on page B-26.

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” on page B-29.

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 StorageWorks 330fx Library” on page B-49.

Refer to

http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported devices.

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.

- ✓ On an HP-UX system, 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 device with the correct SCSI addresses.

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” on page B-36.

- ✓ On a Solaris system, 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.

Appendix B

Connecting Backup Devices

- ✓ On a Windows system, 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, run:

```
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.

- ✓ On an AIX system, use the `lsdev` utility

```
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. Refer to the online Help for detailed steps.

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. See the online Help index: “configuring, backup devices” for more information about further configuration tasks.

You must have a Media Agent installed on your system. See “Remote Installation of the Data Protector Clients” on page 45 for instructions how to do that.

The following sections describe how to connect an HP StorageWorks Standalone 24 Tape Device, HP StorageWorks 12000e Library, and HP StorageWorks DLT Library 28/48-Slot to an HP-UX and a Windows system.

Connecting an HP StorageWorks 24 Standalone Device

The StorageWorks 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 StorageWorks 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” on page 65.
2. Determine an unused SCSI address that can be used by the tape drive. See “Finding the Unused SCSI Addresses on HP-UX” on page B-40.
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 online 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 StorageWorks 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 a Windows System” on page B-48.

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 StorageWorks 24 Standalone device.

What's Next?

After properly connecting the device, see the online Help index: “configuring, backup devices” for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting an HP StorageWorks DAT Autoloader

Both the HP StorageWorks 12000e and the StorageWorks 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 StorageWorks 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” on page 65.
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” on page B-31.
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” on page B-40.

NOTE

The HP StorageWorks 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” on page 36.
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 online 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 StorageWorks 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 a Windows System” on page B-48.
3. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.

NOTE

The HP StorageWorks 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, run:

```
devbra -dev
```

In the output of the `devbra` command, you should find the newly connected tape drive and the robotics of the HP StorageWorks 12000e Library device.

What's Next?

After properly connecting the library device, see the online Help index: “configuring, backup devices” for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting an HP StorageWorks DLT Library 28/48-Slot

The HP StorageWorks 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 StorageWorks 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” on page 65.
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” on page B-31.
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” on page B-40.

NOTE

The HP StorageWorks 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” on page B-36.
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 StorageWorks DLT Library 28/48-Slot library device, see the online 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
```

Appendix B

Connecting Backup Devices

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 that 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 StorageWorks DLT Library 28/48-Slot library device, see the online 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 StorageWorks 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 a Windows System” on page 48.
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.

NOTE

The HP StorageWorks 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, run:

```
devbra -dev
```

In the output of the `devbra` command, you should find the newly connected tape drives and the robotics of the HP StorageWorks DLT Library 28/48-Slot library device.

What's Next?

After properly connecting the HP StorageWorks DLT Library 28/48-Slot library device, see the online 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 online 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 a Windows System” on page 48.
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.
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, run:

```
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 online 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

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 number> <compression>
```

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 StorageWorks 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.

Checking the General Media Agent Installation on Novell NetWare

- ✓ 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.

Checking the General Media Agent Installation on Novell NetWare

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 number> <flipping 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 number> <block 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
```

Checking the General Media Agent Installation on Novell NetWare

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
```

Installing Data Protector on Microsoft Cluster 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” on page 160.

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. Run the `omnisv -stop` command on the Cell Manager to stop the Data Protector services/processes:

```
<Data_Protector_home>\bin\omnisv -stop
```

2. Define a new system environment variable `OB2CLUSTERDISKTYPES` with Volume Manager Disk Group as a value, or set the `omnirc` variable on both cluster nodes as follows:

```
OB2CLUSTERDISKTYPES=Volume Manager Disk Group
```

If you want 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 variables, see the *HP OpenView Storage Data Protector Troubleshooting Guide*.

3. Run the `omnisv -start` command to start the services/processes:

```
<Data_Protector_home>\bin\omnisv -start
```

Configuration Files Path Changes in Data Protector A.06.00

The default paths of some configuration, log and (on UNIX) database files has been changed in Data Protector A.06.00. Some of the files are now split in the `server` and `client` directory.

Check the following tables for the changes and modify the paths, if necessary.

Configuration Files on UNIX

Client Configuration Files

The following table represents the files and directory that are moved from the `/etc/opt/omni` to the `/etc/opt/omni/client` directory during the upgrade.

Table B-1

The Content of the New `/etc/opt/omni/client` Directory

Old Path	Current Path
<code>/etc/opt/omni/cell/cell_server</code>	<code>/etc/opt/omni/client/cell_server</code>
<code>/etc/opt/omni/cell/omni_format</code>	<code>/etc/opt/omni/client/omni_format</code>
<code>/etc/opt/omni/cell/omni_info</code>	<code>/etc/opt/omni/client/omni_info</code>
<code>/etc/opt/omni/cell/allow_hosts</code>	<code>/etc/opt/omni/client/allow_hosts</code>
<code>/etc/opt/omni/cell/deny_hosts</code>	<code>/etc/opt/omni/client/deny_hosts</code>
<code>/etc/opt/omni/customize</code>	<code>/etc/opt/omni/client/customize</code>

Cell Manager Configuration and Log Files

The rest of the content of the `/etc/opt/omni` directory is moved to the `/etc/opt/omni/server` directory. For example, the `/etc/opt/omni/cell/cell_info` file is now located in the `/etc/opt/omni/server/cell` directory.

The following table represents the files and directories that are moved from the /var/opt/omni directory to the /var/opt/omni/server directory during the upgrade.

Table B-2

The Content of the New /var/opt/omni/server Directory

Old Path	Current Path
/var/opt/omni/db40	/var/opt/omni/server/db40
/var/opt/omni/sessions	/var/opt/omni/server/sessions
/var/opt/omni/log/<log_file>	/var/opt/omni/server/log/<log_file>

where <log_file> represents any of the following files: HealthCheck.log, Check_*.txt, Ob2Event*, lic.log, omnisv.log, media.log, sm.log, crsevents.log, security.log, purge.log, readascii.log, cleaning.log, upgrade.log, trace.log, and cluster.log.

All other directories (for example, /var/opt/omni/tmp, /var/opt/omni/windu, or /var/opt/omni/emc) and log files (for example, /var/opt/omni/log/debug.log) are not moved.

Configuration Files on Windows

Client Configuration Files

The following table represents the files and directories that are moved from the <Data_Protector_home>\Config directory to the <Data_Protector_home>\Config\client and the <Data_Protector_home>\tmp directories during the upgrade.

Table B-3

The Content of the New <Data_Protector_home>\Config\client Directory

Old Path	Current Path
<Data_Protector_home>\Config\cell\cell_server	<Data_Protector_home>\Config\client\cell_server
<Data_Protector_home>\Config\cell\omni_format	<Data_Protector_home>\Config\client\omni_format
<Data_Protector_home>\Config\cell\omni_info	<Data_Protector_home>\Config\client\omni_info
<Data_Protector_home>\Config\cell\allow_hosts	<Data_Protector_home>\Config\client\allow_hosts

Table B-3 **The Content of the New <Data_Protector_home>\Config\client Directory**

Old Path	Current Path
<Data_Protector_home>\Config\cell\deny_hosts	<Data_Protector_home>\Config\client\deny_hosts
<Data_Protector_home>\Config\EMC	<Data_Protector_home>\Config\client\EMC
<Data_Protector_home>\Config\tmp\EMC	<Data_Protector_home>\tmp\EMC

Cell Manager Configuration Files

The rest of the content of the <Data_Protector_home>\Config directory is moved to the <Data_Protector_home>\Config\Server directory. For example, the <Data_Protector_home>\Config\cell\cell_info file is now located in the <Data_Protector_home>\Config\Server\cell directory.

Log Files

The following files are moved from the <Data_Protector_home>\log directory to the <Data_Protector_home>\log\server directory: HealthCheck.log, Check_*.txt, Ob2Event*, lic.log, omniv.log, media.log, sm.log, crsevents.log, security.log, purge.log, readascii.log, cleaning.log, upgrade.log, trace.log, and cluster.log.

All other log files (for example, <Data_Protector_home>\log\debug.log) are not moved.

Command Line Changes After Upgrading to Data Protector A.06.00

The commands listed in this chapter have been changed or provide extended functionality in terms of new options in Data Protector A.06.00. Check and modify the scripts that use the old commands. Refer to the corresponding man pages for usage synopses.

Depending on the version from which you upgraded your Cell Manager, refer to the corresponding table:

- After upgrading from Data Protector A.05.00, see Table B-4 on page B-74.
- After upgrading from Data Protector A.05.10, see Table B-5 on page B-81.
- After upgrading from Data Protector A.05.50, see Table B-6 on page B-87.

Table B-4

Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
ob2install	-sapdb	NEW SOFTWARE COMPONENTS
	-evaa	
	-smisa	
	-db2	
	-acs	SOFTWARE COMPONENTS OBSOLETE
	-das	
omniamo		NEW COMMAND

Table B-4 Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnib	-db2_list	NEW INTEGRATIONS
	-msvssw_list	
	-sapdb_list	
	-mbx_list	
	-share_info	NEW OPTIONS
	-mirror	
	-enh_incr	
omnicc	-check_licenses	NEW OPTIONS
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omnicheck		NEW COMMAND
omniclus	-applid	CHANGED OPTION

Table B-4

Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnicreatedl	-snapshot	NEW OPTIONS FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-eva	
	-smis	
	-instant_recovery	
	-snapshots <number>	
	-snapshot_type standard	
	-snapshot_type vsnap	
	-snapshot_type clone	
	-snapshot_policy strict	
	-snapshot_policy loose	
	-wait_cloncopy <number>	
omnidb	-db2	NEW INTEGRATIONS
	-vss	
	-sapdb	
	-mbx	
	-copyid	
	-listcopies	
omnidbeva		NEW COMMAND
omnidbsmis		NEW COMMAND
omnidbupgrade		NEW COMMAND

Table B-4 Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnidbutil	-extendtblspace	NEW OPTION
	-readdb	CHANGED OPTION
omnidbvss		NEW COMMAND
omnidlc		NEW COMMAND
omniinstlic		NEW COMMAND
omniiso		NEW COMMAND
omnimcopy	-permanent -until	NEW OPTION
omnimmm	- [no_]free_pool	CHANGED OPTION
	-create_free_pool	NEW OPTION
omnimigrate.pl		NEW COMMAND
omniminit	- [no]barcode_as_label	NEW OPTION
omniobjcopy		NEW COMMAND
omniobjconsolidate		NEW COMMAND

Table B-4

Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnir	-db2	NEW INTEGRATIONS
	-sapdb	
	-newinstance	NEW OPTIONS FOR SAP DB
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	
	-force_prp_replica	NEW OPTION FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instance <SourceInstanceName>	NEW OPTIONS FOR MS SQL
	-destinstance <DestinationInstanceName>	
	-asbase <NewDBName>	
	-file <LogicalFileName>	

Table B-4 Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnir	-instance	NEW OPTIONS FOR IBM DB2 UDB
	-logfile	
	-newdbname	
	-offline	
	-rollforward	
	-tsname	
	-msvssw	NEW INTEGRATIONS
	-mbx	
	-share_info	NEW OPTION
	-oracle	NEW ORACLE AND SAP R/3 INSTANT RECOVERY OPTIONS
	-sap	
	-user	
	-group	
	-recover	
	-restore <tree>	
	-open	
	-resetlogs	
	-paralleism	NEW VSS INSTANT RECOVERY OPTIONS
	-restore	
	-session	
-vss	NEW OPTION	
-copyid		

Table B-4

Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnirpt	media_list_extended	NEW REPORT
	-smtp	NEW OPTION
omniresolve		NEW COMMAND
omnisetup.sh	-CM	NEW OPTIONS
	-IS	
	-autopass	
	db2	NEW SOFTWARE COMPONENTS
	evaa	
	smisa	
	sapdb	
	acs	SOFTWARE COMPONENTS OBSOLETE
das		
omnisrdupdate	-asr	NEW OPTIONS
	-location	
omniusers		NEW COMMAND
sanconf	-[no_]multipath	NEW OPTIONS
	-remove_hosts	
	-sanstableaddressing	
uma	-scsiType	replaced by the -interface option
	-interface	replaced the -scsiType option
upgrade_cfg_from_evaa		NEW COMMAND

Table B-5 Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
ob2install	-sapdb	NEW SOFTWARE COMPONENTS
	-smisa	
	-acs	SOFTWARE COMPONENTS OBSOLETE
	-das	
omnib	-sapdb_list	NEW INTEGRATION
	-vss_list	OPTION OBSOLETE
	-msvssw_list	NEW OPTIONS
	-share_info	
	-mirror	
	-enh_incr	
omnicc	-check_licenses	NEW OPTIONS
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omniclus	-applid	CHANGED OPTION

Table B-5

Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
omnicreated1	-smis	NEW OPTIONS FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instant_recovery	
	-snapshots <number>	
	-snapshot_type clone	
	-wait_clonecopy <number>	
omnidb	-sapdb	NEW INTEGRATION
	-copyid	NEW OPTIONS
	-listcopies	

Table B-5 Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
omnidbeva	-hwrescan [<i><EVA_name></i>]	NEW OPTIONS
	-dgrules	
	-list	
	-show	
	-sync	
	-delete	
	-put <i><filename></i>	
	-get <i><filename></i>	
	-check <i><EVA_name></i> <i><DG_name></i>	
	-init	
	-session [-ir]	
	-snapshot [-ir]	
	-purge	
	-session <i><sessionID></i>	
	-datalist <i><DatalistName></i>	
-preview		
-snapshot <i><VirtualDiskID></i> <i><EVA_ID></i>		
omnidbsmis		NEW COMMAND
omidbupgrade		NEW COMMAND
omnidbvss		NEW COMMAND

Table B-5

Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
omnidbutil	-extendtblspace	NEW OPTION
	-readdb	CHANGED OPTION
omnidlc		NEW COMMAND
omnimigrate.pl		NEW COMMAND
omniminit	- [no]barcode_as_label	NEW OPTION
omnimmm	- [no_]free_pool	CHANGED OPTION
	-create_free_pool	NEW OPTION
omniinstlic		NEW COMMAND
omniiso		NEW COMMAND
omniobjcopy		NEW COMMAND
omniobjconsolidate		NEW COMMAND

Table B-5

Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
omnir	-sapdb	NEW INTEGRATION
	-newinstance	NEW OPTIONS FOR SAP DB
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	
	-force_prp_replica	NEW OPTION FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instance <SourceInstanceName>	NEW OPTIONS FOR MS SQL
	-destinstance <DestinationInstanceName>	
	-asbase <NewDBName>	
	-file <LogicalFileName>	

Table B-5

Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status
omnir	-oracle	NEW ORACLE AND SAP R/3 INSTANT RECOVERY OPTIONS
	-sap	
	-user	
	-group	
	-recover	
	-open	
	-resetlogs	
	-paralleism	NEW OPTIONS FOR MS EXCHANGE SINGLE MAILBOX
	-public	
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	NEW VSS INSTANT RECOVERY OPTIONS
	-exclude	
-restore		
-session	NEW OPTION	
-vss		
-copyid	NEW OPTION	
omnirpt	-smtp	NEW OPTION
omniresolve		NEW COMMAND

Table B-5 Upgrade From Data Protector A.05.10

Command	Subcommand/Option	Status	
omnisetup.sh	-CM	NEW OPTIONS	
	-IS		
	-autopass		
	smisa	sapdb	NEW SOFTWARE COMPONENTS
			SOFTWARE COMPONENTS OBSOLETE
	acs	SOFTWARE COMPONENTS OBSOLETE	
	das		
omniusers		NEW COMMAND	
sanconf	- [no_]multipath	NEW OPTIONS	
	-remove_hosts		
	-sanstableaddressing		
upgrade_cfg_fr om_evaa		NEW COMMAND	

Table B-6 Upgrade From Data Protector A.05.50

Command	Subcommand/Option	Status
omnib	-enh_incr	NEW OPTION
omnidbsmis		NEW COMMAND

Table B-6

Upgrade From Data Protector A.05.50

Command	Subcommand/Option	Status
omnidbutil	-extendtblspace	NEW OPTION
	-readdb	CHANGED OPTION
omnidbvss		NEW COMMAND
omnidlc	-debug_loc	NEW OPTION
omnimigrate.pl		UPDATED COMMAND
omnimmm	-[no_]free_pool	CHANGED OPTION
	-create_free_pool	NEW OPTION
omniobjconsolidate		NEW COMMAND
omnir	-public	NEW OPTIONS FOR MS EXCHANGE SINGLE MAILBOX
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-restore	NEW VSS INSTANT RECOVERY OPTIONS
	-session	
-vss		
omnirpt	-smtp	NEW OPTION

| **C** **Appendix C**

Using CD-ROMs As the Installation Media

Data Protector A.06.00 is alternatively also available on installation CD-ROMs. All system requirements, pre-installation and post-installation tasks are the same as with the installation from the DVD-ROM media. However, because the packages for one platform, such as HP-UX or Solaris, do not fit on only one CD-ROM, additional steps are required during the installation procedure.

This appendix lists the product structure on the installation CD-ROMs, the differences in the installation procedures and additional limitations that apply to the installation from the CD-ROMs

Data Protector Installation CD-ROMs

Data Protector supports various operating systems on several processor architectures. As a consequence, 8 CD-ROMs are required to cover all platforms. For details which components are found on which CD-ROM, refer to “Data Protector CD-ROM List” on page 2.

The way a particular CD-ROM for the HP-UX or Solaris platform is referenced in the documentation depends on the Data Protector component which is installed from it, that is: as Cell Manager installation CD-ROM for the CD-ROM that is used for installing the Cell Manager, and Installation Server installation CD-ROM for the CD-ROM that holds the Installation Server and the clients.

Table C-1 **Data Protector CD-ROM List**

CD Num.	CD-ROM Title	Contents
1	HP OpenView Storage Data Protector for HP-UX 11.23 IA-64 Management System <i>Referenced as Data Protector HP-UX Cell Manager installation CD-ROM.</i>	<ul style="list-style-type: none">• Cell Manager for HP-UX 11.23 (IA-64 architecture)• All English manuals in PDF format (in the DOCS directory)• OpenView Integration Packages for HP-UX• NAS8000 package• Autopass for HP-UX• Omnisetup.sh installation script

Table C-1 Data Protector CD-ROM List

CD Num.	CD-ROM Title	Contents
2	HP OpenView Storage Data Protector for HP-UX 11.23 IA-64 Installation Server <i>Referenced as Data Protector HP-UX Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Installation Server for HP-UX 11.23 (IA-64 architecture) including all UNIX clients • <code>Omnisetup.sh</code> installation script
3	HP OpenView Storage Data Protector for HP-UX 11.x PA-RISC Management System <i>Referenced as HP-UX Cell Manager installation CD-ROM.</i>	<ul style="list-style-type: none"> • Cell Manager for HP-UX 11.x (PA-RISC architecture) • DOCS directory containing all English manuals in PDF format • OpenView Integration Packages for HP-UX • NAS8000 package • Autopass for HP-UX • <code>Omnisetup.sh</code> installation script
4	HP OpenView Storage Data Protector for HP-UX 11.x PA-RISC installation server <i>Referenced as Data Protector HP-UX Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Installation Server for HP-UX 11.x (PA-RISC architecture) including all UNIX clients • <code>Omnisetup.sh</code> installation script
5	HP OpenView Storage Data Protector for Solaris 7, 8 & 9 Management System <i>Referenced as Data Protector Solaris Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Cell Manager for Solaris 7/8/9 • All English manuals in PDF format (in the DOCS directory) • OpenView Integration Packages for Solaris • NAS8000 package • Autopass for Solaris • <code>Omnisetup.sh</code> installation script

Table C-1 Data Protector CD-ROM List

CD Num.	CD-ROM Title	Contents
6	HP OpenView Storage Data Protector for Solaris 7, 8 & 9 Installation Server <i>Referenced as Data Protector Solaris Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Installation Server for Solaris 7/8/9 including all UNIX clients^a • Omnisetup.sh installation script
5	HP OpenView Storage Data Protector for Linux management system <i>Referenced as Data Protector Linux Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Cell Manager for Linux • All English manuals in PDF format (in the DOCS directory) • Autopass for Linux • Omnisetup.sh installation script
6	HP OpenView Storage Data Protector for Linux Installation Server <i>Referenced as Data Protector Solaris Installation Server installation CD-ROM.</i>	<ul style="list-style-type: none"> • Installation Server for Linux including all UNIX clients^a • Omnisetup.sh installation script
7	HP OpenView Storage Data Protector for Windows Management System <i>Referenced as Data Protector Windows installation CD-ROM.</i>	<ul style="list-style-type: none"> • Cell Manager for Windows • Installation Server for Windows • Novell Netware clients • OpenVMS clients • MPE clients • All English manuals in PDF format (in the Docs directory) • Open File Manager installation package • Product Demo for Windows platforms • Product information

Table C-1 Data Protector CD-ROM List

CD Num.	CD-ROM Title	Contents
7	HP OpenView Storage Data Protector for Windows for Windows x86_64 Management System <i>Referenced as Data Protector Windows x86_64 installation CD-ROM.</i>	<ul style="list-style-type: none"> • Cell Manager for Windows • Installation Server for Windows • All English manuals in PDF format (in the Docs directory) • Open File Manager installation package • Product Demo for Windows platforms • Product information
8	HP OpenView Storage Data Protector - Media Operations for Windows	<ul style="list-style-type: none"> • Installation package for Media Operations • Documentation for Media Operations

- a. Local installation of UNIX clients from the Solaris or Linux Installation Server installation CD-ROM is not possible. Instead, one of the HP-UX Installation Server CD-ROMs must be used.

Additional Steps and Tasks When Installing Data Protector From CD-ROMs

The procedure for installing Data Protector from the CD-ROM is similar to the procedure for installing from DVD-ROM. On UNIX platforms, the installation packages are split to 3 CD-ROMs (one for the Cell Manager and two for the Installation Server).

Installing the UNIX Cell Manager From CD-ROMs

TBD

TIP

If you install the Cell Manager and Installation Server on the same system, you can perform the installation in one step by copying the DP_DEPOT directory to the disk and then running `omnisetup.sh -CM -IS1 -IS2`.

For a description of the `omnisetup.sh` command, refer to the `README` file located in the `<Mount_point>/LOCAL_INSTALL` directory on the CD-ROM or to the *HP OpenView Storage Data Protector Command Line Interface Reference* located in the `<Mount_point>/DOCS/C/MAN` directory on the CD-ROM.

Installing the UNIX Installation Server From CD-ROMs

The Installation Server for UNIX is packed on two installation CDs. Therefore, the installation procedure requires two steps instead of one:

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

1. Insert and mount the appropriate Installation Server installation CD-ROM to a mount point.

For example:

```
mkdir /cddrom
mount /dev/dsk/c0t0d0 /dvdrom
```

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

- To copy the `DP_DEPOT`, and `LOCAL_INSTALL` directories, where the installation files are stored, to your local disk, run:

```
mkdir <directory>
cp -r /cdrom/<platform_dir>/DP_DEPOT <directory>
cp -r /cdrom/<platform_dir>/LOCAL_INSTALL <directory>
```

Mount the second CD-ROM and copy all the files from the `LOCAL_INSTALL` directory to the installation directory as well.

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

```
cp -r /cddrom <cd_image_dir>
```

2. Run the `omnisetup.sh` command.

To run this command from the CD-ROM, type:

```
cd /cddrom/LOCAL_INSTALL
./omnisetup.sh -IS1
```

To start the installation from disk:

- If you have copied the DP_DEPOT directory from both CD-ROMs to your local disk as *<directory>/DP_DEPOT*, go to the directory where the *omnisetup.sh* command is stored, and run:

```
./omnisetup.sh -source <directory> -IS1 -IS2
```

- If you have copied the whole CD-ROM to *<cd_image_dir>*, run the *omnisetup.sh* command with the *-CM* parameter:

```
cd <dvd_image_dir>/LOCAL_INSTALL  
./omnisetup.sh -IS1
```

3. If you are installing from the mounted CD-ROM or the CD-ROM image, repeat the steps 1 and 2 with the second Installation Server installation CD-ROM, but use the *omnisetup.sh -IS2* parameter instead of *-IS1*.

Installing UNIX Clients From CD-ROMs

Local installation of UNIX packages is possible only from the HP-UX Installation Server installation CD-ROM. This includes all UNIX clients. This means that you need to install the Solaris client from the HP-UX Installation Server installation CD-ROM and not from the Solaris Installation Server installation CD-ROM.

Appendix C
Using CD-ROMs As the Installation Media

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.

AML (*EMASS/GRAU specific term*)

Automated Mixed-Media library.

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.

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 one (or more) archived log destination(s). This copy is the Archived Redo Log. The presence or absence of an Archived Redo Log is determined by the mode that the database is using:

- ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered from an instance and disk failure. The “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.

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.

ASR Set

A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk

Glossary

(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 `<Data_Protector_home>\Config\Server\dr\asr` on a Windows Cell Manager or in `/etc/opt/omni/server/dr/asr/` on a UNIX Cell Manager) as well as on the backup medium. The ASR archive file is extracted to three diskettes for 32-bit Windows systems or four diskettes for 64-bit Windows systems after a disaster occurs. You need these diskettes to perform ASR.

autochanger

See **library**

autoloader

See **library**

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

This relates to a situation where full and incremental backups are performed. Based on the level of the incremental backups used (`Incr`, `Incr 1`, `Incr 2`, and so on), simple or rather complex dependencies of incrementals to previous incrementals can exist. The backup chain are all backups, starting from the full backup plus all the dependent incrementals up to the desired point in time.

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.

Glossary

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 entity or a disk image (rawdisk).

A backup object is defined by:

- **Client name:** hostname of the Data Protector client where the backup object resides.
- **Mount point:** the access point in a directory structure (drive on Windows and mount point on UNIX) on the client where the backup object is located.
- **Description:** uniquely defines backup objects with identical client name and mount point.
- **Type:** backup object type (for example filesystem or Oracle).

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 (full or incremental). The result of a backup session is a set of media, which was written to, also called the backup or media set.

*See also **incremental backup** and **full 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, 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

Glossary

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 target volumes of one or multiple application systems. The backup system is typically connected to a backup device to perform the backup of the data in a 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 (*HP StorageWorks Disk Array XP specific term*)

The Business Copy XP allows to maintain internal copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data backup or data duplication. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system for various purposes, such as backup and development. For backup purposes, P-VOLs should be connected to the application system, and one of the S-VOL mirror sets to the backup system. *See also* **HP StorageWorks Disk Array XP LDEV, CA, Main Control Unit, application system, and backup system.**

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.**

BC VA (*HP StorageWorks Virtual Array specific term*)

Business Copy VA allows you to

Glossary

maintain internal copies of HP StorageWorks Virtual Array LUNs for data backup or data duplication within the same virtual array. The copies (child or Business Copy LUNs) can be used for various purposes, such as backup, data analysis or development. When used for backup purposes, the original (parent) LUNs are connected to the application system and the Business Copy (child) LUNs are connected to the backup system.

See also **HP StorageWorks Virtual Array LUN, application system, and backup system.**

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 splittable 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 online 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 **SAPDBA, 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 **SAPDBA, 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

Glossary

- 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 **SAPDBA**, **BRBACKUP** and **BRARCHIVE**.

BSM

The Data Protector Backup Session Manager controls the backup session. This process always runs on the Cell Manager system.

CA (*HP StorageWorks Disk Array XP specific term*)

Continuous Access XP allows you to create and maintain remote copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data duplication, backup, and disaster recovery. CA operations involve the main (primary) disk arrays and the remote (secondary) disk arrays. The main disk arrays contain the CA primary volumes (P-VOLs), which contain the original data and are connected to the application system. The remote disk arrays contain the CA secondary volumes (S-VOLs) connected to the backup system.

See also **BC** (*HP StorageWorks Disk*

Array XP specific term), **Main Control Unit** and **HP StorageWorks Disk Array XP LDEV**.

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 backups, object copies, restores, media management sessions, and backed up data. 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.

Glossary

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. 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.

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 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 filesystems mounted on a client. Filesystems mounted on the client after the backup specification was created are not automatically detected.

client backup with disk discovery

A backup of all filesystems mounted on a client. When the backup starts, Data Protector discovers the disks on the clients. Client backup with disk

Glossary

discovery simplifies backup configuration and improves backup coverage of systems that often mount or dismount disks.

client or client system

Any system configured with any Data Protector functionality and configured in a cell.

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 ...).

CMD Script for OnLine Server

(Informix specific term)

Windows CMD script that is created in INFORMIXDIR when Informix OnLine Server is configured. The CMD script is a set of system commands that export environment variables for OnLine 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 MoM Manager. A reliable network connection between the MoM cell and the other Data Protector cells is highly recommended
See also MoM.

COM+ Registration Database

(Windows specific term)

The COM+ Registration Database and the Windows Registry store COM+ application attributes, class attributes, and computer-level attributes. This guarantees consistency among these attributes and provides common operation on top of these attributes.

command-line interface

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.

Command View (CV) EVA

(HP StorageWorks EVA specific term)

The user interface that allows you to configure, manage, and monitor your HP StorageWorks EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, creating snapclones and snapshots of virtual disks. The Command View EVA software runs on the HP OpenView

Glossary

Storage Management Appliance, and is accessed by a Web browser.

See also **HP StorageWorks EVA Agent (legacy)** and **HP StorageWorks EVA SMI-S Agent**.

concurrency

See **Disk Agent concurrency**.

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.

CRS

The Cell Request Server process (service) runs on the Data Protector Cell Manager. It starts and controls the backup and restore sessions. The service is started as soon as Data Protector is installed on the Cell Manager. CRS runs under the account root on UNIX systems, and under any Windows account. By default, it runs under the account of the user, specified at installation time.

CSM

The Data Protector Copy Session Manager process controls the object copy session and runs on the Cell Manager system.

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 Protector Event Log

A central repository of all Data Protector related notifications. By default, all notifications are sent to the Event Log. The Event Log is accessible only to Data Protector users in the Admin group and to Data Protector users who are granted the Reporting and notifications user rights. You can view or delete all events in the Event Log.

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

Glossary

membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

data stream

Sequence of data transferred over the communication channel.

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, the 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.

Dboject (*Informix specific term*)

An Informix physical database object. It can be a blob space, db space, or logical-log file.

DC directory

The Detail Catalog (DC) directory consists of 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 in the `<Data_Protector_home>\db40` directory on a Windows Cell Manager and in the `/var/opt/omni/server/db40` directory on a UNIX Cell Manager. You can create more DC directories and locate them as appropriate to you. Up to 10 DC directories are supported per cell. The default maximum size of a DC directory is 4 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.

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

Glossary

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 configuration of IP addresses and related information.

differential backup

An incremental backup (incr) based on any previous Data Protector backup (full or any incremental), which must still be protected.

See **incremental backup**.

differential backup (*MS SQL 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.

direct backup

A SAN-based backup solution in which data movement directly from disk to tape (or to other secondary storage) is facilitated by the SCSI Extended Copy (Xcopy) command. Direct backup lessens the backup I/O load on systems in a SAN environment. The data movement is facilitated directly from disk to tape (or to other secondary storage) by the SCSI Extended Copy (XCOPY) command. The command is provided by any element of the infrastructure including bridges, switches, tape libraries, and disk subsystems.

See also **XCOPY engine**.

Glossary

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.

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.

Disk Agent concurrency

The number of Disk Agents that are allowed to send data to one Media Agent concurrently.

disk discovery

The detection of disks during client backup with disk discovery. During this backup, Data Protector discovers (detects) the disks that are present on the client — even though they might not have been present on the system when the backup was configured — and backs

them up. This is particularly useful in dynamic environments, where configurations change rapidly. After the disks are expanded, each inherits all options from its master client object. Even if pre- and post-exec commands are specified once, they are started many times, once per each object.

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 (rawdisk) backup

A high-speed backup where Data Protector backs up files as bitmap images. A disk image (rawdisk) 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

Glossary

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 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

A disaster recovery operating system is an operating system environment in which disaster recovery runs. It provides Data Protector a basic runtime environment (disk, network, tape, and filesystem access). The OS has to be installed and configured before the Data Protector disaster recovery can be performed. DR OS not only hosts the Data Protector disaster recovery process but is also 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.

Glossary

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.

dynamic client

See **client backup with disk discovery**.

EMC Symmetrix Agent (SYMA)

(EMC Symmetrix specific term)

See **Symmetrix Agent (SYMA)**

emergency boot file *(Informix specific term)*

An Informix configuration file that resides in the <INFORMIXDIR>\etc directory (on HP-UX) or <INFORMIXDIR>/etc directory (on Windows) and is called ixbar.<server_id>, where <INFORMIXDIR> is the OnLine 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.

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 Logs

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.

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.

failover

Transferring of the most important cluster data, called group (on Windows)

Glossary

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.

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 bidirectional 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 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.

Glossary

first level mirror (*HP StorageWorks Disk Array XP specific term*)

HP StorageWorks Disk Array XP allows up to three mirror copies of a Primary Volume and each of these copies can have additional two copies. The three mirror copies are called first level mirrors.

See also **Primary Volume**, and **MU numbers**.

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 (media 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 backup in which all selected objects are backed up, even if there are no changes from the previous backup.

See also **incremental ZDB**.

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 in the /etc/opt/omni/server/options directory on HP-UX and Solaris systems and in the <Data_Protector_home>\Config\Server\Options directory on Windows systems.

Glossary

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 cross-platform (HP-UX, Solaris, and Windows) graphical user interface, provided by Data Protector for easy access to all configuration, administration, and operation tasks.

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: `/etc/opt/omni/server/Holidays` on the UNIX Cell Manager and `<Data_Protector_home>\Config\Server\holidays` on the Windows Cell Manager.

host backup

See **client backup with disk discovery**.

hosting system

A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.

HP ITO

See **OVO**.

HP OpC

See **OVO**.

HP OpenView SMART Plug-In (SPI)

A fully integrated, out-of-the-box solution which "plugs into" HP OpenView Operations, extending the managed domain. Through the Data Protector integration, which is implemented as an HP OpenView SMART Plug-In, a user can have an

Glossary

arbitrary number of Data Protector Cell Managers monitored as an extension to HP OpenView Operations (OVO).

HP OVO

See **OVO**.

HP StorageWorks Disk Array XP LDEV

A logical partition of a physical disk within an HP StorageWorks Disk Array XP. LDEVs are entities that can be replicated in the Continuous Access XP (CA) and Business Copy XP (BC) configurations, or can be used as standalone entities.

See also **BC** (*HP StorageWorks Disk Array XP specific term*), **CA** (*HP StorageWorks Disk Array XP specific term*), and **replica**.

HP StorageWorks EVA Agent (legacy)

A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array integration operating on HP StorageWorks EVA with Command View (CV) EVA software v3.1 or lower, and the EVA VCS firmware v3.01x or lower.

See also **Command View (CV) EVA** and **HP StorageWorks EVA SMI-S Agent**.

HP StorageWorks EVA SMI-S Agent

A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array integration operating on HP StorageWorks EVA with Command View (CV) EVA software starting with v3.2. With the EVA SMI-S Agent, the control over the array is established through HP StorageWorks SMI-S EVA provider, which directs communication between incoming requests and CV EVA.

See also **Command View (CV) EVA**, **HP StorageWorks SMI-S EVA provider**, and **HP StorageWorks EVA Agent (legacy)**.

HP StorageWorks SMI-S EVA provider

An interface used for controlling HP StorageWorks Enterprise Virtual Array. SMI-S EVA provider runs as a separate service on the HP OpenView Storage Management Appliance system and acts as a gateway between incoming requests and Command View EVA. With the Data Protector HP StorageWorks EVA integration, SMI-S EVA provider accepts standardized requests from the EVA SMI-S Agent, communicates with Command View EVA for information or method invocation, and returns standardized responses.

See also **HP StorageWorks EVA SMI-**

Glossary

S Agent and Command View (CV) EVA.

HP StorageWorks Virtual Array LUN

A logical partition of a physical disk within an HP StorageWorks Virtual Array. LUNs are entities that can be replicated in the HP StorageWorks Business Copy VA configuration, or can be used as standalone entities.
See also **BC VA** and **replica**.

HP VPO
See **OVO**.

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 is an embedded database located on the Cell Manager that keeps information regarding which data is backed up, on which media it is backed up, how backup and restore sessions are run, and which devices and libraries are configured.

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 backup

A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, allowing selective backup of only files that have changed since the last incremental backup.
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.

incremental1 mailbox backup

An incremental1 mailbox backup backs up all the changes made to the mailbox after the last full backup.

Glossary

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 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 ZDB to tape or ZDB to disk+tape session in which only changes from the last full or incremental protected backup are streamed to tape.

See also **full ZDB**.

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

Glossary

that are shared among several users.
See also **Key Management Service** and **Site Replication Service**.

initializing

See **formatting**.

Installation Server

A computer system that holds a repository of the Data Protector software 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 sessions, 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/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**.

integrated security (*MS SQL specific term*)

Integrated security allows the Microsoft SQL Server to use Windows authentication mechanisms to validate Microsoft SQL Server logins for all connections. Using integrated security means that users have one password for both Windows and Microsoft SQL Server. Integrated security should be used in environments where all clients support trusted connections. Connections validated by Windows Server and accepted by Microsoft SQL Server are referred to as trusted connections. Only trusted connections are allowed.

integration object

A backup object of a Data Protector integration, such as Oracle or SAP DB.

Internet Information Server (IIS)

(*Windows specific term*)

Microsoft Internet Information Server 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).

IP address

Internet Protocol address is a numeric address of a system used to uniquely identify the system on the network. The

Glossary

IP address consists of four groups of numbers separated by periods (full stops).

ISQL (*Sybase specific term*)

A Sybase utility used to perform system administration tasks on Sybase SQL Server.

ITO

See **OVO**.

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”.

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**.

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.

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

Glossary

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.

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 UNIX specific term*)

A script provided by ON-Bar that you

can use to start backing up logical-log files when OnLine Server issues a log-full event alarm. The Informix ALARMPROGRAM configuration parameter defaults to the `<INFORMIXDIR>/etc/log_full.sh`, where `<INFORMIXDIR>` is the OnLine 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 or object copying. 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

Glossary

committed as well as roll back any transactions that have not been committed.

login ID (*MS 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 been granted Oracle SYSDBA or SYSOPER rights.
- <password> is a string used for data security and known only to its owner. Passwords are entered to connect to an operating system or software application. The password has to 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 has to be the owner of the Oracle Recovery (Oracle) 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

Glossary

consists of several volume groups, where each volume group has several volumes.

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 about 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 StorageWorks Disk Array XP specific term*)

An HP StorageWorks XP disk array that contains the primary volumes for the Continuous Access configuration and acts as a master device.

See also **BC** (*HP StorageWorks Disk Array XP specific term*), **CA** (*HP StorageWorks Disk Array XP specific term*), and **HP StorageWorks Disk Array XP LDEV**.

Manager-of-Managers (MoM)

See **Enterprise Cell Manager**.

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 session, a Media Agent locates data on the backup medium and sends it to the Disk Agent. The Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

MAPI (*Microsoft Exchange specific term*)

The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

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.

Glossary

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 ID

A unique identifier assigned to a medium by Data Protector.

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.

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**.

MFS

The Migrating File System enables a standard JFS filesystem with migration capabilities (on HP-UX 11.00). The MFS is accessed via a standard filesystem interface (DMAPI), it is mounted to a directory the same way as any HP-UX filesystem. In an MFS, only the superblock, the inode and the 'extended attribute' information remain

Glossary

permanently on the hard disk and are never migrated.

See also **VBFS**.

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, writer**.

mirror *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*

See **target volume**.

mirror rotation *(HP StorageWorks Disk Array XP specific term)*

See **replica set rotation**.

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

Glossary

environment, this part of the database can be common to all cells.
See also **CMMDB, 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 MoM allows you to configure and manage multiple cells from a central point.

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.

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.

MSM

The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.

MU number (*HP StorageWorks Disk Array XP specific term*)

A Mirror Unit number is an integer

number (0, 1 or 2), used to indicate a first level mirror.

See also **first level mirror.**

multi-drive server

A license that allows you to run an unlimited number of Media Agents on a single system. This license, which is bound to the IP address of the Cell Manager, is no longer available.

obdrindex.dat

An IDB file 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, on a separate physical disk from other IDB directories, and, additionally, to make a copy of the file and locate it where you want.

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.

object

See **backup 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.

Glossary

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.

offline backup

A backup during which an application database cannot be used by the application.

- For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to the tape is finished.
- For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

*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***

OmniStorage

Software providing transparent migration of less frequently used data to the optical library while keeping more

Glossary

frequently used data on the hard disk. HP OmniStorage runs on HP-UX systems.

On-Bar (*Informix specific term*)

A backup and restore system for OnLine Server. ON-Bar enables you to create a copy of your OnLine Server data and later restore the data. The ON-Bar backup and restore system involves the following components:

- onbar utility
- Data Protector, as the backup solution
- XBSA interface
- ON-Bar catalog tables, which are used to back up dobjects and track instances of dobjects through multiple backups.

onbar utility (*Informix specific term*)

The Informix utility that communicates backup and restore requests to OnLine Server. The utility uses XBSA to exchange control data and back up and restore data with Data Protector.

ONCONFIG (*Informix specific term*)

An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, OnLine uses the configuration values

from the file `<INFORMIXDIR>/etc/onconfig` (on HP-UX) or `<INFORMIXDIR>\etc\onconfig` (on Windows).

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 that the backup application requires access to the original data objects. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly.

- For simple backup methods (non ZDB), backup mode is required for the whole backup period (~minutes/ hours). For instance, for backup to tape, until streaming of data to tape is finished.
- For ZDB methods, backup mode is required for the short period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

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**.

Glossary

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.

OnLine Server (*Informix specific term*)

Refers to INFORMIX-OnLine Dynamic Server.

OpC

See OVO.

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.

OVO

HP OpenView Operations for Unix provides powerful capabilities for operations management of a large number of systems and applications on in a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for OVO management servers on HP-UX and Solaris. Earlier versions of OVO were called IT/Operation, Operations Center and Vantage Point Operations.

See also merging.

ownership

The ownership of a backup determines who can restore from the backup. The user who starts an interactive backup is the session owner. If a user starts an existing backup specification without modifying it, the session is not considered interactive. In that case, if the backup owner has been defined in the backup specification, they remain the session owner. Otherwise, the session owner becomes the user who started the backup in question. For the scheduled backups, by default, the session owner is for the UNIX Cell

Glossary

Manager: root.sys@<Cell Manager>, and for the Windows Cell Manager, the user that was specified during the installation of the Cell Manager. It is possible to modify the ownership, so that the specific user becomes the session owner.

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

<Data_Protector_home>\Config\Server\dr\p1s directory on a Windows Cell Manager or in /etc/opt/omni/server/dr/p1s directory on a UNIX Cell Manager 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 StorageWorks Disk Array XP specific term*)

A mirrored pair of disks can have various status values depending on the action performed on it. The three most important status values are:

- **COPY** - The mirrored pair is currently resynchronizing. Data is transferred from one disk to the other. The disks do not contain the same data.
- **PAIR** - The mirrored pair is completely synchronized and both disks (the primary volume and the mirrored volume) contain identical data.
- **SUSPENDED** - The link between the mirrored disks is suspended. That means that both disks are accessed and updated independently. However, the mirror relationship is still maintained and the pair can be resynchronized without transferring the complete disk.

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.

Glossary

parallelism

The concept of reading multiple data streams from an online database.

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.

prealloc list

A subset of media in a media pool that specifies the order in which media are used for backup.

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**.

Primary Volume (P-VOL) (*HP*

StorageWorks Disk Array XP specific term)

Standard HP StorageWorks Disk Array XP LDEVs that act as a primary volume for the CA and BC configurations. The P-VOL is located in the MCU.

See also **Secondary Volume (S-VOL)**.

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:

Glossary

- 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

RAID

Redundant Array of Inexpensive Disks.

RAID Manager Library (*HP StorageWorks Disk Array XP specific term*)

The RAID Manager Library is used internally by Data Protector on Solaris systems to allow access to HP StorageWorks Disk Array XP configuration, status, and performance data and to key HP StorageWorks Disk Array XP features through the use of function calls translated into a sequence of low level SCSI commands.

RAID Manager XP (*HP StorageWorks Disk Array XP specific term*)

The RAID Manager XP application provides an extensive list of commands to report and control the status of the CA and BC applications. The commands communicate through a RAID Manager instance with the HP StorageWorks Disk Array XP Disk Control Unit. This instance translates the commands into a sequence of low level SCSI commands.

rawdisk backup

See disk image backup.

RCU (*HP StorageWorks specific term*)

The Remote Control Unit acts as a slave of an MCU in a CA configuration. In bidirectional configurations, the RCU can act as an MCU.

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,

Glossary

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.

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.

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.

recycle

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 StorageWorks Disk Array XP specific term)

The Remote Control Unit (RCU) acts as a slave of an MCU in a CA configuration. In bidirectional configurations, the RCU can act as an MCU.

Removable Storage Management Database (*Windows specific term*)

A Windows service used for managing removable media (such as tapes and

Glossary

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/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 a virtual copy (for example, a snapshot). From a host's perspective, on a basic UNIX or Windows system, the complete physical disk containing a backup object is replicated. However, if a volume manager is used on UNIX, the whole volume/disk group containing a

backup object 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 session

A process that copies data from backup media to a client.

RMAN (*Oracle specific term*)

See **Recovery Manager**.

RSM

The Data Protector Restore Session Manager controls the restore session. This process always runs on the Cell Manager system.

Glossary

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.

SAPDBA (*SAP R/3 specific term*)

An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.

scan

A function that 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).

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 StorageWorks Disk Array XP specific term*)

Secondary Volumes, or S-VOLs, are XP LDEVs that act as a secondary CA or BC mirror of another LDEV (a P-VOL). In the case of CA, S-VOLs can be used as failover devices in a MetroCluster configuration. The S-VOLs are assigned separate SCSI addresses, different from the addresses used by the P-VOLs. *See also* **Primary Volume (P-VOL)**.

session

See **backup session**, **media management session**, and **restore session**.

session ID

An identifier of a backup, restore, object copy, or media management session, consisting of the date when the session ran and a unique number.

session key

This environment variable for the Pre- 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

Glossary

it is used for specifying options for the omnimnt, omnistat and omniabort CLI commands.

shadow copy (*MS 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**.

shadow copy provider (*MS 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 (*MS VSS specific term*)

A collection of shadow copies created at the same point in time.

See also **shadow copy**.

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 meta data. This data is necessary to perform restore of NDMP objects.

Site Replication Service (*Microsoft Exchange Server specific term*)

The Microsoft Exchange Server 2000/2003 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.

SMB

See **split mirror backup**.

SMBF

The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, object copy, restore, and media

Glossary

management sessions. One binary file is created per session. The files are grouped by year and month.

snapshot (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

A form of replica produced using snapshot creation techniques. A range of snapshot types is available, with different characteristics, depending on the arrays/techniques used. Such replicas are dynamic and may be either virtual copies, still reliant upon the contents of the source volumes, or independent exact duplicates (clones), depending on the snapshot type and the time since creation.

See also **replica** and **snapshot creation**.

snapshot backup (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

snapshot creation (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

A replica creation technique, in which copies of source volumes are created using storage virtualization techniques. The replicas are considered to be created at one particular point-in-time, without pre-configuration, and are immediately available for use. However background

copying processes normally continue after 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 -high-speed databases If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror (*EMC Symmetrix and HP StorageWorks Disk Array XP specific term*)

A replica created using split mirror techniques. Such a replica provides an independent, exact duplicate, or clone, of the contents of the source volumes. *See also* **replica** and **split mirror creation**.

Glossary

split mirror backup (*EMC Symmetrix specific term*)

See **ZDB to tape**.

split mirror backup (*HP StorageWorks Disk Array XP specific term*)

See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

split mirror creation (*EMC Symmetrix and HP StorageWorks Disk Array XP 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 StorageWorks Disk Array XP specific term*)

A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is restored from tape media to a split mirror replica, which is then synchronized to the source volumes. 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 (*Informix specific term*)

An Informix connectivity-information file 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

The Data Protector System Recovery Data (SRD) file contains system information required for installing and configuring the operating system in case of a disaster. The SRD file is an ASCII file, generated when a CONFIGURATION backup is performed on a Windows client and stored on the Cell Manager.

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 (*HP StorageWorks Disk Array XP specific term*)

A Data Protector software module that executes all tasks required for a split mirror backup integration. It communicates with the HP StorageWorks Disk Array XP storing system using the RAID Manager XP

Glossary

utility (HP-UX and Windows systems) or RAID Manager Library (Solaris systems).

sst.conf file

The file `/usr/kernel/drv/sst.conf` is required on each Data Protector Sun 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.

standard security (*MS SQL specific term*)

Standard security uses the login validation process of the Microsoft SQL Server for all connections. Standard security is useful in network environments with a variety of clients, some of which may not support trusted connections. It also provides backward compatibility for older versions of the Microsoft SQL Server.

See also **integrated security**.

Storage Group

(*Microsoft Exchange Server specific term*)

A collection of databases (stores) that share a common set of transaction log files. Exchange manages each storage group with a separate server process.

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.

storage volume (*ZDB specific term*)

A storage volume represents an object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, file systems, or other objects may exist. The volume management

Glossary

systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

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.

Symmetrix Agent (SYMA) (*EMC Symmetrix specific term*)

The Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

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 disk

A system disk is a disk containing operating system files. Microsoft terminology defines the system disk as a disk containing the files required for initial step of boot process.

system partition

A system partition is a partition containing operating system files. Microsoft terminology defines a system partition as a partition containing the files required for initial step of boot process.

System State (*Windows specific term*)

The System State data comprises the Registry, COM+ Class Registration

Glossary

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 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.

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 database (*Oracle specific term*)

In RMAN, the target database is the database that you are backing up or restoring.

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 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 crashed 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.

Glossary

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 (*MS 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.

Glossary

transaction logs (*Data Protector specific term*)

Keeps 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.

transaction log table (*Sybase specific term*)

A system table in which all changes to the database are automatically recorded.

transportable snapshot (*MS VSS specific term*)

A shadow copy that is created on the application system and can be presented to the backup system which performs the backup.

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 text file located in the SYS:SYSTEM\TSA directory on the server where TSANDS.NLM is loaded.

unattended operation

See **lights-out operation**.

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 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.

Glossary

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.

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.

VBFS (*OmniStorage specific term*)

A Very Big File System is an extension of the standard HP-UX file system on HP-UX 9.x. It is mounted to a directory the same way as any HP-UX file system. In a VBFS, only the superblock, the inode and the 'extended attribute' information remain permanently on the hard disk and are never migrated.
See also MFS.

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 StorageWorks EVA specific term)

The firmware that manages all aspects of storage system operation, including communication with Command View EVA through the HSV controllers.

See also Command View (CV) EVA.

Virtual Device Interface (*MS SQL Server specific term*)

This is a SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk (*HP StorageWorks EVA specific term*)

A unit of storage allocated from an HP StorageWorks Enterprise Virtual Array storage pool. Virtual disks are the entities that are replicated using the HP StorageWorks Enterprise Virtual Array snapshot functionality.

See also source volume and target volume.

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

Glossary

resources. This way all requests for a particular virtual server are cached by a specific cluster node.

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**.

VPO

See **OVO**.

VSS

See **Microsoft Volume Shadow Copy service**.

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.

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 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.

Glossary

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

(MS 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.

XBSA interface *(Informix specific term)*

The onbar utility and Data Protector communicate with each other through

the X/Open Backup Specification Services Programmer's Interface (XBSA).

XCOPY engine *(direct backup specific term)*

A SCSI-3 copy command that allows you to copy data from a storage device having a SCSI source address to a backup device having a SCSI destination address, thus enabling direct backup. The data flows from a source device (either block or streaming, that is, disk or tape) to the destination device (either block or streaming) through XCOPY. This releases the controlling server of reading the data from the storage device into memory and then writing the information to the destination device.

See also **direct backup**.

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 for ZDB, instant recovery, and split mirror restore.

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

Glossary

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 on split mirror arrays, 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. On split mirror arrays, split mirror restore can also be used.

See also **zero downtime backup (ZDB), ZDB to disk, instant recovery, ZDB to disk+tape, 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.**

Glossary

A

- access rights
 - adding to root account, on Linux, 75
- ACS Client, 88
- adding
 - access rights, on Linux, 75
 - SCSI robotics driver to kernel, on HP-UX, B-34
- adding software components
 - overview, 216
 - to HP-UX systems, 217
 - to Solaris systems, 218
 - to Windows systems, 216
- ADIC library. *See* ADIC/GRAU library
- ADIC/GRAU library
 - connecting drives, 88
 - installing Media Agent to clients, 90
 - Media Agent installation, 87
 - preparing clients, 88
- AIX client
 - connecting backup devices, 80
 - installing, 79
- `allow_hosts` file, 193, 195, 196
- authorized systems list, security, 191
- AutoPass utility
 - installing, on UNIX, 21
 - installing, on Windows, 31
 - licensing, 294
 - uninstalling, on HP-UX, 209
 - uninstalling, on Solaris, 213
 - uninstalling, on Windows, 208

B

- backup devices
 - setting SCSI IDs, for HP StorageWorks 330fx Library, B-49
- backup devices, connecting
 - ADIC/GRAU library drives, 88
 - AIX clients, 80
 - HP StorageWorks DAT 24 Tape Drive, B-54
 - HP StorageWorks DLT Library 24/48-Slot, B-57
 - HP Surestore 12000e Autoloader, B-55
 - HP-UX clients, 67
 - Linux clients, 78
 - overview, B-50
 - SCO clients, 86
 - Seagate Viper 200 LTO Tape Drive, B-61
 - Siemens Sinix clients, 82

- Solaris clients, 73
 - Tru64 clients, 84
 - Windows clients, 62
- backup environment concepts, 3

C

- cell
 - concepts, 3
 - enabling security, 193
 - exporting clients, 184
 - exporting Microsoft Cluster Server client, 185
 - importing clients, 177
 - importing clusters, 180
 - importing Installation Server, 179
 - licenses, 279, 280
 - securing clients, 192
 - upgrading, overview, 224
 - verifying DNS connections, 306
- cell configuration, licenses, A-19
- Cell Manager
 - automatically configured files, on UNIX, 23
 - Cell Request Server (CRS) service, 24, 32
 - changing software components, 216
 - changing the name, B-21
 - checking configuration changes, 235
 - choosing the system, 10, 11
 - concepts, 3
 - configuring for Veritas Volume Manager, on Microsoft Cluster Server, B-70
 - directory structure, on UNIX, 22
 - functions, 10
 - installation prerequisites, on UNIX, 18
 - installation prerequisites, on Windows, 26
 - installation sequence, 17
 - installation, troubleshooting, 305
 - installing, on HP-UX, 20
 - installing, on HP-UX, using native tools, B-3
 - installing, on MC/ServiceGuard, 158
 - installing, on Microsoft Cluster Server, 160
 - installing, on Solaris, using native tools, B-5
 - installing, on Windows, 26
 - Media Management Daemon (MMD) service, 24
 - preparing NIS server, B-24
 - Raima Database Server (RDS) service, 24, 32
 - security concepts, 187

Index

- setting environment variables, on UNIX, 24
- troubleshooting, 309, 310, 314, 315
- troubleshooting installation, on UNIX, 25
- uninstalling, from HP-UX, 208
- uninstalling, from MC/ServiceGuard, 209
- uninstalling, from Solaris, 212
- uninstalling, from Windows, 207
- upgrading from Data Protector A.05.x, on HP-UX, 226, 229
- upgrading from Windows NT to a newer Windows version, 262
- upgrading manually, on UNIX, 314
- upgrading SSE, 260
- upgrading, on MC/ServiceGuard, 269
- upgrading, on Microsoft Cluster Server, 273
- Cell Request Server (CRS) service, 24, 32
- cell_info file, 219
- changing
 - Cell Manager name, B-21
 - default port, B-23
 - software components, 216
- checking
 - General Media Agent installation, on Novell NetWare, B-64
 - installation on clients, 313
 - licenses, 280
 - log files, installation, 315
 - patches, 203
 - TCP/IP setup, on Windows, B-19
- CLI. *See* command-line interface
- client
 - adding root access rights, on Linux, 75
 - changing software components, 216
 - checking TCP/IP setup, on Windows, B-19
 - cluster-aware integration installation, overview, 121
 - cluster-aware, importing to a cell, 180
 - concepts, 3
 - configuring after installation, on Solaris, 69
 - configuring for backup devices usage, on Solaris, B-43
 - configuring for Veritas Volume Manager, on Microsoft Cluster Server, B-70
 - configuring kernel, on Linux, 77
 - configuring TCP/IP, on Windows, B-15
 - creating device files, on HP-UX, B-36
 - creating device files, on Solaris, B-46
 - denying access from hosts, 196
 - enabling access verification, 192
 - exporting from a cell, 184
 - importing to a cell, 177
 - installation, overview, 42
 - integration installation, overview, 118
 - local installation, on Novell NetWare, 96
 - local installation, on OpenVMS, 103
 - Microsoft Cluster Server, exporting from a cell, 185
 - preparing for ADIC/GRAU library, 88
 - preparing for StorageTek ACS library, 93
 - remote installation, overview, 45
 - removing access verification, 195
 - securing, 192
 - security concepts, 187
 - troubleshooting, 309, 311, 315
 - uninstalling remotely, 206
 - upgrading from Data Protector A.05.x, 237
 - upgrading from Data Protector A.05.x, on MC/ServiceGuard, 238
 - upgrading, on Microsoft Cluster Server, 276
 - verifying installation, 313
- client, connecting backup devices
 - ADIC/GRAU library drives, 88
 - AIX clients, 80
 - HP-UX clients, 67
 - Linux clients, 78
 - SCO clients, 86
 - Siemens Sinix clients, 82
 - Solaris clients, 73
 - Tru64 clients, 84
 - Windows clients, 62
- client, installing
 - DB2 integration, 125
 - HP StorageWorks EVA integration, 142
 - HP StorageWorks VA integration, 136
 - HP StorageWorks XP integration, 130
 - Informix integration, 122
 - Lotus integration, 126
 - Media Agent for ADIC/GRAU library, 90
 - Media Agent for StorageTek ACS library, 95
 - Microsoft Exchange integration, 121
 - Microsoft SQL integration, 122
 - Microsoft Volume Shadow Copy integration, 126
 - NDMP integration, 126
 - NNM integration, 125
 - on AIX systems, 79
 - on HP-UX systems, 64

- on Linux systems, 74
- on MC/ServiceGuard systems, 159
- on Microsoft Cluster Server systems, 168
- on MPE/iX systems, 110
- on Novell NetWare Cluster Services systems, 172
- on Novell NetWare systems, 96
- on OpenVMS systems, 103
- on SCO systems, 85
- on Siemens Sinix systems, 81
- on Solaris systems, 67
- on Tru64 systems, 83
- on UNIX systems, 113
- on Veritas Cluster systems, 171
- on Windows systems, 58
- Oracle integration, 124
- SAP DB integration, 123
- SAP R/3 integration, 123
- Single Server Edition, 154
- Sybase integration, 122
- cluster
 - changing software components, 216
 - importing to a cell, 180
 - installing Cell Manager, 160
 - installing clients, 168, 171, 172
 - installing integrations, 121
 - Microsoft Cluster Server, exporting from a cell, 185
 - uninstalling, 206
- command-line interface (CLI), 3, 12
- commands
 - CLI changes, after upgrade, B-74
 - infs, B-36
 - ioscan, B-33, B-36, B-40
 - netstat, B-23
 - omnicc, 289
 - omnicheck, 204, 306
 - omnisetup.sh, 114, 151, 226, 229
 - omnisv, 226
- concepts
 - backup environment, 3
 - cell, 3
 - Cell Manager, 3
 - client, 3
 - Disk Agent, 3
 - exporting, 184
 - graphical user interface (GUI), 12, 13
 - IDB filename conversion, 250
 - importing, 177
 - Installation Server, 3
 - Media Agent, 3
 - NDMP Media Agent, 3
 - remote installation, 6
 - User Interface, 3
- configuration files
 - automatically configured files, on UNIX
 - Cell Manager, 23
 - cell_info, 219
 - changes, after upgrade, B-71
 - checking changes after upgrade from Data Protector A.05.x, 235
 - global, 235
 - inet.conf, B-24
 - installation_servers, 37
 - modifying, Solaris client installation, 69
 - nsswitch.conf, B-24
 - omni_info, 219
 - omnirc, 236
 - sst.conf, B-45
 - st.conf, B-43
 - st.conf file, 69
 - upgrade problems, 314
- configuring
 - Cell Manager with Veritas Volume Manager, on MSCS, B-70
 - clients with Veritas Volume Manager, on Microsoft Cluster Server, B-70
 - Disk Agent, on OpenVMS, 107
 - kernel, on Linux clients, 77
 - Media Agent, on Novell NetWare, 102
 - Media Agent, on OpenVMS, 108
 - SCSI robotics, on HP-UX, B-31
 - Solaris clients, after installation, 69
 - Solaris clients, before using backup devices, B-43
 - sst.conf file, B-45
 - st.conf file, 69, B-43
 - TCP/IP, on Windows, B-15
- connecting backup devices
 - ADIC/GRAU library drives, 88
 - AIX clients, 80
 - HP StorageWorks DAT 24 Tape Drive, B-54
 - HP StorageWorks DLT Library 24/48-Slot, B-57
 - HP Surestore 12000e Autoloader, B-55
 - HP-UX clients, 67
 - Linux clients, 78
 - overview, B-50

Index

- SCO clients, 86
- Seagate Viper 200 LTO Tape Drive, B-61
- Siemens Sinix clients, 82
- Solaris clients, 73
- Tru64 clients, 84
- Windows clients, 62
- conventions, xi
- conversion of filenames. *See* IDB filename conversion
- creating
 - device files, on HP-UX, B-36
 - device files, on Solaris, B-46
 - device files, on Windows, B-29
 - execution trace files, installation, 318
- CRS. *See* Cell Request Server (CRS) service

D

- DAS Client, 88
- Data Protector Inet service, 32
- database growth. *See* IDB
- DB2 integration, installing, 125
- debug option
 - overview, 318
- debugging installation, 318
- default gateway, TCP/IP, B-15
- default port, changing, B-23
- deny_hosts file, 196
- denying access from hosts, 196
- determining
 - installed licenses, 299
 - required licensing passwords, 292
 - unused SCSI addresses, on HP-UX, B-40
 - unused SCSI addresses, on Solaris, B-42
 - unused SCSI addresses, on Windows, B-48
- device file
 - creating, on HP-UX, B-36
 - creating, on Solaris, B-46
 - creating, on Windows, B-29
- disabling SCSI robotics drivers, on Windows, B-27
- Disk Agent
 - concepts, 3
 - configuring, on OpenVMS, 107
- DNS
 - omnicheck command, 306
 - verifying connections in a cell, 306
- DNS check tool, B-20
- domain name system. *See* DNS
- drive licenses, 279

E

- enabling access verification
 - on a cell, 193
 - on a client, 192
- environment variables, setting on UNIX Cell Manager, 24
- EVA integration
 - upgrading from Data Protector A.05.x, 246
- excessive logging, 196
- execution trace files
 - creating, 318
 - debug option, 318
- exporting
 - clients, 184
 - Microsoft Cluster Server client, 185

F

- filenames
 - conversion. *See* IDB filename conversion
 - encoding. *See* IDB filename conversion
- files
 - allow_hosts, 193, 195, 196
 - deny_hosts, 196
 - HPDEVBRA.NLM, B-67
 - HPUMA.NLM, B-67
 - services, B-23
- Functional Extensions, licensing, 279

G

- General Media Agent
 - checking installation, on Novell NetWare, B-64
- global file, 235
- graphical user interface (GUI)
 - concepts, 12, 13
 - starting, UNIX, 12
 - views, 13
- GRAU library. *See* ADIC/GRAU library
- GUI. *See* graphical user interface

H

- HP StorageWorks 330fx Library, setting SCSI IDs, B-49
- HP StorageWorks DAT 24 Tape Drive, connecting, B-54
- HP StorageWorks DLT Library 24/48-Slot, connecting, B-57
- HP StorageWorks EVA integration
 - installing, 142

- HP StorageWorks VA integration
 - installing, 136
- HP StorageWorks XP integration
 - installing, 130
- HP Surestore 12000e Autoloader, connecting, B-55
- HPDEVBRA.NLM file, B-67
- HPUMA.NLM file, B-67
- HP-UX Cell Manager
 - automatically configured files, 23
 - directory structure, 22
 - installation prerequisites, 18
 - installing, 20
 - installing, using native tools, B-3
 - setting environment variables, 24
 - troubleshooting, 25, 314, 315
 - troubleshooting installation, 25
 - uninstalling, 208
 - upgrading from Data Protector A.05.x, 226, 229
- HP-UX client
 - connecting backup devices, 67
 - installing, 64
 - troubleshooting, 311
- HP-UX Installation Server
 - installing, using native tools, B-7
- I**
- IDB
 - growth, 10
 - troubleshooting upgrade, 314
- IDB filename conversion
 - concepts, 250
- importing
 - clients, 177
 - clusters, 180
 - Installation Server, 179
 - multiple LAN card clients, 178
 - NDMP clients, 178
 - OpenVMS clients, 178
- Inet service. *See* Data Protector Inet service
- inet.conf file, B-24
- inet.log file, 193, 195, 196, 272
- Informix integration
 - upgrading from Data Protector A.05.x, on UNIX, 241
 - upgrading from Data Protector A.05.x, on Windows, 243
- Informix integration, installing, 122
- infs command, B-36
- installation
 - client installation, overview, 42
 - cluster-aware integrations, 121
 - components. *See* installation components
 - creating execution trace files, 318
 - debugging, 318
 - general steps, 5
 - integrations, overview, 118
 - log files, 315
 - overview, 3
 - pkgadd utility, 212, 213
 - remote installation, overview, 45
 - remote, concepts, 6
 - software component codes, 115
 - software components, 54
 - troubleshooting Cell Manager, on Solaris, 310
 - troubleshooting clients, on UNIX, 311
 - troubleshooting, on Windows, 309
 - verifying clients, 313
- installation components
 - Disk Agent, 3
 - General Media Agent, 3
 - Installation Server, 3
 - Media Agent, 3
 - NDMP Media Agent, 3
 - User Interface, 3
- Installation Server
 - concepts, 3
 - directory structure, on UNIX, 22
 - importing to a cell, 179
 - installation overview, 33
 - installation prerequisites, on UNIX, 34
 - installation prerequisites, on Windows, 37
 - installation sequence, 17
 - installing, on HP-UX, using native tools, B-7
 - installing, on Solaris, using native tools, B-8
 - installing, on UNIX, 34
 - installing, on Windows, 37
 - uninstalling, from HP-UX, 208
 - uninstalling, from MC/ServiceGuard, 209
 - uninstalling, from UNIX, 213
 - uninstalling, from Windows, 207
 - upgrading from Data Protector A.05.x, on HP-UX, 226
 - upgrading from Data Protector A.05.x, on Windows, 231
 - upgrading manually, on UNIX, 314

- installation_servers file, 37
- installing
 - AutoPass utility, on UNIX, 21
 - AutoPass utility, on Windows, 31
 - Cell Manager, troubleshooting, 305
 - clients locally, 58, 103, 110, 113
 - clients, troubleshooting, 309
 - cluster-aware Cell Manager, 158, 160
 - cluster-aware clients, 159, 168, 171, 172
 - DB2 integration, 125
 - HP StorageWorks EVA integration, 142
 - HP StorageWorks VA integration, 136
 - HP StorageWorks XP integration, 130
 - Informix integration, 122
 - integrations, 118
 - localized user interface, 149
 - Lotus integration, 126
 - Media Agent for ADIC/GRAU library, 87, 90
 - Media Agent for StorageTek ACS library, 87, 95
 - Microsoft Exchange integration, 121
 - Microsoft SQL integration, 122
 - Microsoft Volume Shadow Copy integration, 126
 - NDMP integration, 126
 - NNM integration, 125
 - Oracle integration, 124
 - permanent licensing passwords, 294–298
 - SAP DB integration, 123
 - SAP R/3 integration, 123
 - Single Server Edition, 154
 - Sybase integration, 122
 - Web Reporting, 156
- installing Cell Manager
 - on HP-UX systems, 20
 - using native tools, B-3
 - on MC/ServiceGuard systems, 158
 - on Microsoft Cluster Server systems, 160
 - on Solaris systems
 - using native tools, B-5
 - on Windows systems, 26
 - prerequisites, on UNIX, 18
 - prerequisites, on Windows, 26
- installing clients
 - on AIX systems, 79
 - on HP-UX systems, 64
 - on Linux systems, 74
 - on MC/ServiceGuard systems, 159
 - on Microsoft Cluster Server systems, 168
 - on MPE/iX systems, 110
 - on Novell NetWare Cluster Services systems, 172
 - on Novell NetWare systems, 96
 - on OpenVMS system, 103
 - on SCO systems, 85
 - on Siemens Sinix systems, 81
 - on Solaris systems, 67
 - on Tru64 systems, 83
 - on UNIX systems, 113
 - on Veritas Cluster systems, 171
 - on Windows systems, 58
- installing Installation Server
 - on HP-UX systems
 - using native tools, B-7
 - on Solaris systems
 - using native tools, B-8
 - on UNIX systems, 34
 - on Windows systems, 37
 - overview, 33
 - prerequisites, on UNIX, 34
 - prerequisites, on Windows, 37
- integration client, 118
 - See also* integrations
- integrations
 - cluster-aware installation, 121
 - EVA, 246
 - local installation, 120
 - Oracle, on UNIX, 239
 - overview, 118
 - remote installation, 121
 - SAP R/3, on UNIX, 241
 - upgrading EVA, 246
 - upgrading Informix, on UNIX, 241
 - upgrading Informix, on Windows, 243
 - upgrading Oracle, on Windows, 239
 - upgrading SAP R/3, on Windows, 241
 - upgrading Sybase, on UNIX, 244
 - upgrading Sybase, on Windows, 245
- integrations, installing
 - DB2 integration, 125
 - HP StorageWorks EVA integration, 142
 - HP StorageWorks VA integration, 136
 - HP StorageWorks XP integration, 130
 - Informix integration, 122
 - Lotus integration, 126
 - Microsoft Exchange integration, 121
 - Microsoft SQL integration, 122

- Microsoft Volume Shadow Copy
 - integration, 126
 - NDMP integration, 126
 - NNM integration, 125
 - Oracle integration, 124
 - SAP DB integration, 123
 - SAP R/3 integration, 123
 - Sybase integration, 122
 - internationalization, IDB, 250
 - ioscan command, B-33, B-36, B-40
 - IP address, TCP/IP, B-15
- K**
- kernel
 - adding SCSI robotics driver, on HP-UX, B-34
 - configuring on Linux clients, 77
 - rebuilding, on HP-UX, B-34
- L**
- license-to-use. *See* licenses
 - licensing
 - AutoPass utility, 294
 - capacity based licenses, 281
 - capacity based licensing, examples, 285–288
 - cell configurations, A-19
 - cell manager related licenses, 280
 - centralized licensing, configuring, 301
 - checking and reporting licenses, 280
 - determining installed licenses, 299
 - determining required passwords, 292
 - Drive Extensions, A-5
 - drive licenses, 279
 - emergency passwords, 293
 - entity based licenses, 281
 - Functional Extensions, 279, A-7
 - Instant-On passwords, 293
 - license migration, A-16
 - licensing forms, A-25
 - migrating Data Protector A.05.x licenses, A-16
 - migrating support contract, A-17
 - moving licenses, 299
 - obtaining and installing permanent passwords, 294–298
 - overview, 290
 - password types, 293
 - permanent passwords, 293
 - permanent passwords, obtaining and installing, 294–298
 - producing license reports, 289
 - product licensing overview, 290
 - product overview, A-4
 - product structure, 279, A-3
 - Single Server Edition, A-15
 - Starter Packs, 279
 - support contract migration, A-17
 - upgrade from Data Protector A.05.x, 226
 - upgrade from SSE, 259
 - using licenses, after upgrade, 226, 259
 - verifying passwords, 298
 - licensing forms, A-25
 - limitations
 - on UNIX systems, 113
 - on Windows systems, 38, 58
 - Single Server Edition, 154
 - upgrade, 223
 - upgrade of Manager-of-Managers, 225
 - Linux client
 - configuring kernel, 77
 - connecting backup devices, 78
 - installing, 74
 - troubleshooting remote installation, 75
 - local installation, clients, 58, 103, 110, 113
 - localized user interface. *See* User Interface
 - log files
 - checking, installation, 315
 - description, 316
 - inet.log, 193, 195, 196, 272
 - location, 316
 - Lotus integration, installing, 126
 - LTU. *See* licenses
- M**
- Manager-of-Managers
 - upgrade overview, 225
 - upgrading from Data Protector A.05.x, 249
 - MC/ServiceGuard
 - excessive logging to inet.log file, 196
 - importing, 182
 - installing Cell Manager, 158
 - installing clients, 159
 - uninstalling Cell Manager, 209
 - uninstalling Installation Server, 209
 - upgrading Cell Manager, 269
 - upgrading clients from Data Protector A.05.x, 238

Index

Media Agent
 concepts, 3
 configuring, on Novell NetWare, 102
 configuring, on OpenVMS, 108
 installing for ADIC/GRAU library, 90
 installing for StorageTek ACS library, 95
 types, 3
Media Management Daemon (MMD) service, 24
Microsoft Cluster Server
 configuring Cell Manager with Veritas
 Volume Manager, B-70
 configuring clients with Veritas Volume
 Manager, B-70
 exporting, 185
 importing, 180
 installing Cell Manager, 160
 installing clients, 168
 upgrading Cell Manager, 273
 upgrading clients, 276
Microsoft Exchange 2000 integration
 installing on systems with HP
 StorageWorks EVA disk array, 147
 installing on systems with HP
 StorageWorks VA disk array, 141
 installing on systems with HP
 StorageWorks XP disk array, 135
Microsoft Exchange integration
 installing, 121
Microsoft Installer, 27, 223, 273, 309
Microsoft SQL integration
 installing, 122
 installing on systems with HP
 StorageWorks EVA disk array, 147
 installing on systems with HP
 StorageWorks VA disk array, 142
 installing on systems with HP
 StorageWorks XP disk array, 136
Microsoft Terminal Services Client, 27
Microsoft Volume Shadow Copy integration,
 installing, 126
migrating
 licenses, A-16
 support contract, A-17
minimizing network traffic, on Novell
 NetWare clients, 101
MMD. *See* Media Management Daemon
 (MMD) service
moving licenses, 299
MPE/iX client, installing, 110

MSI. *See* Microsoft Installer
multibyte characters, 250
multiple LAN card client, importing, 178

N

NDMP client, importing, 178
NDMP integration, installing, 126
NDMP Media Agent, concepts, 3
 netstat command, B-23
NIS server, preparing, B-24
NNM integration, installing, 125
Novell NetWare client
 checking General Media Agent installation,
 B-64
 configuring Media Agent, 102
 HPDEVBRA.NLM file, B-67
 HPUMA.NLM file, B-67
 installing, 96
 minimizing network traffic, 101
Novell NetWare Cluster Services
 importing, 182
 installing clients, 172
 limitations, failover, 172
nsswitch.conf file, B-24

O

obtaining permanent licensing passwords,
 294–298
omni_info file, 219
omnicc command, 289
omnicheck command, 204, 306
omniinet process. *See* Data Protector Inet
 service
omnirc file, 236
omnisetup.sh command
 installation, 114, 151
 upgrade, 226, 229
omnisv command, 226
OpenVMS client
 configuring Disk Agent, 107
 configuring Media Agent, 108
 importing, 178
 uninstalling, 206
operating system
 upgrading Windows NT to a newer
 Windows version, 262
Oracle integration
 installing, 124
 installing on systems with EMC Symmetrix
 disk array, 128

- installing on systems with HP
 - StorageWorks EVA disk array, 143
- installing on systems with HP
 - StorageWorks VA disk array, 137
- installing on systems with HP
 - StorageWorks XP disk array, 131
- uninstallation specifics, 218
- upgrading from Data Protector A.05.x, 239
- overview
 - changing software components, 216
 - connecting backup devices, B-50
 - debug option, 318
 - execution trace files, 318
 - importing application cluster packages, 180
 - importing cluster-aware client, 180
 - installing clients, 42
 - installing cluster-aware integrations, 121
 - installing Installation Server, 33
 - installing integrations, 118
 - integrations, 118
 - licensing, 290
 - product structure, 279
 - remotely installing clients, 45
 - software components, 54
 - uninstallation, 205
 - upgrade, 223
 - upgrading from Data Protector A.05.x, 226

P

- patches
 - omnicheck command, 204
 - verifying, 203
- pkgadd utility, 212, 213
- pkgrm utility, 212, 213
- preparing NIS server, B-24
- prerequisites
 - Cell Manager installation, on UNIX, 18
 - Cell Manager installation, on Windows, 26
 - Installation Server installation, on UNIX, 34
 - Installation Server installation, on Windows, 37
 - upgrade from Data Protector A.05.x, 226
- processes
 - Cell Request Server (CRS) service, 24, 32
 - Data Protector Inet service, 32
 - Media Management Daemon (MMD) service, 24

- Raima Database Server (RDS) service, 24, 32

R

- Raima Database Server (RDS) service, 24, 32
- RDS. *See* Raima Database Server (RDS) service
- rebuilding kernel, on HP-UX, B-34
- remote installation
 - clients, 45
 - integrations, 121
 - troubleshooting, on Linux, 75
- removing
 - access verification on a client, 195
 - Data Protector software manually, from UNIX, 214
 - software components, from UNIX, 217, 219
 - software components, from Windows, 216
 - software components, overview, 216
- reporting licenses, 280
- robotics. *See* SCSI interface

S

- SAP DB integration, installing, 123
- SAP R/3 integration
 - installing, 123
 - installing on systems with EMC Symmetrix disk array, 129
 - installing on systems with HP
 - StorageWorks EVA disk array, 144
 - installing on systems with HP
 - StorageWorks VA disk array, 138
 - installing on systems with HP
 - StorageWorks XP disk array, 132
 - upgrading from Data Protector A.05.x, 241
- SCO client
 - connecting backup devices, 86
 - installing, 85
- SCSI addresses. *See* SCSI interface
- SCSI controller. *See* SCSI interface
- SCSI interface
 - adding robotics driver to kernel, on HP-UX, B-34
 - configuring robotics, on HP-UX, B-31
 - determining unused addresses, on HP-UX, B-40
 - determining unused addresses, on Solaris, B-42

Index

- determining unused addresses, on
 - Windows, B-48
 - disabling robotics drivers, on Windows, B-27
 - setting controller parameters, on Windows, B-39
 - setting IDs, for HP StorageWorks 330fx Library, B-49
 - using tape drivers, on Windows, B-26
- SCSI robotics. *See* SCSI interface
- SCSI tape drivers. *See* SCSI interface
- Seagate Viper 200 LTO Tape Drive, connecting, B-61
- securing
 - cell, 193
 - client, 192
- security
 - allow_hosts file, 193, 195, 196
 - deny_hosts file, 196
 - denying access from hosts, 196
 - enabling security for a cell, 193
 - enabling security for a client, 192
 - excessive logging to `inet.log` file, 196
 - list of authorized systems, 191
 - potential problems, 191
 - removing access verification on a client, 195
- services file, B-23
- setting
 - environment variables, on UNIX Cell Manager, 24
 - SCSI controller parameters, on Windows, B-39
 - SCSI IDs, for HP StorageWorks 330fx Library, B-49
- Siemens Sinix client
 - connecting backup devices, 82
 - installing, 81
- Single Server Edition
 - installing, 154
 - license types, A-15
 - limitations, 154
 - product overview, licenses, A-4
 - upgrading from multiple installations, 260
 - upgrading to Data Protector A.05.50, 259
 - upgrading to Data Protector A.05.50 SSE, 259
- software components
 - adding, to HP-UX, 217
 - adding, to Solaris, 218
 - adding, to Windows, 216
 - changing, on cluster clients, 216
 - changing, overview, 216
 - component codes, 115
 - dependencies, on HP-UX, 217
 - dependencies, on Solaris, 218
 - overview, 54
 - removing, from UNIX, 217, 219
 - removing, from Windows, 216
- Solaris Cell Manager
 - automatically configured files, 23
 - directory structure, 22
 - installation prerequisites, 18
 - installing, using native tools, B-5
 - setting environment variables, 24
 - troubleshooting, 25, 310, 314, 315
 - troubleshooting installation, 25
 - uninstalling, 212
- Solaris client
 - configuring, after installation, 69
 - connecting backup devices, 73
 - installing, 67
 - troubleshooting, 311
- Solaris Installation Server
 - installing, using native tools, B-8
- SSE. *See* Single Server Edition
- `sst.conf` file, B-45
- `st.conf` file, 69, B-43
- Starter Packs, licensing, 279
- starting
 - GUI, UNIX, 12
- STK ACS. *See* StorageTek ACS library
- StorageTek ACS library
 - connecting drives, 88
 - installing Media Agent to clients, 95
 - Media Agent installation, 87
 - preparing clients, 93
- StorageTek library. *See* StorageTek ACS library
- subnet mask, TCP/IP, B-15
- support contract migration, A-17
- `swagent` daemon, 311
- Sybase integration
 - upgrading from Data Protector A.05.x, on UNIX, 244
 - upgrading from Data Protector A.05.x, on Windows, 245
- Sybase integration, installing, 122

T

tape drivers. *See* SCSI interface

- TCP/IP
 - checking setup, on Windows, B-19
 - configuring, on Windows, B-15
 - default gateway, B-15
 - IP address, B-15
 - subnet mask, B-15
- Terminal Services Client, 27
- trace files. *See* execution trace files
- troubleshooting
 - installing Cell Manager, Windows, 305
 - installing clients, Windows, 309
- troubleshooting installation
 - Cell Manager, on Solaris, 310
 - Cell Manager, on UNIX, 25
 - Cell Manager, on Windows, 33
 - clients, on HP-UX, 311
 - Data Protector software, on Windows, 309
 - debug option, 318
 - debugging, 318
 - execution trace files, 318
 - localized user interface, 152
 - log files, 315
 - Microsoft Installer problems, 309
 - omnicheck command, 306
 - remote installation, on Linux, 75
 - remote installation, on UNIX, 311
 - swagent daemon, 311
- troubleshooting localized user interface, 152
- troubleshooting upgrade
 - configuration files not available, 314
 - Data Protector patches, 314
 - Data Protector software, on Windows, 309
 - IDB not available, 314
 - Microsoft Installer problems, 309
- Tru64 client
 - connecting backup devices, 84
 - installing, 83
- typographical conventions, xi
- U**
- uninstallation
 - Oracle integration specifics, 218
 - overview, 205
 - pkgmgr utility, 212, 213
 - prerequisites, 205
- uninstalling
 - AutoPass utility, on HP-UX, 209
 - AutoPass utility, on Solaris, 213
 - AutoPass utility, on Windows, 208
 - Cell Manager, from HP-UX, 208
 - Cell Manager, from MC/ServiceGuard, 209
 - Cell Manager, from Solaris, 212
 - Cell Manager, from Windows, 207
 - clients, from OpenVMS, 206
 - clients, remotely, 206
 - cluster clients, 206
 - Installation Server, from HP-UX, 208
 - Installation Server, from
 - MC/ServiceGuard, 209
 - Installation Server, from UNIX, 213
 - Installation Server, from Windows, 207
- unused SCSI addresses. *See* SCSI interface
- upgrade
 - before upgrading, 223
 - CLI changes, B-74
 - configuration files changes, B-71
 - global file, 235
 - limitations, 223
 - omnirc file, 236
 - omnisetup.sh command, 226, 229
 - omnisv command, 226
 - overview, 223
 - sequence, 224
 - troubleshooting IDB, 314
 - troubleshooting, on UNIX, 314
 - troubleshooting, on Windows, 309, 314
- upgrading
 - manually, on UNIX, 314
 - SSE to Data Protector A.05.50, 259
 - SSE to Data Protector A.05.50 SSE, 259
 - Windows NT to a newer Windows version, 262
- upgrading from Data Protector A.05.x
 - Cell Manager, on HP-UX, 226, 229
 - Cell Manager, on MC/ServiceGuard, 269
 - Cell Manager, on Microsoft Cluster Server, 273
 - checking configuration changes, 235
 - clients, 237
 - clients, on MC/ServiceGuard, 238
 - clients, on Microsoft Cluster Server, 276
 - EVA integration, 246
 - Informix integration, on UNIX, 241
 - Informix integration, on Windows, 243
 - Installation Server, on HP-UX, 226
 - Installation Server, on Windows, 231
 - Manager-of-Managers, 249
 - migrating licenses, A-16

Index

- migrating support contract, A-17
- omnisv command, 226
- Oracle integration, 239
- overview, 226
- prerequisites, 226
- SAP R/3 integration, 241
- Sybase integration, on UNIX, 244
- Sybase integration, on Windows, 245
- upgrading from OmniBack II A.03.x
 - migrating support contract, A-17
- upgrading from OmniBack II A.04.10
 - Cell Manager, on MC/ServiceGuard, 269
 - Cell Manager, on Microsoft Cluster Server, 273
 - clients, on Microsoft Cluster Server, 276
- upgrading from OmniBack II A.04.x
 - migrating support contract, A-17
- Upgrading to HP-UX 11.23, 264
- User Interface
 - choosing the system, 12
 - concepts, 3
 - installing localized user interface, 149
 - troubleshooting localized user interface
 - installation, 152
- user interface
 - See* command-line interface (CLI),
graphical user interface (GUI)
- using
 - licenses, 223, 226
 - log files, 315
 - SCSI tape drivers, on Windows, B-26

V

- verifying
 - client installation, 313
 - DNS connections in a cell, 306
 - licensing passwords, 298
 - patches, 203
- Veritas Cluster
 - importing, 182
 - installing clients, 171
 - limitations, failover, 171
- Veritas Volume Manager
 - configuring Cell Manager, on Microsoft Cluster Server, B-70
 - configuring clients, on Microsoft Cluster Server, B-70
- views, graphical user interface, 13
- virtual server, importing to a cell, 180

W

- Web Reporting, installing, 156
- Windows Cell Manager
 - installation prerequisites, 26
 - installing, 26
 - troubleshooting, 309, 314
 - troubleshooting installation, 33
 - uninstalling, 207
- Windows client
 - connecting backup devices, 62
 - installing, 58
 - troubleshooting, 309, 315
- Windows NT, upgrading to a newer Windows version, 262

Z

- ZDB integration client, 118
 - See also* integrations