

HP OpenView Storage Data Protector Installation and Licensing Guide

Manual Edition: May 2003



Manufacturing Part Number: B6960-90079

Release A.05.10

© Copyright Hewlett-Packard Development Company, L.P.2003.

Legal Notices

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Company
United States of America

Copyright Notices. ©Copyright 1983-2003 Hewlett-Packard Development Company, L.P. all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

©Copyright 1979, 1980, 1983, 1985-93 Regents of the University of California

This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

©Copyright 1986-1992 Sun Microsystems, Inc.

©Copyright 1985-86, 1988 Massachusetts Institute of Technology

©Copyright 1989-93 The Open Software Foundation, Inc.

©Copyright 1986-1997 FTP Software, Inc. All rights reserved

©Copyright 1986 Digital Equipment Corporation

©Copyright 1990 Motorola, Inc.

©Copyright 1990, 1991, 1992 Cornell University

©Copyright 1989-1991 The University of Maryland

©Copyright 1988 Carnegie Mellon University

©Copyright 1991-1995 by Stichting Mathematisch Centrum,
Amsterdam, The Netherlands

©Copyright 1999, 2000 Bo Branten

Trademark Notices. UNIX® is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

X Window System is a trademark of the Massachusetts Institute of Technology.

Motif is a trademark of the Open Software Foundation, Inc. in the U.S. and other countries.

Windows NT™ is a U.S. trademark of Microsoft Corporation. Microsoft®, MS-DOS®, Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle®, SQL*Net®, and Net8® are registered U.S. trademarks of Oracle Corporation, Redwood City, California. Oracle Reports™, Oracle8™, Oracle8 Server Manager™ and Oracle8 Recovery Manager™ are trademarks of Oracle Corporation, Redwood City, California.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

ARM® is a registered trademark of ARM Limited.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

VisiCalc® is a U.S. registered trademark of Lotus Development Corp.

HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation.

OpenView® is a registered U.S. trademark of Hewlett-Packard Company.

© 2003 Bristol Technology, Inc., Bristol Technology, Wind/U, HyperHelp and Xprinter are registered trademarks of Bristol Technology Inc.

Other reserved names are trademarks of the respective companies.

1. Overview of the Installation Procedure

In This Chapter	2
Overview of the Installation Procedure	3
The Concept of the Installation	6
Choosing the Cell Manager System	9
Choosing the Data Protector User Interface System	11
The Data Protector Graphical User Interface	12

2. Installing Data Protector on Your Network

In This Chapter	14
Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS) . . .	15
Installing a UNIX Cell Manager	16
Installing a Windows Cell Manager	25
Installing Installation Servers	30
Installing Data Protector Clients	39
Distributing the Data Protector Software to Clients	43
Installing Windows Clients	51
Installing HP-UX Clients	58
Installing Solaris Clients	61
Installing AIX Clients	68
Installing Siemens Sinix Clients	71
Installing Tru64 Clients	73
Installing SCO Clients	75
Installing Linux Clients	78
Installing the DAS Media Agent to Use the ADIC/GRAU Library	83
Installing the ACS Media Agent to Use the StorageTek Library	89
Local Installation of the Novell NetWare Clients	92
Local Installation of OpenVMS Clients	99
Installing MPE/iX Clients	105
Local Installation of UNIX Clients	108
Installing MS Exchange 5.x Clients	112
Installing MS Exchange 2000 Clients	113
Installing MS SQL 7.0/2000 Clients	114
Installing Sybase Clients	115
Installing Informix Clients	116
Installing SAP R/3 Clients	116
Installing Oracle8/9 Clients	118
Installing DB2 Clients	119

Contents

Installing NNM Clients	120
Installing NDMP Integration.....	120
Installing EMC Symmetrix Integration	121
Installing HP StorageWorks XP Integration.....	122
Installing the HP StorageWorks Virtual Array Integration	124
Installing the HP StorageWorks Enterprise Virtual Array Integration	125
Installing the HP StorageWorks Modular SAN Array 1000 Integration	126
Installing MS Volume Shadow Copy Integration	127
Installing Lotus Domino Server Clients	128
Installing Localized Data Protector User Interface	130
Installing Localized Data Protector User Interface on Windows Systems	130
Installing Localized Data Protector User Interface on UNIX Systems	132
Troubleshooting	133
Installing the Data Protector Single Server Edition	135
Limitations of SSE for Windows	135
Limitations of SSE for HP-UX and Solaris	135
Installing Data Protector Web Reporting	137
Installing Data Protector on MC/ServiceGuard.....	139
Installing a Cluster-Aware Cell Manager	139
Installing a Cluster-Aware Client	140
Installing Data Protector on Microsoft Cluster Server	141
Installing a Cluster-Aware Cell Manager	141
Installing a Cluster-Aware Client	145
Installing Data Protector Clients on a Veritas Cluster	148
Installing a Client.....	148
Installing Data Protector Clients on a Novell NetWare Cluster.....	149
Installing a Client.....	149

3. Maintaining the Installation

In This Chapter	154
Importing Clients to a Cell	155
Importing an Installation Server to a Cell	157
Importing Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell	158
Exporting Clients from a Cell	161
Security Considerations.....	164
The allow_hosts and deny_hosts Files.....	170
Excessive Logging to inet.log Files	170

Verifying Which Data Protector Patches Are Installed	172
Verifying Data Protector Patches Using the GUI	172
Verifying Data Protector Patches Using the CLI	173
Uninstalling Data Protector Software	175
Uninstalling a Data Protector Client	176
Uninstalling the Cell Manager and Installation Server	177
Manual Removal of Data Protector Software on UNIX	182
Changing Data Protector Software Components	183

4. Upgrading to Data Protector A.05.10

In This Chapter	188
Upgrade Overview	189
Upgrading from OmniBack II A.03.50	191
Upgrading the HP-UX Cell Manager and Installation Server	193
Upgrading the Windows Cell Manager and Installation Server	199
Checking Configuration Changes	203
Upgrading the Clients	205
Upgrading in a MoM Environment	214
Upgrading from OmniBack II A.03.51	215
Upgrading the Solaris Cell Manager and Installation Server	215
Checking Configuration Changes	222
Upgrading the Clients	223
Upgrading in a MoM Environment	232
Upgrading from OmniBack II A.04.x	233
Upgrading the HP-UX Cell Manager and Installation Server	233
Upgrading the Windows Cell Manager and Installation Server	235
Checking Configuration Changes	237
Upgrading the Clients	239
Upgrading in a MoM Environment	246
Upgrading from Data Protector A.05.00	247
Upgrading the UNIX Cell Manager and Installation Server	247
Upgrading the Windows Cell Manager and Installation Server	251
Checking Configuration Changes	253
Upgrading the Clients	255
Upgrading in a MoM Environment	257
Upgrading from the Single Server Edition	258
Upgrading from Earlier Versions of SSE to Data Protector A.05.10 SSE	258
Upgrading from Data Protector A.05.10 SSE to Data Protector A.05.10	258

Contents

Upgrading from HP-UX 10.20 to HP-UX 11.x Systems	261
Upgrading from Windows NT to Newer Version of Windows	263
OmniBack II A.03.50, A.04.x, or Data Protector A.05.00 Installed on Windows NT	263
Data Protector A.05.10 Installed on Windows NT	264
Upgrading the Cell Manager Configured on MC/ServiceGuard	265
Upgrading the Cell Manager Configured on Microsoft Cluster Server	269

5. Data Protector Licensing

In This Chapter	274
Introduction	275
Which Licenses Are Available?	276
Password Considerations	277
Data Protector Passwords	278
Obtaining a Permanent Password	279
Installing a Password on the Cell Manager	280
Finding the Number of Installed Licenses	282
Moving Licenses to Another Cell Manager System	283
Centralized Licensing	284

6. Troubleshooting Installation

In This Chapter	286
Before Calling Your Support Representative	287
Ease of Deployment	289
Verifying DNS Connections within Data Protector Cell	290
Installing and Upgrading Data Protector on Windows	293
Installing the Data Protector Cell Manager on Solaris	294
Installing UNIX Clients.	295
Remote Installation of UNIX Clients Fails	295
Problems with the Installation of an HP-UX client	295
Verifying Data Protector Client Installation	296
Troubleshooting Upgrade	298
IDB and Configuration Files Are not Available After Upgrade.	298
Upgrade of the IDB Core Part	298
Upgrade of the IDB Detail Part	299
Manual Upgrade Procedure	301
Using Log Files.	303
Data Protector Log Files.	304
Creating Installation Execution Traces	305

Debug Syntax	306
--------------------	-----

A. Appendix A

In This Appendix	A-2
Data Protector A.05.10 Product Structure and Licenses	A-3
Starter Packs	A-5
Single Drive Extensions	A-7
Functional Extensions	A-8
Single Server Editions	A-14
License Migration to Data Protector A.05.10	A-16
Support contract migration	A-16
Data Protector Cell Configurations	A-19
Data Protector Licensing Forms	A-24

B. Appendix B

In This Appendix	B-2
Setting Up the TCP/IP Protocol on Windows Systems	B-3
Installing and Configuring the TCP/IP Protocol on Windows NT Systems	B-4
Installing and Configuring the TCP/IP Protocol on Windows 2000/XP/Server 2003 Systems	B-6
Checking the TCP/IP Setup	B-8
Changing the Cell Manager Name	B-10
Changing the Default Port Number	B-12
Preparing a NIS Server	B-13
Using Tape and Robotics Drivers on Windows	B-15
Creating Device Files (SCSI Addresses) on Windows	B-19
Checking the Kernel Configuration on HP-UX	B-23
SCSI Robotic Configuration on HP-UX	B-25
Creating Device Files on HP-UX	B-30
Setting a SCSI Controller's Parameters	B-33
Finding the Unused SCSI Addresses on HP-UX	B-34
Finding the Unused SCSI Target IDs on Solaris	B-36
Command Line Changes After Upgrading to Data Protector A.05.10	B-37
Updating the Device and Driver Configuration on a Solaris System	B-59
Updating Configuration files	B-59
Creating and Checking Device Files	B-62
Finding Unused SCSI Target IDs on a Windows System	B-64
Setting SCSI IDs on an HP StorageWorks 330fx Library	B-65

Contents

Connecting Backup Devices	B-66
Connecting an HP StorageWorks 24 Standalone Device	B-70
Connecting an HP StorageWorks DAT Autoloader.....	B-71
Connecting an HP StorageWorks DLT Library 28/48-Slot.....	B-73
Connecting a Seagate Viper 200 LTO Ultrium Tape Drive	B-77
Checking the Media Agent Installation on Novell NetWare	B-80
Identifying the Storage Device.....	B-80
Testing the Media Agent Startup	B-80
Testing the HPUMA.NLM and the HPDEVBRA.NLM Startup	B-83
Installing Data Protector on Microsoft Cluster with Veritas Volume Manager....	B-86

Glossary

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
B6960-90058	August 2002	Data Protector Release A.05.00
B6960-90079	May 2003	Data Protector Release A.05.10

Conventions

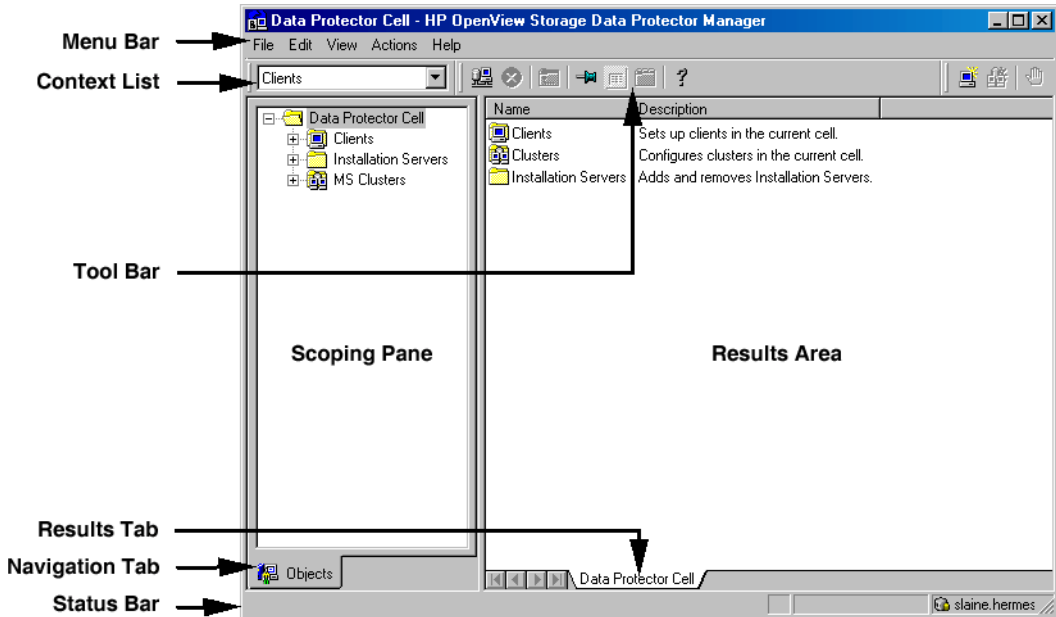
The following typographical conventions are used in this manual.

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 *HP OpenView Storage Data Protector Administrator's Guide* 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>

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 Software Release Notes*.

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 Administrator's Guide

This manual describes typical configuration and administration tasks performed by a backup administrator, such as device configuration, media management, configuring a backup, and restoring data.

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 Integration Guide

This manual describes how to configure and use Data Protector to back up and restore various databases and applications. There are two versions of this manual:

- ***HP OpenView Storage Data Protector Windows Integration Guide***

This manual describes integrations running the Windows operating systems, such as Microsoft Exchange, Microsoft SQL, Oracle, SAP R/3, Informix, Sybase, NetApp Filer, HP OpenView Network Node Manager, and Lotus Domino R5 Server.

- *HP OpenView Storage Data Protector UNIX Integration Guide*

This manual describes integrations running on the UNIX operating system, such as Oracle, SAP R/3, Informix, Sybase, NetApp Filer, IBM DB2 UDB, HP OpenView Network Node Manager, and Lotus Domino R5 Server.

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 *HP OpenView Storage Data Protector Administrator's Guide*.

HP OpenView Storage Data Protector EMC Symmetrix Integration Guide

This manual describes how to install, configure, and use the EMC Symmetrix integration. It is intended for backup administrators or operators.

It describes the integration of Data Protector with the EMC Symmetrix Remote Data Facility and TimeFinder features for Symmetrix Integrated Cached Disk Arrays. It covers the backup and restore of file systems and disk images, as well as online databases, such as Oracle and SAP R/3.

HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3, Microsoft Exchange, and Microsoft SQL.

HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array or HP StorageWorks Modular SAN Array 1000. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3, Microsoft Exchange, and Microsoft SQL.

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, HP OpenView Service Desk, 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 MPE/iX System User Guide

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

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations

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).

HP OpenView Storage Data Protector Software Release Notes

This manual gives a description of new features of HP OpenView Storage Data Protector A.05.10. 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.

Online Help

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

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 in order 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 13.
- Chapter 3** “Maintaining the Installation” on page 153.
- Chapter 4** “Upgrading to Data Protector A.05.10” on page 187.
- Chapter 5** “Data Protector Licensing” on page 273.
- Chapter 6** “Troubleshooting Installation” on page 285.
- 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 the **Media Agent** component installed. This software manages backup devices and media.

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 Software Release Notes* 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 the 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 Software Release Notes* for the supported operating system versions.

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.

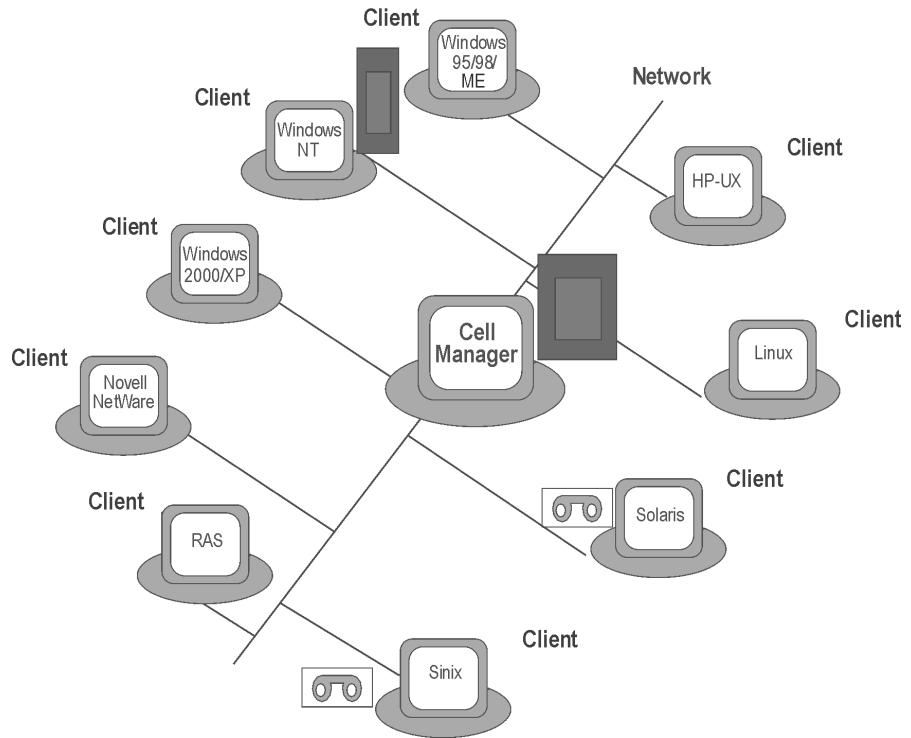
3. Installing the Installation Server(s) and the User Interface.
4. Installing client systems either remotely (recommended option, where possible), or locally from the CD-ROM.

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 CD-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 98/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 98/Me/XP HE, from an Installation Server for Windows.

Windows 98/Me/XP HE client systems must be installed locally from the Data Protector CD-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 Software Release Notes*), you can remotely install client software on HP-UX, Solaris, Sinix, Linux, AIX, and other supported UNIX operating systems.

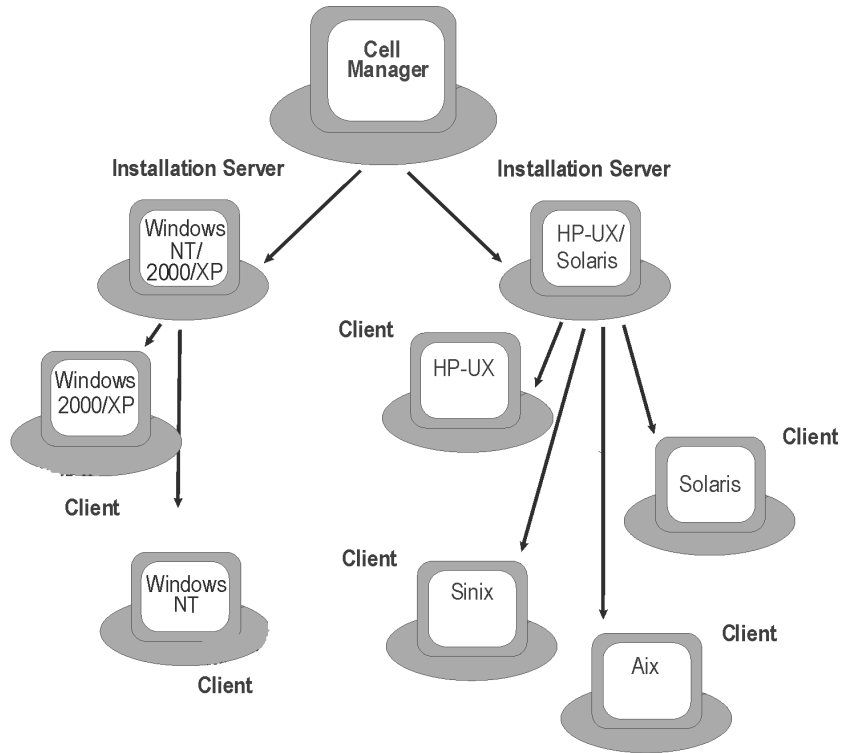
For UNIX operating systems for which remote installation is not supported, or if you do not install an Installation Server for UNIX, you can install UNIX clients locally, from the Data Protector HP-UX installation CD-ROM.

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 39.

For the procedure for installing UNIX clients locally, refer to “Local Installation of UNIX Clients” on page 108.

Figure 1-2 Data Protector Installation Concept



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 Software Release Notes* 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.

✓ IDB format

- On Windows, the IDB stores all text information in Unicode, double-byte format, which allows full support of the filenames and messages localized to other languages.
- Filenames from UNIX clients are always stored as-is and are displayed according to locale settings of the user running the GUI.

Data from Windows clients, however, can only be stored correctly for Latin 1 characters. Filenames containing other characters cannot be selected for backup or restore (but can be backed up or

restored within selectable trees). For more information, refer to the Appendix B of the *HP OpenView Storage Data Protector Software Release Notes*.

✓ Database growth and required disk space

The database on the Windows Cell Manager grows slightly faster than the database on UNIX, because information is stored in double-byte format (Unicode). This mostly concerns the information on filenames. On UNIX (HP-UX or Solaris), the database size will depend on whether single- or double-byte information is stored, the result being generally smaller than that for Windows.

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 Software Release Notes* for details 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 15.

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. Therefore, it should run on the platform that will simplify Data Protector configuration and administration tasks. For example, if you are working in a UNIX environment where files with Japanese filenames are regularly backed up and restored, this can be supported using a GUI on Solaris or HP-UX.

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.

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.

See the *HP OpenView Storage Data Protector Software Release Notes* 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 the Appendix B of the *HP OpenView Storage Data Protector Software Release Notes*.

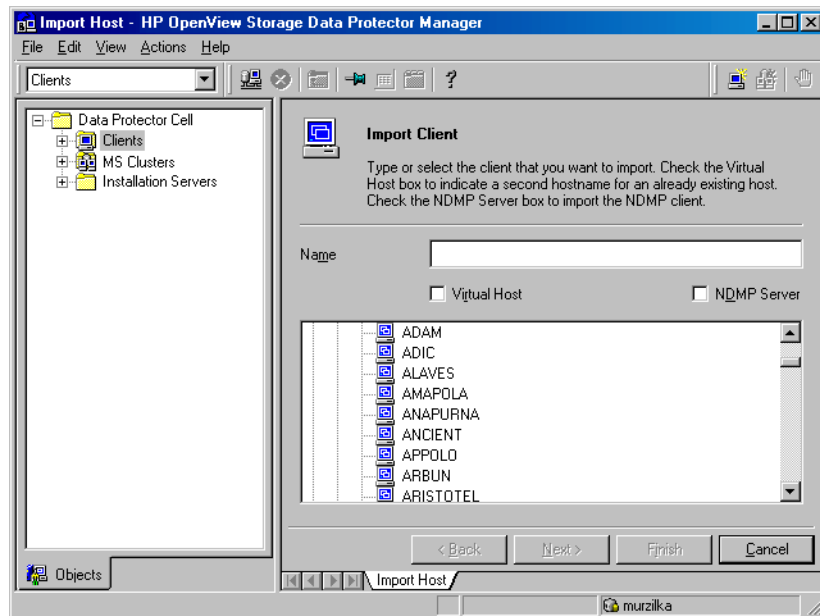
Once you have installed the user interface on a system in the cell, you can remotely access the Cell Manager from that system. You do not have to use the graphical user interface system on the Cell Manager.

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, Backup, Restore, Devices&Media, 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.

2 **Installing Data Protector on Your Network**

In This Chapter

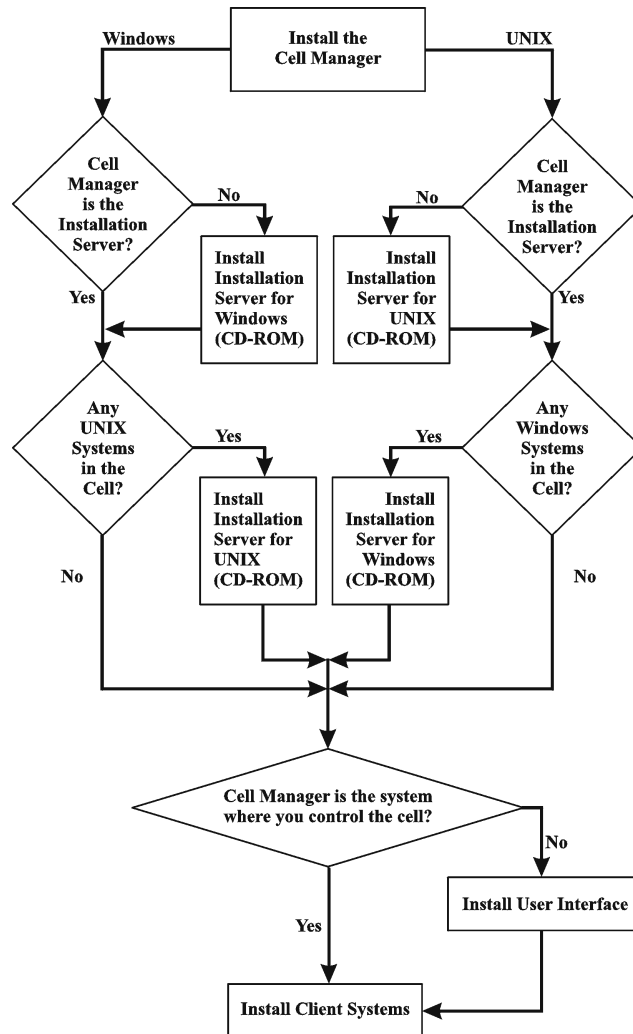
This chapter contains detailed instructions about:

- 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 15.
- Installing the Data Protector clients. Refer to “Installing Data Protector Clients” on page 39.
- Installing the localized Data Protector user interface. Refer to “Installing Localized Data Protector User Interface” on page 130.
- Installing the Data Protector Single Server Edition. Refer to “Installing the Data Protector Single Server Edition” on page 135.
- Installing Data Protector Web Reporting. Refer to “Installing Data Protector Web Reporting” on page 137.
- Installing Data Protector on MC/ServiceGuard. Refer to “Installing Data Protector on MC/ServiceGuard” on page 139.
- Installing Data Protector on a Microsoft Cluster Server. Refer to “Installing Data Protector on Microsoft Cluster Server” on page 141.
- Installing Data Protector Clients on a Veritas Cluster. Refer to “Installing Data Protector Clients on a Veritas Cluster” on page 148.
- Installing Data Protector Clients on a Novell NetWare Cluster. Refer to “Installing Data Protector Clients on a Novell NetWare Cluster” on page 149.

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.

Installing a UNIX Cell Manager

This section provides step-by-step instructions on how to install a UNIX Cell Manager. If you want to install the Windows Cell Manager only, refer to “Installing a Windows Cell Manager” on page 25.

Prerequisites for the UNIX Platform

The UNIX system that will become the Cell Manager must:

- ✓ Have HP-UX or Solaris operating systems installed. See the *HP OpenView Storage Data Protector Software Release Notes* for details on supported operating system versions, platforms, processors and Data Protector components.
- ✓ Have sufficient disk space for the Data Protector software. Refer to the *HP OpenView Storage Data Protector Software Release Notes* 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 page 21 and “Troubleshooting” on page 24.
- ✓ 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 Software Release Notes* for details. Note that the current IDB design allows the database binary files to be relocated if growth in database size makes it necessary. Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* for details.
- ✓ Support long filenames.
- ✓ Have the `inetd` daemon up and running.
- ✓ Have the port number 5555 (default) free. If this is not the case, refer to Appendix B, “Changing the Default Port Number” on page B-12.
- ✓ Have the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames.

- ✓ Have access to an input device that is appropriate for the type of installation media, for example, a CD-ROM drive.
- ✓ Recognize the Cell Manager, if using a NIS server. Refer to Appendix B, “Preparing a NIS Server” on page B-13.

NOTE

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

Local Installation

You install the Cell Manager locally from the CD-ROM. At this stage you must decide whether you want to have the Installation Server and the Cell Manager:

- ✓ On the same system (which is the default option on HP-UX). Follow the procedure described in the “Installing a Cell Manager on HP-UX” on page 17. Select the Installation Server software component during the procedure.
- ✓ On separate systems. Follow the procedure described in the “Installing a Cell Manager on HP-UX” on page 17. Deselect the Installation Server software component during the procedure. To install the Installation Server on a separate system, refer to “Installing Installation Servers” on page 30.

NOTE

To perform the installation, you will need either `root` access or an account with `root` capabilities.

Installing a Cell Manager on HP-UX

IMPORTANT

It is recommended that the kernel parameter `maxdsiz` (Max Data Segment Size) is set to at least 131072000 Bytes (128 MBytes). After this the kernel should be recompiled and the machine rebooted.

Follow the procedure below to install the UNIX Cell Manager (and the Installation Server, if required) on an HP-UX system:

1. Insert the HP-UX installation CD-ROM and run the `/usr/sbin/swinstall` utility.
2. In the Specify Source window, select Network Directory/CDROM, and then enter `<Mount_point>/DP-DEPOT/DP_A0510_UX11x.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-IS	Installation Server for UNIX
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.

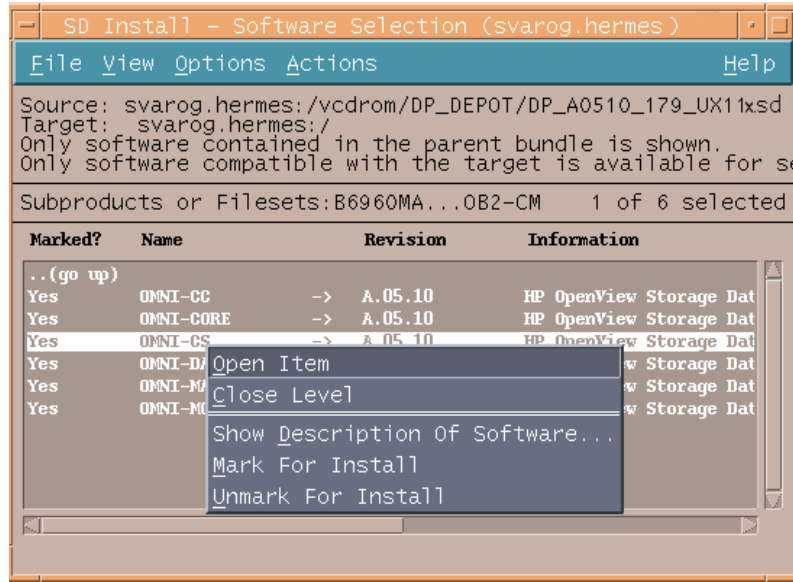
Make sure that the Marked? status value next to the OB2-CM and OB2-IS packages is set to Yes if you are installing the Cell Manager and the Installation Server for UNIX on the system. Refer to Figure 2-2.

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 2-2 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

Follow the procedure below to install the Cell Manager on a Solaris system:

1. Insert the Solaris installation CD-ROM.
2. Change to the main *<package_source>* directory, i.e. the directory that contains the installation depot file (in this case *<Mount_point>/DP-DEPOT*).

The following sub-product packages related to Cell Manager installation are included in the product:

- | | |
|----------|------------------------------------|
| OB2-CORE | Data Protector Core software. |
| OB2-C-IS | Installation Server 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	Media Agent. This is required if you want to attach a backup device to the Cell Manager.
OB2-DOCS	Data Protector online manuals.
OB2-INTEGP	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_A0510_SUN78.pkg <package_name>
```

4. Restart the Data Protector services:

```
/opt/omni/sbin/omnisv stop
```

```
/opt/omni/sbin/omnisv start
```

If you want to install an Installation Server for UNIX on your Cell Manager, you can do it at this point. Refer to “Installing the Installation Server for UNIX” on page 30 for the additional steps required.

The Installed Directory Structure

When the installation completes, the core Data Protector software is located in the `/opt/omni/bin` directory and the Installation Server for UNIX in the `/opt/omni/databases/vendor` directory. The following list shows the Data Protector subdirectories and their contents (*See the important note below if you wish to use a different directory structure*):

<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</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
<code>/var/opt/omni/db40</code>	IDB files. Refer to the <i>HP OpenView Storage Data Protector Administrator's Guide</i> for details.

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 “Troubleshooting” on page 24 for more information.

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.

HP-UX

The following files are automatically configured:

<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 <code>omni</code> variable defining: <code>omni=1.....Data Protector is automatically stopped and started at system reboot. This is the default option.</code> <code>omni=0.....Data Protector is not automatically stopped and started at system reboot.</code>

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

<code>/etc/services</code>	The Data Protector port number for the service is added to the file.
<code>/opt/omni/sbin/crs</code>	The Data Protector CRS service is added.

Solaris

The following files are automatically configured:

<code>/etc/init.d/omni</code>	A script with startup and shutdown procedures.
-------------------------------	--

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

<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.

HP-UX/Solaris

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

<code>/opt/omni/sbin/crs</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>/opt/omni/sbin/rds</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>/opt/omni/sbin/mmd</code>	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 Cell Manager described earlier also installs the Data Protector user interface.

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/bin/man` to the `MANPATH` variable

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

Also, before attempting to use the graphical user interface, please make sure that the `DISPLAY` variable is 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 Software Release Notes* for the limitations incurred.

Troubleshooting

You need a considerable amount of disk space to install the UNIX Cell Manager, in particular on the `/opt` directory and later on the `/var` directory where the database is stored (about 2% of the planned backup data). 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?

You should have the Cell Manager, and if you chose to have it on the same system, an Installation Server for UNIX installed at this stage. Your next tasks are:

1. To install an Installation Server for UNIX on another system, if you wish to have this. Refer to “Installing the Installation Server for UNIX” on page 30.
2. To install an Installation Server for Windows, if you wish to push install software to Windows clients. Refer to “Installing an Installation Server for Windows” on page 35.
3. To distribute the software to clients. Refer to “Installing Data Protector Clients” on page 39.

Installing a Windows Cell Manager

Prerequisites for Windows Platforms

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 Software Release Notes* 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 Software Release Notes* for details.
- ✓ Have a C: disk drive.
- ✓ Do not have any files or folders called “Program*” other than the Program Files folder on the drive on which you intend to install Data Protector.
- ✓ Have sufficient disk space (about 2% of the backed up data) for the IDB. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for details.
- ✓ Have the port number 5555 (default) free. Refer to Appendix B, “Changing the Default Port Number” on page B-12.
- ✓ 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 Appendix B, "Setting Up the TCP/IP Protocol on Windows Systems" on page B-3 for information on installation and configuration of the TCP/IP protocol.
- ✓ Have access to the input device that is appropriate for the type of installation media, for example, a CD-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 2.0 prior to installing Data Protector A.05.10. If you have an older version of Microsoft Installer, 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.

It is recommended that you upgrade your Microsoft Installer to the version 2.0 before installing Data Protector A.05.10. Consult Microsoft Support for Microsoft Installer 2.0 prerequisites on the various Windows operating systems.

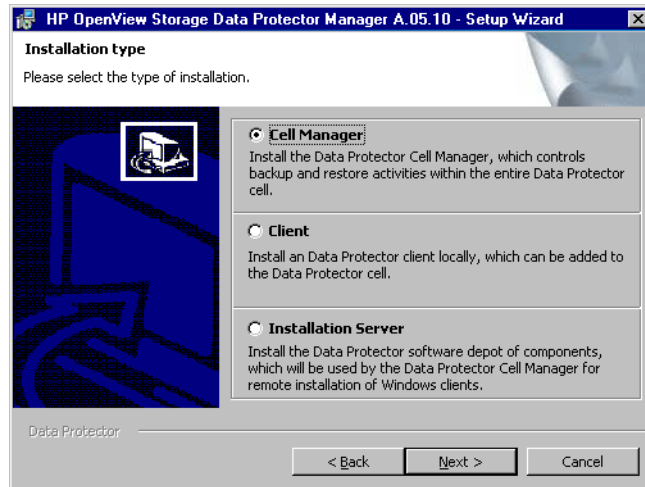
Local Installation

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

1. Insert the Windows installation CD-ROM and run `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.

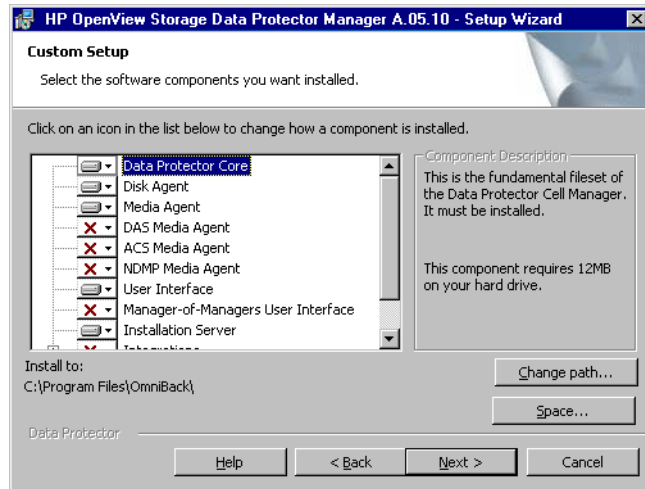
3. You may enter your name and the name of your organization. Click Next to continue.
4. In the Installation Type page, select Cell Manager and then click Next to install Data Protector Cell Manager software.

Figure 2-3 Selecting the Installation Type



5. In the Custom Setup window, select the components you want to install.

Figure 2-4 **Selecting Software Components**



Data Protector Core, Disk Agent, Media Agent, User Interface, and Installation Server are selected by default.

IMPORTANT

The Data Protector Core component cannot be unselected, as it contains the files needed for Data Protector to operate properly.

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 Software Release Notes* for the limitations incurred. To view the *HP OpenView Storage Data Protector Software Release Notes* online, you need Acrobat Reader 4.0 or higher.

Click Change Path to change the destination folder. Note that you can change the destination folder only when a component to be installed is selected.

6. Click Next.
7. Click Install to start installing the selected components. This may take several minutes.

To start using Data Protector immediately after setup, select **Launch Data Protector Manager** and then click **Finish**.

After the Installation

As soon as the setup 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 <i>Cell Request Server (CRS)</i> 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 <i>Raima Database Server (RDS)</i> 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 <code>Inet</code> 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 Software Release Notes* for the limitations incurred.

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 for Windows Platforms” on page 25.

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?

You should have the Cell Manager and Installation Server for Windows installed at this stage. Your next tasks are:

1. To install the Installation Server for UNIX on an HP-UX or Solaris system, if you have a mixed backup environment. Refer to “Installing Installation Servers” on page 30. Skip this step if you do not need the Installation Server for UNIX.
2. To distribute the software to clients. Refer to “Installing Data Protector Clients” on page 39.

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 Software Release Notes* for details on supported operating systems for the Installation Server.

If you want to keep the Installation Servers on systems separate from the Cell Manager you have to install the corresponding software depot locally. The detailed procedure is described in this section.

An Installation Server can also be installed on the Cell Manager at the same time as installing the Cell Manager on Windows, HP-UX, or Solaris. This procedure is described as part of the Cell Manager installation procedure. Refer to “Installing a UNIX Cell Manager” on page 16 or “Installing a Windows Cell Manager” on page 25 for details.

If you have installed a Cell Manager on any of the supported operating systems without an Installation Server, you can use the procedure in this section to add one to the Cell Manager.

Installing the Installation Server for UNIX

Prerequisites for the UNIX Platform

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

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

- ✓ Have HP-UX or Solaris operating system installed. For details on supported operating systems for the Installation Server, refer to the *HP OpenView Storage Data Protector Software Release Notes*.
- ✓ Have the `inetd` daemon up and running.
- ✓ Have the port number 5555 (default) free. This can be another port number used by the Cell Manager setup. Refer to the Appendix B, “Changing the Default Port Number” on page B-12.
- ✓ 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 Software Release Notes* for details.
- ✓ Have an input device that is appropriate for the type of installation media, for example, a CD-ROM drive.

Local Installation on HP-UX

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

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.

1. Insert the HP-UX installation CD-ROM.
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 `<Mount_point>/DP-DEPOT/DP_A0510_UX11x.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 HP-UX installation CD-ROM.

Local Installation on Solaris

To install the Installation Server for UNIX on a Solaris system:

1. Insert the Solaris installation CD-ROM.
2. Change to the main `<package_source>` directory, i.e. the directory that contains the installation depot file (in this case `<Mount_point>/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-INTEGP	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_A0510_SUN78.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	Oracle8/9 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 HP-UX installation CD-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 23 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 Software Release Notes* 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 157.

NOTE

When an Installation Server is imported, the file `/etc/opt/omni/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 35.

3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 39.

Installing an Installation Server for Windows

Prerequisites for the Windows Platforms

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 Software Release Notes* 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 Software Release Notes* for details.
- ✓ Have access to an input device that is appropriate for the type of installation media, for example, a CD-ROM drive.
- ✓ Do not have any files or folders called “Program*” other than the Program Files folder on the drive on which you intend to install Data Protector.
- ✓ 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 Appendix B, “Setting Up the TCP/IP Protocol on Windows Systems” on page B-3 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 2.0 prior to installing Data Protector A.05.10. If you have an older version of Microsoft Installer, 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.

It is recommended that you upgrade your Microsoft Installer to the version 2.0 before installing Data Protector A.05.10. 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 CD-ROM.

NOTE

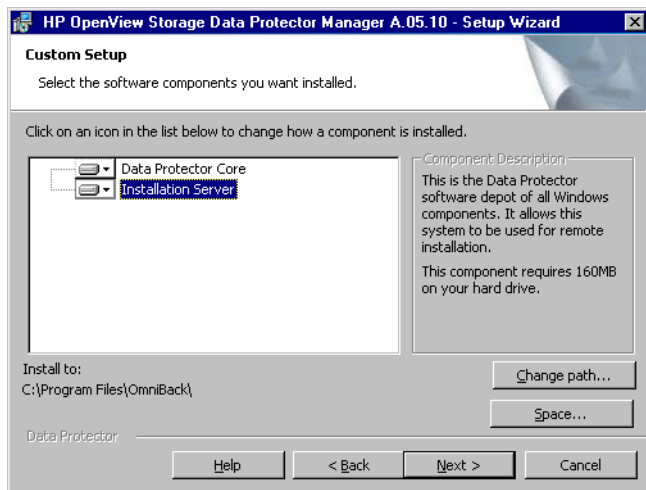
You cannot remotely install a Data Protector client on the Windows system after an Installation Server has been installed on this system. To install an Installation Server and client component(s) on the same system, you must perform a local client installation. During the installation procedure, select all desired client components and the Installation Server component. Refer to “Installing Windows Clients” on page 51.

Local Installation

Follow these steps to install the Installation Server for Windows:

1. Insert the Windows installation CD-ROM and run `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. You may enter your name and the name of your organization. Click `Next` to continue.
4. In the `Installation Type` page, select `Installation Server` and then click `Next` to install the Data Protector software depot. Click `Next`.
5. Select the components you want to install.

Figure 2-5 **Selecting Software Components**



Data Protector Core and Installation Server components are selected by default.

If you want to change the destination folder, click Change Path.

IMPORTANT

The Data Protector Core component cannot be unselected, as it contains the files needed for Data Protector to operate properly.

6. Click Next.
7. Click Install to start installing the selected components. This may take several minutes. After the installation, 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 157.

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

2. Install an Installation Server for UNIX on HP-UX or Solaris if you have a mixed backup environment. Refer to “Installing the Installation Server for UNIX” on page 30.
3. Distribute the software to clients. Refer to “Installing Data Protector Clients” on page 39.

Installing Data Protector Clients

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

After you have installed the Data Protector clients and eventually imported them into the Data Protector cell, it is highly recommended to protect clients from unwarranted access. For more information on security protection, refer to “Security Considerations” on page 164.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* for the information on supported platforms, Data Protector components, and for disk space requirements.

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

Table 2-1

Data Protector Client System Installation

Client System	Installation Type & Reference
Windows NT/2000/XP Pro/XP 64-bit Edition/Server 2003 (32 and 64-bit)	Remote and local installation; see “Installing Windows Clients” on page 51.
Windows 98/Me/XP HE	Local installation; see “Local Installation of Windows Clients” on page 57.
HP-UX	Remote and local installation; see “Installing HP-UX Clients” on page 58 and “Local Installation of UNIX Clients” on page 108.
AIX	Remote and local installation; see “Installing AIX Clients” on page 68 and “Local Installation of UNIX Clients” on page 108.
Solaris	Remote and local installation; see “Installing Solaris Clients” on page 61 and “Local Installation of UNIX Clients” on page 108.

Table 2-1 Data Protector Client System Installation

Client System	Installation Type & Reference
Tru64	Remote and local installation; see “Installing Tru64 Clients” on page 73 and “Local Installation of UNIX Clients” on page 108.
Siemens Sinix	Remote and local installation; see “Installing Siemens Sinix Clients” on page 71 and “Local Installation of UNIX Clients” on page 108.
SCO	Remote and local installation; see “Installing SCO Clients” on page 75 and “Local Installation of UNIX Clients” on page 108.
Linux	Remote and local installation; see “Installing Linux Clients” on page 78 and “Local Installation of UNIX Clients” on page 108.
DAS Agent	Remote and local installation; see “Installing the DAS Media Agent to Use the ADIC/GRAU Library” on page 83 and “Local Installation of UNIX Clients” on page 108.
ACS Agent	Remote and local installation; see “Installing the ACS Media Agent to Use the StorageTek Library” on page 89 and “Local Installation of UNIX Clients” on page 108.
Novell NetWare	Local installation; see “Local Installation of the Novell NetWare Clients” on page 92.
OpenVMS	Local installation; see “Local Installation of OpenVMS Clients” on page 99.
MPE/iX	Local installation; see “Installing MPE/iX Clients” on page 105.

Table 2-1 Data Protector Client System Installation

Client System	Installation Type & Reference
Other UNIX clients	Local installation; see “Local Installation of UNIX Clients” on page 108.

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 Integration component for backing up the MS Exchange 2000 database, Oracle8 Integration component for backing up Oracle8 database, and so on). Refer to Table 2-2 for the references.

Table 2-2 Installing Integrations

Application	Reference
MS Exchange 5.x	See “Installing MS Exchange 5.x Clients” on page 112.
MS Exchange 2000	See “Installing MS Exchange 2000 Clients” on page 113.
SQL 7.0/2000	See “Installing MS SQL 7.0/2000 Clients” on page 114.
Sybase	See “Installing Sybase Clients” on page 115.
Informix	See “Installing Informix Clients” on page 116.
SAP R/3	See “Installing SAP R/3 Clients” on page 116.
Oracle	See “Installing Oracle8/9 Clients” on page 118.
IBM DB2 UDB	See “Installing DB2 Clients” on page 119.
NNM	See “Installing NNM Clients” on page 120.

Table 2-2 **Installing Integrations**

Application	Reference
NDMP	See “Installing NDMP Integration” on page 120.
EMC Symmetrix	See “Installing EMC Symmetrix Integration” on page 121.
HP StorageWorks XP	See “Installing HP StorageWorks XP Integration” on page 122.
HP StorageWorks Virtual Array	See “Installing the HP StorageWorks Virtual Array Integration” on page 124.
HP StorageWorks Enterprise Virtual Array	See “Installing the HP StorageWorks Enterprise Virtual Array Integration” on page 125.
HP StorageWorks Modular SAN Array 1000	See “Installing the HP StorageWorks Modular SAN Array 1000 Integration” on page 126.
MS Volume Shadow Copy	See “Installing MS Volume Shadow Copy Integration” on page 127.
Lotus Domino Server	See “Installing Lotus Domino Server Clients” on page 128.

Table 2-3 **Other Installations**

Installation	Reference
Localized User Interface	See “Installing Localized Data Protector User Interface” on page 130.
Web Reporting	See “Installing Data Protector Web Reporting” on page 137.
MC/ServiceGuard	See “Installing Data Protector on MC/ServiceGuard” on page 139.
Microsoft Cluster Server	See “Installing Data Protector on Microsoft Cluster Server” on page 141.

Table 2-3 **Other Installations**

Installation	Reference
Veritas Cluster Server	See “Installing Data Protector Clients on a Veritas Cluster” on page 148
Novell NetWare Cluster	See “Installing Data Protector Clients on a Novell NetWare Cluster” on page 149

Distributing the Data Protector Software to Clients

This section describes the procedure for distributing the Data Protector software to clients using the Installation Server (remote installation or upgrade procedure), which is valid for all client platforms supporting remote installation.

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 39 and in Table 2-2 on page 41. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for the information on supported platforms, Data Protector components, and for disk space requirements.

At this point, you should have the Cell Manager and 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.

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.

Using the Data Protector GUI

Procedure

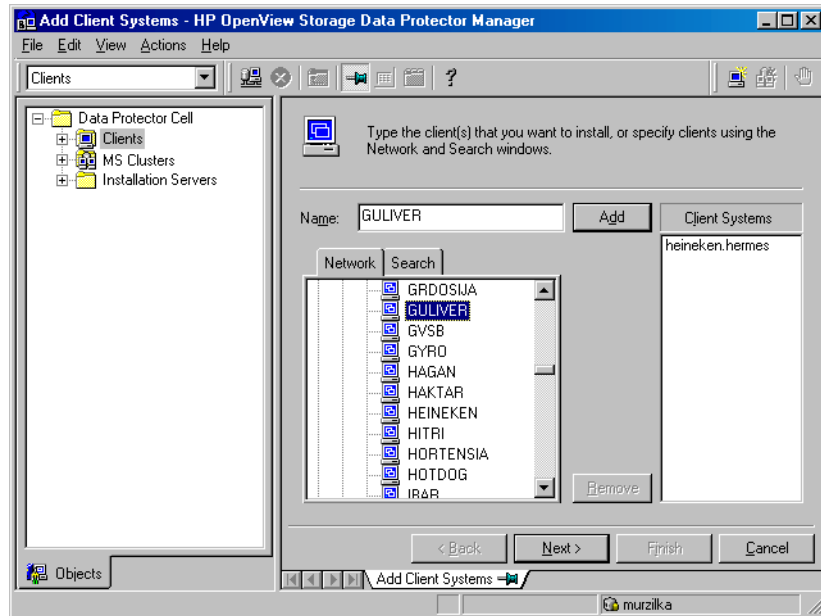
To distribute the Data Protector software to clients, follow the procedure described below:

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 *HP OpenView Storage Data Protector Administrator's Guide* or online Help for details on the Data Protector graphical user interface.

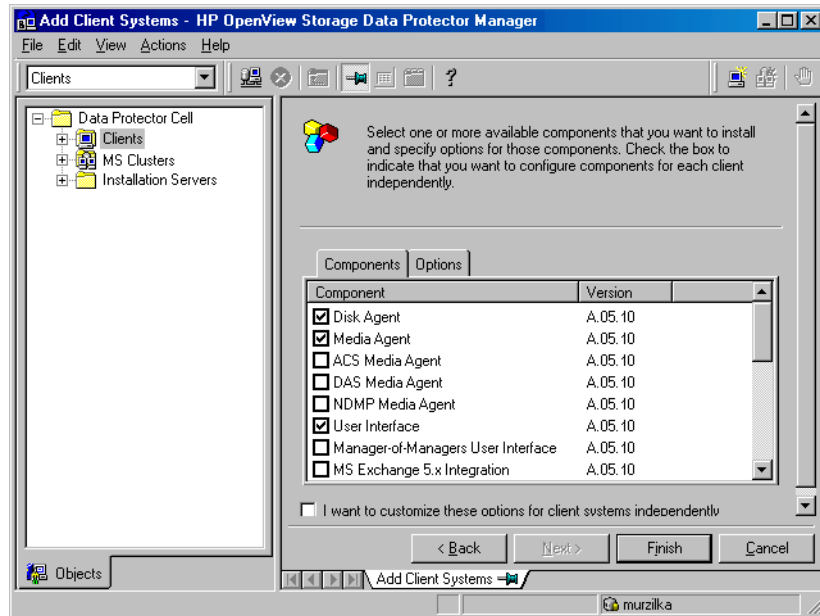
2. In the Data Protector Manager, switch to the Clients context.
3. In the Scoping Pane, right-click Clients and select Add Clients to start the wizard.
Refer to the online Help for details on each wizard page.
4. Select the client system platform (UNIX or Windows) and the Installation Server. If you have more than one Installation Server configured, a wizard page is displayed that enables you to select the Installation Server and the system platform.
5. Enter or select the client you want to install as shown in Figure 2-6.

Figure 2-6 **Selecting the Client(s)**



6. Click **Next** to proceed.
7. Select the Data Protector components you want to distribute to the Data Protector client(s). Refer to “Data Protector Components” on page 47.

Figure 2-7 Selecting the Components



8. Click the Options tab if you want to change the default user account and target directory for the components you are going to install.
9. In case you want to customize the options for each client system independently, select I want to customize this option for client systems independently and then click Next.
10. Select the components that you want installed on each client system. Click Finish to add the client to the cell.

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

NOTE

Before you can 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 *HP OpenView Storage Data Protector Administrator's Guide* or online Help.

Troubleshooting

As soon as the remote installation has finished, you can restart any failed installation procedures in the GUI by clicking *Actions, Restart Failed Clients*.

If the installation fails again, refer to Chapter 6, "Troubleshooting Installation," on page 285.

Data Protector Components

For the latest information on the supported platforms, visit the HP OpenView 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 Software Release Notes* 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.
Media Agent	The Media Agent component must be installed on clients that have backup devices connected and will be managed by Data Protector.
ACS Media Agent	The ACS Media Agent component must be installed on the systems that are directly connected to a backup drive in a StorageTek ACS library and on clients that control a StorageTek ACS library robotics.
DAS Media Agent	The DAS Media Agent component must be installed on clients that are directly connected to a backup drive in an ADIC/GRAU library and on clients that control an ADIC/GRAU library robotics
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.

Oracle8 Integration	The Oracle8 Integration component must be installed on clients that have an Oracle8/9 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.
Informix Integration	The Informix Integration component must be installed on clients that have an Informix 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 Agent	The HP StorageWorks EVA Agent component must be installed on the application and backup system to integrate HP StorageWorks Enterprise Virtual Array with Data Protector.

HP StorageWorks Modular SAN Array 1000 Agent	The HP StorageWorks Modular SAN Array 1000 Agent component must be installed on the application and backup system to integrate HP StorageWorks Modular SAN Array 1000 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 7.0/2000 database which will be backed up with Data Protector.
MS Exchange 5.x Integration	The MS Exchange 5.x Integration component must be installed on clients that have an MS Exchange 5.x database that will be backed up with Data Protector.
MS Exchange 2000 Integration	The MS Exchange 2000 Integration component must be installed on clients that have an MS Exchange 2000 database that will be backed up with Data Protector.
Cluster Integration	The Cluster Integration component must be installed on all Data Protector cluster-aware clients.
NNM 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 in the cell where an NDMP Media Agent will run, to integrate NetApp Filer or Celerra with Data Protector.

Lotus Notes Integration	The Lotus Notes Integration component must be installed on all clients in the cell that have a Lotus 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 can install only one of the following components on the same client: Media Agent, ACS Media Agent, DAS Media Agent, or NDMP Media Agent.

Installing Windows Clients

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

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 a supported Windows version installed. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for details.

Installing Data Protector Clients

- ✓ 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 Software Release Notes* for details.
- ✓ Have port number 5555 (default) free.
- ✓ Have a C: disk drive.
- ✓ Not have any files or folders called “Program*” other than the Program Files folder on the drive on which you intend to install Data Protector.
- ✓ 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 Appendix B, “Setting Up the TCP/IP Protocol on Windows Systems” on page B-3 for information on 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

On each Windows client, check if you have Microsoft Installer 2.0 prior to installing Data Protector A.05.10. If you have an older version of the Microsoft Installer, 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, you restart the installation.

It is recommended that you upgrade Microsoft Installer to the version 2.0 on each client before installing Data Protector A.05.10. Consult Microsoft Support for Microsoft Installer 2.0 prerequisites on the various Windows operating systems.

Clients with 32-bit Processors

Remote Installation

You can remotely install Windows clients that use a 32-bit processor 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 15 for instructions.

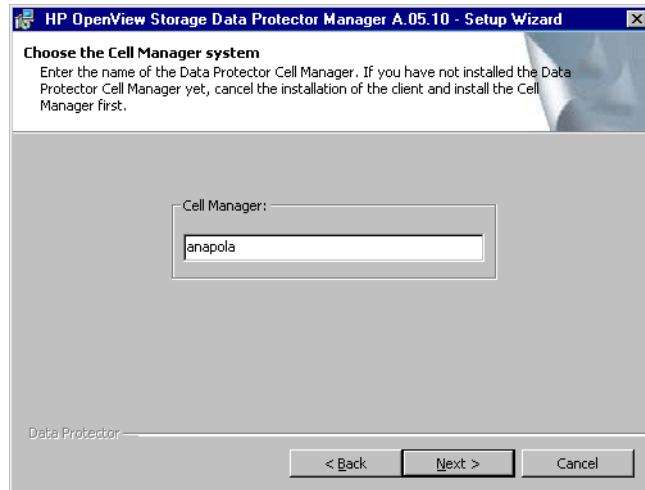
You can distribute the Windows client software from the Installation Server for Windows using the Data Protector graphical user interface. For the step-by-step procedure, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the Windows systems:

- Disk Agent** Select the Disk Agent component to be able to back up filesystem data with Data Protector.
- User Interface** Select the User Interface component if you want to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.
- Media Agent** Select the Media Agent component only if the client system has a backup device connected.
- Automatic Disaster Recovery** Select the Automatic Disaster Recovery component to provide automatic preparation of your system for disaster recovery. It 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.
- For information on other Data Protector components, refer to “Data Protector Components” on page 47.
- 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 that use 32-bit processors can also be installed locally, from the `i386` directory on the CD-ROM.

The local installation can be done as follows:

1. Insert the CD-ROM and run `i386\setup.exe`.
2. In the Installation Type page, select Client.
3. Enter the name of the Cell Manager. Refer to Figure 2-8.

Figure 2-8 Choosing the Cell Manager



4. Follow the wizard. Select the Data Protector components that you want to install. The Data Protector Core, Disk Agent, Media Agent, Installation Server, User Interface, and Languages\English are selected by default. The Data Protector Core Client component cannot be unselected, as it installs the Data Protector services on your computer.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

Clients with Itanium Processors

Remote Installation

You can remotely install clients on 64-bit Windows systems running on platforms with Itanium processors 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 15 for instructions. For details on supported platforms and components for a particular Windows operating system, refer to *HP OpenView Storage Data Protector Software Release Notes*.

You can distribute the client software from the Installation Server for Windows using the Data Protector graphical user interface. For the step-by-step procedure, refer to “Distributing the Data Protector Software to Clients” on page 43.

- Disk Agent** Select the Disk Agent component to be able to back up filesystem data with Data Protector.
- User Interface** Select the User Interface component if you want to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.
- Media Agent** Select the Media Agent component only if the client system has a backup device connected.
- 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 that use an Itanium processor can also be installed locally, from the ia64 directory on the CD-ROM.

The local installation can be done as follows:

1. Insert the CD-ROM and run ia64\setup.exe.
2. In the Installation Type page, select Client.
3. Enter the fully qualified name of the Cell Manager.
4. Follow the wizard. The Data Protector Core and Disk Agent are selected by default. These components cannot be unselected.

Clients with Alpha Processors

On computers with Alpha processors, only local Data Protector client installation is supported. To do so, insert the CD-ROM and run Alpha\setup.exe. Besides the obligatory Data Protector Core Client component, which installs Data Protector services on your computer, you can also select the Disk Agent component, which enables you to back up filesystem data using Data Protector.

Connecting a Backup Device to Windows Systems

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

Installing Data Protector Clients

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 Appendix B, “Finding Unused SCSI Target IDs on a Windows System” on page B-64.
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 Appendix B, “Using Tape and Robotics Drivers on Windows” on page B-15. For more information on creating a device filename, refer to Appendix B, “Creating Device Files (SCSI Addresses) on Windows” on page B-19.

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 *HP OpenView Storage Data Protector Administrator’s Guide* for information on configuration tasks.

Local Installation of Windows Clients

Installation Procedure

You must install the Windows 98/Me/XP HE systems locally because there is no remote installation from the Installation Server for Windows. Using the CD-ROM, proceed as follows:

1. Insert the Windows installation CD-ROM and run `\i386\setup.exe`.
2. In the Installation Type page, click Client. Click Next to proceed.
3. Follow the wizard to complete the installation. Select Data Protector Disk Agent and User Interface components. For information on other Data Protector components, refer to “Data Protector Components” on page 47.

What’s Next?

As soon as the Setup wizard has finished, the software is installed and the Data Protector services are started. You then need to manually add (import) the client system to the Data Protector cell. See “Importing Clients to a Cell” on page 155.

Installing HP-UX Clients

See the *HP OpenView Storage Data Protector Software Release Notes* for details on supported operating system versions, platforms, processors and Data Protector components.

Prerequisites

- To install an HP-UX client, you will need either *root* access or an account with *root* capabilities.
- 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 15 for instructions.
- For system requirements, disk space requirements, supported platforms and Data Protector components, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Local Installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the HP-UX installation CD-ROM. See “Local Installation of UNIX Clients” on page 108 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 “Distributing the Data Protector Software to Clients” on page 43.

Check if the components you select when installing the Data Protector software to the UNIX system are supported on HP-UX. For supported Data Protector components for a particular HP-UX version refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client.

Media Agent

Select the Media Agent component if the client system has, or will have, a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

Once you have installed the Media Agent on your client, you must physically connect the backup device to the system. You should have the appropriate device drivers, depending on the type of your device, already built in the kernel. This is why you have to check your kernel configuration first.

With remote installation using an Installation Server, as soon as the client components have been installed, the target system automatically becomes a member of the Data Protector cell.

With local installations, however, the target system has to be manually imported into the cell. See also “Importing Clients to a Cell” on page 155.

Kernel Configuration

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 Appendix B, “SCSI Robotic Configuration on HP-UX” on page B-25 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, then type `sam`.
2. In the System Administration Manager window, double-click Kernel Configuration, and then double-click 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 2-9. 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 listed if you intend to connect a tape device to the system. For example, the `stape` driver is used for generic SCSI tape drives like DLT or LTO, and the `tape2` driver is used for DDS devices.

If you will be using an HP-UX 11.00 system with a Quantum DLT 4000 device connected, we recommend using `tape2` rather than `stape`.

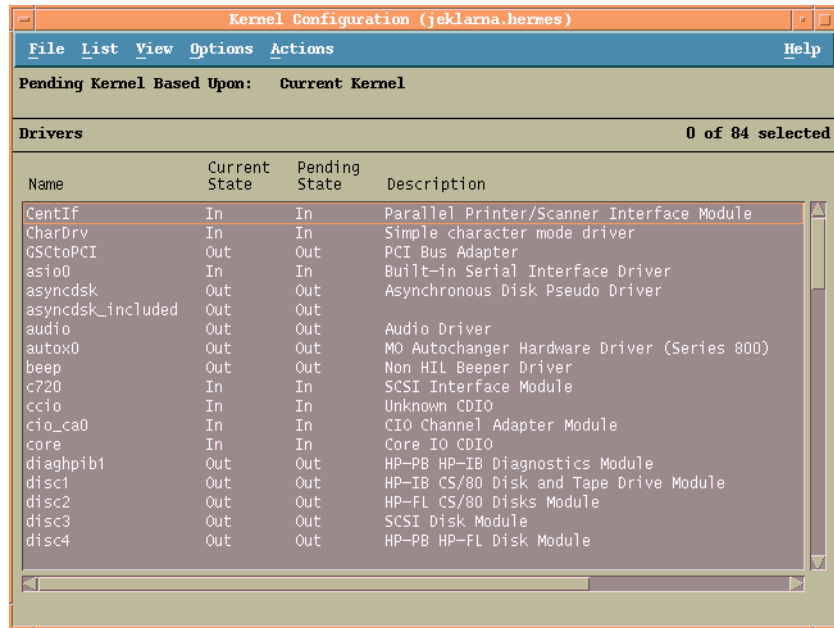
Installing Data Protector on Your Network

Installing Data Protector Clients

- 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 Appendix B, “SCSI Robotic Configuration on HP-UX” on page B-25 for details.

Figure 2-9 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:
 - a. 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 Appendix B, “Finding the Unused SCSI Addresses on HP-UX” on page B-34 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 Appendix B, “Creating Device Files on HP-UX” on page B-30.

Once the installation procedure has been completed and the backup devices have been properly connected to the system, refer to the *HP OpenView Storage Data Protector Administrator's Guide* for detailed information about configuring devices and media pools or other Data Protector configuration tasks.

Installing Solaris Clients

Prerequisites

- To install a Solaris client, you will need either *root* access or an account with *root* capabilities.

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 15 for instructions.
- For system requirements, disk space requirements, supported platforms and Data Protector components, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

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

Local Installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the HP-UX installation CD-ROM. Refer to “Local Installation of UNIX Clients” on page 108 for instructions.

Remote Installation

You can install a Solaris client by distributing the Data Protector components from the Installation Server for UNIX to the Solaris system, using the Data Protector graphical user interface.

At this point you should have the Installation Server for UNIX already installed on your system. Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

For the step-by-step procedure for distributing the software, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the Solaris system.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector graphical user interface and command-line interface on the client.

NOTE

If you install the User Interface (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 23 for more information.

If you install the User Interface on a Solaris 2.6 client, only the command-line interface will be installed.

Media Agent

Select the Media Agent component only if the client has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Post-Installation Configuration

Configuration Files

Once you have the 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.

- ✓ For DLT, DLT1, SuperDLT, LTO 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",  
"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", "SDLT-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;  
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 - II 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:

On 32 bit Solaris

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

On 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.

Installing Data Protector Clients

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
```

Installing Data Protector Clients

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/ohb` (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 *HP OpenView Storage Data Protector Administrator's Guide* for more information about configuring backup devices, media pools, or other configuration tasks.

Installing AIX Clients

Data Protector supports client systems running on the AIX platform.

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

Prerequisites

- 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 15 for instructions.
- For system requirements, disk space requirements, supported platforms and Data Protector components, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

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 Data Protector CD-ROM for UNIX. See “Local Installation of UNIX Clients” on page 108 for instructions.

Remote Installation

At this point, you must have the Installation Server for UNIX already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an AIX client system by distributing the Data Protector components from the Installation Server for UNIX to the AIX system using the Data Protector graphical user interface. For the step-by-step procedure for distributing the software, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the AIX system.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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 the 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 *HP OpenView Storage Data Protector Administrator's Guide* 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 HP-UX installation CD-ROM, or remotely using the Installation Server for UNIX.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported Siemens Sinix platform versions.

Prerequisites

- 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 15 for instructions.
- For system requirements, disk space requirements, supported platforms and Data Protector components, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Local Installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the HP-UX installation CD-ROM. See “Local Installation of UNIX Clients” on page 108 for instructions.

Remote Installation

At this point you should have the Installation Server for UNIX already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install a Sinix client by distributing the Data Protector components from the Installation Server for UNIX to the Sinix system, using the Data Protector graphical user interface. For the step-by-step procedure for distributing the software, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the Sinix system:

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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

Connecting Backup Devices to Siemens Sinix System

Once you have the 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.

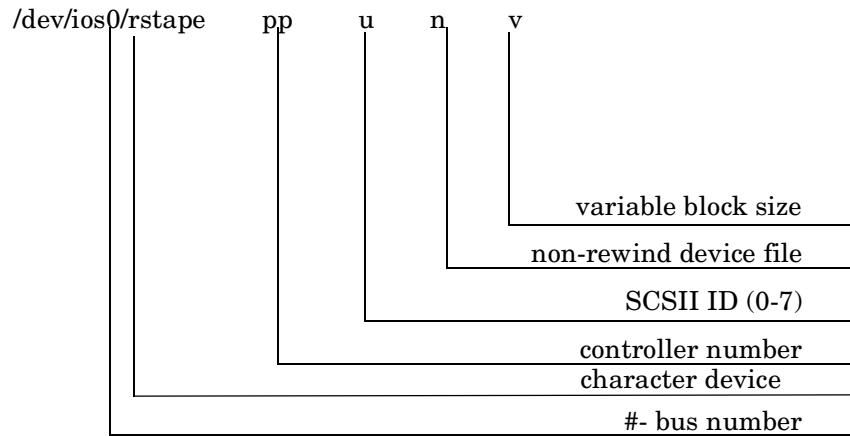
Since Data Protector can use only a character device, the letter `r` is added in front of the `stape006`.

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 2-10.

Figure 2-10

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 *HP OpenView Storage Data Protector Administrator's Guide* for information about configuring backup devices and media pools, or other configuration tasks.

Installing Tru64 Clients

Data Protector supports client systems running on the Tru64 platform.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported Tru64 platform versions and components.

Prerequisites

- 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 15 for instructions.

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

Local Installation If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the Data Protector CD-ROM for UNIX. See “Local Installation of UNIX Clients” on page 108 for instructions.

Remote Installation At this point, you must have the Installation Server for UNIX already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install a Tru64 client system by distributing the Data Protector components from the Installation Server for UNIX to the Tru64 system using the Data Protector graphical user interface. For the step-by-step procedure for distributing the software, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the Tru64 system.

Disk Agent Select the Disk Agent component to be able to back up filesystem data with Data Protector.

Media Agent The Media Agent component is needed only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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 Tru64 Client

Once you have the 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 *HP OpenView Storage Data Protector Administrator's Guide* 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 HP-UX installation CD-ROM, or remotely using the Installation Server for UNIX. See http://www.openview.hp.com/products/datapro/spec_0001.html/ for details about supported SCO platform versions.

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

Prerequisites

- 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 15 for instructions.
- For system requirements, disk space requirements, supported platforms and Data Protector components, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Local Installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the HP-UX installation CD-ROM. See “Local Installation of UNIX Clients” on page 108 for instructions.

**Remote
Installation**

At this point you should have the Installation Server for UNIX already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an SCO client system by distributing the Data Protector components from the Installation Server for UNIX to the SCO system, using the Data Protector graphical user interface. For the step-by-step procedure for distributing the software, refer to “Distributing the Data Protector Software to Clients” on page 43. Before that, note which components you select when distributing the Data Protector software to the SCO system.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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

Connecting Backup Devices to an SCO System

Once you have the 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.

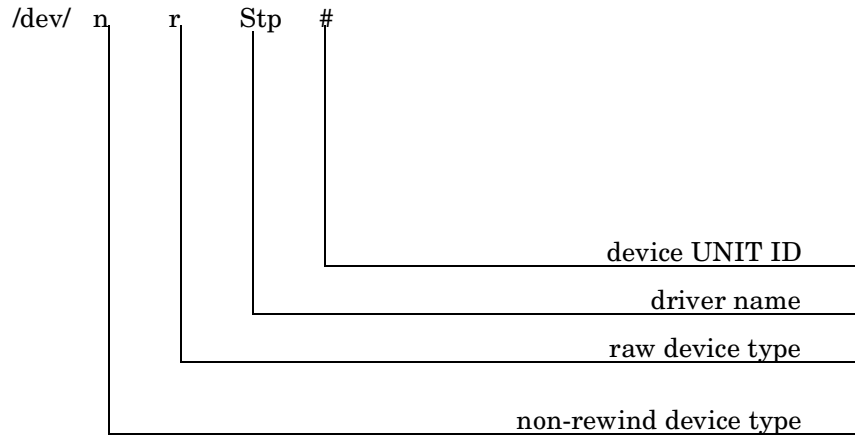
5. After you have configured the device and restarted the system, check in the `/etc/conf/cf.d/m SCSI` file if your device was connected properly.
6. Select the appropriate device filename from the `/dev` directory.
Use the `nrStp#` name, where # stands for UNIT ID of the device. The UNIT ID of the device is defined in the step 4. The `/dev/nrStp#` device filename is explained in Figure 2-11.

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 2-11

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 *HP OpenView Storage Data Protector Administrator's Guide* for information about configuring backup devices and media pools or other configuration tasks.

Installing Linux Clients

See the *HP OpenView Storage Data Protector Software Release Notes* for details on supported operating system versions, platforms, processors and Data Protector components.

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

See http://www.openview.hp.com/products/datapro/spec_0001.html/ for details about supported Linux platform versions and Data Protector components.

Prerequisites

- 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 15 for instructions.

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

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 Appendix B , “Changing the Default Port Number,” on page B-12.

Local Installation

If you do not have an Installation Server for UNIX installed in your environment, you have to perform local installation from the HP-UX installation CD-ROM. See “Local Installation of UNIX Clients” on page 108 for instructions.

Remote Installation

At this point you should have the Installation Server for UNIX already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

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 “Distributing the Data Protector Software to Clients” on page 43.

Check if the components you select when installing the Data Protector software to the UNIX system are supported on HP-UX. For supported Data Protector components for a particular HP-UX version refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component if you want to have access to the Data Protector command-line interface on the client.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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:

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 RedHat 6.1) 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 Clients” on page 108.

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 82.

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:

Installing Data Protector Clients

- 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.
- 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 the 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 *HP OpenView Storage Data Protector Administrator's Guide* for information about configuring backup devices and media pools, or other configuration tasks.

Installing the DAS Media Agent to Use the ADIC/GRAU Library

Data Protector provides a dedicated ADIC/GRAU library policy used to configure an ADIC/GRAU library. Install the Data Protector DAS Media Agent component on every system that will be physically connected to a drive in the ADIC/GRAU library and, in case of a multihost configuration, on the systems that control the ADIC/GRAU library robotics. Note that a multihost configuration is a configuration where the library and drive are not connected to the same computer.

For supported operating systems and platforms for DAS Media Agent, refer to *HP OpenView Storage Data Protector Software Release Notes*.

NOTE

You need special licenses, depending on the number of drives and slots used in the ADIC/GRAU library. Refer to Chapter 5, “Data Protector Licensing,” on page 273 for more information.

The DAS Agent includes standard Media Agent functionality; thus the Media Agent must not be installed over an existing DAS Agent.

**Connecting
Library Drives**

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

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

See “Installing HP-UX Clients” on page 58 for information about how to physically attach a backup device to a UNIX system.

See “Installing Windows Clients” on page 51 for information about how to physically attach a backup device to a supported Windows system.

**Preparing for
Installation**

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

- 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 with the DAS Media Agent installed must be defined.

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))
```

These names must be configured on each Data Protector DAS Media Agent client as the omnirc variable `DAS_CLIENT`. The omnirc file is either the `<Data_Protector_home>\omnirc` file (on Windows) or the `/opt/omni.omnirc` file (on UNIX). For example, on the system with an IP address 19.18.17.15, the appropriate line in the omnirc file is `DAS_CLIENT=DP_C1`.

- 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 2000/XP/Server 2003.

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

Prerequisites

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

- ✓ The ADIC/GRAU library must be configured and running. See the documentation that comes with the ADIC/GRAU library.

Installing Data Protector Clients

- ✓ Data Protector must be installed and configured. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15 in this chapter.
- ✓ DAS server must be up and running and DAS clients must be properly configured.

To control the ADIC/GRAU library, the DAS software is required. It consists of a DAS server and multiple DAS clients. 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 DAS 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.

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 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 the DAS 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 61.

- A list of SCSI addresses for the drives, if you want to install DAS 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 55.

**Remote
Installation**

The installation procedure consists of the following steps:

1. Distribute the DAS Media Agent component to clients using the Data Protector graphical user interface and Installation Server. See “Distributing the Data Protector Software to Clients” on page 43 in this chapter.
2. Install the ADIC/GRAU library:
 - On Windows, 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.)

Installing Data Protector Clients

- 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 `Services (Windows NT)` or `Administrative Tools, Services (other Windows systems)` 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 `Services (Windows NT)` or `Administrative Tools, Services (other Windows systems)` and check the status of the services).
- On an HP-UX system, copy the `libaci.sl` shared library into the `<Data_Protector_home>/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 `<Data_Protector_home>/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: `<Data_Protector_home>/lbin/devbra -dev`
- On AIX: `lsdev -C`

You should see the library drives with corresponding device files displayed in the list.

What's Next?

Once the DAS Media Agent is installed and the ADIC/GRAU library is physically connected to the system, refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information about additional configuration tasks, such as configuring backup devices and media pools.

Installing the ACS Media Agent to Use the StorageTek Library

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

The ACS Media Agent component includes the standard Data Protector Media Agent functionality; thus the Media Agent must not be installed over existing ACS software.

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 273 for more information.

Connecting Library Drives

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

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

See "Installing HP-UX Clients" on page 58 for information about how to physically attach a backup device to the system. Also see the documentation that comes with the StorageTek library.

See "Installing Windows Clients" on page 51 for information on how to physically attach a backup device to a supported Windows system. Also see the documentation that comes with the StorageTek library.

Prerequisites

The following prerequisites for installation must be met before installing the ACS 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 15.
- ✓ The following information must be obtained before you start installing the ACS Media Agent software:

- The *<hostname>* of the host where ACSLS is running.
- A list of ACS drive IDs that you want to use with Data Protector. 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, log in 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 the ACS Media Agent on 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 61.

- A list of SCSI addresses for the drives, if you want to install the ACS 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 55.

- ✓ 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>
```

Remote Installation

The installation procedure consists of the following steps:

1. Distribute the ACS Media Agent component to clients using the Data Protector graphical user interface and Installation Server for UNIX. See “Distributing the Data Protector Software to Clients” on page 43 in this chapter.
2. Start the ACS `ssi` daemon:

- On UNIX ACS clients, run the following command:

```
<Data_Protector_home>/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.

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 UNIX ACS client: /opt/omni/lbin/devbra -dev
- On Windows ACS client: <Data_Protector_home>\bin\devbra -dev

You should see the library drives with corresponding device files/SCSI addresses displayed in the list.

What's Next?

Once the ACS Media Agent is installed and the StorageTek library is physically connected to the system, refer to the *HP OpenView Storage Data Protector Administrator's Guide* 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 the Media Agent on the systems running Novell NetWare 4.x or later. For information on Data Protector components, refer to "Data Protector Components" on page 47.

Refer to http://www.openview.hp.com/products/datapro/spec_0001.html/ for details about supported devices or Novell NetWare platform versions. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for known problems and workarounds.

Prerequisites

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

- ✓ Make sure the TCP/IP transport protocol is installed and functional.
- ✓ Set the TIMEZONE variable on your Novell NetWare server:
 - On a NetWare 4.x, 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 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.

Installation

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

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

1. Run a command prompt on your Windows system and change the current path to the CD-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:

Installing Data Protector Clients

```
NWInstall <target server name> <NetWare version>  
<ALL|DA|MA> <port_number>
```

The second parameter is Novell NetWare target server version.

The third 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 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.

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. Once the files are copied, you are ready to load `HPINET.NLM`.

Before proceeding, make sure that you have the following modules loaded on your system :

- `NETDB.NLM`, `FPSM.NLM`, `TSA410.NLM`, `TSANDS.NLM`, and `CLIBAUX.NLM` on Novell NetWare 4.x
- `NETDB.NLM`, `TSAxx0.NLM` (`TSA0.NLM`, `TSA510.NLM`, `TSA600.NLM`), and `TSANDS.NLM` on Novell NetWare 5.x and 6.x

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 NetWare 6.0 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 database, complete the following steps:

1. Define the user account to be used when performing backup and restore of the NDS.
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 database:

Installing Data Protector Clients

- NDS 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 Object Name:

This is the Common Name of the user object that will be used as a valid NDS user for logging in to the NDS database when Data Protector Disk Agent performs backup or restore of the NDS. 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 Object Password:

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

If changes are made on the NDS 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 the NetWare Directory Services (NDS) 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 tree. You can download the latest versions of `TSANDS.NLM` and `SMDR.NLM` from the Web at:
http://support.novell.com/search/ff_index.htm

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 partition.

Now you have fulfilled the requirements for the backup and restore of the NDS. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* 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 Media Agent to use backup devices connected to the Novell NetWare server.

Data Protector supports the Adaptec SCSI host adapter controller and ASPI drivers, also referred to as ASPI Managers. The Data Protector Media Agent can access the desired SCSI host adapter through the ASPI interface. Therefore, you need to install the Adaptec ASPI driver and the related ASPI transport layer component.

IMPORTANT

On Novell NetWare 5.x and 6.x, only the new NWPA driver architecture is supported. You should therefore install the Adaptec ASPI driver with `.HAM` suffix and the corresponding ASPI transport layer component `NWASPI.CDM`. On the Novell NetWare 4.x, however, Data Protector also

supports the old driver architecture. If new NWPA architecture is not used, you should install the Adaptec ASPI driver with the .DSK suffix and the corresponding ASPI transport layer component ASPITRAN.DSK.

You can download the latest versions of Adaptec ASPI drivers from <http://www.adaptec.com>.

The Adaptec ASPI driver can be loaded automatically when the server is started 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 *ASPI Driver User's Guide* for a list of available options and calculation of the slot number.

Example 1

The following example shows the LOAD command in the STARTUP.NCF file on the Novell NetWare 4.x server for the AHA-2940 Adaptec ASPI driver:

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

where SLOT defines the location of the host adapter device and lun_enable is a mask that 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.

Example 2

The following example shows the LOAD command in the STARTUP.NCF file on the Novell NetWare 5.x server for the AHA-2940 Adaptec ASPI driver:

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

where SLOT defines the location of the host adapter device and lun_enable is a mask that enables scanning for specific LUNs (Logical Unit Numbers) 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.

The Media Agent configuration is now complete.

What's Next?

Once you have the Media Agent software successfully installed on the Novell NetWare platform, it is advisable to check the Data Protector Media Agent installation. See Appendix B, “Checking the Media Agent Installation on Novell NetWare” on page B-80.

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 *HP OpenView Storage Data Protector Administrator's Guide* 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, Media Agent, and the User Interface (command-line interface only) on systems running OpenVMS 7.3-1 or above. For information on Data Protector components, refer to “Data Protector Components” on page 47.

Refer to http://www.openview.hp.com/products/datapro/spec_0001.html/ for details about supported devices or OpenVMS platform versions. Refer to the *HP OpenView Storage Data Protector Software Release Notes* 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.
- ✓ 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.

- ✓ Make sure that you have access to the Data Protector installation CD-ROM containing the OpenVMS client installation package.

Installation

The installation procedure can be performed from the Data Protector Windows installation CD-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 A05.10-01 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, Media Agent, and User Interface will all be installed, or you 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 A05.10-01: HP AXPVMS Data Protector A.05.10
```

```
Copyright 2003 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 A05.10-01: HP AXPVMS Data Protector A.05.10
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$ROOT` logical name. Any other site-specific setup can be added to this command procedure.
- `SYS$STARTUP:OMNI$SHUTDOWN.COM`
This is the command procedure that shuts down Data Protector on this node.
- `OMNI$ROOT: [BIN] OMNI$STARTUP_INET.COM`
This is the command procedure that is used to start the `INET` process, which then executes the commands sent by the Cell Manager.
- `OMNI$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.

Installing Data Protector Clients

Execute this command procedure from the `login.com` procedures for all users who will use the CLI interface.

A logical name, `decc$argv_parse_style` is defined in this procedure, and your `process_parse_style` is set to `extended` to allow for case-sensitive filename parsing for ODS-5 disks.

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. 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 155:

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 useable 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

There is no need to configure the Data Protector Disk Agent on OpenVMS. 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.

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 robot device.

NOTE

This command sequence must be executed after a system boot.

For SAN attached tape libraries the `GGAn` device name from your SAN setup will be used.

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 HSJ controllers cannot be auto-configured. Use manual configuration methods to add these devices to Data Protector.

Media Agent in a Cluster

When dealing with devices attached to cluster systems:

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

Example

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

NOTE

For MSCP served tape devices in a cluster, for all tape devices connected via an HSx controller and for all tape devices connected via Fibre Channel, follow the guidelines for SAN configurations in the *HP OpenView Storage Data Protector Administrator's Guide*.

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.

What's Next?

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information on additional configuration tasks.

Installing MPE/iX Clients

Data Protector supports client systems running on the MPE/iX platform. 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 (either on HP-UX, Solaris, or Windows), the guide is available as `MPE_user.pdf` in `<Data_Protector_home>` or on the Data Protector installation CD-ROM in the `docs` directory.

Refer to “Data Protector Components” on page 47 for information about the components you need to install.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* for information about supported devices and MPE/iX platform versions.

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 of host files) is enabled.
- ✓ For disk space requirements refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Installation

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

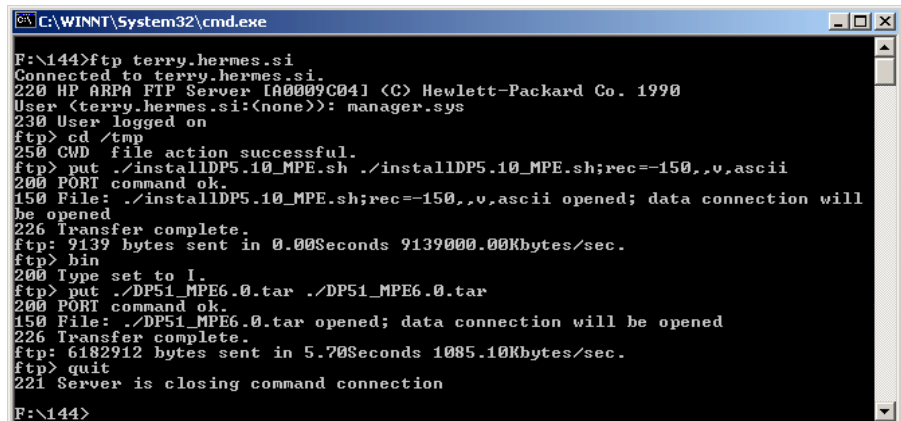
1. Transfer `installDP5.10_MPE.sh` and the `DP5.10_MPE6.0.tar` package, or `DP5.10_MPE6.5.tar` package, or `DP5.10_MPE7.0.tar` package (depending on the MPE/iX OS version) to the `/tmp` directory, using the `ftp` utility. See Example 2-1 on page 106.

It is important that you transfer the `installDP5.10_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

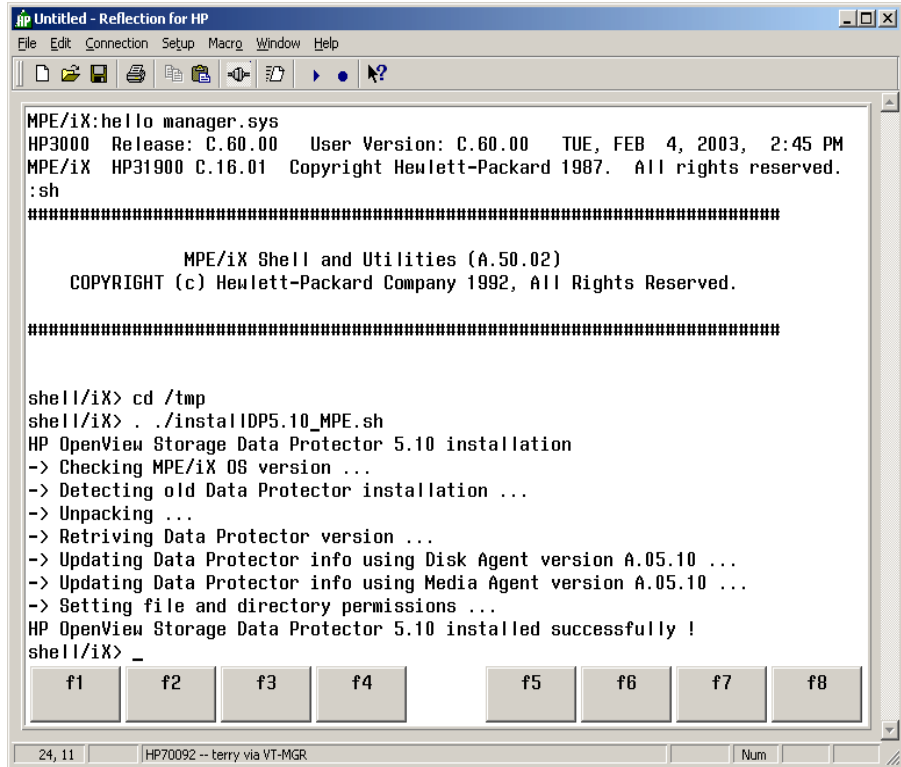
Transfer of the `installDP5.10_MPE.sh` script and `DP5.10_MPE6.0.tar` (`DP5.0_MPE6.5.tar`) package



```
C:\WINNT\System32\cmd.exe
F:\144>ftp terry.hermes.si
Connected to terry.hermes.si.
220 HP ARPA FTP Server [A0009C041] (C) Hewlett-Packard Co. 1990
User (terry.hermes.si:(none)): manager.sys
230 User logged on
ftp> cd /tmp
250 CWD file action successful.
ftp> put ./installDP5.10_MPE.sh ./installDP5.10_MPE.sh;rec=-150,,v,ascii
200 PORT command ok.
150 File: ./installDP5.10_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 ./DP51_MPE6.0.tar ./DP51_MPE6.0.tar
200 PORT command ok.
150 File: ./DP51_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



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
```

Installing Data Protector Clients

- 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 155.
- 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 CD-ROM at `\Docs\MPE_administration.pdf`.

Local Installation of UNIX Clients

For the information on supported Data Protector clients and components, disk space and system requirements refer to the *HP OpenView Storage Data Protector Software Release Notes*.

NOTE

You must have root permissions on every target system.

Local Installation

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 HP-UX installation CD-ROM.

Refer to “Data Protector Components” on page 47 for information about the components you need to install. For the information on supported Data Protector clients, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

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.

1. Insert the HP-UX installation CD-ROM.
2. From the `<Mount_Point>/LOCAL_DP_AGENT_INSTALL` directory run the following command:

```
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 where you want to install 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 the case of upgrade of 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.

Table 2-4 Data Protector Component Codes

Component Code	Component
cc	User Interface
momgui	MoM User Interface
da	Disk Agent
ma	Media Agent
das	DAS Media Agent
acs	ACS Media Agent
ndmp	NDMP Media Agent
emc	EMC Symmetrix Agent
informix	Informix Integration
lotus	Lotus Notes Integration
oracle8	Oracle8/9 Integration
sap	SAP R/3 Integration
ov	HP OpenView Network Node Manager
omnist	OmniStorage Integration
sybase	Sybase Integration
sap	SAP R/3 Integration

Table 2-4 Data Protector Component Codes

Component Code	Component
db2	DB2 Integration
ssea	HP StorageWorks Disk Array XP
snapa	HP StorageWorks VA
evaa	HP StorageWorks EVA
saa	HP StorageWorks Modular SAN Array 1000
fra_ls	French Language Support
jpn_ls	Japanese Language Support

Example

The example below shows how you can install the Disk Agent, 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 CD-ROM to your computer and run the installation/upgrade of UNIX clients from the hard disk, copy at least the DP_DEPOT directory and the

LOCAL_DP_AGENT_INSTALL/omnisetup.sh command. For example, if you copy installation packages to /var/dp51, DP_DEPOT must be a subdirectory of /var/dp51:

```
# pwd
/var/dp51
# ls
DP_DEPOT
omnisetup.sh
```

Installing Data Protector on Your Network

Installing Data Protector Clients

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/dp51
```

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 155. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information on additional configuration tasks.

Installing MS Exchange 5.x Clients

The MS Exchange 5.x client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an MS Exchange 5.x client system by distributing the Data Protector components from the Installation Server to the MS Exchange 5.x system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the MS Exchange 5.x client, you select the following components:

MS Exchange 5.x

Select the MS Exchange 5.x component to be able to back up the MS Exchange 5.x database with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing MS Exchange 2000 Clients

The MS Exchange 2000 client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an MS Exchange 2000 client by distributing the Data Protector components from the Installation Server to the MS Exchange 2000 system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the MS Exchange 2000 client, you select the following components:

MS Exchange 2000 Select the MS Exchange 2000 Integration component to be able to back up the MS Exchange 2000 database with Data Protector.

Disk Agent Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing MS SQL 7.0/2000 Clients

The MS SQL 7.0/2000 client system can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Limitation Only one MS SQL integration is supported on one client at the same time.

Remote Installation At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an MS SQL 7.0/2000 client system by distributing the Data Protector components from the Installation Server to the MS SQL 7.0/2000 system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the MS SQL 7.0/2000 client, you select the following components:

MS SQL 7.0/2000 Select the MS SQL 7.0/2000 Integration component to be able to back up the MS SQL 7.0/2000 database with Data Protector.

Disk Agent Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing Sybase Clients

The Sybase client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Before you start installing your integration software, ensure that your Sybase Backup Server is running.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install a Sybase client system by distributing the Data Protector components from the Installation Server to the Sybase system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the Sybase client, you select the following components:

Sybase Integration

Select the Sybase Integration component to be able to back up the Sybase database with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing Informix Clients

The Informix client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Before you start installing your integration software, ensure that your OnLine Server is running.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an Informix client by distributing the Data Protector components from the Installation Server to the Informix system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the Informix client, you select the following components:

Informix Integration

Select the Informix Integration component to be able to back up the Informix database with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing SAP R/3 Clients

The SAP R/3 client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

NOTE

The Data Protector SAP R/3 integration is 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.

**Remote
Installation**

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an SAP R/3 client system by distributing the Data Protector components from the Installation Server to the SAP R/3 system using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the SAP R/3 client, you select the following components:

**SAP R/3
Integration**

Select the SAP R/3 Integration component to be able to back up the SAP R/3 database with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector. Note that this component is required for Data Protector SAP R/3 integration.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing Oracle8/9 Clients

The Oracle8/9 client can be installed locally by using the installation media, or remotely from the Installation Server.

NOTE

On Windows systems, before you install or upgrade the Data Protector software on the Oracle8/9 Server system, stop all Oracle8 services. You can verify if the respective server is down by querying the database.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an Oracle8 client system by distributing the Data Protector components from the Installation Server to the Oracle8 system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the Oracle8 client, you select the following components:

Oracle8/9 Integration

Select the Oracle8/9 Integration component to be able to back up the Oracle8/9 database with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing DB2 Clients

The DB2 client can be installed locally by using the installation media, or remotely from the Installation Server.

Prerequisite

For a list of supported platforms for the DB2 integration, refer to *HP OpenView Storage Data Protector Software Release Notes*.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install a DB2 client system by distributing the Data Protector components from the Installation Server to the DB2 system using the Data Protector GUI. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the DB2 client, select the following components:

DB2 Integration

Select the DB2 Integration component to be able to back up DB2 database objects with Data Protector.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector GUI and the Data Protector CLI on the client system. (On HP-UX systems only; on AIX systems, only the Data Protector CLI is supported.)

Media Agent

Select the Media Agent component only if the client system has a backup device connected.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing NNM Clients

The NNM client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an NNM client system by distributing the Data Protector components from the Installation Server to the NNM system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the NNM client, select the following components:

NNM Integration

Select the NNM Integration component to be able to back up the NNM database with Data Protector.

Disk Agent

Select the Disk Agent component, which runs pre-backup and post-backup scripts used for backup purposes.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing NDMP Integration

The NDMP integration can be installed remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an NDMP client system by distributing the Data Protector components from the Installation Server to the client, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software, you select the following components:

NDMP Media Agent

Select the NDMP Media Agent component in order to integrate Data Protector with the NDMP. The NDMP Media Agent implements the NDMP client functionality. You need to install this module on all the hosts in the cell where the NDMP Media Agent will run. This module is responsible for connection to the NDMP server.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

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.

Installing EMC Symmetrix Integration

The EMC Symmetrix Agent can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an EMC Symmetrix client system by distributing the Data Protector components from the Installation Server to both the application and backup systems, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the application and backup systems, select the following components:

EMC Symmetrix Agent	Select the EMC Symmetrix Agent component in order to integrate Data Protector with EMC Symmetrix.
Disk Agent	Select the Disk Agent component to be able to back up filesystem data and disk image with Data Protector.
User Interface	Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.
Media Agent	Select the Media Agent component only on the Backup (R2) System. For information on other Data Protector components, refer to “Data Protector Components” on page 47.

NOTE

If you install the EMC Symmetrix Agent with some other integration (Oracle8, SAP R/3), make sure that you also distribute the Data Protector component specific for the particular integration to the application and backup systems.

For example, when installing EMC Symmetrix Oracle8 integration, you need to distribute the Oracle8 Integration component too. For detailed information, refer to the *HP OpenView Storage Data Protector EMC Symmetrix Integration Guide*.

What's Next?

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

Installing HP StorageWorks XP Integration

The HP StorageWorks XP Agent can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install the HP StorageWorks XP client system by distributing the Data Protector components from the Installation Server to both the application and backup systems, using the Data Protector graphical user

interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the application and backup Systems, select the following components:

- | | |
|---------------------------------|--|
| HP StorageWorks XP Agent | Select the HP StorageWorks XP Agent component in order to integrate Data Protector with HP StorageWorks XP. |
| Disk Agent | Select the Disk Agent component to be able to back up filesystem data and disk image with Data Protector. |
| User Interface | Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system. |
| Media Agent | Select the Media Agent on the backup system to back up the bulk data, whereas on the application system, it is needed to back up archive logs or to restore to the application system. |
- For information on other Data Protector components, refer to “Data Protector Components” on page 47.

NOTE

If you install the HP StorageWorks XP Agent with some other integration (MS Exchange, Oracle8, SAP R/3), make sure that you also distribute the Data Protector component specific for the particular integration to the application and backup systems.

For example, when installing HP StorageWorks XP with the Oracle8 integration, you need to distribute the Oracle8 component too. For detailed information, refer to the *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide*.

What's Next?

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

Installing the HP StorageWorks Virtual Array Integration

The HP StorageWorks Virtual Array (VA) Agent (also known as `snapa`, short for Snapshot Agent) can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an HP StorageWorks Virtual Array client system by distributing the Data Protector components from the Installation Server to both the application and backup systems, using the Data Protector graphical user interface. For the step-by-step procedure on distributing the Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the application and backup systems, select the following components:

HP StorageWorks VA Agent

Select the `HP StorageWorks VA Agent` component in order to integrate Data Protector with the HP StorageWorks Virtual Array.

Disk Agent

Select the `Disk Agent` component to be able to back up filesystem data and disk image with Data Protector.

User Interface

Select the `User Interface` component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client.

Media Agent

Select the `Media Agent` component. On the backup system, it is needed to back up the bulk data, while on the application system, it is needed to back up archive logs or to restore to the application system.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

NOTE

If you install the `HP StorageWorks VA Agent` component with some other integration (for example, Oracle8 or SAP R/3), make sure that you also distribute the Data Protector component specific for the particular integration to the application and backup systems.

For example, when installing HP StorageWorks Virtual Array with the Oracle8 integration, you need to distribute the Oracle8 Integration component too. For detailed information, refer to the *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*.

What's Next?

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

Installing the HP StorageWorks Enterprise Virtual Array Integration

The HP StorageWorks Enterprise Virtual Array (EVA) Agent (also known as evaa) can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an HP StorageWorks Enterprise Virtual Array client system by distributing the Data Protector components from the Installation Server to both the application and backup systems, using the Data Protector graphical user interface. For the step-by-step procedure on distributing the Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the application and backup systems, select the following components:

HP StorageWorks EVA Agent

Select the HP StorageWorks EVA Agent component in order to integrate Data Protector with the HP StorageWorks Enterprise Virtual Array.

Disk Agent

Select the Disk Agent component to be able to back up filesystem data and disk image with Data Protector.

User Interface

Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client.

Media Agent

Select the `Media Agent` component. On the backup system, it is needed to back up the bulk data, while on the application system, it is needed to back up archive logs or to restore to the application system.

For information on other Data Protector components, refer to “Data Protector Components” on page 47.

NOTE

If you install the `HP StorageWorks EVA Agent` component with some other integration (for example, `Oracle8` or `SAP R/3`), make sure that you also distribute the Data Protector component specific for the particular integration to the application and backup systems.

For example, when installing `HP StorageWorks Enterprise Virtual Array` with the `Oracle8` integration, you need to distribute the `Oracle8 Integration` component too. For detailed information, refer to the *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*.

What’s Next?

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

Installing the HP StorageWorks Modular SAN Array 1000 Integration

The `HP StorageWorks Modular SAN Array 1000 Agent` (also known as `saa`) can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

Remote Installation

At this point you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install an `HP StorageWorks Modular SAN Array 1000 client` system by distributing the Data Protector components from the Installation Server to both the application and backup systems, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the application and backup systems, select the following components:

- HP StorageWorks Modular SAN Array 1000 Agent** Select the HP StorageWorks Modular SAN Array 1000 Agent component in order to integrate Data Protector with the HP StorageWorks Modular SAN Array 1000.
- Disk Agent** Select the Disk Agent component to be able to back up filesystem data and disk image with Data Protector.
- User Interface** Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client.
- Media Agent** Select the Media Agent component. On the backup system, it is needed to back up the bulk data, while on the application system, it is needed to back up archive logs or to restore to the application system.
- For information on other Data Protector components, refer to “Data Protector Components” on page 47.

NOTE

If you install the HP StorageWorks Modular SAN Array 1000 Agent component with some other integration (for example, Microsoft Exchange 2000 or Microsoft SQL Server 2000), make sure that you also distribute the Data Protector component specific for the particular integration to the application and backup systems.

For example, when installing HP StorageWorks Modular SAN Array 1000 Microsoft with the Exchange 2000 integration, you need to distribute the MS Exchange 2000 Integration component too. For detailed information, refer to the *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*.

What's Next?

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

Installing MS Volume Shadow Copy Integration

The MS Volume Shadow Copy integration can be installed locally from the Windows installation CD-ROM, or remotely from the Installation Server for Windows.

[Installing Data Protector on Your Network](#)
Installing Data Protector Clients

- Prerequisite** MS Volume Shadow Copy integration is supported on Windows Server 2003 operating system.
- Remote Installation** At this point, you should have the Installation Server for Windows already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.
- You can install the MS Volume Shadow Copy integration by distributing the Data Protector components from the Installation Server to the client, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.
- When distributing the software to the VSS client, select the following components:
- VSS Integration** Select the MS Volume Shadow Copy Integration component to be able to coordinate the backup of the VSS-aware writers.
- User Interface** Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the VSS client.
- Media Agent** Select the Media Agent component only if the client has a backup device connected.
- For information on other Data Protector components, refer to “Data Protector Components” on page 47.
- What’s Next?** When the installation has been completed, refer to the *HP OpenView Storage Data Protector Windows Integration Guide* for information on configuring the integration.

Installing Lotus Domino Server Clients

The Lotus Domino Server client can be installed locally from the installation CD-ROM, or remotely from the Installation Server.

- Remote Installation** At this point, you should have the Installation Server already installed on your system. See “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

You can install a Lotus Domino Server client by distributing the Data Protector components from the Installation Server to the Lotus Domino Server system, using the Data Protector graphical user interface. For the step-by-step procedure on distributing Data Protector components, refer to “Distributing the Data Protector Software to Clients” on page 43.

When distributing the software to the Lotus Domino Server client, select the following components:

- Lotus Notes** Select the Lotus Notes Integration component to be able to back up the Lotus Domino Server database with Data Protector.
- Disk Agent** Select the Disk Agent component to be able to back up filesystem data with Data Protector.
- User Interface** Select the User Interface component to have access to the Data Protector graphical user interface and the Data Protector command-line interface on the client system.
- Media Agent** Select the Media Agent component only if the client has a backup device connected.
- For information on other Data Protector components, refer to “Data Protector Components” on page 47.
- 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.

Installing Localized Data Protector User Interface

Data Protector A.05.10 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 Software Release Notes*.

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.

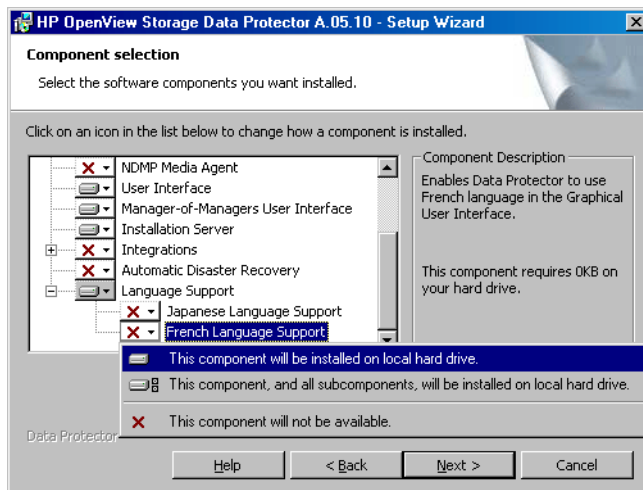
Installing Localized Data Protector User Interface on Windows Systems

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 2-12.

For the local installation procedure, refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

Figure 2-12 **Selecting Language Support at Setup**

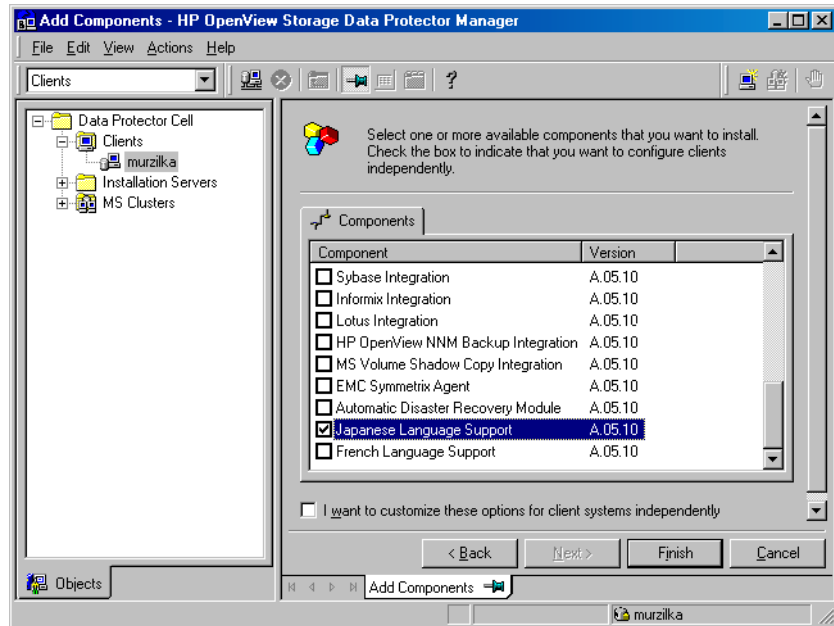


Remote Installation

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 2-13.

For the procedure on how to remotely add the Data Protector software components to clients, refer to “Distributing the Data Protector Software to Clients” on page 43.

Figure 2-13 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 Clients” on page 108.

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 2-13.

For the procedure on how to remotely add the Data Protector software components to clients, refer to “Distributing the Data Protector Software to Clients” on page 43.

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`.

Installing Localized Data Protector User Interface

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 15.

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 Software Release Notes*.

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 Software Release Notes*.

Installing a Password

For the step-by-step instructions on how to install a password on the Cell Manager, refer to “Installing a Password on the Cell Manager” on page 280.

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 Software Release Notes* 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:
`<Data_Protector_home>/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 *HP OpenView Storage Data Protector Administrator's Guide*.

What's Next?

When the installation has been completed, refer to the *HP OpenView Storage Data Protector Administrator's Guide* 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 Software Release Notes*.

If your Cell Manager is to be cluster-aware, note that the cluster package 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 15.

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 *HP OpenView Storage Data Protector Administrator’s Guide* 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 58 for detailed instructions.

What’s Next?

When the installation has been completed, you must import the application cluster package to the Data Protector cell. See “Importing Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell” on page 158.

Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* 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 Software Release Notes*.

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 under the directory specified by the user. 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.

- ✓ Setup must be started under the cluster service account on the system (node) where the *<File Share>* resource is active, so that the *<File Share>* can be directly accessed. The resource owner (the system where resource is active) can be determined using Cluster Administrator.
- ✓ 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.
- ✓ If Oracle8 is installed on cluster nodes, stop Oracle8 database services on the cluster nodes.

Local Installation

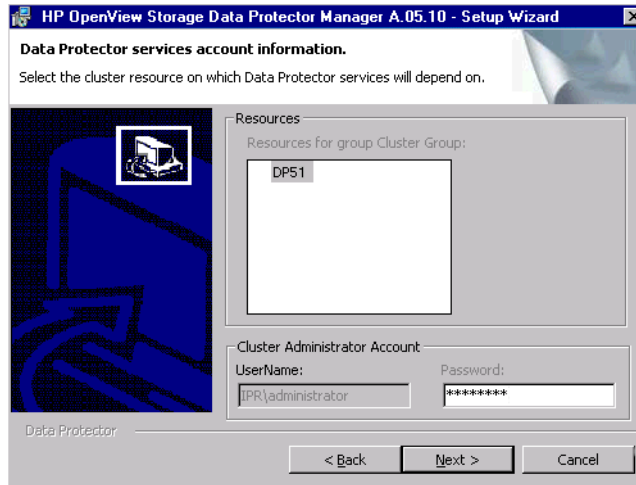
The Data Protector cluster-aware Cell Manager software must be installed locally, from the CD-ROM. This can be done as follows:

1. From the installation CD-ROM, run `\i386\setup.exe` on the active node. Accept the terms of the license agreement.
2. Enter the username and the name of organization, and select the Cell Manager type of the installation.

Setup automatically detects that it is running in a cluster environment. Click *Yes* to enable a cluster setup.

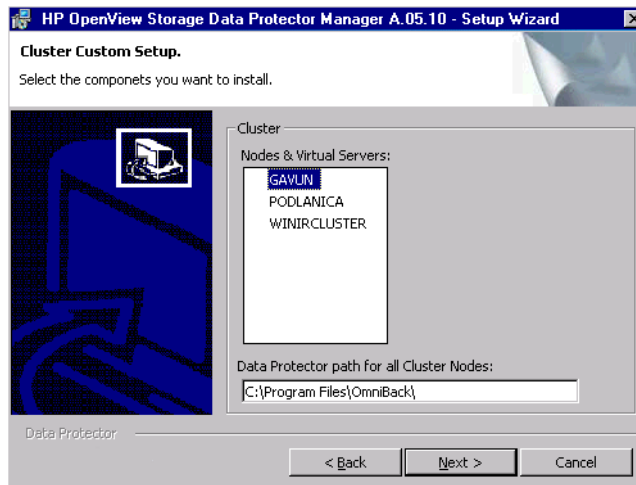
3. Follow the wizard to select the cluster group and the cluster *<File Share>* resource on which Data Protector shared files and the database will reside. Enter the Cluster Administrator Account that will be used to start Data Protector services

Figure 2-14 **Selecting the Cluster Resource**



4. Select the Data Protector Virtual Server name. Click **Next**.

Figure 2-15 **Selecting the Virtual Server Name**



5. In the Custom Setup window, select the components you want to install on all cluster nodes and cluster virtual servers. Click **Next**.

NOTE

The Cluster Integration component is selected by default.

The selected components will be installed on all the cluster nodes and virtual servers, regardless of which systems you select to add the components to.

6. Click `Install` 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. 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.

2. 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

The Data Protector cluster-aware clients must be installed locally, from the CD-ROM, on each cluster node. The cluster nodes (Data Protector cluster clients) are imported to the specified cell during the installation process.

The cluster client setup is the same as for the Windows client setup, except that the cluster Administrator account is required to perform the installation. In addition, 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 51 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 and prompts you to specify the Cell Manager (cell) for the Data Protector cluster clients to be imported to.

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.

If you want an application integration to be cluster-aware, so that it is accessible through the virtual server, the following requirements 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.
- ✓ If a system in the cluster has the Data Protector software installed, you need to uninstall it prior to the setup.
- ✓ If Oracle8 is installed on cluster nodes, stop Oracle8 database services (recommendation) on the cluster nodes.

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. Switch to the `<Data_Protector_home>\bin` directory.
2. 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 Appendix B , “Installing Data Protector on Microsoft Cluster with Veritas Volume Manager,” on page B-86, 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 Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell” on page 158.

Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* 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 61 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 Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell” on page 158.

Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* 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 6.0 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.

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 the TSA600.NLM module with the /cluster=off parameter. For more information, refer to the Novell Support Knowledge database for “Known Backup/Restore Issues for NetWare 6”.

Perform the following steps to edit the smsrun.bas script:

1. Change the write protection for the SYS:NSN/user/smsrun.bas script from read only to read/write and open it in a standard console editor.
2. Change the nlmArray = Array("SMDR", "TSA600", "TSAPROXY") line in the Sub Main() section to nlmArray = Array("SMDR", "TSA600 /cluster=off", "TSAPROXY") and 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 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 92 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 Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell” on page 158.

Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* for more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks.

Installing Data Protector on Your Network

Installing Data Protector Clients on a Novell NetWare Cluster

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 155.
- 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 157.
- How to export clients using the graphical user interface. Refer to “Exporting Clients from a Cell” on page 161.
- How to import clusters/virtual servers using the graphical user interface. Refer to “Importing Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell” on page 158.
- How to ensure security using the graphical user interface. Refer to “Security Considerations” on page 164.
- How to verify which Data Protector patches are installed. Refer to “Verifying Which Data Protector Patches Are Installed” on page 172.
- How to uninstall the Data Protector software. Refer to “Uninstalling Data Protector Software” on page 175.
- How to add or remove Data Protector software components. Refer to “Changing Data Protector Software Components” on page 183.

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 161.

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 then click **Import Client** to start the wizard. See Figure 3-1 on page 156.

NOTE

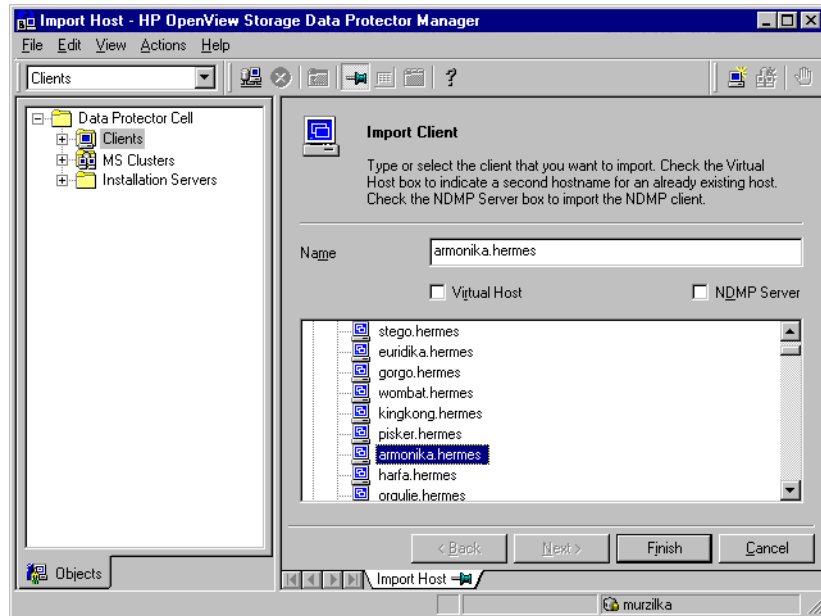
If you are importing a client configured with multiple LAN cards, check the **Virtual Host** check box in the wizard. This way you import all multiple names of the same system.

If you are importing an NDMP client system, click the **NDMP Server** check box.

If you are importing an OpenVMS client, enter the TCP/IP name of the OpenVMS client in the **Name** text-box.

3. Follow the wizard to add a system to the cell. Refer to online Help for details.

Figure 3-1 Importing a Client System to the Cell



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 `Add Installation Server` to start the wizard. See Figure 3-1 on page 156.
3. Follow the wizard to add a system to the cell. Refer to online Help for details.

Importing Cluster Virtual Server Hostnames or Application Cluster Packages to a Cell

After the local installation of Data Protector software on cluster-aware clients, you must import virtual server hostnames (Microsoft Cluster Server, Veritas Cluster and Novell NetWare 6 Cluster Services) or application cluster packages (MC/ServiceGuard) to a cell.

Before importing virtual server hostnames, make sure that:

- ✓ Data Protector clients are installed on all of the nodes (clients) in the cluster
- ✓ All cluster packages are running within the cluster

The following is an example of importing virtual server hostnames.

NOTE

The procedure for importing a Microsoft Cluster Server hostname is different from procedures on MC/ServiceGuard, Veritas Cluster and Novell NetWare 6 Cluster Services.

Microsoft Cluster Server

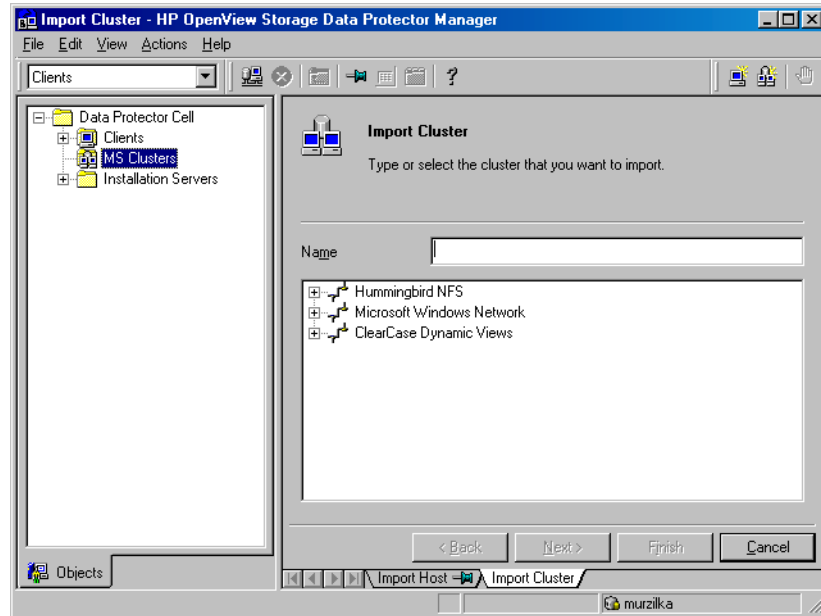
You import a Microsoft cluster/virtual server using the Data Protector GUI by performing the following steps:

1. In the Context List, click `Clients`.
2. In the Scoping Pane, right-click `MS Clusters`, and then click `Import Cluster`.
3. In the Results Area, enter the name of the virtual server or browse the network to select the cluster.

To import specific cluster nodes/virtual servers, in the Scoping Pane, double-click the specific cluster nodes or virtual server, then click the appropriate cluster node or virtual server.

4. Click `Finish`.

Figure 3-2 Importing Cluster Virtual Server Hostnames to a Cell on Microsoft Cluster Server



**MC/ServiceGuard,
Veritas and Novell
NetWare 6 Cluster
Services**

After local installation of the Data Protector software on the cluster-aware clients, if you want to configure backups of data on a shared disk, you need to import the virtual server hostname.

Before importing virtual server hostnames, make sure that Data Protector clients are installed on all of the nodes in the cluster and that all nodes are imported into the cell.

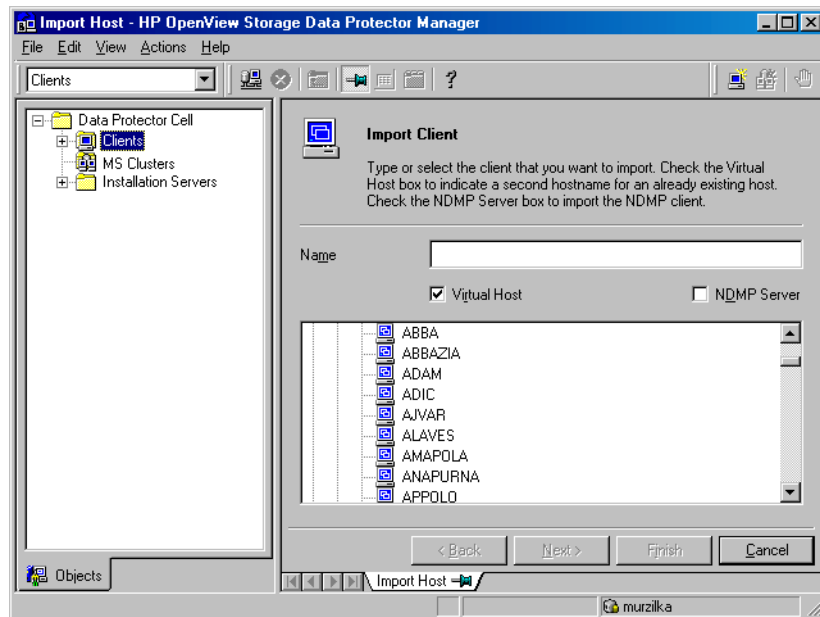
You import an MC/ServiceGuard, Veritas or Novell NetWare 6 Cluster Services cluster package/resources using the Data Protector GUI by performing the following steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients**, and then click **Import Client** to start the wizard. See Figure 3-1 on page 156.

To import an MC/ServiceGuard, Veritas or Novell NetWare application cluster package, enter the hostname for the application cluster package.

- Select the `Virtual Host` check box in the wizard to indicate that this is as an application cluster package. See Figure 3-3 on page 160.
3. Follow the wizard to import the application cluster package to the cell.

Figure 3-3 Importing an Application Cluster Package to a Cell on MC/ServiceGuard



What's Next?

If you also want to be able to configure backups of data on the local disks of the cluster nodes, you need to import the physical Data Protector clients too. For the procedure refer to “Importing Clients to a Cell” on page 155.

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:

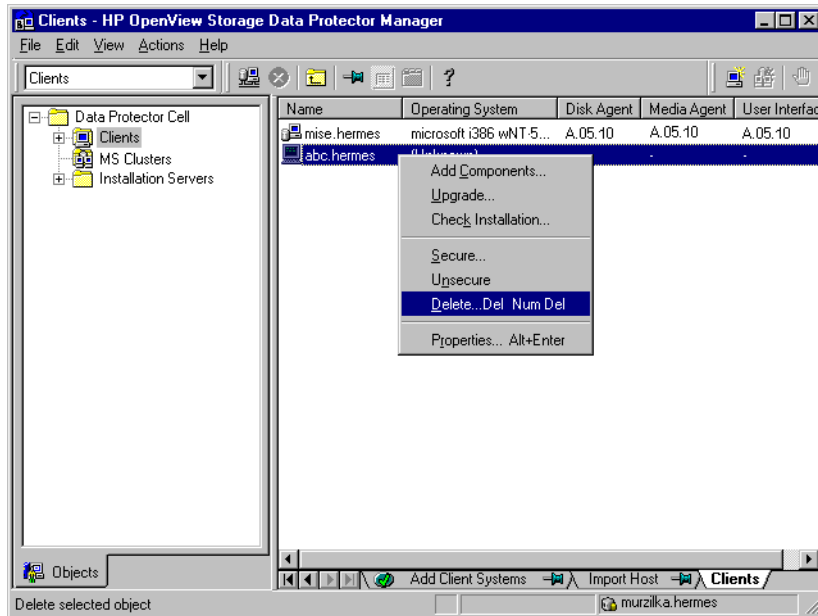
- ✓ All the occurrences of the client have been removed from backup specifications. Otherwise, Data Protector will try to back up unknown clients and this part of the backup specification will fail. Refer to online Help for instructions on how to modify backup specifications.
- ✓ The client does not 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 162.

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.

Cluster Clients

If you have clusters in your cell, you can export them by following these steps:

1. In the Context List, click Clients.
2. In the Scoping Pane, right-click MS Clusters, and then click Delete to start the wizard. You will be asked whether you want to uninstall the Data Protector software as well.

3. Click **No** to export the cluster client, and then click **Finish**.
The cluster client will be removed from the list in the **Results Area**.

Security Considerations

Why Offer a Security Mechanism?

Data Protector offers a security mechanism that can be configured for some, or all, Data Protector clients. This mechanism allows you to specify from which Cell Manager a client can be accessed. Consequently, other Cell Managers will not be able to access such a client.

After you have installed Data Protector clients and imported them to a cell, it is highly recommended that clients be protected from access by unwanted Cell Managers.

For activities like backup and restore, starting pre- or post-execution scripts, or importing and exporting clients, the client checks whether the Cell Manager which triggers one of these tasks via the known Data Protector port (default 5555) is allowed to do so. This security mechanism instructs the client to accept such actions only from a specified Cell Manager.

Consider Exceptional Situations

Before you start limiting the access to clients, consider the following circumstances which may cause problems:

- The Cell Manager has several LAN cards and several IP addresses/hostnames.
- The Cell Manager is cluster-aware.
- The Cell Manager has moved due to disaster recovery.
- 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 which are explicitly authorized to connect as a Cell Manager to the client. To avoid failure, prepare in advance such a list of all possible valid hostnames for alternate Cell Managers.

The list should include:

- All additional hostnames (for all LAN cards) on the Cell Manager.
- All cluster nodes hostnames where the Cell Manager might failover, as well as a cluster virtual server hostname.

- The target system name to which the Cell Manager will be moved in case of a total hardware failure of the Cell Manager. This target system has to be defined in the disaster recovery strategy.
- For hosts that are allowed to access a host that controls the robotics of a library, all hosts that use the drives of that library.

IMPORTANT

If additional client names are not added to the list, then only requests from the Cell Manager defined by its own primary hostname are approved. You cannot exclude the Cell Manager from the list.

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, or clients to clients.

NOTE

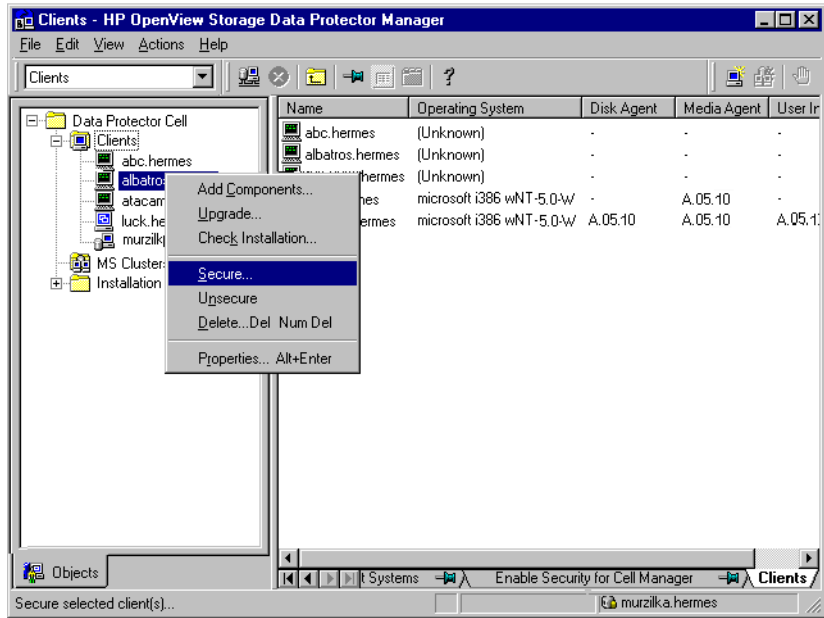
If the Installation Server residing on a system other than the Cell Manager is not added to the list of allowed hosts, it will not have access to a secured client. In this case, the operations dependent on the Installation Server (such as checking installation, adding components and removing clients)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

How to Add Security

To enable Cell Manager verification on the client side, perform the following steps in the Data Protector GUI:

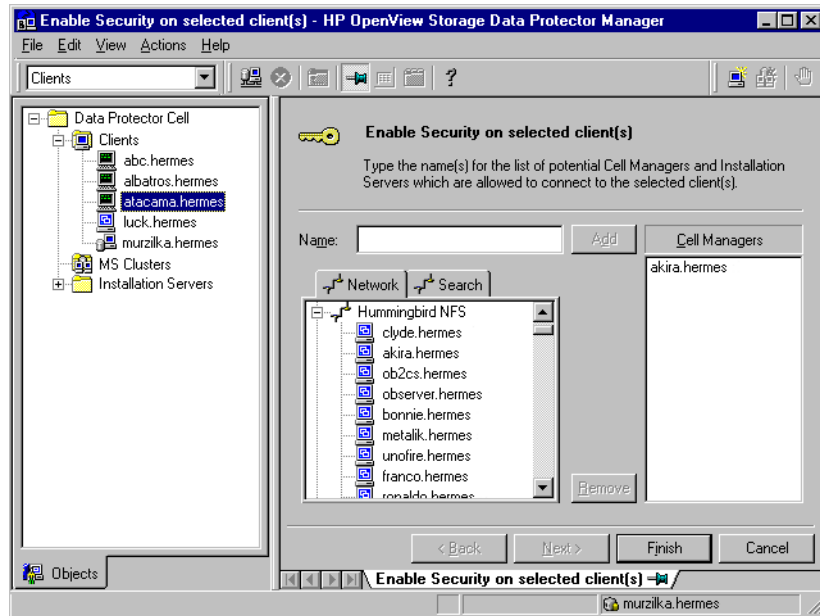
1. In the Context List, switch to the `Clients` context.
2. In the Scoping Pane, right-click the client(s) to which you want to add security, and then click `Secure`. Refer to Figure 3-5 on page 166.

Figure 3-5 **Securing a Client**



3. In the Enable Security on selected client(s) window, enter the Cell Manager(s) or clients you want to provide with access, or select them using the Network and Search tabs. See Figure 3-6 on page 167.

Figure 3-6 Enabling Security on Selected Client(s)



4. Click Add, and then click Finish.

What Happens?

Clients will verify the source for each request from other hosts and deny requests received from hosts not 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 and Solaris: `/var/opt/omni/log`

IMPORTANT

If you do not select a Cell Manager in the Enable Security for Cell Manager window and you just click Finish, your Cell Manager will be automatically provided with access and added to the Cell Managers list.

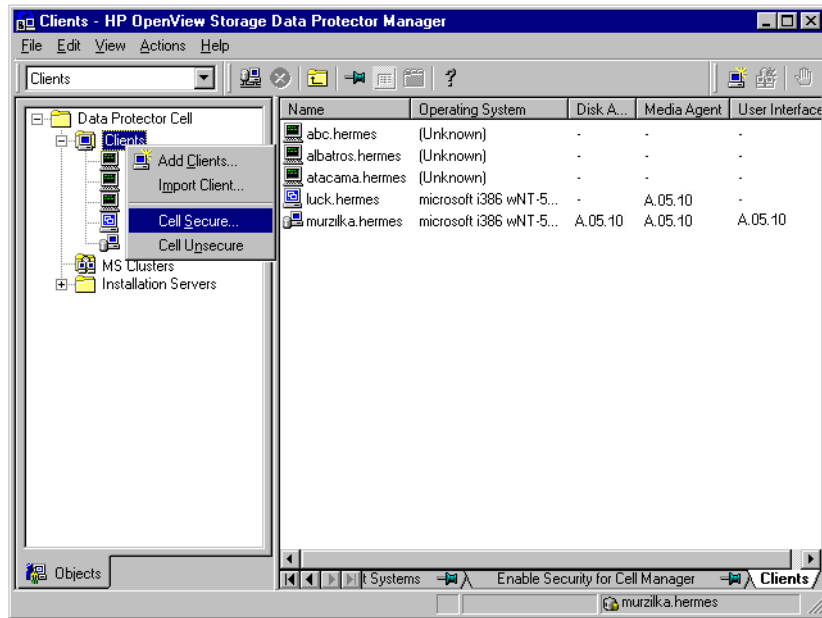
To enable security for all the clients in the cell, perform the following steps:

Maintaining the Installation

Security Considerations

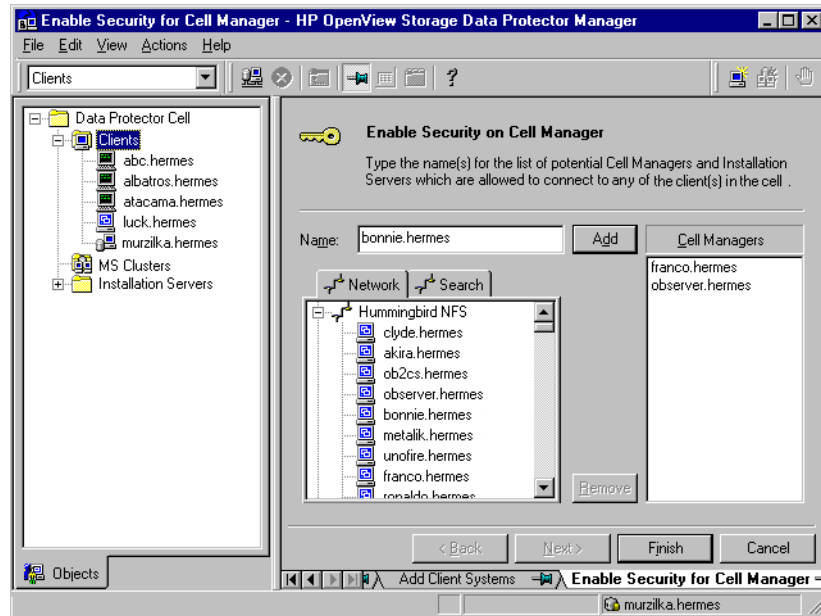
1. In the Data Protector Manager, switch to the Clients context.
2. In the Scoping Pane, expand Data Protector Cell, right-click Clients, and then select Cell Secure. Refer to Figure 3-7.

Figure 3-7 **Securing a Cell**



3. In the Enable Security on Cell Manager window, enter the Cell Manager(s) or clients you want to provide with access, or select them using the Network and Search tabs. Refer to Figure 3-8.

Figure 3-8 Enabling Security for All Clients in the Cell



4. Click Add, and then click Finish.

What Happens?

Clients will verify the source of each request and deny requests received from hosts not 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 and Solaris: `/var/opt/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 client system(s), perform the following steps:

1. In the Data Protector Manager, click Clients.
2. In the Scoping Pane, right-click the client(s) from which you want to remove security, and then 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 that are imported to the cell, proceed as follows:

1. In the Data Protector Manager, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell**, right-click **Clients**, and then click **Cell Unsecure**.
3. Click **Yes** to confirm that you allow access to all the selected client(s) in your cell.

The `allow_hosts` and `deny_hosts` Files

When you secure a client, the hostnames of the Cell Managers and clients allowed to access a client are written to the `allow_hosts` file. You can also explicitly deny access to a client from certain hosts by adding their names to the `deny_hosts` file. These files are located in the following directories:

- On Windows: `<Data_Protector_home>\Config\cell\`
- On HP-UX and Solaris: `/etc/opt/omni/cell/`
- On other UNIX systems: `/usr/omni/config/cell`

Specify each hostname on a separate line.

On Windows systems, the files are in double-byte format (Unicode), whereas on HP-UX and Solaris systems the files are in single-byte format or double-byte format (for example, Shift-JIS).

Excessive Logging to `inet.log` Files

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 hosts are allowed, but logged to the `inet.log` file.

When a client is secured, requests from the hosts listed in the `allow_hosts` file are accepted, and are thus not logged. Requests from other hosts are denied.

Securing clients can be used as a workaround to prevent unnecessary entries in `inet.log` files. However, all possible hostnames 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.

NOTE

If you accidentally lock-out a client, you can manually edit the `allow_hosts` file on this client.

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.

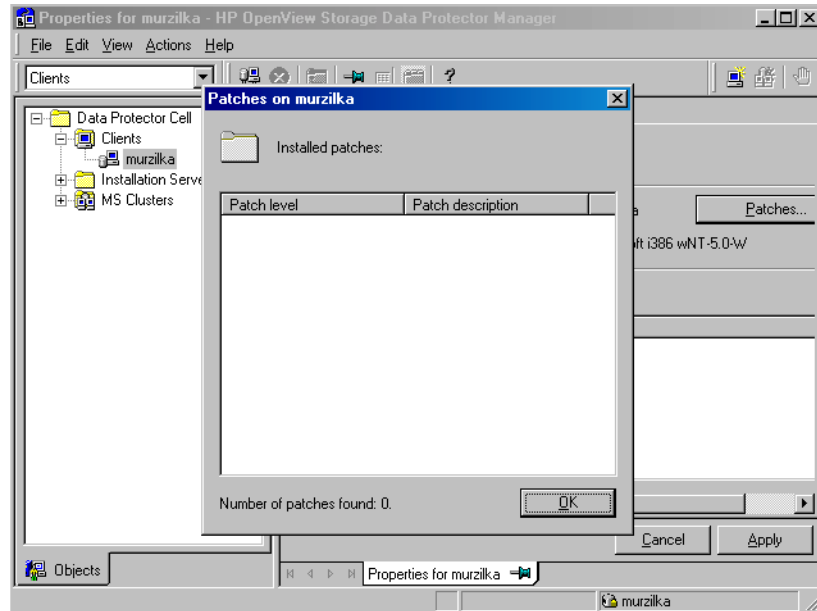
To verify which Data Protector patches are installed on a particular system in a cell, use the Data Protector GUI or CLI.

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: `/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 176.
2. Uninstalling Data Protector Cell Manager and Installation Server. See “Uninstalling the Cell Manager and Installation Server” on page 177.

You can also uninstall Data Protector software components without uninstalling the Cell Manager or client. See “Changing Data Protector Software Components” on page 183

You can also manually remove the Data Protector software. See “Manual Removal of Data Protector Software on UNIX” on page 182.

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 clusters 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 177.

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.

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 161.

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

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. Select HP OpenView Storage Data Protector A.05.10 and click Add/Remove (on Windows NT) or Remove (on other Windows systems).
4. When uninstalling is completed, click Finish to exit the wizard.

Uninstalling from HP-UX 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`.

Maintaining the Installation

Uninstalling Data Protector Software

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.

To remove the remaining Data Protector directories from your system refer to “Manual Removal of Data Protector Software on UNIX” on page 182.

Uninstalling the Cell Manager and/or Installation Server Configured on MC/ServiceGuard

If your Cell Manager and/or Installation Server is configured on an MC/ServiceGuard cluster, perform the following steps to uninstall the software.

Primary Node

Log on to the primary node and perform the following steps:

1. Stop the Data Protector package:

```
cmhaltpkg <pkg_name>
```

where `<pkg_name>` stands for the name of the cluster package.

For example:

```
cmhaltpkg ob2cl
```

2. Deactivate the cluster mode for the volume group:

```
vgchange -c n <vg_name>
```

(where `<vg_name>` stands for the path name of the volume group located in the subdirectory of the `/dev` directory).

For example:

```
vgchange -c n /dev/vg_ob2cm
```

3. Activate the volume group:

```
vgchange -a y -q y <vg_name>
```

For example:

```
vgchange -a y -q y /dev/vg_ob2cm
```

4. Mount the logical volume to the shared disk:


```
mount <lv_path> <shared_disk>
```

(where *<lv_path>* stands for the path name of the logical volume and *<shared_disk>* stands for the mount point or shared directory).

For example:

```
mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
```

5. Remove Data Protector by using the `swremove` utility.

6. Remove the soft links:

```
rm /etc/opt/omni
```

```
rm /var/opt/omni
```

7. Remove the backup directories:

```
rm -rf /etc/opt/omni.save
```

```
rm -rf /var/opt/omni.save
```

8. Remove the Data Protector directory with its contents:

```
rm -rf /opt/omni
```

9. Unmount the shared disk:

```
umount <shared_disk>
```

For example:

```
umount /omni_shared
```

10. 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.

Maintaining the Installation

Uninstalling Data Protector Software

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/var_opt_omni
```

8. Unmount the shared disk:

```
umount <shared_disk>
```

9. 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 `pkgadd` utility. Therefore, it must be uninstalled locally, using the `pkgrm` utility.

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.

Installation Server

The Installation Server for UNIX on Solaris is always installed locally, using the `pkgadd` utility. 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 161.

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 Software Release Notes*.

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 “Distributing the Data Protector Software to Clients” on page 43.

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 Windows Control Panel click Add/Remove Programs.
2. Select HP OpenView Storage Data Protector A.05.10 and click Add/Remove (on Windows NT) or Change (on other Windows systems) to open the Setup Wizard. Click Next.
3. In the Program Maintenance window, click Modify and then click Next.
4. In the Custom Setup window, select the components you want to add and/or unselect the software components you want to remove. Click Next.
5. Click Install to start the installing or removing the software components you specified in the Custom Setup window.
6. When the procedure is completed, click Finish to exit the wizard.

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	OMNI-CORE
OMNI-DAS, OMNI-ACS, OMNI-NDMP	OMNI-MA
OMNI-DAS-P, OMNI-ASC-P, OMNI-NDMP-P	OMNI-CORE-IS
OMNI-INF-P, OMNI-SYB-P, OMNI-ORA-P, OMNI-OR8-P, OMNI-SAP-P, OMNI-EMC-P, OMNI-SNAPA-P, OMNI-SSEA-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.

- 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 Oracle8/9 integration on an Oracle8/9 server system, the Oracle8/9 server software is still linked to the Data Protector Database Library. You have to remove this link, otherwise the Oracle8/9 server cannot be started after removing the integration. Refer to the *HP OpenView Storage Data Protector Integration Guide*, “Using Oracle8/9 After Removing the Data Protector Oracle8/9 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	OB2-CORE
OB2-DASP, OB2-ACSP, OB2-NDMPP	OB2-MA
OB2-SOLUX	OB2-C-IS
OB2-INFP, OB2-SYBP, OB2-OR8P, OB2-SAPP, OB2-EMCP, OB2-SNAPP, OB2-SSEAP	OB2-INTGP OB2-C-IS

Table 3-2 Data Protector Software Component Dependencies on Solaris

Components	Depend on
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>
```

4

**Upgrading to Data Protector
A.05.10**

In This Chapter

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

- How to upgrade from OmniBack II release A.03.50 to Data Protector A.05.10.
Refer to “Upgrading from OmniBack II A.03.50” on page 191.
- How to upgrade from OmniBack II release A.03.51 to Data Protector A.05.10.
Refer to “Upgrading from OmniBack II A.03.51” on page 215.
- How to upgrade from OmniBack II release A.04.x to Data Protector A.05.10.
Refer to “Upgrading from OmniBack II A.04.x” on page 233.
- How to upgrade from Data Protector release A.05.00 to Data Protector A.05.10.
Refer to “Upgrading from Data Protector A.05.00” on page 247.
- How to upgrade from the Data Protector Single Server Edition.
Refer to “Upgrading from the Single Server Edition” on page 258.
- How to upgrade from HP-UX 10.20 to HP-UX 11.x.
Refer to “Upgrading from HP-UX 10.20 to HP-UX 11.x Systems” on page 261.
- How to upgrade from Windows NT to Windows 2000/XP.
Refer to “Upgrading from Windows NT to Newer Version of Windows” on page 263.
- How to upgrade the existing product version to Data Protector A.05.10 in the MC/ServiceGuard environment. Refer to “Upgrading the Cell Manager Configured on MC/ServiceGuard” on page 265.
- How to upgrade the existing product version to Data Protector A.05.10 in the Microsoft Cluster Server environment. Refer to “Upgrading the Cell Manager Configured on Microsoft Cluster Server” on page 269.

Upgrade Overview

Before upgrading an existing product version to Data Protector A.05.10, consider the following:

- Refer to the *HP OpenView Storage Data Protector Software Release Notes* for information about supported platforms and versions.
- Perform a backup of the existing Cell Manager system and the internal database (IDB).
- 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.
- HP-UX 10.20 is no longer a supported Cell Manager platform. For the procedure on how to upgrade the OmniBack II A.03.50 or the OmniBack II A.04.x Cell Manager running on HP-UX 10.20, refer to “Upgrading from HP-UX 10.20 to HP-UX 11.x Systems” on page 261.
- If you have a permanent license for OmniBack II A.03.50, A.03.51, A.04.x, or Data Protector A.05.00, it can be used with Data Protector A.05.10.

Otherwise, be aware that you work with an Instant-On license, which will be valid for 60 days from the date of installation.

For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

Limitations

- The upgrade to Data Protector A.05.10 is only supported for OmniBack II A.03.5x, OmniBack II A.04.x, and Data Protector A.05.00.
- Changing the Cell Manager platform is not supported in the A.05.10 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 5.5 or Microsoft Exchange 2000 Server single mailbox backups is not possible after the upgrade to Data Protector A.05.10. However, you can restore the existing backups to a .pst file using a filesystem restore.

Upgrade Overview

- If you are upgrading to Data Protector A.05.10 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. However, you must restart the system for the changes to take effect, and then restart the installation. Consult Microsoft Support about the MSI 2.0 prerequisites for various Windows operating systems.

Upgrade Sequence

To upgrade your cell from the earlier versions of the product to Data Protector A.05.10, proceed as follows:

1. Upgrade the Cell Manager and Installation Server to Data Protector A.05.10. The steps are different for UNIX and Windows platforms.
2. Upgrade the GUI clients together with the Cell Manager.
3. Upgrade the clients that have an online application integration installed, such as Oracle, SAP R/3, Informix, SQL, Exchange, and other, together with the Cell Manager.
4. Upgrade the clients that have the Media Agent installed together with the Cell Manager. You can perform backups once this state is reached.
5. Upgrade the clients that have the filesystem Disk Agent installed within the next two weeks.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.05.10, 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 and restores, but other MoM functionality is not available. Note that device sharing between the Data Protector A.05.10 MoM cell and the cells with earlier versions of the product installed is not supported.

Upgrading from OmniBack II A.03.50

The OmniBack II A.03.50 release version can be directly upgraded to Data Protector A.05.10 for UNIX and Windows platforms.

Licenses

The existing OmniBack II A.03.50 licenses will remain valid after the upgrade to Data Protector A.05.10. However, some license types are not available for repurchasing, they are replaced by new licenses. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

Upgrade Sequence

For information about the upgrade sequence, refer to “Upgrade Overview” on page 189.

IDB Disk Space Requirements

A considerable amount of disk space is required for the upgrade since the old database is left on the system. That is why it is important to calculate the disk space requirements and verify that enough disk space is available.

To get the estimate of the required disk space, the following needs to be taken into account:

- The old OmniBack II A.03.50 IDB is kept throughout the upgrade process and remains unchanged.
- The new IDB will be roughly the size of the A.03.50 IDB, except that the fileversion part will be half the size of the fileversion part in the A.03.50 IDB.
- During the upgrade, the OmniBack II A.03.50 and the Data Protector A.05.10 IDBs need to be accommodated on the Cell Manager system. Once the upgrade (including the IDB detail part upgrade) is completed and the Data Protector cell is operational, the OmniBack II A.03.50 IDB can no longer be accessed.

To calculate the disk space needed for the new IDB, proceed as follows:

1. Check the size of the `/var/opt/omni/db` directory on HP-UX systems and the `<Data_Protector_home>\db` directory on Windows systems.
2. Using the `omnidbutil -extendinfo` command, check the size and location of the extension files (`fvers` and `fnames`).

If all extension files are located in the `db` directory, the size of the `db` directory is the total size of OmniBack II A.03.50 database.

If some extension files are located elsewhere, sum up the size of these files and calculate the size of OmniBack II A.03.50 database as follows:

$$\text{OldDatabaseSize} = \text{dbSize} + \text{extSize}$$

3. Subtract the size of all `fvers` extension files (`fversSize`) from the total database size to get the size of the database without file versions:

$$\text{BaseSize} = \text{OldDatabaseSize} - \text{fversSize}$$

During the core part upgrade, the IDB is upgraded without filenames and file versions. To calculate the size of the database, upgraded during the core part upgrade (`CUDatabaseSize`), subtract the size of `fnames` and `fvers` files from the total database size:

$$\text{CUDatabaseSize} = \text{OldDatabaseSize} - \text{fversSize} - \text{fnamesSize}$$

4. The size of `fvers` extension files, divided by two, is the space required for `dcbf` directories:

$$\text{DCBFSize} = \frac{\text{fversSize}}{2}$$

5. Add this number to the base database size to calculate the initial size of the A.05.10 IDB after the upgrade:

$$\text{NewDatabaseSize} = \text{BaseSize} + \text{DCBFSize}$$

6. To ensure proper usage of the disk space by Data Protector, configure the `dcbf` directories using the GUI after the core part upgrade has been finished:

- Specify the location for `dcbf` directories.
- Specify the appropriate maximum size for each `dcbf` directory.

Example

To calculate the initial size of the A.05.10 IDB on HP-UX, follow the procedure described below:

1. Suppose that the size of the `db` directory is 9,8 GB.
2. Run the `omnidbutil -extendinfo` command to get the size and location of the extension files (`fvers` and `fnames`):

```
/var/opt/omni/db/cdb/fvers.dat 2,5 GB
```

```
/var/opt/omni/db/cdb/fvers.dat1 2,5 GB
/var/opt/omni/db/cdb/fvers.dat2 2 GB
/var/opt/omni/db/cdb/fnames.dat2 2 GB
/disk/fnames.dat1 1,4 GB
```

3. The `fnames.dat1` file is not located in the `db` directory, so add its size to the size of `db` directory to get the total size of OmniBack II A.03.50 database (`OldDatabaseSize`):

$$9,8\text{GB} + 1,4\text{GB} = 11,2\text{GB}$$

4. Calculate the size of the database without file versions (`BaseSize`):

$$11,2\text{GB} - 7\text{GB} = 4,2\text{GB}$$

The size of the database, upgraded during the core part upgrade (`CUDatabaseSize`), is:

$$11,2\text{GB} - 7\text{GB} - 3,4\text{GB} = 0,8\text{GB}$$

5. Calculate the size needed for `dcbf` directories (`DCBFSize`):

$$(2,5\text{GB} + 2,5\text{GB} + 2\text{GB}) / 2 = 3,5\text{GB}$$

6. Calculate the initial size of the A.05.10 IDB (`NewDatabaseSize`):

$$4,2\text{GB} + 3,5\text{GB} = 7,7\text{GB}$$

Time Requirements

The IDB core part upgrade procedure lasts from 30 minutes to two hours depending on the database size and the system speed and load. The IDB detail part upgrade takes 3-6 hours per gigabyte of data, it can be done later, even after the cell is upgraded and some backups are performed. For the above described example, the detail part upgrade would take 18-36 hours.

Upgrading the HP-UX Cell Manager and Installation Server

Prerequisite

Stop all OmniBack II services before the upgrade procedure by running the `/opt/omni/sbin/omnisv.sh -stop` command.

NOTE

You must have root permissions to perform the upgrade.

Upgrading the HP-UX Cell Manager

The HP-UX Cell Manager is upgraded automatically when the `omnisetup.sh` command is run. This command removes the existing package set using the `swremove` utility and installs the `OMNI-CORE`, `OMNI-CC`, `OMNI-CS`, `OMNI-DA`, and `OMNI-MA` packages using the `swinstall` utility. If the Installation Server is present, it is upgraded as well. The detailed steps you need to follow when upgrading the HP-UX Cell Manager are described in “Step-by-Step Upgrade Procedure” on page 196.

Database Upgrade The old database remains in the `/var/opt/omni/db` folder. However, old `/var/opt/omni/db/catalog` is moved to `/var/opt/omni/db/catalog.OLD`. The new database is installed in the `/var/opt/omni/db40` folder. The database upgrade consists of:

1. Upgrading of the core part of the IDB.
2. Upgrading of the detail part of the IDB.

IDB Core Part Upgrade

The IDB core part upgrade procedure, which transfers vital data from the old to the new database, is started unconditionally as a part of the upgrade when the `omnisetup.sh` command is run. The entire MMDB, as well as the session information part, is transferred. However, session messages, filenames, and file versions are not transferred during the core part upgrade.

After the database core part upgrade, all the Data Protector functionality is available, except for browsing of single files and directories. Refer to Table 4-1 on page 195.

IDB Detail Part Upgrade

The IDB detail part upgrade procedure is started by running the `/opt/omni/bin/xomnidbupg` command. The process goes over all detail catalogs and imports the data into the A.05.10 IDB. During the upgrade, the session messages are also imported. At the same time, the obsolete sessions (which media have either been overwritten or exported) are removed. The catalogs belonging to unprotected objects (the objects that

do not have protected copies) are also skipped from the upgrade. The number of skipped (not upgraded) objects is reported in the `upgrade.log` file residing in the `/var/opt/omni/log` directory.

During the detail part upgrade, you can perform backup, restore, and media management operations; however, some limitations need to be considered. Refer to Table 4-1 on page 195 for details.

The upgrade will be suspended while backup, restore or media management operations are running.

The detail part upgrade wizard displays the progress status, as well as time and size estimates.

The detail part upgrade procedure is recoverable. If the system fails at any stage or if Data Protector shuts down, the upgrade is resumed automatically when the services are restarted.

The following table presents the Data Protector functionality available after the upgrade.

Table 4-1

Upgrade of the A.03.50 IDB - Core and Detail Part

IDB Upgrade	What Is Upgraded	Data Protector Behavior
Upgrade of the core part	The IDB without file versions, filenames and session messages	All functionality available except for browsing of single files and directories.
Upgrade of the detail part	The whole IDB except for obsolete sessions and the catalogs that belong to unprotected objects	All functionality available except for filename purge. Browsing of objects that reside on tapes that have not been upgraded yet, will not work or will work partially. Tapes with detail catalogs that have not been upgraded yet will not be allocated for appended backups.

MC/ServiceGuard The upgrade procedure for the Cell Manager, configured on MC/SG, is different 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 265.

Upgrading the HP-UX Installation Server

In the following cases, the HP-UX Installation Server is upgraded automatically when the `omnisetup.sh` command is run:

- If it is installed together with the Cell Manager.
- If it is installed without client components.

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 157.

Step-by-Step Upgrade Procedure

Prerequisite

It is recommended that the kernel parameter `maxdsiz` (Max Data Segment Size) be set to at least 131072000 bytes (128 MBytes). After setting this parameter, recompile the kernel and restart the machine.

To upgrade the HP-UX Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert and mount the HP-UX installation CD-ROM to a mount point, for example:

```
mkdir /cdrom
mount /dev/cd0 /cdrom
```

If you want to have on your local disk the `DP_DEPOT` directory, where the installation files are stored, run the following command:

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
```

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

```
cp -r /cdrom <cd_image_dir>
```

2. Run the `./omnisetup.sh` command. To run this command from the CD-ROM, execute:

```
cd /cdrom/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

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 CD-ROM to *<cd_image_dir>*, run the omnisetup.sh command without any parameters:

```
cd <cd_image_dir>/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

Refer to the omnisetup.sh man page for a description of the omnisetup.sh command.

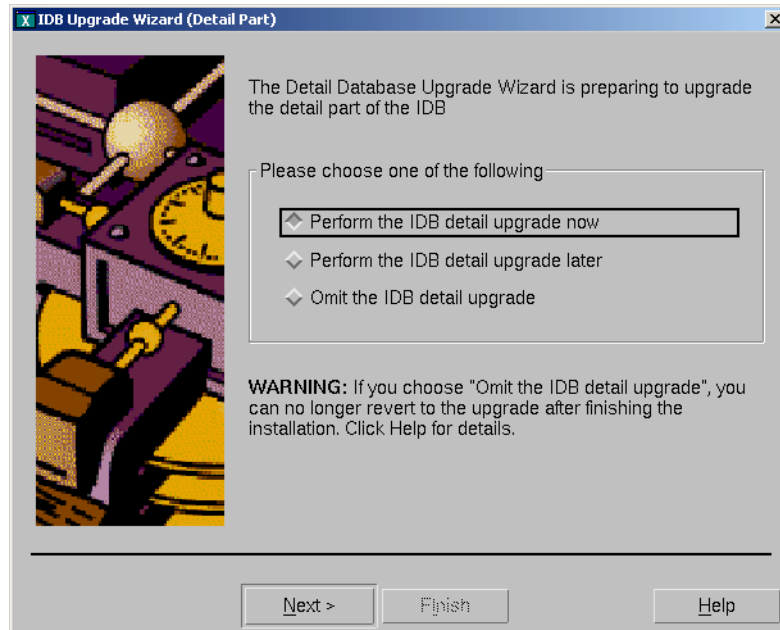
3. After the A.03.50 version of OmniBack II is detected, the IDB core part upgrade is automatically started. If you want to perform a clean installation (the database of the previous version will be deleted), uninstall the old version and restart the installation.

As soon as the installation script finishes, the IDB core part is upgraded. If you want to verify that the core part upgrade finished successfully, run the `/opt/omni/sbin/omnidbutil -upgrade_info` command, which displays the current upgrade status.

Once the core part of the IDB is upgraded, you can start using Data Protector. To proceed with the upgrade, perform the detail part upgrade following the steps described below:

1. Start the Data Protector Database Upgrade Wizard (Detail Part) by running the `/opt/omni/bin/xomnidbupg` command.
2. Select Perform the IDB detail upgrade now and click Next. Refer to Figure 4-1 on page 198.

Figure 4-1 **The Database Upgrade Wizard**



The upgrade wizard checks the A.03.50 database and disk space. When this is done, click **Next**.

3. Add extension files and DC binary files if you need more space than currently allocated, and then click **Next** to proceed.
4. Data Protector gives you the estimated time required for performing the upgrade. You can also monitor the progress of the upgrade session if you check the **I would like to monitor the upgrade session** option.

Click **Finish** to start the detail part upgrade.

The progress of the detail part upgrade can be monitored in the Data Protector GUI. In the **Monitor** context, click the detail part upgrade session to get the information about the session.

Upon completion of the task, a dialog box indicating the status is displayed.

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 203.

Upgrading the Windows Cell Manager and Installation Server

The Windows installation is based on Microsoft Installer (MSI). When the previous version of OmniBack II is detected, the same component set as installed is assumed by the operating system (without obsoleted components). You can change the component set during the process. However, the installation directory cannot be changed. The existing package set is removed and the new package set is installed.

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 OmniBack II A.03.50 to Data Protector A.05.10. For details, refer to “Upgrading from Windows NT to Newer Version of Windows” on page 263.

Upgrading the Windows Cell Manager

The Windows Cell Manager is upgraded automatically when the `setup.exe` command is run. If the Installation Server is present, it is upgraded as well. The detailed steps you need to follow when upgrading the Windows Cell Manager are described in “Step-by-Step Upgrade Procedure” on page 201.

Database Upgrade The old database remains in the `<Data_Protector_home>\db` folder, while the new database is installed in the `<Data_Protector_home>\db40` folder. The database upgrade consists of the following:

1. Upgrade of the core part of the IDB.
2. Upgrade of the detail part of the IDB.

IDB Core Part Upgrade

The IDB core part upgrade procedure, which transfers vital data from the old to the new database, is started unconditionally as a part of the upgrade. The entire MMDB as well as the session information part is transferred. Session messages, filenames and file versions are not transferred during the core part upgrade.

After the database core part upgrade, all the Data Protector functionality is available, except for browsing of single files. Refer to Table 4-1 on page 195.

IDB Detail Part Upgrade

The IDB detail part upgrade procedure can be started as a part of the installation procedure, or anytime later. The process goes over all detail catalogs and imports the data into the A.05.10 IDB. During the upgrade, the session messages are also imported. At the same time, the obsolete sessions (whose media have either been overwritten or exported) are removed. The catalogs belonging to unprotected objects (the objects that do not have protected copies) are also skipped from the upgrade. The number of skipped (not upgraded) objects is reported in the `upgrade.log` file residing in the `<Data_Protector_home>\log` directory.

During the detail part upgrade, you can perform backup, restore and media management operations; however, some limitations need to be considered. Refer to Table 4-1 on page 195 for details.

The detail part upgrade will be suspended while backup, restore or media management operations are running.

The detail part upgrade wizard displays the progress status as well as time and size estimates.

The detail part upgrade procedure is recoverable. If the system fails at any stage or if Data Protector shuts down, the upgrade is resumed automatically when the services are restarted.

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 269.

Upgrading the Windows Installation Server

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.

IMPORTANT

Reimport the upgraded Installation Server after the installation procedure has finished. For the procedure, refer to “Importing an Installation Server to a Cell” on page 157.

Step-by-Step Upgrade Procedure

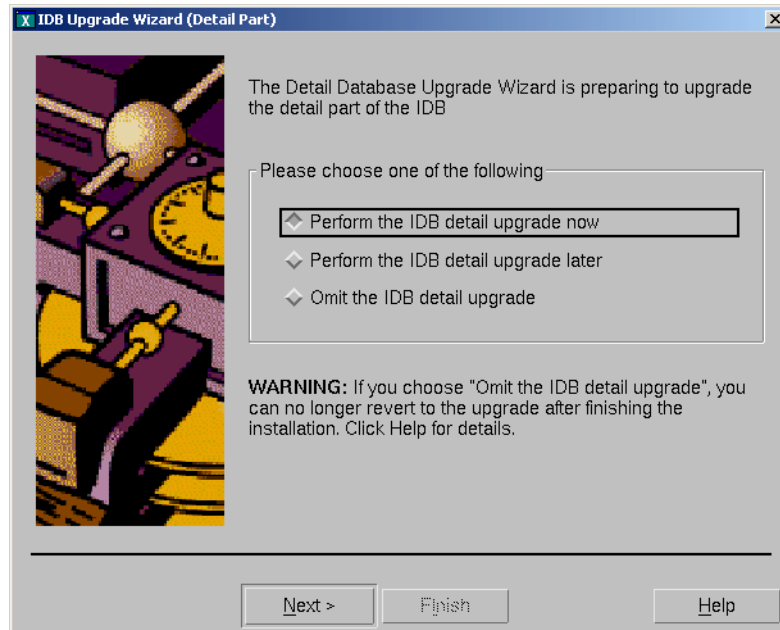
To upgrade the Windows Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert the Windows installation CD-ROM and run the `i386\setup.exe` command.
2. After the A.03.50 version of OmniBack II is detected, the IDB core part upgrade 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. On the Custom Setup page, the components previously installed on the system are selected. Note that you can change the component set.

Once the core part of the IDB is upgraded, you can start using Data Protector. To proceed with the upgrade, perform the detail part upgrade procedure, which is started automatically as soon as the core part upgrade is finished:

1. From the Data Protector Database Upgrade Wizard (Detail Part) window, select Perform the IDB detail upgrade now and click Next. Refer to Figure 4-2 on page 202.

Figure 4-2 **The Database Upgrade Wizard**



The upgrade wizard checks the A.03.50 database and disk space. When this is done, click **Next**.

2. Add extension files and DC binary files if you need more space than currently allocated, and then click **Next** to proceed.
3. Data Protector gives you the estimated time required for performing the upgrade. You can monitor the progress of the upgrade session if you check the I would like to monitor the upgrade session option.

Click **Finish** to start the detail part upgrade.

The progress of the detail part upgrade can be monitored in the Data Protector GUI. In the **Monitor** context, click the detail part upgrade session to get the information about the session.

Upon completion of the task, a dialog box indicating the status is displayed.

NOTE

You can start the detail part upgrade later by running the `<Data_Protector_home>\bin\omnidbupgrade -udp` command, or by using a supplied shortcut (Start->Programs->HP OpenView Storage Data Protector->Detail Upgrade), which is available only after the IDB core part upgrade has successfully finished and Data Protector A.05.10 is installed on your system.

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 203.

Checking Configuration Changes

Global Options File

During the upgrade, the contents of the *old* global options file residing in the `/etc/opt/omni/options` directory on HP-UX Cell Manager, or in the `<Data_Protector_home>\Config\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/options - HP-UX Cell Manager`
- `<Data_Protector_home>\NewConfig\Options - Windows Cell Manager`

The *merged* file, which is named `global`, resides in the `/etc/opt/omni/options` directory on HP-UX Cell Manager, or in the `<Data_Protector_home>\Config\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.05.10
```

- `# 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.05.10
# 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.05.10
# 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/options/global` on HP-UX Cell Manager and `<Data_Protector_home>\config\options\global` on Windows Cell Manager. The section “Global Options File” in the *HP OpenView Storage Data Protector Administrator’s 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 Administrator’s Guide*.
- Command line

Refer to Appendix B, “Command Line Changes After Upgrading to Data Protector A.05.10” on page B-37 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, proceed with distributing the software to clients. Refer to “Upgrading the Clients” on page 205.

Upgrading the Clients

Prerequisite

If you are upgrading the Oracle8 integration or the SAP R/3 integration installed together with the Oracle8 integration, the Oracle8 services must be stopped before the upgrade.

Upgrade Sequence

For information about the sequence in which the client upgrade is performed, refer to “Upgrade Overview” on page 189.

Upgrading Clients Remotely

For the procedure on how to upgrade the clients using the Installation Server, refer to “Distributing the Data Protector Software to Clients” on page 43.

Upgrading Clients Locally

If you do not have the 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 “Local Installation of Windows Clients” on page 57. To upgrade UNIX clients locally, refer to “Local Installation of UNIX Clients” on page 108. Note that for the local upgrade of Solaris clients the HP-UX, and not the Solaris installation CD-ROM must be used.

Novell NetWare

After upgrading any Novell NetWare 4.x or 5.0 client, you need to perform some additional steps, which will enable you to perform any backup and restore of the NDS (Novell NetWare 4.x) / NDS eDirectory (Novell 5.x and later) database. Refer to “Local Installation of the Novell NetWare Clients” on page 92 for details.

Upgrading Clients with Integrations

If you are upgrading the Data Protector client that has integrations installed (such as Oracle8, SAP R/3, Exchange 2000, 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 Oracle8 integration, refer to “Upgrading the Oracle8 Integration on UNIX Systems” on page 206 and “Upgrading the Oracle8 Integration on Windows Systems” on page 209.
- For instructions on how to upgrade the SAP R/3 integration, refer to “Upgrading the SAP R/3 Integration on UNIX Systems” on page 210 and “Upgrading the SAP R/3 Integration on Windows Systems” on page 212.
- For instructions on how to upgrade MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, and EMC Symmetrix integrations, refer to “Upgrading Other Integrations” on page 213.

Upgrading Clients Configured on MC/ServiceGuard

If you are upgrading the client that uses MC/ServiceGuard, 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
```

To upgrade the clients configured on MC/ServiceGuard that have the Oracle8 or the SAP R/3 integration installed, follow the procedure described in “Upgrading the Oracle8 Integration on UNIX Systems” on page 206 or “Upgrading the SAP R/3 Integration on UNIX Systems” on page 210.

Upgrading the Oracle8 Integration on UNIX Systems

Perform the following steps to upgrade the Oracle8 integration on UNIX systems:

1. Stop all Oracle8 services. Otherwise, the Oracle8 integration library, which must be replaced during the upgrade procedure, is locked and thus remains unchanged.

2. Upgrade the client that has the Oracle8 integration installed either locally by running the `omnisetup.sh -install oracle8` command or remotely by pushing the Oracle8 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install oracle8`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If you are using Oracle 8.0.5 (all UNIX platforms) or Oracle 8.0.6 32-bit version on Solaris, relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the `libob2oracle8.a` (AIX systems), or the `libob2oracle8.so` (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the `libob2oracle8.so` Database Library has changed from `/usr/omni/lib` to `/opt/omni/lib`. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If you are using the Oracle8i database on Solaris, remove only the soft link pointing to `/usr/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`) and point it to a new location: `/opt/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`).

4. Start the Oracle8 services.
5. It is recommended that you move the environmental variables set in the `omnirc` file or in `/etc/opt/omni/oracle8/<ORACLE_SID>/ .profile` (HP-UX systems) and in `/usr/omni/config/oracle8/<ORACLE_SID>/ .profile` (other UNIX systems) files to Data Protector Oracle8 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the `/opt/omni/newconfig/etc/opt/omni/dltemplates/lists/oracle8` directory to the `/etc/opt/omni/dltemplates/lists/oracle8` directory, where the old templates are stored.

If your Oracle8 integration is running in the ZDB environment, you need to perform additional steps, described on page 208, to successfully finish the upgrade.

MC/ServiceGuard To work in the MC/ServiceGuard environment, perform the following steps after the physical nodes upgrade has completed:

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
```
3. Reconfigure the Oracle8 integration on the virtual host. Note that on physical nodes the necessary reconfiguration is performed automatically.

The reconfiguration consists of configuring the integration for the virtual host. Refer to the *HP OpenView Storage Data Protector Integration Guide* for information on configuring the Oracle8 integration.

If your Oracle8 integration is running in the ZDB environment, you need to perform additional steps, described on page 226, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the Oracle8 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, the Oracle8i backup specifications must be upgraded to use the Data Protector A.05.10 ZDB functionality. The backup specifications upgrade needs to be performed after the standard Oracle8 integration upgrade procedure for UNIX systems has completed.

Note that the Oracle8.0 backup specifications do not need to be upgraded.

Perform the following steps to upgrade the Oracle8i integration running in the ZDB environment:

1. Reconfigure the Oracle8i integration by running on the application system the `util_oracle8.exe -CONFIG_SMB <ORACLE_SID> <ORACLE_HOME> <INIT_FILE> <CONTROL_FILE_LOCATION> <TARGET_DATABASE_LOGIN> <RECOVERY_CATALOG_LOGIN>` command located in the `/opt/omni/lbin` directory on HP-UX systems and in the `/usr/omni/bin` directory on other UNIX systems. Refer to the *HP*

OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide, the HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide, or the HP OpenView Storage Data Protector EMC Symmetrix Integration Guide for a description of these command parameters.

2. After upgrading all Oracle8 clients, perform the upgrade of all Oracle8i backup specifications stored on the Cell Manager by running the `/opt/omni/sbin/mrgcfg -ora_barlists` command on the UNIX Cell Manager or the `<Data_Protector_home>\bin\mrgcfg -ora_barlists` command on the Windows Cell Manager.

NOTE

After the upgrade procedure has completed, you can safely remove any Oracle8i binaries from the backup system, as they are not required by Data Protector A.05.10.

Upgrading the Oracle8 Integration on Windows Systems

Perform the following steps to upgrade the Oracle8 integration on Windows systems:

1. Stop all Oracle8 services. Otherwise, the `orasbt.dll` file in the `<%SystemRoot%>\setup32` folder, which must be replaced during the upgrade procedure, is locked and remains unchanged until the next system restart.
2. Upgrade the client that has the Oracle8 integration installed either locally by running the `setup.exe` command or remotely by pushing the Oracle8 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8 services.
4. It is recommended that you move the environmental variables set in the `omnirc` file to Data Protector Oracle8 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the `<Data_Protector_home>\NewConfig\dltemplates\lists\oracle8`

directory to the

`<Data_Protector_home>\Config\dltemplates\lists\oracle8`
directory, where the old templates are stored.

MS Cluster Server During the upgrade in the MS Cluster Server environment, the Oracle configuration files are transferred to the Cell Manager under the virtual server name of the cluster instead of the virtual server name of the Oracle resource group. Rename these configuration files so that they contain the virtual server name of the Oracle resource group. The files are located on the Cell Manager in the following directories:

- On Windows:
`<Data_Protector_home>\Config\Integ\Config\Oracle8`
- On HP-UX: `etc/opt/omni/integ/config/Oracle8`

Upgrading the SAP R/3 Integration on UNIX Systems

Perform the following steps to upgrade the SAP R/3 integration on UNIX systems:

1. If the Oracle8 integration is installed together with the SAP R/3 integration on the same client system, stop the Oracle8 services before the upgrade.
2. Upgrade the client either locally by running the `omnisetup.sh -install sap` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install sap`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If SAP R/3 uses the Oracle 8.0.5 database (all UNIX platforms) or the Oracle 8.0.6 database (32-bit version on Solaris), relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the `libob2oracle8.a` (AIX systems), or the `libob2oracle8.so` (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the `libob2oracle8.so` Database Library has changed from `/usr/omni/lib` to `/opt/omni/lib`. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If SAP R/3 uses the Oracle8i database on Solaris, remove only the soft link pointing to `/usr/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`) and point it to a new location: `/opt/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`).

4. Start the Oracle8 services if they were stopped.
5. Start the transfer of compression statistics files from the client system to the Data Protector SAP R/3 configuration file by running on the client system the `/opt/omni/sbin/upgrade_cfg -sid <ORACLE_SID> -ratio_file <path_and_filename> command` (HP-UX systems) or the `/usr/omni/bin/upgrade_cfg -sid <ORACLE_SID> -ratio_file <path_and_filename> command` (other UNIX systems) for every compression statistics file. The `<path_and_filename>` parameter is the path and the name of a compression statistics file. The reason for transferring this data manually is that this data may reside in more than one file, and only one file is transferred automatically at the time this command is run. That is why you should start this command as many times as many compression statistics files you have.

If the information about a file is present in two or more compression statistics files, and you are upgrading all these files, only the information from the latest upgraded compression statistics file is saved in the Data Protector SAP R/3 configuration file.

NOTE

If you had any of the following variables: `SAPSEARCH`, `SAPBACKUP`, `SAPCHECK`, `SAPDATA_HOME`, `SAPLOCALHOST`, `SAPREORG`, `SAPSTAT`, and `SAPTRACE` exported in the `omnisap.exe` file or in `/etc/opt/omni/sap/<ORACLE_SID>/.profile` (HP-UX systems) or `/usr/omni/config/sap/<ORACLE_SID>/.profile` (other UNIX systems) files, they will be automatically moved to the Data Protector SAP R/3 configuration file. All other variables as well as commented lines will not be moved.

If your SAP R/3 integration is running in the ZDB environment, you need to perform additional steps, described on page 212, to successfully finish the upgrade.

MC/ServiceGuard

To work in the MC/ServiceGuard environment, perform the following steps after the physical nodes upgrade has completed:

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
```
3. Reconfigure the SAP R/3 integration on the virtual host. Note that on physical nodes the necessary reconfiguration is performed automatically.

The reconfiguration consists of configuring the integration for the virtual host. Refer to the *HP OpenView Storage Data Protector Integration Guide* for information on configuring the SAP R/3 integration.

If your SAP R/3 integration is running in the ZDB environment, you need to perform additional steps, described on page 212, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the SAP R/3 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, first upgrade the SAP R/3 integration following the standard SAP R/3 integration upgrade procedure for UNIX systems, and then proceed as follows:

1. Make sure the SAP R/3 Database Server is configured on the application system. If not, configure it following the procedure described in the *HP OpenView Storage Data Protector UNIX Integration Guide*.
2. Change the value of the SAP R/3 parameter `primary_db` from `<SERVICE_NAME>` to `LOCAL` in the SAP R/3 initialization profile (`<ORACLE_HOME>/dbs/init<SID>.sap`).

NOTE

On the backup system, any SAP R/3 and Oracle8i application binaries can be safely removed, as they are not required by Data Protector A.05.10.

Upgrading the SAP R/3 Integration on Windows Systems

Perform the following steps to upgrade the SAP R/3 integration on Windows systems:

1. If the Oracle8 integration is installed together with the SAP R/3 integration on the same client system, stop the Oracle8 services before the upgrade.
2. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8 services if they were stopped.
4. Start the transfer of compression statistics files from the client system to the Data Protector SAP R/3 configuration file by running on the client system the

```
<Data_Protector_home>\bin\upgrade_cfg.exe -sid  
<ORACLE_SID> -ratio_file <path_and_filename>
```

 command for every compression statistics file. The `<path_and_filename>` parameter is the path and the name of the compression statistics file. The reason for transferring this data manually is that this data may reside in more than one file, and only one file is transferred automatically at the time this command is run. That is why you should start this command as many times as many compression statistics files you have.

If the information about a file is present in two or more compression statistics files, and you are upgrading all these files, only the information from the latest upgraded compression statistics file is saved in the Data Protector SAP R/3 configuration file.

MS Cluster Server During the upgrade in the MS Cluster Server environment, the SAP R/3 configuration files are transferred to the Cell Manager under the virtual server name of the cluster instead of the virtual server name of the SAP R/3 resource group. Rename these configuration files so that they contain the virtual server name of the SAP R/3 resource group. The files are located on the Cell Manager in the following directories:

- On Windows:
`<Data_Protector_home>\Config\Integ\Config\SAP`
- On HP-UX: `etc/opt/omni/integ/config/SAP`

Upgrading Other Integrations

If the Data Protector client has the MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, or EMC Symmetrix integration installed, upgrade these clients 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 Clients” on page 108. Note that if you are 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 as installed on the system before the upgrade without issuing a prompt.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.05.10, proceed as follows:

1. Upgrade the MoM Manager to Data Protector A.05.10.

During the upgrade, Cell Managers in the MoM environment must not be operational. After the upgrade, the MoM Manager can still work with A.03.50 Cell Managers. The A.03.50 Cell Managers that have not been upgraded yet are able to access the Central MMDB and perform backups and restores, but other functionality is not available.

2. Upgrade each Cell Manager in a MoM environment.

For the upgrade procedure, refer to “Upgrading the HP-UX Cell Manager and Installation Server” on page 193 and “Upgrading the Windows Cell Manager and Installation Server” on page 199.

NOTE

Device sharing between Data Protector A.05.10 MoM and the cells with earlier versions installed is not supported.

Upgrading from OmniBack II A.03.51

The OmniBack II A.03.51 release version can be directly upgraded to Data Protector A.05.10 for Solaris.

Licenses

The existing OmniBack II A.03.51 licenses are fully compatible and valid for use with Data Protector A.05.10. However, some license types are not available for repurchasing, they are replaced by new licenses. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

Upgrade Sequence

For information about the upgrade sequence, refer to “Upgrade Overview” on page 189.

Upgrading the Solaris Cell Manager and Installation Server

Prerequisites

- Stop all OmniBack II services before the upgrade procedure by running the `/opt/omni/sbin/omnisv.sh -stop` command.
- If you have any OmniBack II patches installed, uninstall them before the upgrade.

NOTE

You must have root permissions to perform the upgrade.

Upgrading the Solaris Cell Manager

To upgrade the Solaris Cell Manager, run the `omnisetup.sh` command. This command removes the existing package set using the `pkgrm` utility and installs OB2-CORE, OB2-CC, OB2-CS, OB2-DA, OB2MA, and OB2-MOM packages using the `pkgadd` utility.

If the Installation Server is installed together with the Cell Manager, or it is installed without client components, it is upgraded automatically when the `omnisetup.sh` command is run. The detailed steps you need to follow when upgrading the Solaris Cell Manager are described in “Step-by-Step Upgrade Procedure” on page 218.

Database Upgrade The old database remains in the `/var/opt/omni/db` folder. However, old `/var/opt/omni/db/catalog` is moved to `/var/opt/omni/db/catalog.OLD`. The new database is installed in the `/var/opt/omni/db40` folder. The whole process is performed in two steps:

1. Upgrade of the core part of the IDB.
2. Upgrade of the detail part of the IDB.

IDB Core Part Upgrade

The IDB core part upgrade procedure transfers vital data from the old to the new database. It is started unconditionally as a part of the upgrade when the `omnisetup.sh` command is run. The entire MMDB as well as the session information part is transferred. However, session messages, filenames and file versions are not transferred during the core part upgrade.

After the database core part upgrade, all the Data Protector functionality is available, except for browsing of single files and directories. Refer to Table 4-2 on page 217.

IDB Detail Part Upgrade

The IDB detail part upgrade procedure is started by running the `/opt/omni/bin/xomnidbupg` command. The process goes over all detail catalogs and imports the data into the A.05.10 IDB. During the upgrade, the session messages are also imported. At the same time, the obsolete sessions (which media have either been overwritten or exported) are removed. The catalogs belonging to unprotected objects (the objects that do not have protected copies) are also skipped from the upgrade. The number of skipped (not upgraded) objects is reported in the `upgrade.log` file residing in the `/var/opt/omni/log` directory.

During the upgrade, you can perform backup, restore and media management operations; however, some limitations need to be considered. Refer to Table 4-2 on page 217 for details.

The upgrade will be suspended while backup, restore or media management operations are running.

The detail part upgrade wizard displays the progress status as well as time and size estimates.

The detail part upgrade procedure is recoverable. If the system fails at any stage or if Data Protector shuts down, the upgrade is resumed automatically when the services are restarted.

The following table presents the Data Protector functionality available after the upgrade.

Table 4-2 Upgrade of the A.03.51 IDB - Core and Detail Part

IDB Upgrade	What Is Upgraded	Data Protector Behavior
Upgrade of the core part	The IDB without file versions, filenames, and session messages	All functionality available except for browsing of single files and directories.
Upgrade of the detail part	The whole IDB except for obsolete sessions and the catalogs that belong to unprotected objects	All functionality available except for filename purge. Browsing of objects that reside on tapes that have not been upgraded yet, will not work or will work partially. Tapes with detail catalogs that have not been upgraded yet will not be allocated for appended backups.

IDB Disk Space Requirements

It is important to calculate the disk space requirements and verify that enough disk space is available to successfully perform the upgrade procedure. The IDB disk space requirements for upgrading from OmniBack II A.03.51 to Data Protector A.05.10 are the same as for upgrading from OmniBack II A.03.50. To get the estimate of the disk space, required for the upgrade, follow the steps described on page 191.

Time Requirements

The IDB core part upgrade procedure lasts from 30 minutes to 2 hours depending on the database size and the system speed and load.

The IDB detail part upgrade takes 3-6 hours per gigabyte of data. For the example given on page 192, the detail part upgrade would take 18-36 hours.

Upgrading the Solaris Installation Server

In the following cases the Solaris Installation Server is upgraded automatically when the `omnisetup.sh` command is run:

- If it is installed together with the Cell Manager.
- If it is installed without client components.

NOTE

The `omnisetup.sh` command checks the presence of the `OB2-C-IS` package to determine the status of the Installation Server. If this package is present, the Installation Server will be upgraded even if push packets were not originally installed.

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 157.

NOTE

If the Installation Server resides on the system other than the Cell Manager, it should be upgraded locally from the Solaris installation CD-ROM. For the procedure, refer to “Installing the Installation Server for UNIX” on page 30.

Step-by-Step Upgrade Procedure

To upgrade the Solaris Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert and mount the Solaris installation CD-ROM to a mount point, for example:

```
mkdir /cdrom
mount /dev/cd0 /cdrom
```

If you want to have the `DP_DEPOT` directory, where the installation files are stored, on your local disk, proceed as follows:

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
```

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

```
cp -r /cdrom <cd_image_dir>
```

2. Run the `./omnisetup.sh` command. To run this command from the CD-ROM, execute:


```
cd /cdrom/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

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 CD-ROM to `<cd_image_dir>`, run the `omnisetup.sh` command without any parameters:

```
cd <cd_image_dir>/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

Refer to the `omnisetup.sh` man page for a description of this command.

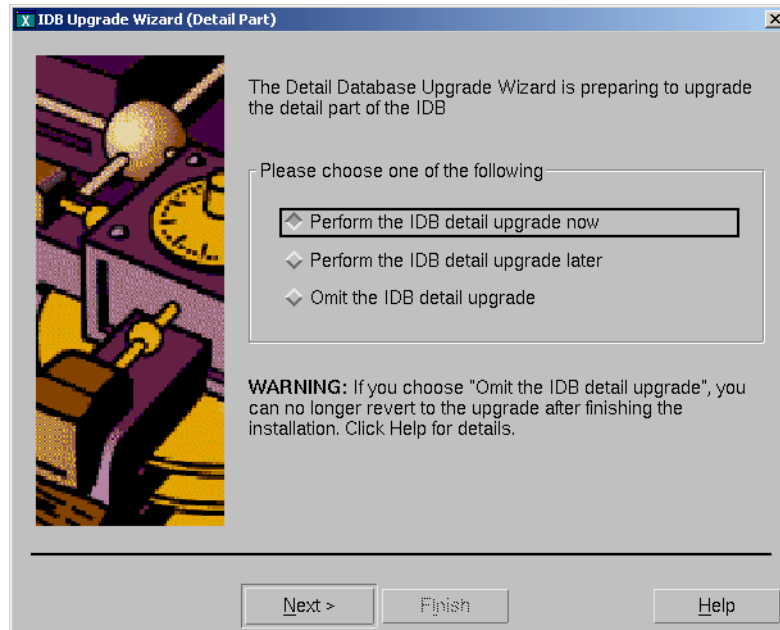
3. After the A.03.51 version of OmniBack II is detected, the IDB core part upgrade is automatically started. If you want to perform a clean installation (the database of the previous version will be deleted), uninstall the old version and restart the installation.

As soon as the installation script finishes, the IDB core part is upgraded. If you want to verify that the core part upgrade finished successfully, run the `/opt/omni/sbin/omnidbutil -upgrade_info` command, which displays the current upgrade status.

Once the core part of the IDB is upgraded, you can start using Data Protector. To proceed with the upgrade, perform the detail part upgrade following the steps described below:

1. Start the Data Protector Database Upgrade Wizard (Detail Part) by running the `/opt/omni/bin/xomnidbupg` command.
2. Select Perform the IDB detail upgrade now and click Next. Refer to Figure 4-3 on page 220.

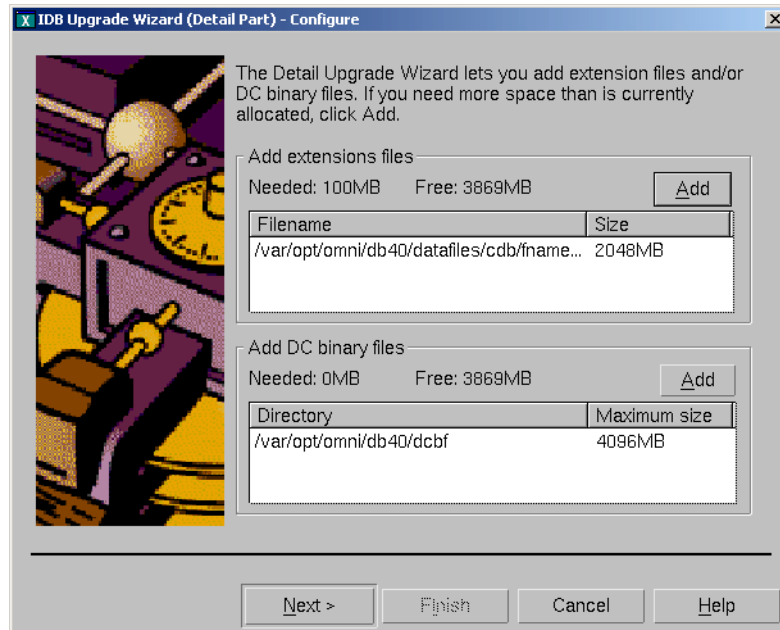
Figure 4-3 **The Database Upgrade Wizard**



The upgrade wizard checks the A.03.51 database and disk space. When it is finished, click **Next**.

3. Add extension files and DC binary files if you need more space than currently allocated, and click **Next**. Refer to Figure 4-4 on page 221.

Figure 4-4 Adding Extension Files and DC Binary Files



4. Data Protector gives you the estimated time required for performing the upgrade. You can also monitor the progress of the upgrade session if you check the I would like to monitor the upgrade session option.

Click **Finish** to start the detail part upgrade.

The progress of the detail part upgrade can be monitored in the Data Protector GUI. In the **Monitor** context, click the detail part upgrade session to get the information about the session.

Upon completion of the task, a dialog box indicating the status is displayed.

What's Next?

Once the Cell Manager and the Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to "Checking Configuration Changes" on page 222.

Checking Configuration Changes

Global Options File

During the upgrade, the contents of the *old* global options file residing in the `/etc/opt/omni/options` directory on the Cell Manager are merged with the contents of the *new* global options file residing in the `/opt/omni/newconfig/etc/opt/omni/options` directory.

The *merged* file, named `global`, resides in the `/etc/opt/omni/options` directory 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.05.10
# 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.05.10
# 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.05.10
# This variable cannot be transferred automatically.
# The previous setting was:
# <variable>=<value>
```

- Comments are not transferred to the newly merged file.

The description of new options is in the merged global options file: `/etc/opt/omni/options/global`. The section “Global Options File” in the *HP OpenView Storage Data Protector Administrator’s 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 Administrator’s Guide*.

- Command line

Refer to Appendix B, “Command Line Changes After Upgrading to Data Protector A.05.10” on page B-37 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, proceed with distributing the software to clients. Refer to “Upgrading the Clients” on page 223.

Upgrading the Clients

Prerequisite

If you are upgrading the Oracle8 integration or the SAP R/3 integration installed together with the Oracle8 integration, the Oracle8 services must be stopped before the upgrade.

Upgrade Sequence

For information about the sequence in which the client upgrade is performed, refer to “Upgrade Overview” on page 189.

Upgrading Clients Remotely

For the procedure on how to upgrade the clients using the Installation Server, refer to “Distributing the Data Protector Software to Clients” on page 43.

Upgrading Clients Locally

If you do not have the 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 “Local Installation of Windows Clients” on page 57. To upgrade UNIX clients locally, refer to “Local Installation of UNIX Clients” on page 108. Note that for the local upgrade of Solaris clients the HP-UX, and not the Solaris installation CD-ROM must be used.

Novell NetWare After upgrading any Novell NetWare 4.x or 5.0 client, you need to perform some additional steps, which will enable you to perform any backup and restore of the NDS (Novell NetWare 4.x) / NDS eDirectory (Novell 5.x and later) database. Refer to “Local Installation of the Novell NetWare Clients” on page 92 for details.

Upgrading Clients with Integrations If you are upgrading the Data Protector client that has integrations installed (such as Oracle8, SAP R/3, Exchange 2000, 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 Oracle8 integration, refer to “Upgrading the Oracle8 Integration on UNIX Systems” on page 225 and “Upgrading the Oracle8 Integration on Windows Systems” on page 227.
- For instructions on how to upgrade the SAP R/3 integration, refer to “Upgrading the SAP R/3 Integration on UNIX Systems” on page 228 and “Upgrading the SAP R/3 Integration on Windows Systems” on page 231.
- For instructions on how to upgrade MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, and EMC Symmetrix integrations, refer to “Upgrading Other Integrations” on page 232.

Upgrading Clients Configured on MC/ServiceGuard If you are upgrading the client that uses MC/ServiceGuard, 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
```

To upgrade the clients configured on MC/ServiceGuard that have the Oracle8 or the SAP R/3 integration installed, follow the procedure described in “Upgrading the Oracle8 Integration on UNIX Systems” on page 225 or “Upgrading the SAP R/3 Integration on UNIX Systems” on page 228.

Upgrading the Oracle8 Integration on UNIX Systems

Perform the following steps to upgrade the Oracle8 integration on UNIX systems:

1. Stop all Oracle8 services. Otherwise, the Oracle8 integration library, which must be replaced during the upgrade procedure, is locked and thus remains unchanged.
2. Upgrade the client that has the Oracle8 integration installed either locally by running the `omnisetup.sh -install oracle8` command or remotely by pushing the Oracle8 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install oracle8`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If you are using Oracle 8.0.5 (all UNIX platforms) or Oracle 8.0.6 32-bit version on Solaris, relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the `libob2oracle8.a` (AIX systems), or the `libob2oracle8.so` (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the `libob2oracle8.so` Database Library has changed from `/usr/omni/lib` to `/opt/omni/lib`. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If you are using the Oracle8i database on Solaris, remove only the soft link pointing to `/usr/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`) and point it to a new location: `/opt/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`).

4. Start the Oracle8 services.
5. It is recommended that you move the environmental variables set in the `omnirc` file or in `/etc/opt/omni/oracle8/<ORACLE_SID>/.profile` (HP-UX systems) and in

`/usr/omni/config/oracle8/<ORACLE_SID>/ .profile` (other UNIX systems) files to Data Protector Oracle8 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the `/opt/omni/newconfig/etc/opt/omni/dltemplates/lists/oracle8` directory to the `/etc/opt/omni/dltemplates/lists/oracle8` directory, where the old templates are stored.

If your Oracle8 integration is running in the ZDB environment, you need to perform additional steps, described on page 226, to successfully finish the upgrade.

MC/ServiceGuard

To work in the MC/ServiceGuard environment, perform the following steps after the physical nodes upgrade has completed:

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
```

3. Reconfigure the Oracle8 integration on the virtual host. Note that on physical nodes the necessary reconfiguration is performed automatically.

The reconfiguration consists of configuring the integration for the virtual host. Refer to the *HP OpenView Storage Data Protector Integration Guide* for information on configuring the Oracle8 integration.

If your Oracle8 integration is running in the ZDB environment, you need to perform additional steps, described on page 226, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the Oracle8 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, the Oracle8i backup specifications must be upgraded to use the Data Protector A.05.10 ZDB

functionality. The backup specifications upgrade needs to be performed after the standard Oracle8 integration upgrade procedure for UNIX systems has completed.

Note that the Oracle8.0 backup specifications do not need to be upgraded.

Perform the following steps to upgrade the Oracle8i integration running in the ZDB environment:

1. Reconfigure the Oracle8i integration by running on the application system the `util_oracle8.exe -CONFIG_SMB <ORACLE_SID> <ORACLE_HOME> <INIT_FILE> <CONTROL_FILE_LOCATION> <TARGET_DATABASE_LOGIN> <RECOVERY_CATALOG_LOGIN>` command located in the `/opt/omni/lbin` directory on HP-UX systems and in the `/usr/omni/bin` directory on other UNIX systems. Refer to the *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide*, the *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*, or the *HP OpenView Storage Data Protector EMC Symmetrix Integration Guide* for a description of these command parameters.
2. After upgrading all Oracle8 clients, perform the upgrade of all Oracle8i backup specifications stored on the Cell Manager by running the `/opt/omni/sbin/mrgcfg -ora_barlists` command on the UNIX Cell Manager or the `<Data_Protector_home>\bin\mrgcfg -ora_barlists` command on the Windows Cell Manager.

NOTE

After the upgrade procedure has completed, you can safely remove any Oracle8i binaries from the backup system, as they are not required by Data Protector A.05.10.

Upgrading the Oracle8 Integration on Windows Systems

Perform the following steps to upgrade the Oracle8 integration on Windows systems:

1. Stop all Oracle8 services. Otherwise, the `orasbt.dll` file in the `<%SystemRoot%>\setup32` folder, which must be replaced during the upgrade procedure, is locked and remains unchanged until the next system restart.

2. Upgrade the client that has the Oracle8 integration installed either locally by running the `setup.exe` command or remotely by pushing the Oracle8 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8 services.
4. It is recommended that you move the environmental variables set in the `omnirc` file to Data Protector Oracle8 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the

`<Data_Protector_home>\NewConfig\dltemplates\lists\oracle8`
directory to the

`<Data_Protector_home>\Config\dltemplates\lists\oracle8`
directory, where the old templates are stored.

MS Cluster Server No further configuration is needed for the Oracle8 integration running in the MS Cluster Server environment.

Upgrading the SAP R/3 Integration on UNIX Systems

Perform the following steps to upgrade the SAP R/3 integration on UNIX systems:

1. If the Oracle8 integration is installed together with the SAP R/3 integration on the same client system, stop the Oracle8 services before the upgrade.
2. Upgrade the client either locally by running the `omnisetup.sh -install sap` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install sap`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If SAP R/3 uses the Oracle 8.0.5 database (all UNIX platforms) or the Oracle 8.0.6 database (32-bit version on Solaris), relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the

libob2oracle8.a (AIX systems), or the libob2oracle8.so (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the libob2oracle8.so Database Library has changed from /usr/omni/lib to /opt/omni/lib. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If SAP R/3 uses the Oracle8i database on Solaris, remove only the soft link pointing to /usr/omni/lib/libob2oracle8.so (libob2oracle8_64bit.so) and point it to a new location: /opt/omni/lib/libob2oracle8.so (libob2oracle8_64bit.so).

4. Start the Oracle8 services if they were stopped.
5. Start the transfer of compression statistics files from the client system to the Data Protector SAP R/3 configuration file by running on the client system the /opt/omni/sbin/upgrade_cfg -sid <ORACLE_SID> -ratio_file <path_and_filename> command (HP-UX systems) or the /usr/omni/bin/upgrade_cfg -sid <ORACLE_SID> -ratio_file <path_and_filename> command (other UNIX systems) for every compression statistics file. The <path_and_filename> parameter is the path and the name of a compression statistics file. The reason for transferring this data manually is that this data may reside in more than one file, and only one file is transferred automatically at the time this command is run. That is why you should start this command as many times as many compression statistics files you have.

If the information about a file is present in two or more compression statistics files, and you are upgrading all these files, only the information from the latest upgraded compression statistics file is saved in the Data Protector SAP R/3 configuration file.

NOTE

If you had any of the following variables: SAPSEARCH, SAPBACKUP, SAPCHECK, SAPDATA_HOME, SAPLOCALHOST, SAPREORG, SAPSTAT, and SAPTRACE exported in the omnisap.exe file or in /etc/opt/omni/sap/<ORACLE_SID>/.profile (HP-UX systems) or /usr/omni/config/sap/<ORACLE_SID>/.profile (other UNIX systems) files, they will be automatically moved to the Data Protector SAP R/3 configuration file. All other variables as well as commented lines will not be moved.

If your SAP R/3 integration is running in the ZDB environment, you need to perform additional steps, described on page 230, to successfully finish the upgrade.

MC/ServiceGuard To work in the MC/ServiceGuard environment, perform the following steps after the physical nodes upgrade has completed:

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
```
3. Reconfigure the SAP R/3 integration on the virtual host. Note that on physical nodes the necessary reconfiguration is performed automatically.

The reconfiguration consists of configuring the integration for the virtual host. Refer to the *HP OpenView Storage Data Protector Integration Guide* for information on configuring the SAP R/3 integration.

If your SAP R/3 integration is running in the ZDB environment, you need to perform additional steps, described on page 230, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the SAP R/3 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, first upgrade the SAP R/3 integration following the standard SAP R/3 integration upgrade procedure for UNIX systems, and then proceed as follows:

1. Make sure the SAP R/3 Database Server is configured on the application system. If not, configure it following the procedure described in the *HP OpenView Storage Data Protector UNIX Integration Guide*.
2. Change the value of the SAP R/3 parameter `primary_db` from `<SERVICE_NAME>` to `LOCAL` in the SAP R/3 initialization profile (`<ORACLE_HOME>/dbs/init<SID>.sap`).

NOTE

On the backup system, any SAP R/3 and Oracle8i application binaries can be safely removed, as they are not required by Data Protector A.05.10.

Upgrading the SAP R/3 Integration on Windows Systems

Perform the following steps to upgrade the SAP R/3 integration on Windows systems:

1. If the Oracle8 integration is installed together with the SAP R/3 integration on the same client system, stop the Oracle8 services before the upgrade.
2. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8 services if they were stopped.
4. Start the transfer of compression statistics files from the client system to the Data Protector SAP R/3 configuration file by running on the client system the

```
<Data_Protector_home>\bin\upgrade_cfg.exe -sid  
<ORACLE_SID> -ratio_file <path_and_filename>
```

command for every compression statistics file. The `<path_and_filename>` parameter is the path and the name of the compression statistics file. The reason for transferring this data manually is that this data may reside in more than one file, and only one file is transferred automatically at the time this command is run. That is why you should start this command as many times as many compression statistics files you have.

If the information about a file is present in two or more compression statistics files, and you are upgrading all these files, only the information from the latest upgraded compression statistics file is saved in the Data Protector SAP R/3 configuration file.

MS Cluster Server No further configuration is needed for the SAP R/3 integration running in the MS Cluster Server environment.

Upgrading Other Integrations

If the Data Protector client has the MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, or EMC Symmetrix integration installed, upgrade these clients 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 Clients” on page 108. Note that if you are 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 as installed on the system before the upgrade without issuing a prompt.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.05.10, proceed as follows:

1. Upgrade the MoM Manager to Data Protector A.05.10.

During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with A.03.51 Cell Managers. The A.03.51 Cell Managers that have not been upgraded yet are able to access the Central MMDb and perform backups and restores, but other functionality is not available.

2. Upgrade each Cell Manager in a MoM environment.

For the upgrade procedure, refer to “Upgrading the Solaris Cell Manager and Installation Server” on page 215.

NOTE

Device sharing between the Data Protector A.05.10 MoM and the cells with earlier versions installed is not supported.

Upgrading from OmniBack II A.04.x

The following OmniBack II A.04.x release versions can be directly upgraded to Data Protector A.05.10 for UNIX and Windows platforms:

- OmniBack II A.04.00 release version
- OmniBack II A.04.10 release version

Licenses

The existing OmniBack II A.04.x licenses are fully compatible and valid for use with Data Protector A.05.10. However, some license types are not available for repurchasing, they are replaced by new licenses. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

Upgrade Sequence

For information about the upgrade sequence, refer to “Upgrade Overview” on page 189.

Upgrading the HP-UX Cell Manager and Installation Server

Prerequisite

Stop all OmniBack II services before the upgrade procedure by running the `/opt/omni/sbin/omnisv -stop` command.

NOTE

You must have root permissions to perform the upgrade.

Upgrading the HP-UX Cell Manager

The HP-UX Cell Manager is upgraded automatically when the `omnisetup.sh` command is run. This command removes the existing package set using the `swremove` utility and installs `OMNI-CORE`, `OMNI-CC`, `OMNI-CS`, `OMNI-DA`, and `OMNI-MA` packages using the `swinstall` utility. If the Installation Server is present, it is upgraded as well. The detailed steps you need to follow when upgrading the HP-UX Cell Manager are described in “Step-by-Step Upgrade Procedure” on page 234.

- Database Upgrade** The database remains in the `/var/opt/omni/db40` folder. After the upgrade procedure is completed, the database can no longer be used with OmniBack II A.04.x.
- MC/ServiceGuard** The upgrade procedure for the Cell Manager, configured on MC/SG, is different 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 265.

Upgrading the HP-UX Installation Server

In the following cases, the HP-UX Installation Server is upgraded automatically when the `omnisetup.sh` command is run:

- If it is installed together with the Cell Manager.
- If it is installed without client components.

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 157.

Step-by-Step Upgrade Procedure

Prerequisite

It is recommended that the kernel parameter `maxdsiz` (Max Data Segment Size) is set to at least 131072000 Bytes (128 MBytes). After setting this parameter, recompile the kernel and restart the machine.

To upgrade the HP-UX Cell Manager and Installation Server, follow the procedure described below:

1. Insert and mount the HP-UX installation CD-ROM to a mount point, for example:

```
mkdir /cdrom  
mount /dev/cd0 /cdrom
```

If you want to have the `DP_DEPOT` directory, where the installation files are stored, on your local disk, proceed as follows:

```
mkdir <directory>  
cp -r /cdrom/DP_DEPOT <directory>
```

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


```
cp -r /cdrom <cd_image_dir>
```

2. Run the `./omnisetup.sh` command. To run this command from the CD-ROM, execute:

```
cd /cdrom/LOCAL_DP_AGENT_INSTALL  
./omnisetup.sh
```

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 CD-ROM to `<cd_image_dir>`, run the `omnisetup.sh` command without any parameters:

```
cd <cd_image_dir>/LOCAL_DP_AGENT_INSTALL  
./omnisetup.sh
```

Refer to the `omnisetup.sh` man page for a description of the `omnisetup.sh` command.

3. After the A.04.x version of OmniBack II 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 Cell Manager” on page 16 and “Installing the Installation Server for UNIX” on page 30.

As soon as the procedure is completed, you can start using Data Protector.

What's Next?

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 237.

Upgrading the Windows Cell Manager and Installation Server

The Windows installation is based on Microsoft Installer 2.0. When the previous version of OmniBack II is detected, the same component set as installed is assumed by the operating system (without obsoleted

components). You can change the component set during the process. However, the installation directory cannot be changed. The existing package set is removed and the new package set is installed.

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.05.10. For details, refer to “Upgrading from Windows NT to Newer Version of Windows” on page 263.

Upgrading the Windows Cell Manager

The Windows Cell Manager is upgraded automatically when the `setup.exe` command is run. If the Installation Server is present, it is upgraded as well. The detailed steps you need to follow when upgrading the Windows Cell Manager are described in “Step-by-Step Upgrade Procedure” on page 237.

Database Upgrade The database remains in the `<Data_Protector_home>\db40` folder. After the upgrade procedure is completed, the database can no longer be used with OmniBack II A.04.x.

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 269.

Upgrading the Windows Installation Server

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 157.

Step-by-Step Upgrade Procedure

To upgrade the Windows Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert the Windows installation CD-ROM and run the `i386\setup.exe` command.
2. After the A.04.x version of OmniBack II is detected, the upgrade procedure is automatically started. If you want to perform a clean upgrade (the database of a previous version will be deleted), uninstall the old version and restart the installation. At the `Custom Setup` page, the components previously installed on the system are selected. Note that you can change the component set.

For details about installation, refer to “Installing a Windows Cell Manager” on page 25 and “Installing an Installation Server for Windows” on page 35.

As soon as the procedure is completed, you can start using Data Protector.

What’s Next?

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 237.

Checking Configuration Changes

Global Options File

During the upgrade, the contents of the *old* global options file residing in the `/etc/opt/omni/options` directory on HP-UX Cell Manager, or in the `<Data_Protector_home>\Config\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/options` - HP-UX Cell Manager

- `<Data_Protector_home>\NewConfig\Options - Windows Cell Manager`

The *merged* file, which is named `global`, resides in the `/etc/opt/omni/options` directory on HP-UX Cell Manager, or in the `<Data_Protector_home>\Config\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.05.10
# 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.05.10
# 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.05.10
# 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/options/global` on HP-UX Cell Manager and `<Data_Protector_home>\config\options\global` on Windows Cell Manager. The section “Global Options File” in the *HP OpenView Storage Data Protector Administrator’s 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 Administrator’s Guide*.

- Command line

Refer to Appendix B, “Command Line Changes After Upgrading to Data Protector A.05.10” on page B-37 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, proceed with distributing the software to clients. Refer to “Upgrading the Clients” on page 239.

Upgrading the Clients

Prerequisite

If you are upgrading the Oracle8/9 integration or the SAP R/3 integration installed together with the Oracle8/9 integration, the Oracle8/9 services must be stopped before the upgrade.

Upgrade Sequence

For information about the sequence in which the client upgrade is performed, refer to “Upgrade Overview” on page 189.

Upgrading Clients Remotely

For the procedure on how to upgrade the clients using the Installation Server, refer to “Distributing the Data Protector Software to Clients” on page 43.

Upgrading Clients Locally

If you do not have the 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 “Local Installation of Windows Clients” on page 57. To upgrade UNIX clients locally, refer to “Local Installation of UNIX Clients” on page 108. Note that for the local upgrade of Solaris clients the HP-UX, and not the Solaris installation CD-ROM must be used.

Upgrading Clients Configured on MC/ServiceGuard

If you are upgrading the client that uses MC/ServiceGuard, 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 the Data Protector client that has integration installed (such as Oracle8/9, SAP R/3, Exchange 2000, Lotus Notes, 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 Oracle8/9 integration, refer to “Upgrading the Oracle8/9 Integration on UNIX Systems” on page 240 and “Upgrading the Oracle8/9 Integration on Windows Systems” on page 243.
- For instructions on how to upgrade the SAP R/3 integration, refer to “Upgrading the SAP R/3 Integration on UNIX Systems” on page 244 and “Upgrading the SAP R/3 Integration on Windows Systems” on page 245.
- For instructions on how to upgrade MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, EMC Symmetrix, etc., refer to “Upgrading Other Integrations” on page 245.

Upgrading the Oracle8/9 Integration on UNIX Systems

Perform the following steps to upgrade the Oracle8/9 integration on UNIX systems:

1. Stop all Oracle8/9 services. Otherwise, the Oracle8/9 integration library, which must be replaced during the upgrade procedure, is locked and thus remains unchanged.
2. Upgrade the client that has the Oracle8/9 integration installed either locally by running the `omnisetup.sh -install oracle8` command or remotely by pushing the Oracle8/9 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install oracle8`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If you are using Oracle 8.0.5 (all UNIX platforms) or Oracle 8.0.6 32-bit version on Solaris, relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the `libob2oracle8.a` (AIX systems), or the `libob2oracle8.so` (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the `libob2oracle8.so` Database Library has changed from `/usr/omni/lib` to `/opt/omni/lib`. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If you are using the Oracle8i/9i database on Solaris, remove only the soft link pointing to `/usr/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`) and point it to a new location: `/opt/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`).

4. Start the Oracle8/9 services.
5. It is recommended that you move the environmental variables set in the `omnirc` file or in `/etc/opt/omni/oracle8/<ORACLE_SID>/.profile` (HP-UX and Solaris systems) and in `/usr/omni/config/oracle8/<ORACLE_SID>/.profile` (other UNIX systems) files to Data Protector Oracle8/9 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the
`/opt/omni/newconfig/etc/opt/omni/dltemplates/lists/oracle8`
directory to the `/etc/opt/omni/dltemplates/lists/oracle8`
directory, where the old templates are stored.

If your Oracle8/9 integration is running in the ZDB environment, you need to perform additional steps, described on page 242, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the Oracle8/9 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, the Oracle8i/9i backup specifications must be upgraded to use the Data Protector A.05.10 ZDB functionality. The backup specifications upgrade needs to be performed after the standard Oracle8/9 integration upgrade procedure for UNIX systems has completed.

Note that the Oracle8.0 backup specifications do not need to be upgraded.

Perform the following steps to upgrade the Oracle8i/9i integration running in the ZDB environment:

1. Reconfigure the Oracle8i/9i integration by running on the application system the `util_oracle8.exe -CONFIG_SMB <ORACLE_SID> <ORACLE_HOME> <INIT_FILE> <CONTROL_FILE_LOCATION> <TARGET_DATABASE_LOGIN> <RECOVERY_CATALOG_LOGIN>` command located in the `/opt/omni/lbin` directory on HP-UX systems and in the `/usr/omni/bin` directory on other UNIX systems. Refer to the *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide*, the *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*, or the *HP OpenView Storage Data Protector EMC Symmetrix Integration Guide* for a description of these command parameters.
2. After upgrading all Oracle8 clients, perform the upgrade of all Oracle8i/9i backup specifications stored on the Cell Manager by running the `/opt/omni/sbin/utilns/mrgcfg -ora_barlists` command on the UNIX Cell Manager or the `<Data_Protector_home>\bin\mrgcfg -ora_barlists` command on the Windows Cell Manager.

NOTE

After the upgrade procedure has completed, you can safely remove any Oracle8i/9i binaries from the backup system, as they are not required by Data Protector A.05.10.

Upgrading the Oracle8/9 Integration on Windows Systems

Perform the following steps to upgrade the Oracle8 integration on Windows systems:

1. Stop all Oracle8/9 services. Otherwise, the `orasbt.dll` file in the `<%SystemRoot%>\setup32` folder, which must be replaced during the upgrade procedure, is locked and remains unchanged until the next system restart.
2. Upgrade the client that has the Oracle8/9 integration installed either locally by running the `setup.exe` command or remotely by pushing the Oracle8/9 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8/9 services.
4. It is recommended that you move the environmental variables set in the `omnirc` file to Data Protector Oracle8/9 configuration files. Refer to “Data Protector Oracle8/9 Configuration Files” in the *HP OpenView Storage Data Protector Integration Guide* for details.

NOTE

After the upgrade to Data Protector A.05.10, copy the new templates from the `<Data_Protector_home>\NewConfig\dltemplates\lists\oracle8` directory to the `<Data_Protector_home>\Config\dltemplates\lists\oracle8` directory, where the old templates are stored.

MS Cluster Server

No further configuration is needed for the Oracle8/9 integration running in the MS Cluster Server environment.

Upgrading the SAP R/3 Integration on UNIX Systems

Perform the following steps to upgrade the SAP R/3 integration on UNIX systems:

1. If the SAP R/3 integration is installed together with the Oracle8/9 integration on the same client system, stop the Oracle8/9 services before the upgrade.
2. Upgrade the client either locally by running the `omnisetup.sh -install sap` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify `-install sap`. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.
3. If SAP R/3 uses the Oracle 8.0.5 database (all UNIX platforms) or the Oracle 8.0.6 database (32-bit version on Solaris), relink the Oracle 8.0.x binary with the `libob2oracle8.sl` (HP-UX systems), the `libob2oracle8.a` (AIX systems), or the `libob2oracle8.so` (Solaris systems) Data Protector Database Library. Note that on Solaris the path to the `libob2oracle8.so` Database Library has changed from `/usr/omni/lib` to `/opt/omni/lib`. For details, refer to “Linking Oracle8/9 with the Data Protector Database Library” in the *HP OpenView Storage Data Protector UNIX Integration Guide*.

If SAP R/3 uses the Oracle8i/9i database on Solaris, remove only the soft link pointing to `/usr/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`) and point it to a new location: `/opt/omni/lib/libob2oracle8.so` (`libob2oracle8_64bit.so`).

4. Start the Oracle8/9 services if they were stopped.

If your SAP R/3 integration is running in the ZDB environment, you need to perform additional steps, described on page 244, to successfully finish the upgrade.

Zero Downtime Backup (ZDB)

If the SAP R/3 integration is used with HP StorageWorks Disk Array XP, HP StorageWorks VA or EMC Symmetrix, first upgrade the SAP R/3 integration following the standard SAP R/3 integration upgrade procedure for UNIX systems, and then proceed as follows:

1. Make sure the SAP R/3 Database Server is configured on the application system. If not, configure it following the procedure described in the *HP OpenView Storage Data Protector UNIX Integration Guide*.
2. Change the value of the SAP R/3 parameter `primary_db` from `<SERVICE_NAME>` to `LOCAL` in the SAP R/3 initialization profile (`<ORACLE_HOME>/dbs/init<SID>.sap`).

NOTE

On the backup system, any SAP R/3 and Oracle8i/9i application binaries can be safely removed, as they are not required by Data Protector A.05.10.

Upgrading the SAP R/3 Integration on Windows Systems

Perform the following steps to upgrade the SAP R/3 integration on Windows systems:

1. If the SAP R/3 integration is installed together with the Oracle8/9 integration on the same client system, stop the Oracle8/9 services before the upgrade.
2. Upgrade the client either locally by running the `setup.exe` command or remotely by pushing the SAP R/3 integration agent to the client using the Data Protector GUI.
3. Start the Oracle8/9 services if they were stopped.

MS Cluster Server No further configuration is needed for the SAP R/3 integration running in the MS Cluster Server environment.

Upgrading Other Integrations

If the Data Protector client has the MS Exchange, MS SQL, Sybase, Informix, HP StorageWorks Disk Array XP, or EMC Symmetrix integration installed, upgrade these clients 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 Clients” on page 108. Note that if you are 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 as installed on the system before the upgrade without issuing a prompt.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.05.10, proceed as follows:

1. Upgrade the MoM Manager to Data Protector A.05.10.

During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with A.04.x Cell Managers.

2. Upgrade each Cell Manager in a MoM environment.

For upgrade procedure, refer to “Upgrading the HP-UX Cell Manager and Installation Server” on page 233 and “Upgrading the Windows Cell Manager and Installation Server” on page 235.

NOTE

Device sharing between the Data Protector A.05.10 MoM and the cells with earlier versions installed is not supported.

Upgrading from Data Protector A.05.00

The Data Protector A.05.00 release version can be directly upgraded to Data Protector A.05.10 for UNIX and Windows platforms.

Licenses

The existing Data Protector A.05.00 licenses are fully compatible and valid for use with Data Protector A.05.10. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

Upgrade Sequence

For information about the upgrade sequence, refer to “Upgrade Overview” on page 189.

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.

NOTE

You must have root permissions to perform the upgrade.

Upgrading on HP-UX Systems

The HP-UX Cell Manager is upgraded automatically when the `omnisetup.sh` command is run. This command removes the existing package set using the `swremove` utility and installs OMNI-CORE, OMNI-CC, OMNI-CS, OMNI-DA, and OMNI-MA packages using the `swinstall` utility.

If the HP-UX Installation Server is installed together with the Cell Manager, or it is installed without client components, it is upgraded automatically when the `omnisetup.sh` command is run.

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 157.

MC/ServiceGuard The upgrade procedure for the Cell Manager, configured on MC/SG, is different 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 265.

Upgrade Procedure To upgrade the HP-UX Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert and mount the HP-UX installation CD-ROM to a mount point, for example:

```
mkdir /cdrom
mount /dev/cd0 /cdrom
```

If you want to have the DP_DEPOT directory, where the installation files are stored, on your local disk, proceed as follows:

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
```

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

```
cp -r /cdrom <cd_image_dir>
```

2. Run the `./omnisetup.sh` command. To run this command from the CD-ROM, execute:

```
cd /cdrom/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

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 CD-ROM to `<cd_image_dir>`, run the `omnisetup.sh` command without any parameters:

```
cd <cd_image_dir>/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

Refer to the `omnisetup.sh` man page for a description of the `omnisetup.sh` command.

3. After the A.05.00 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 Cell Manager” on page 16 and “Installing the Installation Server for UNIX” on page 30.

As soon as the procedure is completed, you can start using Data Protector.

What's Next?

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 253.

Upgrading on Solaris Systems

To upgrade the Solaris Cell Manager, run the `omnisetup.sh` command. This command removes the existing package set using the `pkgrm` utility and installs OB2-CORE, OB2-CC, OB2-CS, OB2-DA, OB2MA, and OB2-MOM packages using the `pkgadd` utility.

If the Installation Server is installed together with the Cell Manager, or it is installed without client components, it is upgraded automatically when the `omnisetup.sh` command is run.

NOTE

The `omnisetup.sh` command checks the presence of the OB2-C-IS package to determine the status of the Installation Server. If this package is present, the Installation Server will be upgraded even if push packets were not originally installed.

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 `pkgadd` utility, and then reimport the upgraded Installation Server. For details, refer to “Importing an Installation Server to a Cell” on page 157.

NOTE

If the Installation Server resides on the system other than the Cell Manager, it should be upgraded locally from the Solaris installation CD-ROM. For the procedure, refer to “Installing the Installation Server for UNIX” on page 30.

To upgrade the Solaris Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert and mount the Solaris installation CD-ROM to a mount point, for example:

```
mkdir /cdrom
mount /dev/cd0 /cdrom
```

If you want to have the DP_DEPOT directory, where the installation files are stored, on your local disk, proceed as follows:

```
mkdir <directory>
cp -r /cdrom/DP_DEPOT <directory>
```

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

```
cp -r /cdrom <cd_image_dir>
```

2. Run the `./omnisetup.sh` command. To run this command from the CD-ROM, execute:

```
cd /cdrom/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

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 CD-ROM to `<cd_image_dir>`, run the `omnisetup.sh` command without any parameters:

```
cd <cd_image_dir>/LOCAL_DP_AGENT_INSTALL
./omnisetup.sh
```

Refer to the `omnisetup.sh` man page for a description of the `omnisetup.sh` command.

3. After the A.05.00 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 Cell Manager” on page 16 and “Installing the Installation Server for UNIX” on page 30.

As soon as the procedure is completed, you can start using Data Protector.

What's Next?

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 253.

Upgrading the Windows Cell Manager and Installation Server

The Windows installation is based on Microsoft Installer 2.0. 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 Cell Manager is upgraded automatically when the `setup.exe` command is run.

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 157.

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.05.10. For details, refer to “Upgrading from Windows NT to Newer Version of Windows” on page 263.

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 269.

Upgrade Procedure

To upgrade the Windows Cell Manager and Installation Server to Data Protector A.05.10, follow the procedure described below:

1. Insert the Windows installation CD-ROM and run the `i386\setup.exe` command.
2. After the A.05.00 version of Data Protector is detected, the upgrade procedure is automatically started. If you want to perform a clean upgrade (the database of a previous version will be deleted), uninstall the old version and restart the installation. At the `Custom Setup` page, the components previously installed on the system are selected. Note that you can change the component set.

For detailed steps, refer to “Installing a Windows Cell Manager” on page 25 and “Installing an Installation Server for Windows” on page 35.

As soon as the procedure is completed, you can start using Data Protector.

What’s Next?

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. Refer to “Checking Configuration Changes” on page 253.

Checking Configuration Changes

Global Options File

During the upgrade, the contents of the *old* global options file residing in the `/etc/opt/omni/options` directory on UNIX Cell Manager, or in the `<Data_Protector_home>\Config\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/options` - UNIX Cell Manager
- `<Data_Protector_home>\NewConfig\Options` - Windows Cell Manager

The *merged file*, which is named `global`, resides in the `/etc/opt/omni/options` directory on UNIX Cell Manager, or in the `<Data_Protector_home>\Config\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.05.10
# 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.05.10
# 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>
```

Upgrading to Data Protector A.05.10

Upgrading from Data Protector A.05.00

```
# Data Protector A.05.10
# 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/options/global` on UNIX Cell Manager and `<Data_Protector_home>\config\options\global` on Windows Cell Manager. The section “Global Options File” in the *HP OpenView Storage Data Protector Administrator’s 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 Administrator’s Guide*.

- Command line

Refer to Appendix B, “Command Line Changes After Upgrading to Data Protector A.05.10” on page B-37 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 255.

Upgrading the Clients

- Prerequisite** If you are upgrading the Oracle8/9 integration or the SAP R/3 integration installed together with the Oracle8/9 integration, the Oracle8/9 services must be stopped before the upgrade.
- Upgrade Sequence** For information about the sequence in which the client upgrade is performed, refer to “Upgrade Overview” on page 189.
- Upgrading Clients Remotely** For the procedure on how to upgrade the clients using the Installation Server, refer to “Distributing the Data Protector Software to Clients” on page 43.
- 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 “Local Installation of Windows Clients” on page 57. To upgrade UNIX clients locally, refer to “Local Installation of UNIX Clients” on page 108. Note that for the local upgrade of Solaris clients the HP-UX, and not the Solaris installation CD-ROM must be used.
- Novell NetWare** After upgrading any Novell NetWare 4.x or 5.0 client, you need to perform some additional steps that will enable you to perform any backup and restore of the NDS (Novell NetWare 4.x) / NDS eDirectory (Novell 5.x and later) database. Refer to “Local Installation of the Novell NetWare Clients” on page 92 for details.
- Upgrading Clients Configured on MC/ServiceGuard** If you are upgrading the client that uses MC/ServiceGuard, 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 the Data Protector client has integrations installed (such as Oracle8/9, SAP R/3, MS Exchange 2000, MS SQL 7.0/2000, HP StorageWorks Disk Array XP, EMC Symmetrix, etc.), first upgrade the Data Protector integration on the client either locally by running 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, and then additional integration specific steps may be required. Note that on UNIX, if you are 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 as installed on the system before the upgrade without issuing a prompt.

Special attention should be paid to the Oracle8/9 integration, the SAP R/3 integration, and the Microsoft SQL 7.0/2000 integration in a zero downtime backup environment.

Oracle8/9 Integration

The clients that have the Oracle8/9 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 Oracle8/9 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 -install oracle8. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

All Oracle8/9 services must be stopped before the upgrade. Otherwise, the Oracle8/9 integration library, which must be replaced during the upgrade procedure, is locked and thus remains unchanged.

After the upgrade procedure has completed, start the Oracle8/9 services.

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 -install sap. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

If the SAP R/3 integration is installed together with the Oracle8/9 integration on the same client system, stop the Oracle8/9 services before the upgrade.

After the upgrade, start the Oracle8/9 services if they were stopped.

MS SQL 7.0/2000 Integration in a ZDB Environment

The Microsoft SQL 7.0/2000 integration in a zero downtime backup environment must be upgraded in order to use the restore to a point of failure functionality. This integration is upgraded automatically during the client upgrade either locally by using the `setup.exe` command, or remotely by pushing the MS SQL 7.0/2000 integration agent to the client using the Data Protector GUI.

For information on the restore to a point of failure functionality, refer to *HP OpenView Storage Data Protector Windows Integration Guide*.

Upgrading in a MoM Environment

To upgrade your MoM environment to Data Protector A.05.10, proceed as follows:

1. Upgrade the MoM Manager to Data Protector A.05.10.

During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with A.05.00 Cell Managers.

2. Upgrade each Cell Manager in a MoM environment.

For upgrade procedure, refer to “Upgrading the UNIX Cell Manager and Installation Server” on page 247 and “Upgrading the Windows Cell Manager and Installation Server” on page 251.

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.05.10 Single Server Edition. For details, refer to “Upgrading from Earlier Versions of SSE to Data Protector A.05.10 SSE” on page 258.
- From Data Protector A.05.10 Single Server Edition to Data Protector A.05.10. For details, refer to “Upgrading from Data Protector A.05.10 SSE to Data Protector A.05.10” on page 258.

Upgrading from Earlier Versions of SSE to Data Protector A.05.10 SSE

The upgrade procedure from earlier versions of SSE to Data Protector A.05.10 SSE is the same as the upgrade procedure from earlier versions of Data Protector to Data Protector A.05.10. For the information, refer to “Upgrading from OmniBack II A.03.50” on page 191, “Upgrading from OmniBack II A.03.51” on page 215, “Upgrading from OmniBack II A.04.x” on page 233, and to “Upgrading from Data Protector A.05.00” on page 247.

Upgrading from Data Protector A.05.10 SSE to Data Protector A.05.10

Licenses

You need to have a license to perform the upgrade from Data Protector A.05.10 Single Server Edition to Data Protector A.05.10. For details about licensing, refer to Chapter 5, “Data Protector Licensing,” on page 273.

The upgrade from Data Protector A.05.10 Single Server Edition to Data Protector A.05.10 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 259.

- 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 259.

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.05.10, refer to “Upgrading from OmniBack II A.03.50” on page 191, “Upgrading from OmniBack II A.03.51” on page 215, “Upgrading from OmniBack II A.04.x” on page 233, or “Upgrading from Data Protector A.05.00” on page 247.

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\Cell\lic.dat`
 - on UNIX:
`rm /etc/opt/omni/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 9.
2. Upgrade the selected Cell Manager by performing the following:
 - a. Remove the Single Server Edition license:
`del <Data_Protector_home>\Config\Cell\lic.dat`
 - 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 175.
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. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for the information about importing media and details about the `List from media restore`.

Upgrading from HP-UX 10.20 to HP-UX 11.x Systems

If you have the Cell Manager installed on the HP-UX 10.20 system, you must upgrade the operating system to HP-UX 11.x, as HP-UX 10.20 is not supported by Data Protector A.05.10 as a Cell Manager platform.

Perform the upgrade procedure as follows:

1. Log in as root and shut down the OmniBack II services on the Cell Manager system 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 services listed after executing the `ps -ef | grep omni` command.
2. Remove old OmniBack II files using the `/usr/sbin/swremove` utility.

Configuration files and the database are preserved during this procedure.
3. Run the `swlist` command to check that OmniBack II is not listed. In the following directories, verify that you only removed the software, and not the database and configuration files:
 - `/opt/omni`
 - `/var/opt/omni`
 - `/etc/opt/omni`
4. Upgrade the HP-UX 10.20 system to 11.x. For more information, refer to HP-UX 11.x documentation.
5. Insert the HP-UX installation CD-ROM and run `/usr/swinstall` to upgrade the Cell Manager and Installation Server to Data Protector A.05.10.

Refer to “Installing the Data Protector Cell Manager (CM) and Installation Server(s) (IS)” on page 15.

The Cell Manager and Installation Server software is installed as for a new installation.

Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. For details, refer to “Checking Configuration Changes” on page 203 and to “Checking Configuration Changes” on page 237.

Upgrading from Windows NT to Newer Version of Windows

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.

There are two possibilities you perform the upgrade from Windows NT to a newer version of Windows depending on the following:

- You have OmniBack II A.03.50, A.04.x, or Data Protector A.05.00 installed on Windows NT.
- You have Data Protector A.05.10 installed on Windows NT.

OmniBack II A.03.50, A.04.x, or Data Protector A.05.00 Installed on Windows NT

If you have the OmniBack II A.03.50, A.04.x, or the Data Protector A.05.00 Cell Manager installed on Windows NT, and you want to upgrade it to Data Protector A.05.10, 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.

IMPORTANT

If you have OmniBack II A.03.50 or OmniBack II A.04.00 on Windows NT, and you are upgrading your operating system from Windows NT to Windows XP or Windows Server 2003, beware that these versions of OmniBack II will not work on Windows XP/Server 2003 platforms. That's why, after the operating system upgrade, you must go directly to upgrading to Data Protector A.05.10 without using OmniBack II A.03.50 or OmniBack II A.04.00 on Windows XP/Server 2003.

2. Upgrade the OmniBack II A.03.50, A.04.x, or the Data Protector A.05.00 Cell Manager to Data Protector A.05.10. For the procedure, refer to “Upgrading from OmniBack II A.03.50” on page 191, “Upgrading from OmniBack II A.04.x” on page 233, or “Upgrading from Data Protector A.05.00” on page 247.

Data Protector A.05.10 Installed on Windows NT

If you already have the Data Protector Cell Manager installed on Windows NT and want to upgrade your operating system, perform the procedure described below:

1. Make a list of components currently installed on your system.
2. Stop all Data Protector services by running the `omnisv -stop` command.
3. Copy `<Data_Protector_home>\config` and `<Data_Protector_home>\db40` folders to a temporary location.
4. Uninstall the Data Protector software. For the procedure, refer to “Uninstalling the Cell Manager and Installation Server” on page 177.
5. Upgrade the operating system from Windows NT to a newer version of Windows. For more information, refer to Windows documentation.
6. Install Data Protector A.05.10. During the installation procedure, select the same set of components as you had installed on the previous system. For the installation procedure, refer to “Installing a Windows Cell Manager” on page 25.
7. Stop all Data Protector services by running the `omnisv -stop` command.
8. Delete `<Data_Protector_home>\config` and `<Data_Protector_home>\db40` folders.
9. From the temporary location, copy `\config` and `\db40` back to `<Data_Protector_home>`.
10. Start the Data Protector services by running the `omnisv -start` command.

If you have Data Protector A.05.10 client(s) installed on Windows NT, and you want to upgrade your operating system from Windows NT to a newer version of Windows, first uninstall the client(s), and then install and configure them again after the operating system upgrade. Refer to “Uninstalling a Data Protector Client” on page 176 and “Installing Windows Clients” on page 51.

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.05.10 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 OmniBack II A.03.50, A.04.x, and Data Protector A.05.00 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 ob2c1
```

2. Deactivate the cluster mode for the volume group:

```
vgchange -c n <vg_name>
```

The `<vg_name>` parameter is 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>
```

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
```

5. Upgrade the Cell Manager following the procedure described in the below sections. Note that the steps are different depending on the product version you are upgrading from to Data Protector A.05.10:
 - To upgrade the OmniBack II A.03.50 Cell Manager, follow the steps described in “Step-by-Step Upgrade Procedure” on page 196 in “Upgrading from OmniBack II A.03.50” chapter.
 - To upgrade the OmniBack II A.04.x Cell Manager, follow the steps described in “Step-by-Step Upgrade Procedure” on page 234 in “Upgrading from OmniBack II A.04.x” chapter.
 - To upgrade the Data Protector A.05.00 Cell Manager, follow the steps described in “Upgrading on HP-UX Systems” on page 247 in “Upgrading from Data Protector A.05.00” chapter.
6. Stop the Data Protector services if they are running:

```
/opt/omni/sbin/omnisv -stop
```

7. Unmount the shared disk:

```
umount <shared_disk>
```

For example:

```
umount /omni_shared
```

8. 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. Deactivate the cluster mode for the volume group:

```
vgchange -c n <vg_name>
```

2. Activate the volume group:

```
vgchange -a y -q y <vg_name>
```

3. Mount the logical volume to the shared disk:

```
mount <lv_path> <shared_disk>
```


4. Upgrade the Cell Manager. The steps are different depending on the product version you are upgrading from to Data Protector A.05.10.
 - When upgrading the Cell Manager on the secondary node from OmniBack II A.03.50, you need to perform the core part upgrade only. Do not perform the detail part upgrade.
To upgrade the OmniBack II A.03.50 Cell Manager, run the `omnisetup.sh` command. Refer to the `omnisetup.sh` man page for a description of this command.
 - To upgrade the OmniBack II A.04.x Cell Manager, follow the steps described in “Step-by-Step Upgrade Procedure” on page 234 in “Upgrading from OmniBack II A.04.x” chapter.
 - To upgrade the Data Protector A.05.00 Cell Manager, follow the steps described in “Upgrading the UNIX Cell Manager and Installation Server” on page 247 in “Upgrading from Data Protector A.05.00” chapter.
5. Copy the new `csfailover.sh` and the `mafailover.ksh` scripts from the `/opt/omni/newconfig/etc/opt/omni/sg` directory to the `/etc/opt/omni/sg` directory.
6. Stop the Data Protector services if they are running:
`/opt/omni/sbin/omnisv -stop`
7. Unmount the shared disk:
`umount <shared_disk>`
8. Deactivate the volume group:
`vgchange -a n <vg_name>`

Primary Node

Log on to the primary node again and perform the following steps:

1. Activate the cluster mode for the volume group:
`vgchange -c y <vg_name>`
2. Restart the Data Protector package:
`cmrunpkg <pkg_name>`

Make sure that the package switching and switching for nodes options are enabled.

3. 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
```
4. Reimport the virtual host:

```
omnicc -import_host <virtual_hostname> -virtual
```
5. Change the Cell Manager name in the IDB:

```
omnidbutil -change_cell_name
```
6. If you have the Installation Server, you need to import the 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 164 for information on how to secure a cell.

Upgrading the Cell Manager Configured on Microsoft Cluster Server

The upgrade of the OmniBack II A.03.50, A.04.x, or Data Protector A.05.00 Cell Manager to Data Protector A.05.10 on Microsoft Cluster Server (MSCS) is performed locally, from the Windows installation CD-ROM.

The setup must be started on the currently active virtual server node. The installation gathers the data, such as the installed component set, configuration settings, etc., from the active node only; the configuration of every node separately is not possible. Other cluster nodes have the binaries and registry entries copied from the active node.

IMPORTANT

All cluster nodes must have MSI 2.0 installed.

To perform the upgrade, follow the steps described below:

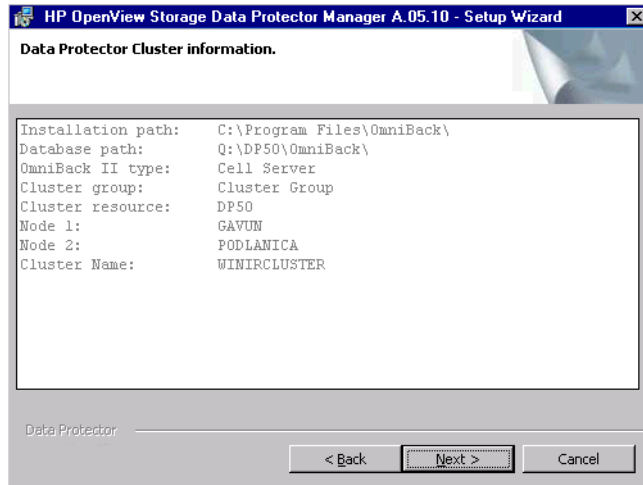
1. Insert the Windows installation CD-ROM and run `i386\setup.exe`.

Setup automatically detects the old version of the product and prompts you to upgrade it to Data Protector A.05.10.

Setup also detects that the old version of the product is running on Microsoft Cluster Server and will ask you if you want to install the Data Protector cluster-aware integration.

The Data Protector cluster information is displayed.

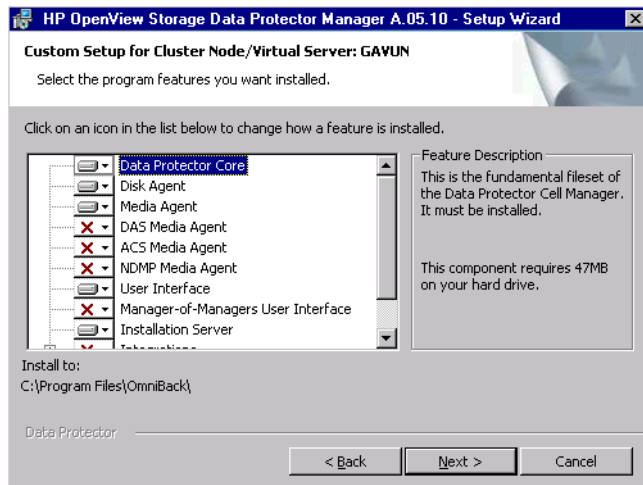
Figure 4-5 Data Protector Cluster Information



Click Next to continue.

2. Select the Data Protector components you want to install.

Figure 4-6 Cluster Common Setup



3. In the next window, click `Install` to perform the upgrade.

Note that after the upgrade, every node has the same component set.

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.

Upgrading to Data Protector A.05.10

Upgrading the Cell Manager Configured on Microsoft Cluster Server

5 **Data Protector Licensing**

In This Chapter

This chapter contains information about how to obtain and install Data Protector passwords.

Introduction

The Data Protector A.05.10 product structure is based in performance. The more drive licenses that are installed, the more tape drives can be used for backup in parallel, thus the faster the backup will be performed.

The product structure is modular and offers a lot of flexibility. You can order the license that provides the Data Protector functionality, which best meets the specific requirements of your environment.

The Data Protector A.05.10 product structure and licensing consists of three main categories:

1. The base Cell Manager product

The Cell Manager is supported on HP-UX, Windows, and Solaris. Regarding the Cell Manager system, you can begin a cell configuration with the single Drive Starter Pack, required once as the initial starting point.

2. Additional tape drive licenses, referred to as Drive Extensions, for one concurrently used backup drive.

3. Data Protector Functional Extensions

The functional extensions licenses are required once per instance (system, library and terabyte) for on-line backup of databases and applications, the Manager-of-Managers functionality, for libraries with more than 60 media slots, for Open File backup, Direct backup, Instant Recovery, NDMP, and zero downtime backup.

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.

Which Licenses Are Available?

Data Protector licenses are available for the UNIX and Windows platforms. All UNIX products include the corresponding Windows and Novell NetWare products. The Windows license includes corresponding Linux and Novell NetWare products.

Figure 5-1

The HP OpenView Storage Data Protector Products Overview

starter packs		any platform	Windows	Solaris	HP-UX
LTU, media & manuals			B6961AA/J/F B6961BA	B6951DA/J B6951CA	B6951AA/J B6951BA
	LTU only				
	media only	B6960MA			
	manuals only	B6960LA/J/F			
drive extensions		SAN, NAS	Windows, Netware, Linux	UNIX/OpenVMS	
LTU		B6953AA	B6963AA	B6953AA	
functional extensions		any platform	Windows	UNIX	
on-line backup LTU	1x system		B6965BA (also Linux)	B6955BA	
open file backup LTU	1x server		B7033AA		
	1x 10-servers		B7033BA		
	1x 5-workstations		B7034AA		
	1x enterprise server		B7035AA (+ Netware)		
manager-of-managers LTU	1x system		B6966AA	B6956AA	
library LTU	1x 61-250 slots	B6957BA			
	1x unlimited slots	B6958BA			
direct backup with NDMP LTU	1x TB		B7022BA		
manuals for functional extensions		B6960EAA/J			
		HP XP or compatible	HP VA/EVA	HP MSA1000	EMC
zero downtime backup LTU	1x TB	B7023CA	B7025CA	B7036AA*	B6959CA
instant recovery	1x TB	B7026CA	B7028AA*	B7037AA*	
direct backup	1x TB	B7027AA	B7029AA*		
single server edition		any platform	Windows	Solaris	HP-UX
LTU, media & manuals			B7030AA/J/F B7030BA	B7020DA/J B7020CA	B7020AA/J B7020BA
	LTU only				
	migration to starter pack		B7031AA	B7021DA	B7021AA

* For the currently supported functionality for the devices associated with these licenses, refer to the support matrix

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.05.10 Product Structure and Licenses” on page A-3 for more 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)*.

If you want to move licenses for products that can no longer be purchased, please use the License Move Forms delivered with OmniBack II A.03.x.

- 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.

Data Protector Passwords

The Data Protector operation is enabled as soon as the passwords are installed on the Cell Manager.

Once you have installed the Data Protector product on your network, 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.

Obtaining a Permanent Password

The following is the procedure to obtain a permanent password:

1. Gather the information required in the Permanent Password *Request Form*. See “Data Protector Licensing Forms” on page A-24 to find the location of the forms and get instructions on how to fill them out.
2. 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)*.

See “Data Protector A.05.10 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.

You will receive your permanent password within 24 hours of sending your *Permanent Password Request Form*.

3. Install the permanent password that the *HP Password Delivery Center (HP PDC)* has sent back to you. See “Installing a Password on the Cell Manager” on page 280.

Installing a Password on the Cell Manager

Prerequisites

You must have received the permanent password 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

A permanent password can be installed on the Cell Manager using the Data Protector GUI. Proceed as follows:

1. Start the Data Protector GUI.
2. In the Context List, select `Clients`. In the Scoping Pane, right-click `Data Protector Cell`, and then select `Add License`.
3. In the `Add License` window, enter 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 for a password:

```
4PXV EG9S B6WS 2VX3 5967 XEZK AAA9 MQJB "Product: B6963AA"
```

After you have typed in your 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.
4. After you have entered the password, click OK to close the window. The password is written to the following file:
 - On Windows:
`<Data_Protector_home>\Config\Cell\lic.dat`
 - On UNIX: `/etc/opt/omni/cell/lic.dat`

Verifying the Password

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

Follow the procedure below to install the permanent password using the command line:

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 in the Password Certificate.

You can also append the password to the following file:

- On Windows: `<Data_Protector_home>\config\cell\lic.dat`
- On UNIX: `/etc/opt/omni/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

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.

IMPORTANT

If you have installed an OmniBack II A.04.x Cell Manager permanent password for Multi-Drive Server, you have to exit the Data Protector Manager and restart the services using the `omnisv -stop`, and then `omnisv -start` command from the `/opt/omni/sbin` directory.

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 GUI.
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-24.

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\cell\lic.dat
 - On UNIX: /etc/opt/omni/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

If you run into problems installing Data Protector, use the suggestions in this section to get back on track. This chapter includes information on:

- Actions you perform before contacting *HP Support*. Refer to “Before Calling Your Support Representative” on page 287.
- Name Resolution Problems. Refer to “Ease of Deployment” on page 289.
- How to verify DNS connections in the cell. Refer to “Verifying DNS Connections within Data Protector Cell” on page 290.
- Troubleshooting the Data Protector installation and upgrade on Windows. Refer to “Installing and Upgrading Data Protector on Windows” on page 293.
- Troubleshooting the Solaris Cell Manager installation. Refer to “Installing the Data Protector Cell Manager on Solaris” on page 294.
- Troubleshooting the HP-UX client installation. Refer to “Installing UNIX Clients” on page 295.
- How to verify your Data Protector installation. Refer to “Verifying Data Protector Client Installation” on page 296.
- Upgrading the IDB on Solaris. Refer to “Troubleshooting Upgrade” on page 298.
- The system’s log files (on UNIX), setup log files (on Windows), and the Data Protector log files, which can give you some helpful information on your problem. Refer to “Using Log Files” on page 303.
- How to create installation execution traces (installation debugs), which the support representative will need in order to determine the problem. Refer to “Creating Installation Execution Traces” on page 305.

Before Calling Your Support Representative

To speed up the process of solving your problem, you should prepare before reporting a problem to HP Customer Support Service. See the suggestions below for preliminary steps you can take.

Check if you encountered any of the problems described in this chapter and perform the recommended tasks. Refer to the following sections:

- “Ease of Deployment” on page 289.
- “Verifying DNS Connections within Data Protector Cell” on page 290.
- “Installing the Data Protector Cell Manager on Solaris” on page 294.
- “Installing and Upgrading Data Protector on Windows” on page 293.
- “Installing UNIX Clients” on page 295.
- “Verifying Data Protector Client Installation” on page 296.
- “Troubleshooting Upgrade” on page 298.

Ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Data Protector limitations and recommendations, as well as on known Data Protector and non-Data Protector problems, see the *HP OpenView Storage Data Protector Software Release Notes*.
- Your problems are not related to third-party hardware and software. If they are, contact the third-party vendor for support.
- You have the latest Data Protector patches installed. Patches can be obtained from the HP OpenView Web site: http://support.openview.hp.com/patches/patch_index.jsp. The list of OS patches is available in the *HP OpenView Storage Data Protector Software Release Notes*.

To check which Data Protector patches are installed on your system, refer to “Verifying Which Data Protector Patches Are Installed” on page 172.

Before Calling Your Support Representative

When reporting to HP Customer Support Service, collect the following data about the problem you encountered:

- A description of your problem, including the session output (or equivalent output, depending on the type of problem).
- Output from the `get_info` command located in the following directory:
 - On UNIX: `/opt/omni/sbin/utilns`
 - On Windows: `<Data_Protector_home>\bin\utilns`

The script collects system data from your Data Protector Cell Manager, and configuration data about your Data Protector installation.

- All log files from the Cell Manager and from all clients involved.

Ease of Deployment

Ease of deployment is used to effectively troubleshoot name resolution problems.

During the installation of the Windows Cell Manager, Data Protector detects and warns you in case the DNS or the LMHOST file is not set up as required. In addition, Data Protector notifies you if the TCP/IP protocol is not installed on your system.

You can get the following warning messages:

Name Resolution Problems

- 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 the LMHOST file, you get a warning message to check your LMHOSTS file configuration.
- If you have not configured either DNS or LMHOST, you get a warning message to enable the DNS or the LMHOSTS resolution in the TCP/IP properties dialog.
- To solve name resolution problems, check your DNS or LMHOST file configuration.

For general information on networking and communication problems refer to the *HP OpenView Storage Data Protector Administrator's Guide*. See online Help for more information.

TCP/IP Protocol Not Installed

- If the TCP/IP protocol is not installed and configured on your system, the installation is aborted.

To determine this problem refer to “Setting Up the TCP/IP Protocol on Windows Systems” on page B-3.

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

Limitations

The `omnicheck` command has the following limitations:

- It 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.

Using the `omnicheck` command

The `omnicheck` command resides on the Cell Manager in the following directory:

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

The synopsis of the `omnicheck` command is as follows:

```
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.

Refer to the omnicheck man page for more information.

Return Messages Table 6-1 lists the return messages for the omnicheck command. If the return message indicates a DNS resolution problem, refer to the “Troubleshooting Networking and Communication” section of the *HP OpenView Storage Data Protector Administrator’s 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 <code><%SystemRoot%>\System32\drivers\etc\hosts</code> (Windows systems) or <code>/etc/hosts</code> (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.	

Installing and Upgrading Data Protector on Windows

After installation or upgrade to Data Protector A.05.10, Windows may report that some applications are not installed or that a reinstall is required.

How to Identify the Problem

The following error messages may be reported by Windows:

- 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.

The reason is an error in 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.

How to Solve the Problem?

This problem is described in the Microsoft Knowledge Base article Q324906. Please refer to this article to solve the problem.

Installing the Data Protector Cell Manager on Solaris

Installation of the Data Protector Cell Manager on Solaris may fail.

How to Identify the Problem?

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>
```

How to Solve the Problem?

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`.

Installing UNIX Clients

Remote Installation of UNIX Clients Fails

How to Identify the Problem Remote installation or upgrade of a UNIX client fails with the following error message:

```
Installation/Upgrade session finished with errors.
```

How to Solve the Problem? 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.

Check if you have enough disk space in the above mentioned directories and restart the installation or upgrade procedure.

For disk space requirements, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

Problems with the Installation of an HP-UX client

How to Identify the Problem When adding a new HP-UX client to a Data Protector cell, the following error message may be 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.
```

How to Solve the Problem? To resolve this problem, 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.

You also need to ensure that you have a local host, loopback entry in the `hosts` file (`/etc/hosts`).

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.

NOTE

An Installation Server must be available for the type of client system (UNIX, Windows) that you select.

You verify a Data Protector installation using the Data Protector GUI by performing the following steps:

NOTE

This procedure is not applicable for Novell NetWare and MPE clients.

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.

Refer to online Help for details.

If your installation has not succeeded, refer to “Using Log Files” on page 303.

For information on how to verify the installation on UNIX systems using the Data Protector command-line interface, refer to the `ob2install` man page.

Troubleshooting Upgrade

IDB and Configuration Files Are not Available After Upgrade

After upgrading the Cell Manager from the previous release versions, IDB and all configuration information are not available. This occurs if the upgrade procedure was interrupted for any reason.

How to Solve the Problem?

Restore OmniBack II/Data Protector from the backup made before the upgrade, eliminate the reason of the interruption, and start the upgrade again.

Upgrade of the IDB Core Part

How to Determine the Status?

You can determine the status of the IDB core part upgrade by using:

- The `upgrade.log` file. This file is created when the IDB core part upgrade is started. It is located in the `/var/opt/omni/log` directory on UNIX systems, and in the `<Data_Protector_home>\log` directory on Windows systems.

The `upgrade.log` file contains core and detail part upgrade messages, which enable you to see the status of the upgrade. You can see when a session was started, when it ended, and any problems that occurred during the upgrade.

- The `omnidbutil -upgrade_info` command, which displays the current state of the IDB. This command is located in the `/opt/omni/sbin` directory on UNIX systems and in the `<Data_Protector_home>\bin` directory on Windows systems. There are five possible states:
 - No upgrade in progress - database was initialized, UCP was not started
 - Upgrade of critical part failed - UCP was started, but failed
 - Upgrade of critical part finished - UCP finished successfully, UDP was not started
 - Upgrade of detail part running - UDP was started and is currently

running

- Upgrade of detail part finished - UDP finished

System Crashes During the Core Part Upgrade

Your Cell Manager crashes during the core part upgrade.

How to Verify?

Check the `upgrade.log` file. It contains "UCP session started" entry but it does not contain either "UCP session finished" or "Session was aborted (Upgrade core part)" log.

You can also verify the status of the core upgrade by using the `omnidbutil -upgrade_info` command, which reports "Core upgrade failed".

How to Solve the Problem?

Check if the services are running. If not, start them. Run the `omnidbinit` command to initialize the new database. The A.03.5x database is set to read-only mode and is therefore left intact. Run the `omnidbupgrade -ucp` to restart the core part upgrade. When the core part upgrade is finished, perform the detail part upgrade.

Upgrade of the IDB Detail Part

How to Determine the Status?

You can determine the status of the upgrade of the detail part by using:

- The `omnistat` command with a subcommand `-session <SessionID> -monitor` to view the progress of the upgrade of the detail part
- The `Monitor` context from the Data Protector GUI where you can also view the details of the progress
- The `upgrade.log` file. You can examine the `upgrade.log` file to see the status of the upgrade, when a session was started and finished, and any errors that might have occurred during the upgrade of the detail part.

Detail Part Upgrade Runs Out of Memory

The detail part upgrade runs out of physical memory on the system.

How to Verify?

The RDS daemon is terminated. However, ASM will report the error and also write an error to the `upgrade.log` file (an entry like Database network communication error. will be displayed.). Also, an event will be fired (Session was aborted. (Upgrade detail part.)).

How to Solve the Problem?

Close any other applications that do not need to run. If the problem reoccurs, restart the computer.

Before you restart the upgrade, stop and restart the Data Protector services by running the following commands from the `/opt/omni/sbin` (UNIX systems) or the `<Data_Protector_home>\bin` (Windows systems) directory:

```
omnisv -stop
```

```
omnisv -start
```

Restart the detail part upgrade by using the `omnidbupgrade -udp` command, which will restart the upgrade process.

In case the problem persists, add more RAM into the computer. You can also configure a bigger data segment. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a list of installation requirements.

Detail Part Upgrade Runs Out of Disk Space

During the IDB detail part upgrade, the disk on which the database resides runs out of space.

How to Verify?

Check the `upgrade.log` file for the error. A log entry "Not enough disk space or not enough configured extension/binary files to perform upgrade" is included after the entry "UDP session started".

Also check the system applications to view the resources available on the disk where the database resides.

How to Verify Required Disk Space?

Run the `omnidbupgrade -udpcheck` command after the core part upgrade has finished to view the disk space required to run the detail part upgrade of the database.

How to Solve the Problem?

Free up space on the disk where the database is located. Run the `omnidbupgrade -udp` command to restart the detail part upgrade of the database.

The Database Is in Incorrect State

When upgrading the IDB detail part, you receive the message that the database is in incorrect state.

How to Verify? Run the `omnidbutil -upgrade_info` command, which reports the following:

```
No upgrade in progress
Upgrade of core upgrade failed
Upgrade of core part finished
Upgrade of detail part running
Upgrade of detail part finished
```

How to Solve the Problem? Run the `omnidbinit` command to initialize the new database. The A.03.5x database is set to read-only mode and is therefore left intact. Run the `omnidbupgrade -ucp` to restart the core upgrade. When the core part upgrade is finished, continue with the detail part upgrade. If the problem persists, run the upgrade with the `debug` option and send the output together with the `upgrade.log` file to your support representative.

Manual Upgrade Procedure

Normally, you upgrade the OmniBack II A.03.5x, OmniBack II A.04.x and Data Protector A.05.00 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 following the steps given below:

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.sh -stop (OmniBack II A.03.5x) or /opt/omni/sbin/omnisv -stop (OmniBack II A.04.x and Data Protector A.05.00)` 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. Remove old OmniBack II/Data Protector files using the `/usr/sbin/swremove` utility on HP-UX systems, or the `/usr/sbin/pkgrm` utility on Solaris systems.

The configuration files and the database are preserved during this procedure.

3. Run the `swlist` command on HP-UX systems, or the `pkginfo` command on Solaris systems to check that OmniBack II/Data Protector is not listed. In the following directories, verify that you only removed the software, and not the database and configuration

files:

- /opt/omni
 - /var/opt/omni
 - /etc/opt/omni
4. Insert the HP-UX or Solaris installation CD-ROM and run `/usr/sbin/swinstall` on HP-UX systems or `/usr/sbin/pkgadd` on Solaris systems to upgrade the Cell Manager and Installation Server to Data Protector A.05.10.

When the command finishes, the Cell Manager and Installation Server software are installed as for a new installation. Note that after this is done, `swinstall` or `pkgadd` will start the Data Protector services, so you do not need to start them manually.

NOTE

If you are upgrading from OmniBack II A.03.5x, be aware that the above-described procedure upgrades only the IDB core part. To proceed with the upgrade, you need to perform the IDB detail part upgrade. Refer to “Upgrading from OmniBack II A.03.50” on page 191 or “Upgrading from OmniBack II A.03.51” on page 215 for the information on how to upgrade the detail part of the IDB.

Using Log Files

If you run into trouble installing Data Protector, you can look at any of the following log files to determine your problem: system log files (UNIX), setup log files (Windows), and the 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 you are using.

Local Installation In case of problems with local installation, check the following log files:

- On HP-UX Cell Manager:

`/var/adm/sw/swinstall.log`

and for more details:

`/var/adm/sw/swagent.log`

- On Solaris Cell Manager:

`/var/opt/omni/log/debug.log`

- On Windows clients (on the system where the setup is running):

`<Temp>\OB2SetupLauncher.log`

and for more details:

`<Temp>\OB2_Setup*.txt`

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*.*`

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 305.

Data Protector Log Files

The directory in which Data Protector log files are kept depends on which operating system you are using:

- On Windows: *<Data_Protector_home>*\log
- On HP-UX and Solaris: /var/opt/omni/log
- On other UNIX systems: /usr/omni/log
- On NetWare: SYS:\USR\OMNI\LOG

The following list shows the log files that are important for troubleshooting installation and describes what the log files do:

debug.log	Unexpected conditions are logged into this file. While some can be meaningful to the user, it will be used mainly by the support organization.
inet.log	Requests made to the Data Protector inet program (a program that starts agents) are logged to this file. It can be useful to check the recent activity of Data Protector on client systems.
IS_install.log	This file contains the trace of the remote installation and is located on the Installation Server.
omnisv.log	Contains data on starting and stopping Data Protector services.
Upgrade.log	This log is created on UNIX during the upgrade and contains traces of the upgrade processing.

Creating Installation Execution Traces

If after checking the log files you still have not found the necessary information for solving your installation problems, you can run the installation with the debug option and send the output (with other important information) to your support representative. See “Using Log Files” on page 303, and “Before Calling Your Support Representative” on page 287.

UNIX

For debugging the installation on a UNIX system, run the Data Protector graphical user interface with the debug option:

```
xomni -debug 1-99 <Debug_postfix>
```

or

```
xomniadmin -debug 1-99 <Debug_postfix>
```

For an explanation of the debug syntax, see “Debug Syntax” on page 306.

Once the session is finished/aborted, collect the debug output from the Installation Server system’s tmp directory.

Windows

For debugging remote installation on a Windows system, run the Data Protector GUI (Manager.exe) with the debug option:

```
Manager -debug 1-99 <Debug_postfix>
```

For an explanation of the debug syntax, see “Debug Syntax” on page 306.

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>
```

Debug Syntax

Almost all Data Protector commands can be started with an additional `-debug` parameter, which has the following syntax:

```
-debug 1-99 <XYZ> [<host>]
```

where:

1-99 is the debug range

<XYZ> is the debug postfix

<host> is the list of hostnames where debugging is turned on.

The range should always be specified as 1-99 unless instructed otherwise.

The list of hostnames limits the hosts where the debug is turned on during execution of the Data Protector command. If there are multiple hosts on the list, they should be delimited by space. The entire list must be enclosed in quotes. For example: "host1.domain host2.domain".

The debug postfix option is used for creating the trace file name. Trace files are created in the following directories:

- On UNIX: /tmp
- On Windows: <Data_Protector_home>\tmp
- On NetWare: SYS:\USR\OMNI\TMP

and named

```
OB2DBG_<did>__<Program>_<Host>_<pid>_<XYZ>
```

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.

<Program> is the code name of the Data Protector program writing the trace.

<Host> is the name where the trace file is created.

<pid> is the process ID.

<XYZ> is the postfix as specified in the `-debug` parameter.

For more general information on creating execution files (debugging), as well as for an example of debugging, refer to the Troubleshooting chapter of the *HP OpenView Storage Data Protector Administrator's Guide*.



A **Appendix A**

In This Appendix

This Appendix provides a description of the Data Protector A.05.10 product structure and Data Protector licensing forms.

Data Protector A.05.10 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 is based on the Single Drive Cell Manager Single Drive as the starting point, the number of 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.

This section explains the *Product Numbers* and types of licenses offered by Data Protector A.05.10 Cell Manager.

NOTE

The licenses delivered for the UNIX products can be applied either to UNIX or Windows.

Data Protector A.05.10 Cell Manager software is available for the HP-UX, Solaris and Windows platforms.

For a product overview, see Figure A-1 on page A-4.

Figure A-1 provides an overview of the available Data Protector A.05.10 products.

Figure A-1

HP OpenView Storage Data Protector Products Overview

starter packs		any platform	Windows	Solaris	HP-UX
LTU, media & manuals			B6961AAJ/F B6961BA	B6951DAJ B6951CA	B6951AAJ B6951BA
	LTU only	B6960MA			
	media only	B6960LAJ/F			
	manuals only				
drive extensions		SAN, NAS	Windows, Netware, Linux	UNIX/OpenVMS	
LTU		B6953AA	B6963AA	B6953AA	
functional extensions		any platform	Windows	UNIX	
on-line backup LTU	1x system		B6965BA (also Linux)	B6955BA	
open file backup LTU	1x server		B7033AA		
	1x 10-servers		B7033BA		
	1x 5-workstations		B7034AA		
	1x enterprise server		B7035AA (+ Netware)		
manager-of-managers LTU	1x system	B6966AA	B6956AA		
library LTU	1x 61-250 slots	B6957BA			
	1x unlimited slots	B6958BA			
direct backup with NDMP LTU	1x TB	B7022BA			
manuals for functional extensions		B6960EAJ			
		HP XP or compatible	HP VA/EVA	HP MSA1000	EMC
zero downtime backup LTU	1x TB	B7023CA	B7025CA	B7036AA*	B6959CA
instant recovery	1x TB	B7026CA	B7028AA*	B7037AA*	
direct backup	1x TB	B7027AA	B7029AA*		
single server edition		any platform	Windows	Solaris	HP-UX
LTU, media & manuals			B7030AAJ/F	B7020DAJ	B7020AAJ
	LTU only		B7030BA	B7020CA	B7020BA
	migration to starter pack		B7031AA	B7021DA	B7021AA

* For the currently supported functionality for the devices associated with these licenses, refer to the support matrix

IMPORTANT

Data Protector functionality for some licenses related to StorageWorks Enterprise Virtual Array and HP StorageWorks Modular SAN Array 1000 will be available after the release of Data Protector A.05.10. For the latest device support for these licenses, marked with * in the above figure, refer to

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

Starter Packs

NOTE

Starter Packs are required once as the initial starting point.

HP OpenView Storage Data Protector Cell Manager Single Drive Starter Pack

LTU, Media, and Manuals

B6951AA	HP-UX - English
B6951AJ	HP-UX - Japanese
B6951DA	Solaris - English
B6951DJ	Solaris - Japanese
B6961AA	Windows - English
B6961AJ	Windows - Japanese
B6961AF	Windows - French

LTU only

B6951BA	HP-UX
B6951CA	Solaris
B6961BA	Windows

Media only

B6960MA	All platforms/languages
---------	-------------------------

Manuals only

B6960LA	English
B6960LJ	Japanese
B6960LF	French

The license-to-use (LTU) in the starter pack is for:

- one management system (Cell Manager) on the specified platform
- one backup drive license (B6951xA contains one B6953AA and B6961xx contains one B6963AA)
- unlimited number of backup agents (clients) on any supported platform
- built in media management

- libraries up to 60 slots (including robotic control)
- the capability to share tape libraries between multiple systems
- Disaster Recovery options
- sophisticated reporting (in Data Protector GUI and via the web)
- cluster support
- SAN support
- service-centric management through integrations into OpenView

Media consist of 3 CDs (one each for Windows, HP-UX, and Solaris).

All UNIX licenses can be used for Windows, Novell NetWare, and Linux.

Order additional licenses in the following cases:

- To obtain additional functionality, please refer to the functional extensions.
- For additional backup drives, please refer to the single drive extensions

Manuals included in the starter pack (all platforms) are:

- *HP OpenView Storage Data Protector Concepts Guide*
- *HP OpenView Storage Data Protector Administrator's Guide*
- *HP OpenView Storage Data Protector Installation and Licensing Guide*
- *HP OpenView Storage Data Protector Quick and Easy Installation Flyer*
- *HP OpenView Storage Data Protector Software Release Notes*

NOTE

With the French products B6961AF and B6960LF, the *HP OpenView Storage Data Protector Administrator's Guide* and the *HP OpenView Storage Data Protector Software Release Notes* are supplied in English.

Single Drive Extensions

HP OpenView Storage Data Protector Single Drive for UNIX, OpenVMS, NAS, SAN

B6953AA

This product includes the license-to-use (LTU) for one additional backup drive directly attached to a UNIX system, an OpenVMS system, a NAS device, used in a SAN, or used for serverless backup.

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.

NOTE

Storage Area Network (SAN) enables sharing storage resources between multiple systems. A Fibre Channel point-to-point connection is not considered to be a SAN. This license is only required in case of SAN storage resource sharing.

This LTU is also required for single drives attached to:

- MPE systems, Network Attached Storage (NAS) file servers, for example, StorageWorks NAS, Network Appliance filers and EMC Celerra File Servers.

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.

It is strongly recommended to order one single drive LTU for use with each existing backup drive. Use means for any purpose: backup, restore AND media copy (source AND target). Drive licenses must not be shared between multiple Cells.

HP OpenView Storage Data Protector Single Drive 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.

NOTE

This license-to-use is not sufficient for storage resource sharing in a SAN (Storage Area Network). B6953AA is required where multiple systems share backup drives in a SAN.

It is strongly recommended to order one single drive LTU for use with each existing backup drive. Use means for any purpose: backup, restore AND media copy (source AND target). Drive licenses must not be shared between multiple Cells.

Functional Extensions

HP OpenView Storage Data Protector Open File Backup

B7033AA	1 server
B7033BA	10 servers

This product contains the Licenses-to-use (LTU) for one or 10 Windows NT/2000/2003 servers for Open File backup of home grown applications, e-mail files (for example, “.pst” - Microsoft Outlook files) and all other databases that are not covered by the Data Protector integration matrix.

Data Protector A.05.10 supports the Windows 2003 file system snapshot feature VSS (Volume Shadow copy Service) at no extra charge. The VSS backup option can be used for open file backup. Compared to open file backup the VSS backup option does not look for file system inactivity to improve the overall file system consistency.

This license is required once for each server system.

HP OpenView Storage Data Protector Open File Backup 5 Workstation Pack

B7034AA

This product contains a package of five Licenses-to-Use (LTU) for Windows NT/2000/XP Workstations for Open File backup of home grown applications, e-mail files (for example, “.pst” - Microsoft Outlook files), and all other databases that are not covered by the Data Protector integration matrix.

HP OpenView Storage Data Protector Open File Backup Enterprise Server

B7035AA

This product contains the License-to-use (LTU) for one Windows 2000/2003 Advanced Server, Windows NT 4.0 Cluster Server, or NetWare server for open file backup of home grown applications, e-mail files (e.g. the .pst Microsoft Outlook files) and all other databases on Windows 2000 that are not covered by the Data Protector integration matrix.

Data Protector A.05.10 supports the Windows 2003 file system snapshot feature VSS (Volume Shadow copy Service) at no extra charge. The VSS backup option can be used for open file backup. Compared to open file backup the VSS backup option does not look for file system inactivity to improve the overall file system consistency.

This license is required once for each server system.

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.

NOTE

If performing on-line Zero Downtime Backup (ZDB) of databases and applications, an On-line LTU is required in addition to the LTU for the relevant ZDB extension. Refer to “HP OpenView Storage Data Protector Zero Downtime Backup (ZDB) Extension” on page A- 11

- The licenses are required per server, it does not matter how many databases are running on the system. Even if databases of different types are running on the same system, only one license is required.

- In a cluster environment, each system participating in the cluster requires a license-to-use. Only in case of fail over (active/stand by), is just one LTU is required. In case of load sharing (active/active), each system requires an LTU.

Applications/Databases running on Linux require the LTU B6965BA.

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 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 Cell Manager. However, ordering B6966AA is more affordable.

HP OpenView Storage Data Protector 61-250 Slot Libraries Extension

B6957BA

This product contains the License-to-use (LTU) for managing tape libraries with 61-250 slots.

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.

HP OpenView Storage Data Protector Unlimited Slot Libraries Extension

B6958BA

This product contains the License-to-use (LTU) for managing tape libraries with no slot limitation.

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.

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., HP StorageWorks NAS, Network Appliance Filer or EMC Celerra File Server).

Used disk space capacity is the total capacity of all volumes on the disk array 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 Zero Downtime Backup (ZDB) Extension

B7023CA	for HP StorageWorks Disk Array XP
B7025CA	for HP StorageWorks Virtual Array and StorageWorks Enterprise Virtual Array
B7036AA	for HP StorageWorks Modular SAN Array 1000
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 protected by zero downtime backup (ZDB) and utilizing:

- Continuous Access XP
- Business Copy XP/EVA/VA and/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- 9.

IMPORTANT

Functionality related to the HP StorageWorks Modular SAN Array 1000 for these licenses will be available after the release of Data Protector A.05.10. For the latest device support, refer to http://www.openview.hp.com/products/datapro/spec_0001.html.

Used disk space capacity is the total capacity of all volumes on the disk array being backed up via ZDB (Primary/Source Volume). This amount represents the total usable capacity of these volumes matching with their configured LDEV sizes.

- Excludes RAID overhead. This means the RAID configuration does not have to be considered.

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
B7037AA	for HP StorageWorks Modular SAN Array 1000

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 utilizing Zero Downtime Backup (ZDB). 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.

IMPORTANT

Functionality related to the HP StorageWorks Enterprise Virtual Array and HP StorageWorks Modular SAN Array 1000 for these licenses will be available after the release of Data Protector A.05.10. For the latest device support, refer to http://www.openview.hp.com/products/datapro/spec_0001.html.

Used disk space capacity is the total capacity of all volumes on the disk array that are used for Instant Recovery (i.e. Primary/Source Volume). This amount represents the total usable capacity of these volumes corresponding with their configured LDEV sizes.

- 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
B7029AA	for HP StorageWorks Virtual Array and StorageWorks Enterprise Virtual Array

Includes the license-to-use (LTUs) to perform direct backup with HP StorageWorks disk array XP and/or HP StorageWorks Virtual Array/HP StorageWorks Enterprise Virtual Array. 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.

IMPORTANT

Functionality related to the HP StorageWorks Enterprise Virtual Array for these licenses will be available after the release of Data Protector A.05.10. For the latest device support, refer to http://www.openview.hp.com/products/datapro/spec_0001.html.

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 UNIX Integration Guide*
- *HP OpenView Storage Data Protector Windows Integration Guide*
- *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide*
- *HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide*
- *HP OpenView Storage Data Protector EMC Symmetrix Integration Guide*

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
B7030AF	Windows - French

LTU Only

B7020BA	HP-UX
B7020CA	Solaris
B7030BA	Windows

The license-to-use (LTU) in the single server edition can be used to backup one single server (HP-UX, Solaris or Windows) with an unlimited number of UNIX and/or Windows workstations and one concurrently used backup drive. Additionally, this edition can manage one autochanger/library with up to 10 slots.

The manuals supplied with the Single Server Editions are the same as those supplied with the Cell Manager Single Drive Starter Packs.

To obtain the following functionality the Single Server Edition has to be migrated to the Cell Manager Single Drive Starter Pack:

- additional server clients
- additional backup drives
- the ability to manage autoloaders/libraries with more than 10 slots
- Cluster support

To order the migration LTU, a single server edition LTU is required.

NOTE

The Single Server Edition for Windows can manage only Windows workstations.

Order additional licenses in the following cases:

- For Cluster support.
- To use an additional UNIX Server, Windows NT/2000/2003 Server or Novell NetWare Server or OpenVMS.
- To utilize the Data Protector Drive and Functional Extensions for additional backup drives, online backup, Manager-of-Managers, and tape libraries. The Data Protector Single Server Edition must be upgraded to the Data Protector Cell Manager Single Drive.

Migration to the Cell Manager Single Drive

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.05.10

Migration from each of the previous Data Protector/OmniBack II versions to Data Protector A.05.10 is as follows:

From Data Protector A.05.00

Migrate directly to Data Protector A.05.10. No license migration is required or any other kind of migration. Data Protector A.05.00 customers on support contract will receive Data Protector A.05.10 for free. Once they upgrade their environment to Data Protector, the functionality that they were using with A.05.00 will be available with Data Protector A.05.10 at no additional cost. They only need to purchase new licenses if they want to acquire new functional extensions provided with Data Protector.

From OmniBack II A.04.x

Migrate directly to Data Protector A.05.10.

No license migration is required or any other kind of migration.

From OmniBack II A.03.5x

OmniBack II A.03.5x customers can directly migrate to Data Protector A.05.10.

License migration is NOT required. Data Protector A.05.x and OmniBack II A.04.x recognize A.03.x licenses.

Support contract migration

No license (password) migration is required when updating to Data Protector A.05.10. However, support contracts should reflect the appropriate Data Protector A.05.10 product numbers as they get updated.

For example, if a customer had 1 B7023BA (Split Mirror XP) LTU in OmniBack II A.04.00, and migrates to Data Protector A.05.10, 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**

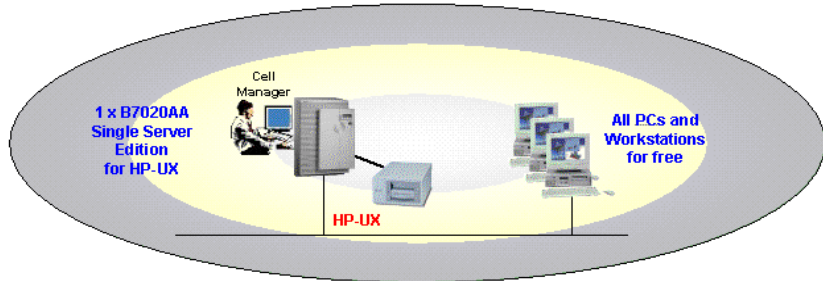


Figure A-3 **Cell Manager - Single Drive for HP-UX, Including up to 60 Slot Single Drive Autochangers**

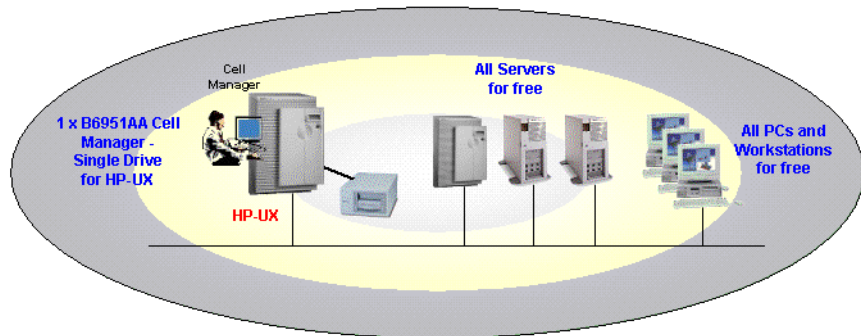


Figure A-4 Mixed Environment

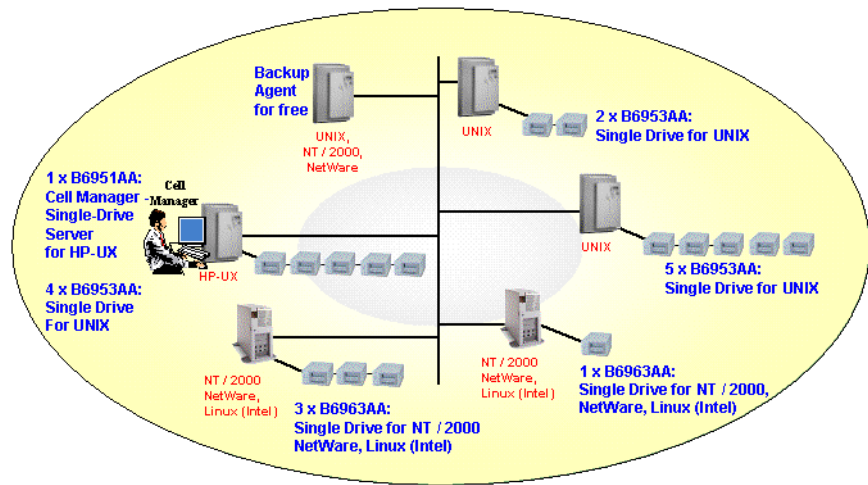


Figure A-5 Online Backup

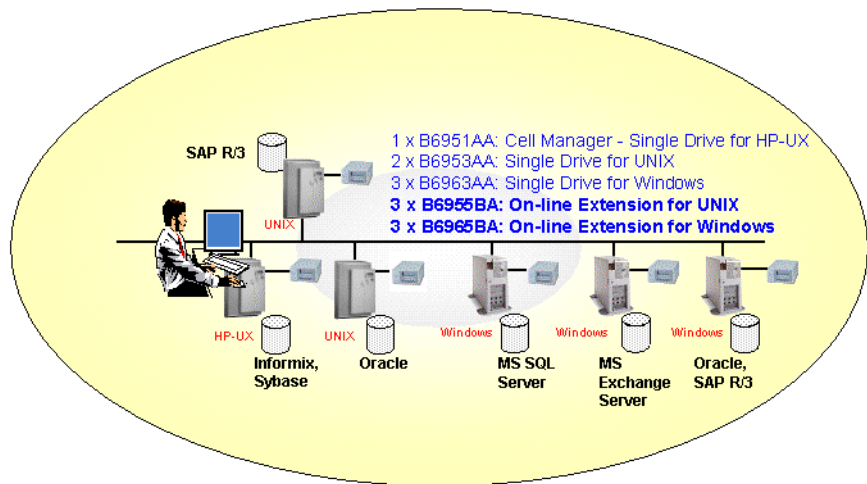


Figure A-6

Application Online Backup

- 1 x B6951AA: Cell Manager - Single Drive for HP-UX
- 3 x B6953AA: Single Drive for UNIX
- 3 x B6963AA: Single Drive for NT
- 4 x B6955BA: Application On-line for UNIX**
- 3 x B6965BA: Application On-line for Windows**

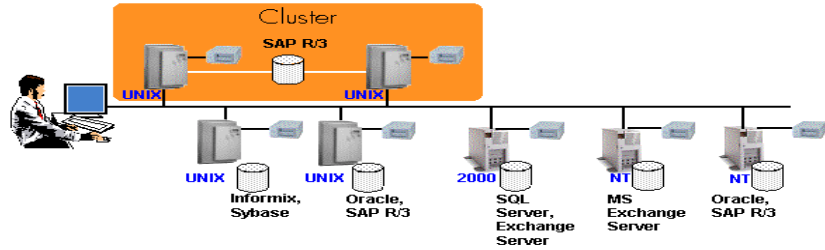


Figure A-7

61 - 250 Slot Libraries

- 1 x B6961AA: Cell Manager - Single Drive for NT / 2000
- 7 x B6963AA: Single Drive for NT / 2000
- 2 x B6953AA: Single Drive for UNIX
- 1 x B6957BA: 61 - 250 Slot Libraries Extension**
- 1 x B6958BA: Unlimited Slot Library Extension**

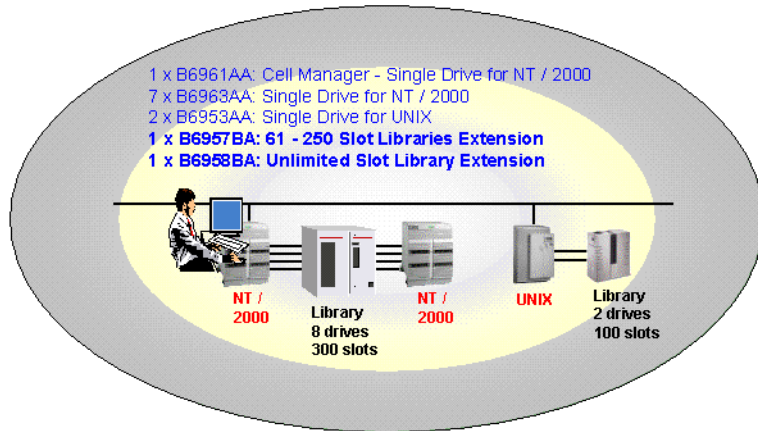
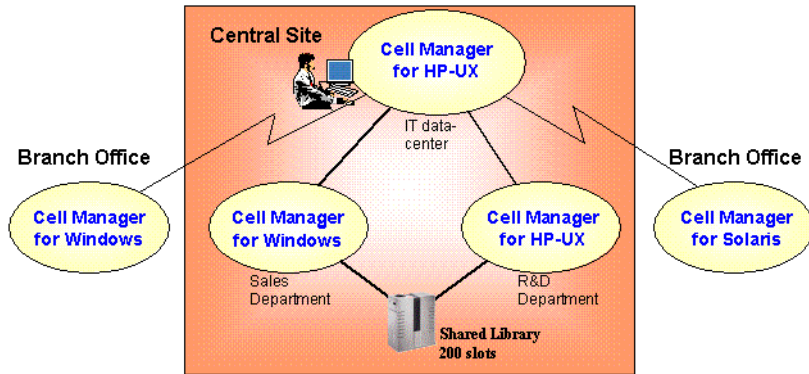
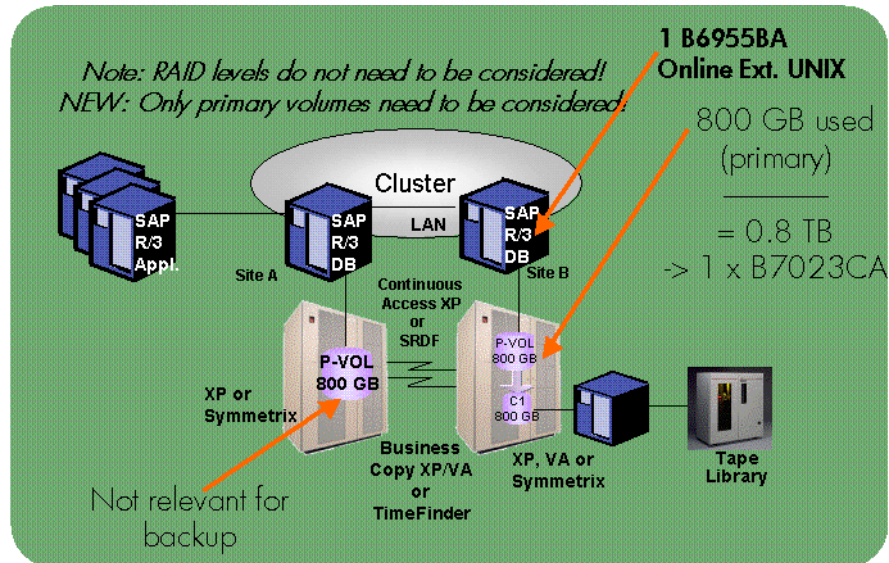


Figure A-8 Manager-of-Managers Environment



3 x B6956AA: Manager-of-Managers Extensions for HP-UX
 2 x B6966AA: Manager-of-Managers Extensions for Windows
 2 x B6957BA: 61 - 250 Slot Libraries Extension

Figure A-9 Zero Downtime Backup



Data Protector Licensing Forms

This chapter discusses Data Protector Licensing forms. Fill them out to order a license.

Either 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)*.

You can also order the licenses 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.
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:

This field defines for which system the *Password Delivery Center* will generate the passwords. In case you want to use centralized licensing (MoM environments only) then this system must be the MoM Manager system.

If the Cell Manager has the several LAN cards, you can enter any of the IP addresses. We recommend that you enter the primary one.

If you have Data Protector in a MC/ServiceGuard or MS Cluster environment, enter the IP address of your virtual server. See the *HP OpenView Storage Data Protector Administrator's Guide* for more information on clusters.

The *Password Delivery Center*
Fax Numbers

Refer to the *Entitlement Certificate*, shipped with your product for contact information.

Product License Type

In the fields next to the *Product Numbers*, enter the quantity of licenses you want to install on this Cell Manager. The quantity can be all or a subset of the licenses purchased with the *Order Number*.

Appendix A
Data Protector Licensing Forms

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.

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.

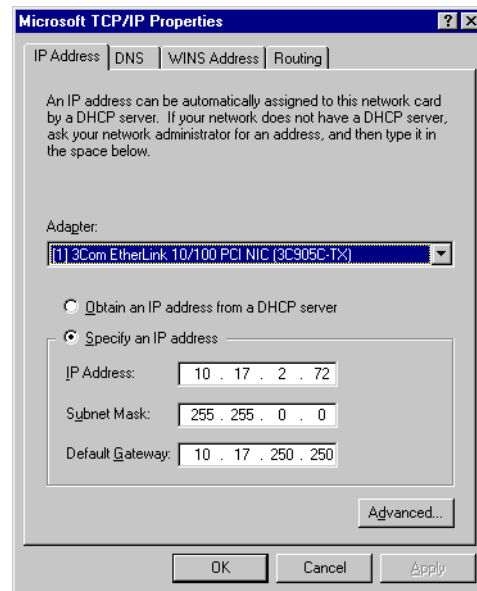
The TCP/IP protocol must be configured manually if there is no DHCP server available on your network or if you configure the TCP/IP protocol on the DHCP server computer. See the Windows online Help for details.

- 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 NT Systems

1. In the Windows Control Panel window, double-click the Network icon to open the Network window.
2. Click Protocols, TCP/IP Protocol and then select Add. Select TCP/IP Protocol and then click OK.
3. You will be asked if there is a DHCP server on the Network. If you will be using the DHCP services, click Yes, if not, click No. A number of files will be installed on your computer.

The TCP/IP Properties window appears on your screen after the installation. You can now start configuring the TCP/IP protocol. See Figure B-1.

Figure B-1 The TCP/IP Properties Window on Windows NT

4. Enter the name of the network adapter in the Adapter text box. If you do not know which network adapters are available, you can list them by clicking the down-arrow on the right side of the Adapter text box.
5. This step depends on whether you will be using DHCP services to configure the TCP/IP protocol automatically or if you will be performing the configuration manually:
 - To obtain an address from a DHCP server, check the Obtain an IP address from a DHCP server option and the TCP/IP protocol will be configured automatically.
 - To specify an IP address, check the Specify an IP address option and enter the corresponding values in the IP Address, Subnet Mask, and Default Gateway text boxes.
6. Click OK when finished and restart your computer to apply new settings.

Installing and Configuring the TCP/IP Protocol on Windows 2000/XP/Server 2003 Systems

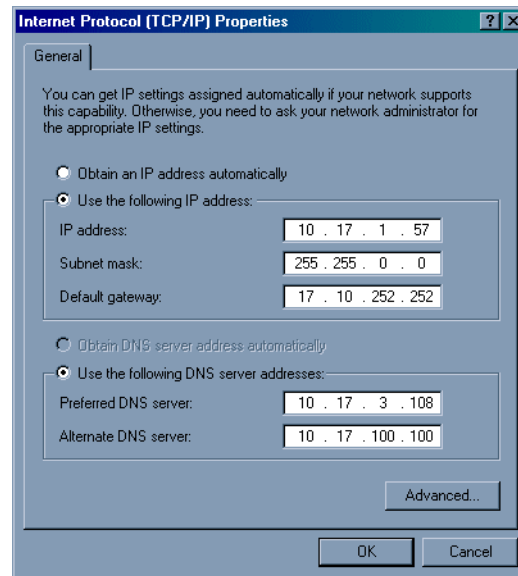
The TCP/IP protocol on Windows 2000/XP/Server 2003 systems is installed during the installation of the operating system.

If you want to check your current TCP/IP settings, 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.

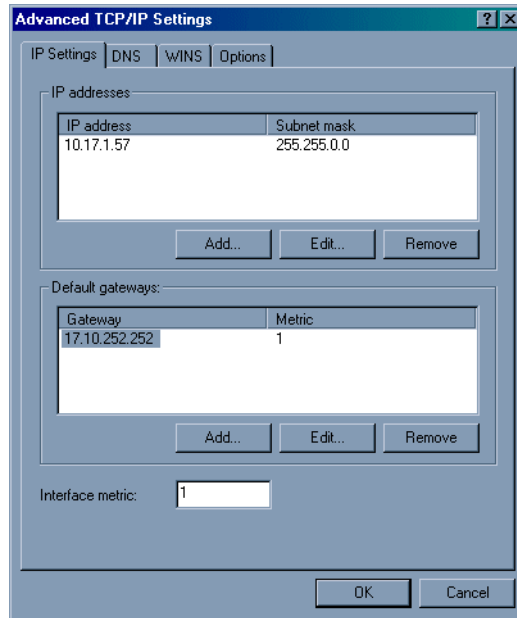
Figure B-2

The TCP/IP Properties Window on Windows 2000/XP/Server 2003



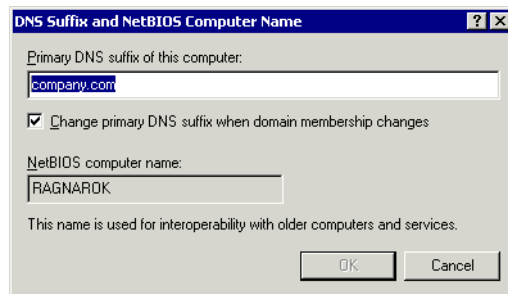
To edit advanced settings, click Advanced.

Figure B-3 **Advanced TCP/IP Settings on Windows 2000/XP/Server 2003**



DNS Suffix To configure the DNS suffix for the system, right-click the My Computer icon on the desktop and then select Properties, Network Identification, Properties, More. Changing the DNS settings will cause your system to reboot.

Figure B-4 **The DNS Suffix and NetBIOS Computer Name on Windows 2000/XP/Server 2003**



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 network 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 specified in the IP settings for each system.

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig` utilities to verify the TCP/IP setup.

1. At the command line, type `ipconfig /all` to display the precise information on your Windows IP configuration and the addresses that have been set for your network adapter. Check whether or not the IP address and subnet mask are what you expected.
2. Type `ping <your_IP_address>` to confirm the software installation and configuration. You should receive, by default, four echo packets.
3. Type `ping <default_gateway>`.

This is the first traffic going out over the network. The gateway should be on your subnet. If you fail to ping the gateway, check if the gateway is up, and if your network is connected correctly.

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:

- On Windows NT:

In the Control Panel, click Network, Protocols, TCP/IP, Properties, and then DNS to verify that the domain name is correct. You should also check the hosts file and the DNS.

- On Windows 2000/XP/Server 2003:

Refer to “Installing and Configuring the TCP/IP Protocol on Windows 2000/XP/Server 2003 Systems” on page B-6, for steps required to access the The TCP/IP Properties window. Here, verify if the domain name is correct. You should also check the hosts file and the DNS.

Be sure that the name resolution for the Cell Manager and 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.

IMPORTANT

The computer name must be the same as the host name. Otherwise, Data Protector setup reports a warning.

To check the hostname, go to Windows Control Panel, Network, Protocols, TCP/IP Protocol, Properties, DNS (Windows NT); or refer to “Installing and Configuring the TCP/IP Protocol on Windows 2000/XP/Server 2003 Systems” on page B-6 for steps required to access the TCP/IP Properties window (Windows 2000/XP/Server 2003).

While connecting to a Cell Manager only the hostnames that are successfully resolved to the fully qualified domain name are stored in the registry. They can, then, be displayed in the list of Cell Managers available for connection.

MS Proxy

If the MS Proxy is installed, the 5555 port number is occupied and the Data Protector services fail. Solve the problem as follows:

1. Add the `wspcfg.ini` file to 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. 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 161. 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 155.

NOTE

Any devices and backup specifications that were configured using the old name must be modified to reflect the correct name.

On UNIX

On a UNIX Cell Manager, do the following:

1. Change the hostname entries in the following files:

```
/etc/opt/omni/cell/cell_server
```

```
/etc/opt/omni/cell/cell_info
```

```
/etc/opt/omni/users/UserList
```

2. Verify that hostname resolution is consistent throughout the 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 hostname entries in the following files:

```
<Data_Protector_home>\config\cell\cell_server  
<Data_Protector_home>\config\cell\cell_info  
<Data_Protector_home>\config\users\UserList
```

2. Change the Cell Manager name in the following registry key:
\\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\
OpenView\OmniBack II\Site

Changing the Default Port Number

Data Protector uses the `inetd` daemon to start other processes. The port number used by Data Protector must be the same 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. 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 <pid>` command.

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 the `HKEY_LOCAL_MACHINE` folder, and then click `Software`, `Hewlett-Packard`, `OpenView`, `OmniBack II`, `Common`.
3. Double-click `InetPort` to open the `Edit DWORD Value` window. 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. Restart the `inet` service. In the Windows Control Panel, go to `Services (Windows NT)` or `Administrative Tools, Services (other Windows systems)`, then select the `Data Protector Inet` service, and restart the service (click `Stop` and then `Start`).

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-12.

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 2000/XP/Server 2003 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. You can either use or disable the native tape drivers for the library's tape drive on the Windows NT systems. On the other hand, the native driver loaded for medium changer devices needs to be disabled if the HP 4mm DDS tape device is connected to the Windows 2000/XP/Server 2003 system and will be configured for use with Data Protector. This section describes the related procedures.

Tape Drivers

Proceed as follows to load the native tape driver for the library tape drive on Windows NT:

1. In the Windows Control Panel, double-click Tape Devices.
2. In the Tape Devices window, select the device for which you want to load the native tape driver, and then click the Drivers tab.
3. Click Add to open the Install Driver window, select the driver file (4mmDAT.sys) for the tape drive, then click OK.
4. Restart the system to apply the changes.

Proceed as follows to unload the native tape driver for the library tape drive on Windows NT:

1. In the Windows Control Panel, double-click Tape Devices.
2. In the Tape Devices window, select the device for which you want to unload the native tape driver, and then click the Drivers tab.
3. Select the driver (4mmDAT.sys), click Remove, then click OK.
4. Restart the system to apply the changes.

On Windows 2000/XP/Server 2003, 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 2000/XP/Server 2003 and can be found at the following site:

<http://www.microsoft.com/hcl/>.

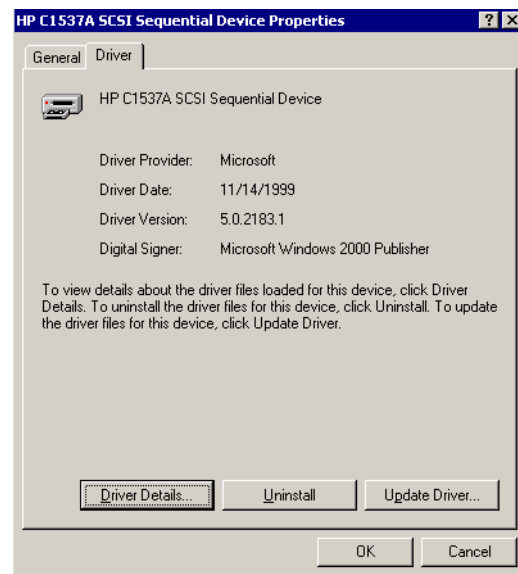
The device drivers then load automatically for all enabled devices once the computer has been started. You do not need to load the native tape driver separately, but you can update it.

To update or replace the native tape driver on a Windows 2000/XP/Server 2003 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. 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-19 for details.

Robotics Drivers

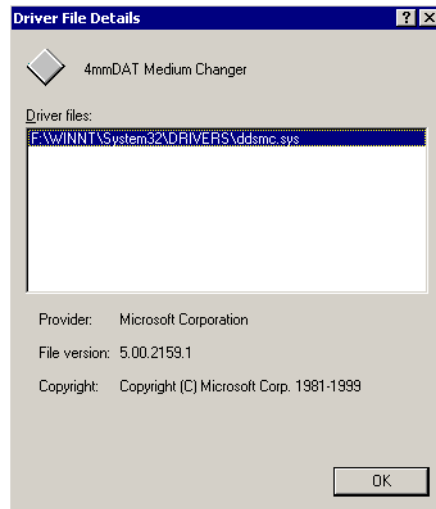
On Windows 2000/XP/Server 2003, the robotics drivers are automatically loaded for enabled tape libraries. In order to use the library robotics with Data Protector, you have to disable the respective driver.

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 2000/XP/Server 2003 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.

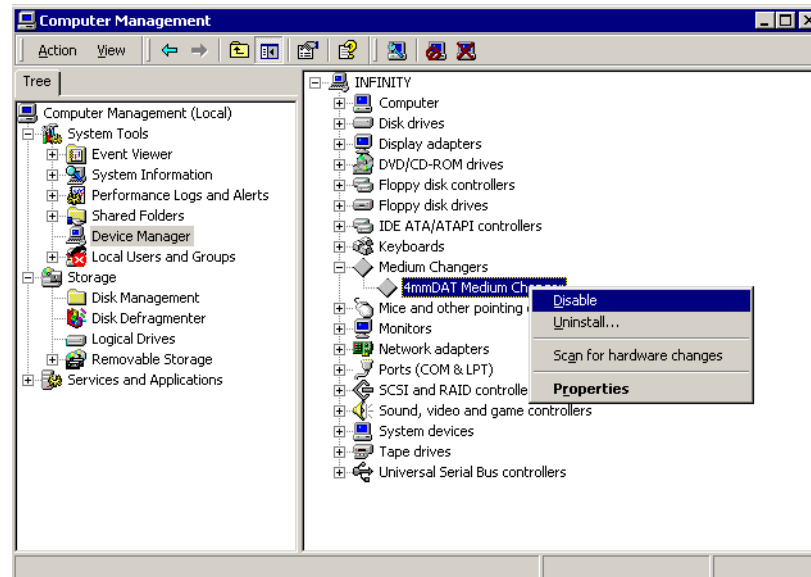
Select Driver tab and click Driver details. In this case, the following window will display:

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

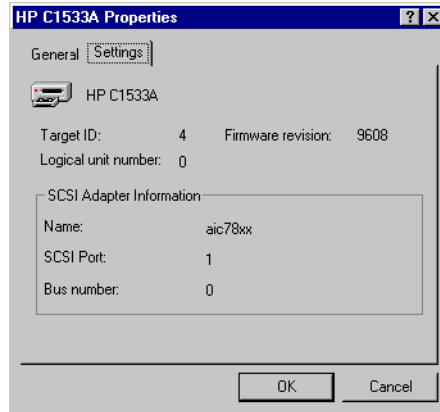
The tape device filename syntax depends on whether the native tape driver was loaded (`tapeN:B:T:L`) or unloaded (`scsiP:B:T:L`) for a tape drive.

Windows NT Without the Native Tape Driver

If you will not be using the native tape driver for the tape drives connected to the system, you need to know the corresponding **SCSI Port (P)**, the **Bus number (B)**, **SCSI Target IDs (T)** and the **Logical Unit Numbers LUNs (L)**. Look up for the properties of the connected tape drives to gather this information. Proceed as follows:

1. In the Windows Control Panel, double-click SCSI Adapters.
2. Double-click the name of a device, and then click Settings, to open the device property page. See Figure B-8 on page B-20.

Figure B-8 **Device Properties**



For the tape drive with the properties shown in Figure B-8, the device filename is `scsi1:0:4:0`.

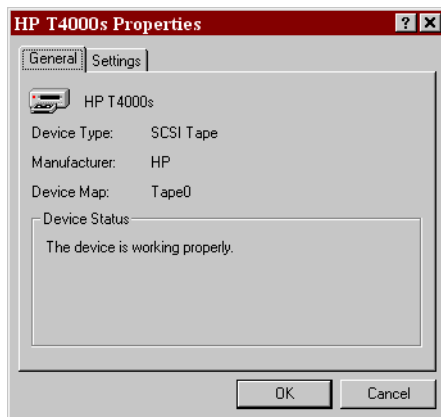
**Windows NT Using
the Native Tape
Driver**

If you will be using the native tape driver, you will need the **Drive instance number (N)** instead of the **SCSI port (P)**. See Figure B-9 on page B-21, where the Device Map stands for N. From the OmniBack II A.03.50 release onwards, the tape drive file can be created using the **Drive instance number (N)** only, for example, `tape0` if N equals 0.

Find the **Drive instance number (N)**, do the following:

1. In the Windows Control Panel, click Tape Devices.
2. Select the driver, and then click Properties, to open the drive property page. See Figure B-9 on page B-21.

Figure B-9 **Drive Properties**



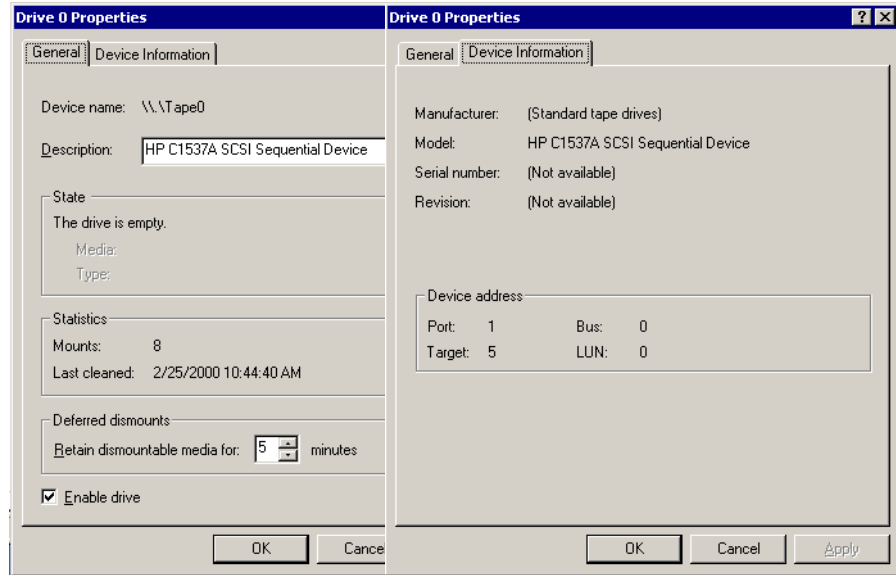
For the tape drive with the properties shown in the Figure B-9, the device filename is tape0.

**Windows
2000/XP/Server
2003 Using the
Native Tape Driver**

To create a device file for a tape drive connected to a Windows 2000/XP/Server 2003 system that uses the native tape driver, proceed as follows:

1. In the Windows Control Panel, double-click Administrative Tools .
2. In the Administrative Tools window, double-click the Computer Management. Expand Removable Storage, then Physical Locations. Right-click the tape drive and select Properties.
3. If the native tape driver is loaded, the device file name is displayed in the General property page. Otherwise, you can find the relevant information in the Device Information property page. See Figure B-10 on page B-22.

Figure B-10 **Tape Drive Properties**



The file name for the tape drive in Figure B-10 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.

Checking the Kernel Configuration on HP-UX

The following example describes how to check or build the kernel on an HP-UX 11.00 system, in case you need to add a new device driver to the kernel.

1. At the command line, enter `sam`.
2. In the System Administration Manager window, double-click Kernel Configuration, and then click Drivers.
3. In the Kernel Configuration window, verify the following:
 - ✓ The drivers for the devices you will use have to be listed among the installed drivers. See Figure B-11. If the driver you are looking for is not listed, you have to install it using the `/usr/bin/swinstall` utility.

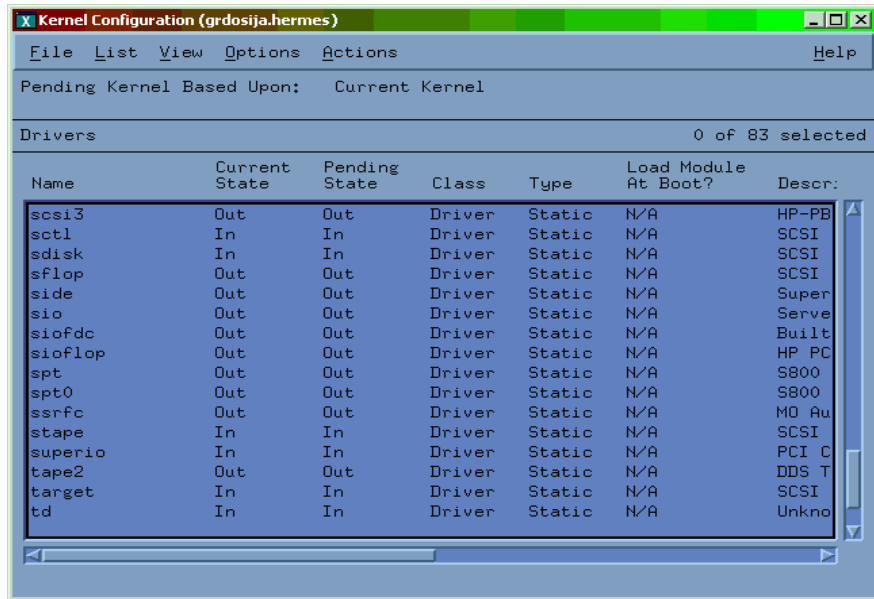
For example:

- A Tape Device Driver (named `stape` or `tape2`) is required for tape devices and must be listed in case you want to connect a tape device to the system.
- A SCSI Pass-Through driver named `sctl`, `spt`, or an autochanger robotics driver named `schgr` (depending on the hardware of the SCSI bus interface) is required for autochanger robotics for tape library devices. See “SCSI Robotic Configuration on HP-UX” on page B-25 for more information.

The drives in tape libraries are addressed through an ordinary tape or disk driver like `stape`, thus no SCSI Pass-Through Driver is required for them.

Figure B-11 shows the drivers installed on an HP-UX 11.00 system. This particular system has the `spt` SCSI Pass-Through driver already built in the kernel. However, the `stape` driver would have to be added to the kernel if you wanted to connect a tape library to the system.

Figure B-11 Kernel Configuration Window



- ✓ The status of a driver displayed in the Current State column must be set to In, meaning that the driver is already built into the current kernel and available for use.

If the status value is set to Out, proceed as follows:

- Select the driver in the list, and then click Actions -> Add Driver to Kernel. In the Pending State column, the status will be set to In.
- Click Actions -> Create a New Kernel to apply the changes, that is to build a Pending Kernel into the Current Kernel. This action requires a reboot of the system.

SCSI Robotic 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-12 SCSI Controlled Devices

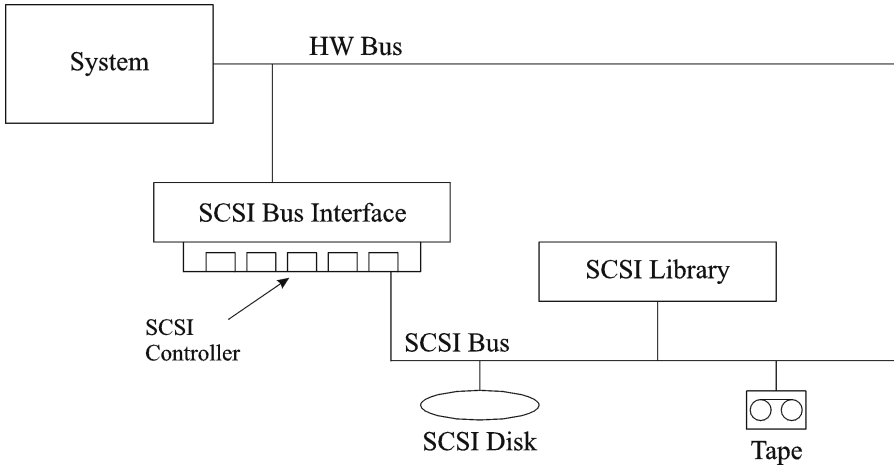
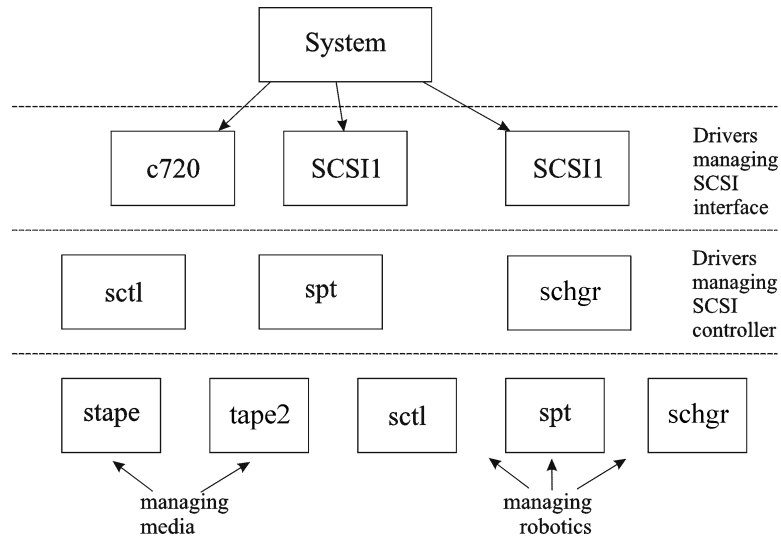


Figure B-13 Managing Devices



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 58 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-14 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 Interface
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-14, 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-15 Status of the SCSI Pass-Through Driver - spt

```
# ioscscan -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
lanmux    0  56        lanmux0  CLAIMED  INTERFACE LAN/Console
tty        0  56.0      mux4     CLAIMED  INTERFACE
lan        0  56.1      lan3     CLAIMED  INTERFACE
lantty    0  56.2      lantty0  CLAIMED  INTERFACE
processor  0  62        processor CLAIMED  PROCESSOR Processor
memory     0  63        memory   CLAIMED  MEMORY      Memory
# █
```

In Figure B-15, 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-15, you can see the output of the `ioscan -f` command on the selected HP-UX system.

Figure B-16

List of Connected Devices

```
# ioscan -f
Class      I  H/W Path  Driver  S/W State H/W Type  Description
-----
bc         0
ext_bus    0  52        scsi1   CLAIMED  INTERFACE HP 28655A - SCSI Interface
target     4  52.1      target  CLAIMED  DEVICE
disk       4  52.1.0    disc3   CLAIMED  DEVICE      SEAGATE ST15150N
target     1  52.2      target  CLAIMED  DEVICE
disk       0  52.2.0    disc3   CLAIMED  DEVICE      TOSHIBA CD-ROM XM-4101TA
target     3  52.4      target  CLAIMED  DEVICE
tape       0  52.4.0    tape2   CLAIMED  DEVICE      HP      C1533A
spt        1  52.4.1    spt     CLAIMED  DEVICE      HP      C1553A
target     6  52.5      target  CLAIMED  DEVICE
disk       5  52.5.0    disc3   CLAIMED  DEVICE      SEAGATE ST15150N
target     2  52.6      target  CLAIMED  DEVICE
disk       1  52.6.0    disc3   CLAIMED  DEVICE      SEAGATE ST15150N
lanmux     0  56        lanmux0 CLAIMED  INTERFACE LAN/Console
tty        0  56.0      mux4    CLAIMED  INTERFACE
lan        0  56.1      lan3    CLAIMED  INTERFACE
lantty    0  56.2      lantty0 CLAIMED  INTERFACE
processor  0  62        processor CLAIMED  PROCESSOR Processor
memory     0  63        memory  CLAIMED  MEMORY      Memory
# █
```


The SCSI bus interface is controlled by the `scsi1` system driver. This is a SCSI NIO interface. To access the library robotics on the SCSI NIO bus we must use the `spt` SCSI Pass-Through driver that is already installed and assigned to the robotics of the HP 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-16) 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 -> The *Instance number* of the SCSI bus interface (NOT of the device) reported by the `ioscan -f` output is in the second column, labeled with **I**. In the example, the instance number is `0`, so we must enter two hexadecimal digits, `00`.

T -> The SCSI address of the library robotics. In the example, the SCSI address is `4`, so we must enter `4`.

L -> The LUN number of the library robotics. In the example, the LUN number is `1`, so we must enter `1`.

00 -> Two hexadecimal zeroes.

Creating the Device File

The following command is used to create the device file:

```
mknod /dev/spt/<devfile_name> c Major # Minor #
```

Usually the device files for `spt` are located in the `/dev/spt` or `/dev/scsi` directory. In this case, we will name the control device file `/dev/spt/SS12000e`.

Thus, the complete command for creating a device file named `SS12000e` in the `/dev/spt` directory is:

```
mknod /dev/spt/SS12000e c 75 0x004100
```

If we create a device file for `sctl`, which is named `SS12000e` and located in the `/dev/scsi` directory, the complete command is:

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

Setting a SCSI Controller's Parameters

Data Protector allows you to change the device's block size, which requires an additional configuration on some SCSI controllers: in order to enable writing of block sizes larger than 64K, some SCSI controllers need to have their parameters set differently.

On Windows systems, you set the SCSI controller's parameters by editing the registry value for Adaptec SCSI controllers, and for some controllers with Adaptec's chipsets:

1. Set the following registry value:
 `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\`
 `Services\aic78xx\Parameters\Device0\MaximumSGList`
2. Enter a DWORD value containing the number of 4 kb blocks, increased by one.

`MaximumSGList = (OBlockSize 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-17, there is the output of the `/usr/sbin/ioscan -f` command on an HP-UX 11.x system.

Figure B-17

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
ext_bus    0  52        scs11    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-17 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.

Command Line Changes After Upgrading to Data Protector A.05.10

The commands listed in this chapter have been changed or provide extended functionality in terms of new options in Data Protector A.05.10. 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 OmniBack II A.03.5x, see Table B-1 on page 37.
- After upgrading from OmniBack II A.04.00, see Table B-2 on page 47.
- After upgrading from OmniBack II A.04.10, see Table B-3 on page 51.
- After upgrading from Data Protector A.05.00, see Table B-4 on page 55.

Table B-1

Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
ob2install	-db2	NEW SOFTWARE COMPONENTS ADDED
	-lotus	
	-snapa	
	-evaa	
omniamo		NEW COMMAND

Table B-1

Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnib	-db2_list	NEW INTEGRATION ADDED
	-disk_only	NEW OPTION
	-expand_sparse	NEW OPTION
	-log_file	NEW OPTION
	-lotus_list	NEW INTEGRATION ADDED
	-mbx_list	NEW OPTION
	-msese_list	NEW OPTION
	-NWuncompress	NEW OPTION
	-ndmp	NEW OPTION
	-ndmp_user	NEW OPTION
	-ndmp_passwd	NEW OPTION
	-ndmp_env	NEW OPTION
	-var[iable]	NEW OPTION
-vss_list	NEW INTEGRATION ADDED	
omnicc	-import_ndmp	NEW SUBCOMMAND
	-type	NEW OPTION
	-port	NEW OPTION
	-user	NEW OPTION
	-passwd	NEW OPTION
omnicellinfo	-cell	OPTION MOVED
omnicheck		NEW COMMAND

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnicreatedl		MS EXCHANGE ZDB ADDED
	-instant_recovery	NEW OPTION FOR HP StorageWorks VIRTUAL ARRAY
	-snapshot	NEW OPTIONS FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-eva	
	-snapshot_type	
	-snapshot_policy	
	-snapshot	NEW OPTIONS FOR HP StorageWorks Modular SAN Array 1000
	-sa	
	-instant_recovery	
	-snapshots <number>	
	-leave_enabled_bs	

Table B-1

Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnidb		MODIFIED OUTPUT
	-db2	NEW INTEGRATION ADDED
	-filesearch	NEW SUBCOMMAND
	-object	NEW SUBCOMMAND
	-listdir	NEW SUBCOMMAND
	-lotus	NEW INTEGRATION ADDED
	-mbx	NEW OPTION
	-vss	NEW INTEGRATION ADDED

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnidbcheck		CHANGED OUTPUT
	-fix	REMOVED
	-quick	NEW SUBCOMMAND
	-hosts	NEW OPTION
	-media	NEW OPTION
	-mpos	NEW OPTION
	-detail	NEW OPTION
	-dumpmedia	NEW OPTION
	-dumpmessages	NEW OPTION
	-summary	NEW OPTION
	-smbf	NEW SUBCOMMAND
	-sibf	NEW SUBCOMMAND
	-core	NEW SUBCOMMAND
	-filenames	NEW SUBCOMMAND
-bf	NEW SUBCOMMAND	
-dc	NEW SUBCOMMAND	
omnidbrestore		NEW COMMAND
omnidbupgrade		NEW COMMAND

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnidbutil		CHANGED OUTPUT
	-list_dcdirs	NEW SUBCOMMAND
	-add_dcdir	NEW SUBCOMMAND
	-modify_dcdir	NEW SUBCOMMAND
	-remove_dcdir	NEW SUBCOMMAND
	-remap_dcdir	NEW SUBCOMMAND
	-fixmpos	NEW SUBCOMMAND
	-writedb	NEW SUBCOMMAND
	-readdb	NEW SUBCOMMAND
	-readascii	OBSOLETE
	-writeascii	OBSOLETE
	-purge	CHANGED SUBCOMMAND AND OUTPUT
	-info	CHANGED OUTPUT
	-upgrade_info	NEW SUBCOMMAND
-show_db_files	NEW SUBCOMMAND	

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
	-free_pool_update	NEW SUBCOMMAND
	-extendinfo	CHANGED OUTPUT
	-maxsize	CHANGED SUBCOMMAND
	-change_objname	OBSOLETE
	-extend	OBSOLETE
omnidbeva		NEW COMMAND
omnidbsa		NEW COMMAND
omnidbva		NEW COMMAND
omnidbxp		NEW COMMAND
omnidr		NEW COMMAND
omnihealthcheck		NEW COMMAND
omnimcopy	-permanent -until	NEW OPTION
omnimlist	-cmlist	NEW OPTION
	-cmformat	NEW OPTION
	-header	NEW OPTION

Table B-1

Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnimmm	-[no_]free_pool	NEW OPTION
	-[no_]move_free_media	NEW OPTION
	-pool	REMOVED (only for the -import_catalog subcommand)
	-disable_lockname	NEW SUBCOMMAND
	-enable_lockname	NEW SUBCOMMAND
	-disable_device	NEW SUBCOMMAND
	-enable_device	NEW SUBCOMMAND
omnioflr		NEW COMMAND

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnir		LOTUS NOTES ADDED
	-auto	NEW OPTION
	-db2	NEW INTEGRATION ADDED
	-disable_all_newer_snapshots	NEW OPTION FOR HP StorageWorks Modular SAN Array 1000
	-last	NEW OPTION
	-instance	NEW OPTION FOR IBM DB2 UDB
	-logfile	NEW OPTION FOR IBM DB2 UDB
	-logpath	NEW OPTION
	-mbx	NEW OPTION
	-mount	NEW OPTION
	-msese	NEW OPTION
	-ndmp_env	NEW OPTION
	-ndmp_passwd	NEW OPTION
	-ndmp_user	NEW OPTION
	-newdbname	NEW OPTION FOR IBM DB2 UDB
	-offline	NEW OPTION FOR IBM DB2 UDB
-rollforward	NEW OPTION FOR IBM DB2 UDB	
-server	NEW OPTION	

Table B-1

Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
	-trustee	NEW OPTION
	-tsname	NEW OPTION FOR IBM DB2 UDB
	-var[iable]	NEW OPTION
	-vss	NEW INTEGRATION ADDED
omnirpt	-header	NEW OPTION
	db_purge_preview	NEW REPORT
	db_system	NEW REPORT
	-expiration	REMOVED
	-[no_]library	NEW OPTION
	media_list_extended	NEW REPORT
	pool_list	NEW REPORT
	-{no_]protection	NEW OPTION
	used_media_extended	NEW REPORT
omnisetup.sh		NEW COMMAND
	db2	NEW SOFTWARE COMPONENTS ADDED
	evaa	NEW SOFTWARE COMPONENT ADDED
omnisrdupdate		NEW COMMAND
	-asr	NEW OPTION
	-location	NEW OPTION

Table B-1 Upgrade From OmniBack II A.03.5x

Command	Subcommand/Option	Status
omnistat		MODIFIED OUTPUT
omnisv		NEW COMMAND
omnisv.sh		OBSOLETE
omnitrig	-run_checks	NEW SUBCOMMAND
uma	-dftype	NEW OPTION
	- [no_]scsiType	NEW OPTION
	-ddt	NEW OPTION
	-ndmpDA	NEW OPTION
	res	REMOVED FUNCTIONALITY
	rel	REMOVED FUNCTIONALITY

Table B-2 Upgrade From OmniBack II A.04.00

Command	Subcommand/Option	Status
ob2install	-db2	NEW SOFTWARE COMPONENTS ADDED
	-lotus	
	-snapa	
	-evaa	
omniamo		NEW COMMAND

Table B-2

Upgrade From OmniBack II A.04.00

Command	Subcommand/Option	Status
omnib	-db2_list	NEW INTEGRATION ADDED
	-disk_only	NEW OPTION
	-lotus_list	NEW INTEGRATION ADDED
	-mbx_list	NEW OPTION
	-vss_list	NEW INTEGRATION ADDED
omnicreatedl		MS EXCHANGE ZDB ADDED
	-instant_recovery	NEW OPTION FOR HP StorageWorks VIRTUAL ARRAY
	-snapshot	NEW OPTIONS FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-eva	
	-snapshot_type	
	-snapshot_policy	
	-snapshot	NEW OPTIONS FOR HP StorageWorks Modular SAN Array 1000
	-sa	
	-instant recovery	
	-snapshots <number>	
-leave_enabled_bs		
omnicheck		NEW COMMAND

Table B-2 Upgrade From OmniBack II A.04.00

Command	Subcommand/Option	Status
omnidb	-db2	NEW INTEGRATION ADDED
	-lotus	NEW INTEGRATION ADDED
	-mbx	NEW OPTION
	-vss	NEW INTEGRATION ADDED
omnidbeva		NEW COMMAND
omnidbsa		NEW COMMAND
omnidbva		NEW COMMAND
omnidbxp		NEW COMMAND
omnidr		NEW COMMAND
omnimcopy	-permanent -until	NEW OPTION
omnimlist	-header	NEW OPTION
omnioflr		NEW COMMAND

Table B-2

Upgrade From OmniBack II A.04.00

Command	Subcommand/Option	Status
omnir		LOTUS NOTES ADDED
	-db2	NEW INTEGRATION ADDED
	-disable_all_newer_snapshots	NEW OPTION FOR HP StorageWorks Modular SAN Array 1000
	-instance	NEW OPTION FOR IBM DB2 UDB
	-logfile	NEW OPTION FOR IBM DB2 UDB
	-mbx	NEW OPTION
	-newdbname	NEW OPTION FOR IBM DB2 UDB
	-offline	NEW OPTION FOR IBM DB2 UDB
	-rollforward	NEW OPTION FOR IBM DB2 UDB
	-trustee	NEW OPTION
	-tsname	NEW OPTION FOR IBM DB2 UDB
-vss	NEW INTEGRATION ADDED	
omnirpt	media_list_extended	NEW REPORT

Table B-2 Upgrade From OmniBack II A.04.00

Command	Subcommand/Option	Status
omnisetup.sh		NEW COMMAND
	db2	NEW SOFTWARE COMPONENTS ADDED
	evaa	
omnisrdupdate		NEW COMMAND
	-asr	NEW OPTION
	-location	NEW OPTION
uma	rel	REMOVED FUNCTIONALITY
	res	REMOVED FUNCTIONALITY

Table B-3 Upgrade From OmniBack II A.04.10

Command	Subcommand/Option	Status
ob2install	-db2	NEW SOFTWARE COMPONENTS ADDED
	-evaa	
omniamo		NEW COMMAND
omnib	-db2_list	NEW INTEGRATION ADDED
	-disk_only	NEW OPTION
	-mbx_list	NEW OPTION
	-vss_list	NEW INTEGRATION ADDED
omnicheck		NEW COMMAND

Table B-3

Upgrade From OmniBack II A.04.10

Command	Subcommand/Option	Status
omnicreatedl	-instant_recovery	NEW OPTION FOR HP StorageWorks VIRTUAL ARRAY
	-snapshot	NEW OPTIONS FOR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-eva	
	-snapshot_type	
	-snapshot_policy	
	-snapshot	NEW OPTIONS FOR HP StorageWorks Modular SAN Array 1000
	-sa	
	-instant recovery	
	-snapshots <number>	
	-leave_enabled_bs	
omnidb	-db2	NEW INTEGRATION ADDED
	-mbx	NEW OPTION
	-vss	NEW INTEGRATION ADDED
omnidbeva		NEW COMMAND
omnidbsa		NEW COMMAND

Table B-3 Upgrade From OmniBack II A.04.10

Command	Subcommand/Option	Status
omnidbva	-init	NEW OPTION
	-delete	NEW OPTION
	-ir	NEW OPTION
	-session	NEW OPTION
	-lun	NEW OPTION
	-vapasswd	NEW OPTION
	-samppasswd	NEW OPTION
	-dbcheck	NEW OPTION
omnidbvp	-cm	COMMAND DEVICE HANDLING ADDED
omnidr	- [no_]cleanup	NEW OPTION
	-msclusdb	NEW OPTION
	-drimini	NEW OPTION
	-target	NEW OPTION
	-report	NEW OPTION
omnimcopy	-permanent -until	NEW OPTION
omnimlist	-header	NEW OPTION

Table B-3

Upgrade From OmniBack II A.04.10

Command	Subcommand/Option	Status
omnir	-db2	NEW INTEGRATION ADDED
	-disable_all_newer_snapshots	NEW OPTION FOR HP StorageWorks Modular SAN Array 1000
	-instance	NEW OPTION FOR IBM DB2 UDB
	-logfile	NEW OPTION FOR IBM DB2 UDB
	-mbx	NEW OPTION
	-newdbname	NEW OPTION FOR IBM DB2 UDB
	-offline	NEW OPTION FOR IBM DB2 UDB
	-rollforward	NEW OPTION FOR IBM DB2 UDB
	-trustee	NEW OPTION
	-tsname	NEW OPTION FOR IBM DB2 UDB
	-vss	NEW INTEGRATION ADDED
omnirpt	media_list_extended	NEW REPORT
omnisetup.sh		NEW COMMAND
	-db2	NEW SOFTWARE COMPONENTS ADDED
	evaa	

Table B-3 Upgrade From OmniBack II A.04.10

Command	Subcommand/Option	Status
omnisrdupdate		
	-asr	NEW OPTION
	-location	NEW OPTION
uma	res	REMOVED FUNCTIONALITY
	rel	REMOVED FUNCTIONALITY

Table B-4 Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
ob2install	-db2	NEW SOFTWARE COMPONENTS ADDED
	-evaa	
omniamo		NEW COMMAND
omnib	-db2_list	NEW INTEGRATION ADDED
	-mbx_list	NEW OPTION
	-vss_list	NEW INTEGRATION ADDED
omnicheck		NEW COMMAND

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	
	-snapshot_type	
	-snapshot_policy	
	-snapshot	NEW OPTIONS FOR HP StorageWorks Modular SAN Array 1000
	-sa	
	-instant recovery	
	-snapshots <number>	
-leave_enabled_bs		
omnidb	-db2	NEW INTEGRATION ADDED
	-mbx	NEW OPTION
	-vss	NEW INTEGRATION ADDED
omnidbeva		NEW COMMAND
omnidbsa		NEW COMMAND
omnimcopy	-permanent -until	NEW OPTION

Table B-4 Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnir	-db2	NEW INTEGRATION ADDED
	-disable_all_newer_snapshots	NEW OPTION FOR HP StorageWorks Modular SAN Array 1000
	-instance	NEW OPTION FOR IBM DB2 UDB
	-logfile	NEW OPTION FOR IBM DB2 UDB
	-mbx	NEW OPTION
	-newdbname	NEW OPTION FOR IBM DB2 UDB
	-offline	NEW OPTION FOR IBM DB2 UDB
	-rollforward	NEW OPTION FOR IBM DB2 UDB
	-tsname	NEW OPTION FOR IBM DB2 UDB
	-vss	NEW INTEGRATION ADDED
omnirpt	media_list_extended	NEW REPORT
omnisetup.sh	db2	NEW SOFTWARE COMPONENTS ADDED
	evaa	

Table B-4

Upgrade From Data Protector A.05.00

Command	Subcommand/Option	Status
omnisrdupdate		
	-asr	NEW OPTION
	-location	NEW OPTION
uma	-scsiType	REPLACED BY THE -interface OPTION
	-interface	REPLACED THE -scsiType OPTION

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 DLT 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 bootup. 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

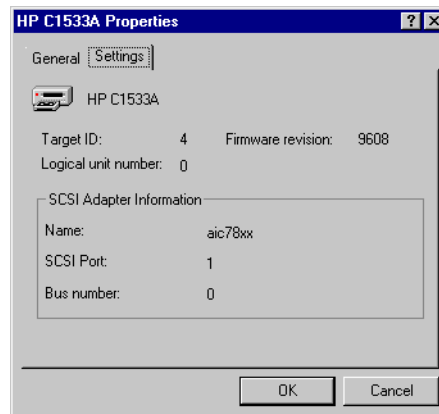
Follow the steps below to determine the unused SCSI Target IDs (SCSI Addresses) on a Windows system:

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-18.

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-18

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 the Data Protector Media Agent on the selected system. See “Distributing the Data Protector Software to Clients” on page 43.
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-34. For Solaris systems, see “Finding the Unused SCSI Target IDs on Solaris” on page B-36. For a Windows system, see “Finding Unused SCSI Target IDs on a Windows System” on page B-64.

- ✓ 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 B-23.

If you need to configure a SCSI Pass-Through Driver, see “SCSI Robotic Configuration on HP-UX” on page B-25.

- ✓ 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-59. 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-15.

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-19.

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-65.

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-30.

- ✓ On a Solaris system, use the `ls -all` utility 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.
- ✓ 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:

Appendix B

Connecting Backup Devices

```
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.

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 the 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 the 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. Refer to the Appendix A in the *HP OpenView Storage Data Protector Administrator's Guide* for more information about further configuration tasks.

You must have the Data Protector Media Agent installed on your system. See Chapter 2, “Distributing the Data Protector Software to Clients” on page 43 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 B-23.
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-34.
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, refer to the Appendix A in the *HP OpenView Storage Data Protector Administrator's Guide* 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-64.

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, refer to the Appendix A in the *HP OpenView Storage Data Protector Administrator's Guide* 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 B-23.
3. Check that the required SCSI Pass-Through drivers (`sctl` or `spt`) are *installed* and *built* into the current kernel. See “SCSI Robotic Configuration on HP-UX” on page B-25.
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-34.

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 30.
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, refer to the Appendix A in the *HP OpenView Storage Data Protector Administrator's Guide* 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-64.

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, refer to the *HP OpenView Storage Data Protector Administrator's Guide* 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 B-23.
2. Check that the required SCSI Pass-Through drivers (`sctl` or `spt`) are *installed* and *built* into the current kernel. See “SCSI Robotic Configuration on HP-UX” on page B-25.

Appendix B

Connecting Backup Devices

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-34.

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-30.
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, refer to the Appendix A of the *HP OpenView Storage Data Protector Administrator's Guide* for instructions about configuring a Data Protector backup device for your newly connected device.

Connecting to a Solaris System

To configure the HP C5173-7000 library device on a Solaris system, follow the steps below. For this example, it is assumed that two drives are to be allocated to Data Protector:

1. Copy the sst driver (module) and configuration file `sst.conf` to the required directory:

- For 32-bit operating systems:

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

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

- For 64-bit operating systems:

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

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

2. Add the driver to the Solaris kernel:

```
add_drv sst
```

3. Remove all existing device files from the `/dev/rmt` directory:

```
cd /dev/rmt  
rm *
```

4. Stop the system by pressing `Stop` and `A`.

5. Run the `probe-scsi-all` command at the "ok" prompt to check which SCSI addresses are available for use.

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

The system may ask you to start the `reset-all` command before executing the `probe-scsi-all` command.

In our case, we will use port 6 for the SCSI control device, port 2 for the first drive, and port 1 for the second drive; lun is 0)

6. Return to normal running:

```
ok go
```

7. Copy the `st.conf` configuration file into the required directory:

```
$cp /opt/omni/spt/st.conf /kernel/drv/st.conf
```

The `st.conf` file is present on each Solaris Data Protector client and contains SCSI addresses for each backup device connected to the client.

8. Edit the `/kernel/drv/st.conf` file and add the following lines:

Appendix B

Connecting Backup Devices

```
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, refer to the Appendix A of the *HP OpenView Storage Data Protector Administrator's Guide* 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 64.

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, refer to the Appendix A of the *HP OpenView Storage Data Protector Administrator's Guide* 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:

Appendix B

Connecting Backup Devices

```
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 `g1m` 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, refer to the Appendix A of the *HP OpenView Storage Data Protector Administrator's Guide* 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 64.
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, refer to the Appendix A of the *HP OpenView Storage Data Protector Administrator's Guide* 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 Media Agent Installation on Novell NetWare

After you have installed Data Protector Media Agent on the Novell NetWare platform, you should verify the installation by performing the following tasks:

- ✓ Identify the storage device.
- ✓ Test the 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 Media Agent Startup

Once you have the 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.

- ✓ The Adaptec ASPI driver and the corresponding transport layer ASPITRAN.DSK (for Novell NetWare 4.x) or NWASPI.CDM (for Novell NetWare 5.x), must be up and running.
- ✓ The Data Protector 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 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 current 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 Data Protector 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 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 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) is 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 current available commands, type `HELP` on HPUMA screen.

Loading `HPDEVBRA.NLM` locally lets you use the Adaptec ASPI interface 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 -tty
```

where the `-tty` option is necessary to interact with the Novell NetWare server's console.

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 141.

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 Administrator's Guide*.

3. Run the `omnisv -start` command to start the services/processes:

```
<Data_Protector_home>\bin\omnisv -start
```

Glossary

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 original units.

See also **backup system** and **original unit**.

archived redo log (*Oracle specific term*)

Also called offline redo log. If the Oracle8/9 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. 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 object

Any data selected for backup, such as a disk, a file, a directory, a database, or a part of it. During the backup session, Data Protector reads the objects, transfers the data (through the network), and writes them to the media residing in the devices.

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

Glossary

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

See **media set**.

backup set (*Oracle specific term*)

Backup for (one or more) Oracle8/9 files, where the files are multiplexed together. The reason for multiplexing is to give performance benefits. Files in backup sets have to be extracted using a restore command. There are two types of backup sets: data file backup set and archive log backup set.

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 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 replica units 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 storage version. *See also* **application system** and **replica unit**.

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**.

Glossary

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 **CA** (*HP StorageWorks Disk Array XP specific term*), **Main Control Unit** and **HP StorageWorks Disk Array XP LDEV**.

BC (*HP StorageWorks Virtual Array specific term*)

Business Copy VA allows you to maintain internal copies of HP StorageWorks Virtual Array LUNs for 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 sets should be connected to the backup system. See also **HP StorageWorks Virtual Array LUN**.

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 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.

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

Glossary

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
- 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

Glossary

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 backup sessions, restore sessions, and backed up data. Depending on the selected log level, it also contains file names and file versions. This part of the database is always local to the cell.

See also **MMDB**.

CDF file (*UNIX specific term*)

A Context Dependent File is a file consisting of several files grouped under the same pathname. The system ordinarily selects one of the files using the context of the process. This mechanism allows machine dependent executables, system data, and device files to work correctly from all hosts in a cluster while using the same pathname.

cell

A set of systems that are under the control of a Cell Manager. The cell typically represents the systems on a site or an organizational entity, which are connected to the same LAN. 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

Glossary

allocate licenses to specific cells to suit your needs.

See also MoM.

Centralized Media Management Database (CMMDB)

See CMMDB.

channel (*Oracle specific term*)

An Oracle8/9 Recovery Manager resource allocation. Every allocated channel starts a new Oracle8/9 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 Oracle8/9 is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

circular logging (*MS Exchange and Lotus Domino Server specific term*)
Microsoft Exchange database and Lotus Domino Server database mode in which transaction log files are automatically overwritten as soon as the data they contain is committed to the database.

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 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.

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

Glossary

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

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.

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.

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

Glossary

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 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 Oracle8/9 Server.

database parallelism

More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.

database server

A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.

Dbobject (*Informix 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 occupying approximately 80% of the IDB. The default DC directory is called the dcbf directory and is located in the `<Data_Protector_home>\db40` directory. 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 2 GB.

DCBF

The Detail Catalog Binary Files (DCBF) are a part of the IDB. The files in store information about file versions and attributes occupying approximately 80% of the IDB. By default, DCBF consist of one DC directory with a maximum size of 2 GB. You can create more DC directories.

Glossary

delta backup

A delta backup is a backup containing all the changes made to the database from the last backup of any type.

See also **backup types**

device

A physical unit which contains either just a drive or a more complex unit such as a library.

device chain

A device chain consists of several standalone devices configured for sequential use. When a medium in one device gets full, the backup automatically continues on a medium in the next device in the device chain.

device group (*EMC Symmetrix specific term*)

A logical unit representing several EMC Symmetrix devices. A device cannot belong to more than a single device group. All devices in a device group must be on the same EMC Symmetrix unit. You can use a device group to identify and work with a subset of the available EMC Symmetrix devices.

device streaming

A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes to write to

the tape, and so on. In other words, if the data rate written to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.

DHCP server

A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic configuration of IP addresses and related information. Data Protector can back up DHCP server data as part of the Windows configuration.

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.

Glossary

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**.

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.

Directory Store (DS) (*MS Exchange specific term*)

A part of the Microsoft Exchange Server directory. The Microsoft Exchange Server directory contains objects used by Microsoft Exchange applications in order to find and access services, mailboxes, recipients, public folders, and other addressable objects within the messaging system.

See also **Information Store (MDB)**.

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.

Glossary

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.

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. The DR OS can be either temporary or active. A temporary DR OS is used exclusively as a host environment for some other operating

Glossary

system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. Active 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.

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)**

EMC Symmetrix Application Programming Interface (SYMAPI)

(EMC Symmetrix specific term)

See **Symmetrix Application Programming Interface (SYMAPI)**

EMC Symmetrix CLI Database File

(EMC Symmetrix specific term)

See **Symmetrix CLI Database File**

EMC Symmetrix Command-Line Interface (SYMCLI) *(EMC Symmetrix specific term)*

See **Symmetrix Command-Line Interface (SYMCLI)**

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

Glossary

Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept.
See also MoM.

EVA Agent (*HP StorageWorks Enterprise Virtual Array specific term*)
A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array snapshot integration on the application system and the backup system. It communicates with the HSV Element Manager to control the HP StorageWorks Enterprise Virtual Array.

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 II 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) (*MS Exchange specific term*)
A database technology used as a storage system for information exchange by Microsoft Exchange 2000 Server.

failover
Transferring of the most important cluster data, called group (on Windows) or package (on Unix) from one cluster node to another. A failover can occur mostly because of software or hardware failures or maintenance on the primary node.

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

Glossary

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 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.

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**.

Glossary

full database backup

A backup of all data in a database regardless of whether it has changed after the last database backup was created. This means that the full database backup does not depend on any other backup media.

full mailbox backup

A full mailbox backup is a backup of the entire mailbox content.

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/options` directory on HP-UX and Solaris systems and in the `<Data_Protector_home>\config\options` directory on Windows systems.

group (*Microsoft Cluster Server specific term*)

A collection of resources (for example disk volumes, application services, IP names and addresses) that are needed to run a specific cluster-aware applications.

GUI

A cross-platform (X11/Motif and Windows) graphical user interface, provided by Data Protector for easy access to all configuration and administration tasks.

hard recovery (*MS Exchange specific term*)

Recovery of data on the level of the database engine (Extensible Storage Engine 98).

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/Holidays` on the UNIX Cell Manager and `<Data_Protector_home>\Config\Holidays` on the Windows Cell Manager.

host backup

See client backup with disk discovery.

Glossary

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 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 (*HP StorageWorks Disk Array XP specific term*)

A logical partition of a physical disk within an HP StorageWorks Disk Array XP. LDEVs are entities that are mirrored using Continuous Access XP (CA) and Business Copy XP (BC) configurations. See also **BC** (*HP StorageWorks Disk*

Array XP specific term) and **CA** (*HP StorageWorks Disk Array XP specific term*).

HP StorageWorks Virtual Array

LUN (*HP StorageWorks Virtual Array specific term*)

A logical partition of a physical disk within an HP StorageWorks Virtual Array. LUNs are entities that are replicated using the HP StorageWorks Business Copy VA configuration. See also **BC** (*HP StorageWorks Virtual Array specific term*).

HP VPO

See **OVO**.

HSV Element Manager (HP

StorageWorks Enterprise Virtual Array specific term)

The HSV Element Manager is used by the Data Protector HP StorageWorks Enterprise Virtual Array integration to provide the features that enable virtualization technology and the management interface for the HP StorageWorks Enterprise Virtual Array environment.

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,

Glossary

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 (*MS Exchange specific term*)

A backup of changes since the last full or incremental backup. Only transaction logs 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.

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

Glossary

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.

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 (MDB) *(MS Exchange specific term)*

This is the default message store provider for the Microsoft Exchange Server. The information store consists of the following stores:

- Public information store (MS Exchange 5.5 Server) or Public folder store (MS Exchange 2000 Server)
- Private information store (MS Exchange 5.5 Server) or Mailbox store (MS Exchange 2000 Server)
- Personal folder store
- Offline information store.

The public information store contains public folders and messages that can be shared among multiple users and applications. A single public store is shared by all users within a Microsoft Exchange Server organization, even if multiple Servers are used. The private information store consists of mail boxes that can belong to users or to applications. The mail boxes reside on the server running the Microsoft Exchange Server.

See also **Directory Store (DS)**.

Initialization Parameter File *(Oracle specific term)*

An Oracle8/9 file that contains information on how to initialize a database and instance.

initializing

See **formatting**.

Installation Server

A computer system that holds a repository of the Data Protector

Glossary

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 where data replicated during the ZDB disk backup or ZDB disk/tape backup is restored at high speed using split mirror or snapshot technology. The restore takes place within the disk array and there is no restore from the standard backup media involved. Full recovery of a database application may require further steps, such as applying the log files, to be performed afterwards. Instant recovery restores the user-selected replica storage version to the original storage.

See also zero downtime backup (ZDB), ZDB disk backup, ZDB tape backup, ZDB disk/tape backup and replica storage pool.

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.

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 identify the system on the network. The 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.

Glossary

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 usage by balancing the number and the size of the objects backed up to each device. Since load balancing is done automatically during backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If load balancing is not selected, you select which device will be used for each object in your 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.

Glossary

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.

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. 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 IDB growth, backup speed, and the convenience of browsing data for restore.

logical-log files

This applies to online database backup. Logical-log files are files in which modified data is first stored before being flushed to disk. In the event of a failure, these logical-log files are used to roll forward all transactions that have been committed as well as roll back any transactions that have not been committed.

login ID (*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

Glossary

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 (Oracle8/9) 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 (Oracle8/9) Catalog.

Lotus C API (*Lotus Domino Server specific term*)

An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

Magic Packet

See **Wake ONLAN**.

mailbox (*MS Exchange specific term*)

The location to which email is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the email delivery location, email is routed from the mailbox to this location.

Mailbox Store (*MS Exchange 2000 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*

Glossary

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, the Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore session, the 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. The Media Agent also manages the robotics control of a library.

MAPI (*MS 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.

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.

Glossary

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 (DMPAPI), 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 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 7.0/2000

A database management system designed to meet the requirements of distributed "client-server" computing.

Glossary

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 (*ZDB specific term*)

See replica unit.

mirror rotation (*HP StorageWorks Disk Array XP specific term*)

See replica storage 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 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 mountpoints 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.

Glossary

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

An object can be one of the following:

- for Windows clients, an object is a logical disk (such as d:);

- for UNIX clients, an object is a mounted filesystem or a mount point;
- for Novell Netware clients, an object is a volume.

The scope of the data can be further reduced by selecting files or directories. Additionally, an object can be a database entity.

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.

offline recovery

Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI-II 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 frequently used data on the hard disk. HP OmniStorage runs on HP-UX systems.

Glossary

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 that is performed while the application (or database) is available for use. Application-specific interfaces allow backup products, like Data Protector, to back up logical units of the database while retaining access for the application. In simple configurations (non ZDB), the application remains in a backup mode for the entire duration of the backup. In contrast to that, for ZDB configurations, the backup mode lasts only for the duration of the split/snapshot operation. After that, the application can resume to the standard mode. Depending on the configuration, resource requirements vary significantly.

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**.

Glossary

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.

original unit (*ZDB specific term*)

A logical unit that is used as a source for data replication using snapshot or split mirror technologies. Depending on the vendor and technology used, an original unit denotes P-VOL on HP StorageWorks Disk Array XP, parent LUN on HP StorageWorks Virtual Array, logical drive on HP StorageWorks Modular SAN Array 1000, or virtual disk on HP StorageWorks Enterprise Virtual Array. Data in an original unit is replicated to data in a replica unit. Original units are on systems interpreted as physical drives

(Windows) or physical volumes (UNIX).

See also **replica unit**, **original storage**, and **replica storage version**.

original storage (*ZDB specific term*)

A set of original units that contain the backup objects selected in one Data Protector backup specification. Data in an original storage is replicated to data in a replica storage version by replicating the set of original units. An original storage is typically used by the application system.

See also **original unit**, **replica unit**, and **replica storage version**.

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

Glossary

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 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.

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

Glossary

data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism

The concept of reading multiple data streams from an online database.

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)**.

Private Information Store (*MS*

Exchange 5.5 Server specific term)

A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text .edb file.

protection

See **data protection** and also **catalog protection**.

Glossary

public folder store (*MS Exchange 2000 Server specific term*)

The part of the Information Store that maintains information in public folders. A public folder store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

public/private backed up data

When configuring a backup, you can select whether the backed up data will be:

- public, that is visible (and accessible for restore) to all Data Protector users
- private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

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

Glossary

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 Oracle8/9 tables and views that are used by Recovery Manager to store information about Oracle8/9 databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle8/9 databases. The recovery catalog contains information about:

- The physical schema of the Oracle8/9 target database
- Data file and archivelog 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 Oracle8/9 command-line interface that directs an Oracle8/9 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 (*HP StorageWorks Disk Array XP specific term*)

The Remote Control Unit (RCU) acts as a slave of an MCU in a CA

Glossary

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 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 unit (*ZDB specific term*)

A logical unit that is used as a target for data replication using snapshot or split mirror technologies. Depending on the vendor and technology used, a replica unit denotes S-VOL on HP StorageWorks Disk Array XP, child (BC) LUN on HP StorageWorks Virtual Array, logical drive on HP StorageWorks Modular SAN Array

1000, or virtual disk on HP StorageWorks Enterprise Virtual Array. Data in an original unit is replicated to data in a replica unit. Replica units are on systems interpreted as physical drives (Windows) or physical volumes (UNIX). A replica unit is also referred to as snapshot or mirror. *See also* **original unit**, **original storage**, and **replica storage version**.

replica storage version (*ZDB specific term*)

A set of replica units, created or reused during one ZDB backup session, which contain replica copies of the backup objects selected in one Data Protector backup specification. Data in an original storage is replicated to data in a replica storage version. A replica storage version is typically used by the backup system. *See also* **original unit**, **replica unit**, and **original storage**.

replica storage pool (*ZDB specific term*)

A number or group of replica storage versions produced during ZDB sessions to be used for the purpose of replica storage rotation, instant recovery, and split mirror restore. The replica storage versions in the replica storage pool are all created using the same backup specification. The size of a replica storage pool is defined for each backup specification as the maximum number

Glossary

of replica storage versions that are to be kept on a disk array before the oldest replica storage version for the backup specification is reused.

See also **replica storage rotation**.

replica storage rotation (*ZDB specific term*)

A ZDB process that denotes either a reuse of the oldest replica storage version in the replica storage pool whenever the size of the replica storage pool is reached or, if the size of the replica storage pool is not reached, a creation of a new replica storage version in the replica storage pool.

See also **replica storage pool**.

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.

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.

SA Agent (*HP StorageWorks Modular SAN Array 1000 specific term*)

A Data Protector software module that executes all tasks required for the HP StorageWorks Modular SAN Array 1000 snapshot integration on the application system and the backup system. It communicates with the HP StorageWorks Modular SAN Array 1000 Business Copy Manager to control the HP StorageWorks Modular SAN Array 1000.

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

Glossary

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

This environment variable is set by Data Protector during actual backup sessions (not during preview). It identifies a session and is recorded in the database.

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 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 (e.g. 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**.

Glossary

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.

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) is a part of the IDB that stores session messages generated during backup and restore sessions. One binary file is created per session. The files are grouped by year and month.

snapshot (*ZDB specific term*)

See **replica unit**.

snapshot backup (*ZDB specific term*)

A ZDB term encompassing ZDB disk backup, ZDB tape backup and ZDB disk/tape backup utilizing snapshot technology.

See also **zero downtime backup (ZDB)**.

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 medium

When copying media, the source medium is the medium that contains backed up data and is being copied.

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 backup (*EMC Symmetrix specific term*)

See **ZDB tape backup**.

Glossary

split mirror backup (*HP StorageWorks Disk Array XP specific term*)
See **ZDB tape backup**, **ZDB disk/tape backup** and **ZDB disk backup**.

split mirror restore (*HP StorageWorks Disk Array XP specific term*)
A process where data backed up using the ZDB tape backup or ZDB disk/tape backup process is restored from tape media to the replica storage version selected by the replica rotation process or by the user. The replica storage version is then synchronized to the original storage. Split mirror restore is limited to filesystem restore.
See also **ZDB tape backup**, **ZDB disk/tape backup**, and **replica storage rotation**.

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 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

Glossary

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.

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

(MS Exchange 2000 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.

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.

Glossary

Symmetrix Application Programming Interface (SYMAPI) *(EMC Symmetrix specific term)*

A linkable library of functions that can interface with EMC Symmetrix units attached to the Data Protector clients. Provided by EMC.

Symmetrix CLI Database File
(EMC Symmetrix specific term)

The EMC Symmetrix database file that stores EMC Symmetrix configuration data on each system with a configured EMC Symmetrix ICDA and installed SYMCLI.

Symmetrix Command-Line Interface (SYMCLI) *(EMC Symmetrix specific term)*

An application written using the Symmetrix Application Programming Interface (SYMAPI) that retrieves data from an EMC Symmetrix unit using special low-level SCSI commands. The SYMCLI allows you to run commands on the client to obtain configuration, status, and performance data from the EMC Symmetrix units attached to clients that are running in an open systems environment.

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 database, system startup files, and the Certificate Services database (if the server is a certificate server). If the

Glossary

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 (*HP StorageWorks Disk Array XP specific term*)

See **ZDB disk backup**.

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 medium

When copying media, the target medium is the medium to which data is copied.

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.

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 7.0/2000 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 (*MS Exchange and Lotus Domino Server specific term*)

Files in which changes made to a database are recorded.

transaction logs (*Data Protector specific term*)

Keeps track of IDB changes. The

Glossary

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.

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.

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.

Glossary

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 Device Interface (*MS SQL Server 7.0/2000 specific term*)

This is a SQL Server 7.0/2000 programming interface that allows fast backup and restore of large databases.

virtual disk (*HP StorageWorks Enterprise Virtual Array 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 **original unit** and **replica unit**.

virtual server

A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

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.

Glossary

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.

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 database repository about a computer's configuration.

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

Glossary

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 disk backup (*ZDB specific term*)

The basic concept of ZDB disk backup is to create a copy of data from the

original storage at a specific point-in-time, and keep this copy of data in the disk array in the replica storage version selected from or created in the replica storage pool. Data in the replica storage version is not moved to standard backup media. The data backed up utilizing the ZDB disk backup functionality can be either restored by utilizing the instant recovery process or used for data mining and similar purposes.

See also **zero downtime backup (ZDB), ZDB tape backup, ZDB disk/tape backup, instant recovery, and replica storage pool**.

ZDB disk/tape backup (*ZDB specific term*)

The basic concept of ZDB disk/tape backup is to create a copy of data from the original storage at a specific point-in-time, and keep this copy of data in the replica storage version. The copy of data in the replica storage version is additionally used for a backup to a standard backup medium, typically a tape. The data backed up using the ZDB disk/tape backup can be restored using the instant recovery or the standard Data Protector restore procedure. It can also be used for data mining and similar purposes.

See also **zero downtime backup (ZDB), ZDB disk backup, ZDB tape backup, instant recovery, and replica storage pool**.

Glossary

ZDB part of the IDB (*ZDB specific term*)

A part of the IDB, storing ZDB related information such as original and replica storage versions, security information and other. The ZDB part of the IDB is used for ZDB, instant recovery, and split mirror restore.

See also **zero downtime backup (ZDB)**.

ZDB tape backup (*ZDB specific term*)

The basic concept of ZDB tape backup is to create a copy of data from the original storage at a specific point-in-time, and use this copy of data in the replica storage version for a backup to a standard backup medium, typically a tape. After the backup is complete, the data in the replica storage version may be overwritten. Instant recovery is not possible from such a backup, the data must be restored following the standard Data Protector restore procedure.

See also **zero downtime backup (ZDB), ZDB disk backup, instant recovery, ZDB disk/tape backup, and replica storage pool**.

zero downtime backup (ZDB)

A backup process utilizing data replication technologies (the split mirror and snapshot technologies) to minimize the backup window for the application system; typically to few minutes. With this technique, application database downtime (offline backup) or backup

mode (online backup) is limited to the very short time it takes to split the mirror disks or to create or reuse snapshots. The application is then returned to normal operation, while the data in the replica storage version is either backed up by streaming the data to tape (ZDB tape backup) or kept in the replica storage pool (ZDB disk backup) for the instant recovery or other purposes or both (ZDB disk/tape backup).

See also **ZDB disk backup, ZDB tape backup, ZDB disk/tape backup, and instant recovery**.

Glossary