

# HP Data Protector

Software Version: 8.10

## Installation Guide

Document Release Date: November 2016

Software Release Date: November 2016



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2016 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)

**HP Software Solutions Now** accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

# Contents

Contents .....	3
Chapter 1: Overview of the installation procedure .....	15
Overview of the installation procedure .....	15
The remote installation concept .....	17
Data Protector installation media .....	18
Choosing the Cell Manager system .....	19
Choosing the Data Protector user interface system .....	21
The Data Protector graphical user interface .....	21
Chapter 2: Installing Data Protector on your network .....	23
Installing the Data Protector Cell Manager and Installation Servers .....	23
Installing a UNIX Cell Manager .....	24
Setting kernel parameters .....	26
Installation procedure .....	27
The installed directory structure on HP-UX and Linux systems .....	28
Configuring automatic startup and shutdown .....	29
Setting environment variables .....	30
What's next? .....	31
Installing a Windows Cell Manager .....	31
Installation procedure .....	32
After the installation .....	36
Troubleshooting .....	37
What's next? .....	38
Installing Installation Servers .....	38
Installing Installation Servers for UNIX systems .....	38
Installing an Installation Server for Windows systems .....	40
Installing Data Protector clients .....	43
Data Protector components .....	46
Installing Windows clients .....	50
Local installation .....	51

Connecting a backup device to Windows systems .....	54
Installing HP-UX clients .....	55
Checking the kernel configuration on HP-UX .....	56
Connecting a backup device to HP-UX systems .....	57
Installing Solaris clients .....	58
Post-installation configuration .....	59
Connecting a backup device to a Solaris system .....	64
Installing Linux clients .....	65
Connecting a backup device to the Linux system .....	68
Installing ESX Server clients .....	69
Installing Mac OS X clients .....	69
Installing IBM AIX clients .....	70
Connecting a backup device to an AIX client .....	71
Installing HP OpenVMS clients .....	71
Remote installation .....	77
Remote installation using secure shell .....	79
Adding clients to the cell .....	81
Adding components to clients .....	83
Local installation on UNIX and Mac OS X systems .....	85
Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library .....	88
Connecting library drives .....	89
Preparing Data Protector clients to use the ADIC/GRAU Library .....	89
Installing a Media Agent to use the ADIC/GRAU Library .....	90
Preparing Data Protector clients to use the StorageTek Library .....	92
Installing a Media Agent to use the StorageTek Library .....	94
Installing the Data Protector integration clients .....	95
Remote installation .....	97
Local installation .....	97
Installing cluster-aware integrations .....	97
Microsoft Exchange Server clients .....	98
Data Protector Microsoft Exchange Server 2007 integration .....	98
Data Protector Microsoft Exchange Server 2010 integration .....	98

Data Protector Microsoft Exchange Server Single Mailbox integration .....	99
Data Protector Microsoft Volume Shadow Copy Service integration .....	99
Data Protector Granular Recovery Extension for Microsoft Exchange Server .....	100
Microsoft SQL Server clients .....	100
Microsoft SharePoint Server clients .....	100
Data Protector Microsoft SharePoint Server 2007/2010/2013 integration .....	101
Data Protector Microsoft SharePoint Server VSS based solution .....	101
Data Protector Microsoft Volume Shadow Copy Service integration .....	102
Data Protector Granular Recovery Extension for Microsoft SharePoint Server .....	102
Microsoft Volume Shadow Copy Service clients .....	102
Sybase Server clients .....	103
Informix Server clients .....	103
IBM HACMP Cluster .....	104
SAP R/3 clients .....	104
SAP MaxDB clients .....	104
SAP HANA Appliance clients .....	105
Oracle Server clients .....	105
IBM DB2 UDB clients .....	105
Lotus Notes/Domino Server clients .....	106
Lotus Domino Cluster .....	106
VMware clients .....	106
Data Protector Virtual Environment integration .....	106
Data Protector Granular Recovery Extension for VMware vSphere .....	107
Microsoft Hyper-V clients .....	109
Data Protector Virtual Environment integration .....	109
Data Protector Microsoft Volume Shadow Copy Service integration .....	109
NDMP Server clients .....	110
Oracle clients .....	110
SAP R/3 clients .....	111
HP P4000 SAN Solutions clients .....	113
HP P6000 EVA Disk Array Family clients .....	113
HP P6000 EVA Disk Array Family integration with Oracle Server .....	114

HP P6000 EVA Disk Array Family integration with SAP R/3 .....	116
HP P6000 EVA Disk Array Family integration with Microsoft Exchange Server .....	118
HP P6000 EVA Disk Array Family integration with Microsoft SQL Server .....	119
HP P9000 XP Disk Array Family clients .....	119
HP P9000 XP Disk Array Family integration with Oracle Server .....	120
HP P9000 XP Disk Array Family integration with SAP R/3 .....	121
HP P9000 XP Disk Array Family integration with Microsoft Exchange Server .....	124
HP P9000 XP Disk Array Family integration with Microsoft SQL Server .....	125
HP 3PAR StoreServ Storage clients .....	125
EMC Symmetrix clients .....	125
EMC Symmetrix Integration with Oracle .....	126
EMC Symmetrix Integration with SAP R/3 .....	127
EMC Symmetrix Integration with Microsoft SQL Server .....	129
Installing the Data Protector Single Server Edition .....	130
Limitations of SSE for Windows .....	130
Limitations of SSE for HP-UX .....	130
Installing the Data Protector web reporting .....	131
Installing Data Protector on an HP Serviceguard .....	132
Installing a cluster-aware Cell Manager .....	132
Installing an Installation Server on cluster nodes .....	133
Installing cluster-aware clients .....	133
Installing Data Protector on a Microsoft Cluster Server .....	133
Installing a cluster-aware Cell Manager .....	133
Installing a cluster-aware Cell Manager for Windows 2012 and Windows 2012 R2 clusters .....	140
To install a cluster-aware Cell Manager .....	140
Installing cluster-aware clients .....	141
Installing Data Protector clients on a Veritas Cluster .....	144
Installing cluster-aware clients .....	144
Installing Data Protector on an IBM HACMP Cluster .....	144
Installing cluster-aware clients .....	144
Installing Data Protector on a Microsoft Hyper-V cluster .....	145

Chapter 3: Maintaining the installation .....	147
Data Protector maintenance mode .....	147
Initiating maintenance mode .....	147
Quitting maintenance mode .....	148
Importing clients to a cell .....	149
Importing an Installation Server to a cell .....	151
Importing a cluster-aware client to a cell .....	151
Microsoft Cluster Server .....	152
Other clusters .....	153
Exporting clients from a cell .....	154
Security considerations .....	156
Security layers .....	156
Client security .....	156
Data Protector users .....	157
Cell Manager security .....	157
Other security aspects .....	158
Securing clients .....	158
The allow_hosts and deny_hosts files .....	163
Excessive logging to the inet.log file .....	163
Strict hostname checking .....	163
Enabling the feature .....	165
Managing encrypted control communication .....	165
Considerations .....	165
Enabling encrypted control communication .....	165
Enabling encrypted control communication with manual distribution of certificates and keys .....	168
Encrypted control communication with user-created certificates .....	173
Selecting TLS version .....	174
Disabling encrypted control communication .....	175
Viewing certificate expiration date in Data Protector GUI .....	177
What happens .....	179
How to add a client to the Security Exceptions list .....	179

Start backup specification user right .....	179
Hiding the contents of backup specifications .....	180
Host trusts .....	180
Monitoring security events .....	181
User authentication and LDAP .....	181
Initializing and configuring the LDAP login module .....	182
Initializing the LDAP login module .....	182
Configuring the LDAP login module .....	183
Granting Data Protector permissions to LDAP users or groups .....	186
Adding LDAP users to user groups .....	186
Adding LDAP groups to user groups .....	186
Logging in using LDAP credentials .....	187
Checking the LDAP configuration .....	187
Certificate Generation Utility .....	188
Syntax .....	188
Examples .....	191
Directory Structure .....	203
Overwriting certificates in existing keystore and truststore files .....	206
Replacing existing server and client store files .....	206
Replacing the CA certificate .....	207
Updating the distinguished name (DN) string .....	207
Overwriting certificates by creating new keystore and truststore files .....	208
Replacing existing server and client store files .....	208
Replacing the CA certificate .....	209
Updating the distinguished Name (DN) string .....	209
Updating the configuration file with the stores password .....	209
Managing Data Protector patches .....	210
Installing patches .....	210
Installing and removing Data Protector patch bundles .....	211
Installing and removing Data Protector patch bundles on UNIX systems .....	211
Installing and removing Data Protector patch bundles on Windows systems .....	211
Verifying which Data Protector patches are installed .....	212



Verifying Data Protector patches using the GUI .....	212
Verifying Data Protector Patches Using the CLI .....	213
Uninstalling Data Protector software .....	213
Uninstalling a Data Protector client .....	214
Uninstalling the Cell Manager and Installation Server .....	215
Uninstalling from Windows systems .....	215
Uninstalling from HP-UX systems .....	216
Uninstalling the Cell Manager and/or Installation Server configured on HP Serviceguard .....	217
Uninstalling from Linux systems .....	220
Manual removal of Data Protector software on UNIX .....	222
Changing Data Protector software components .....	223
On Windows systems .....	223
On HP-UX systems .....	224
On Linux systems .....	224
On other UNIX systems .....	225
Chapter 4: Upgrading to Data Protector 8.10 .....	227
Upgrade overview .....	227
Support for earlier agent versions .....	228
Upgrade sequence .....	229
Upgrading from Data Protector 6.20, 7.00, and 8.00 .....	230
Upgrading the UNIX Cell Manager and Installation Server .....	230
Upgrading a Cell Manager .....	231
Upgrading an Installation Server .....	232
Upgrading the Windows Cell Manager and Installation Server .....	234
Checking configuration changes .....	237
Internal database changes after upgrade from Data Protector 6.20 or 7.00 .....	239
Migrating the Detail Catalog Binary Files (DCBF) .....	239
IDB conversion duration and changes in IDB size and structure .....	240
Importing legacy NDMP media .....	241
Ordinal numbers in session IDs .....	241
Upgrading the clients .....	241
Upgrade sequence .....	241

Upgrading clients remotely .....	241
Upgrading clients locally .....	241
Upgrade-related operating system specifics .....	242
Upgrading the Oracle integration .....	243
User root is no longer required .....	243
Configuring an Oracle instance for instant recovery .....	244
Oracle ASM configurations using HP P6000 EVA Disk Array Family or HP 3PAR StoreServ Storage .....	244
Upgrading the SAP R/3 integration .....	244
SAP compliant ZDB sessions .....	244
Configuring an Oracle instance for instant recovery .....	244
Upgrading the Microsoft Volume Shadow Copy Service integration .....	245
Instant recovery-enabled backup sessions after upgrading from HP Data Protector HP Data Protector HP Data Protector 6.20, Data Protector 7.00, and Data Protector 8.00 .....	245
Upgrading the HP P6000 EVA Disk Array Family integration .....	245
Upgrading the Virtual Environment integration .....	245
Upgrading other integrations .....	246
Upgrading in a MoM environment .....	246
Upgrading from the Single Server Edition .....	246
Upgrading from earlier versions of SSE to Data Protector 8.10 SSE .....	247
Upgrading from Data Protector 8.10 SSE to Data Protector 8.10 .....	247
Upgrading the Cell Manager .....	247
Upgrading from multiple installations .....	248
Migrating the Cell Manager to a different platform .....	248
Migration from PA-RISC HP-UX systems to Intel Itanium HP-UX systems .....	248
Migrating from 32-bit/64-bit Windows to 64-bit Windows/Windows Server 2008 or Windows Server 2012 .....	248
Migrating from Solaris to Linux .....	249
MoM specifics .....	250
Installation Server specifics .....	250
Migrating a Windows Cell Manager Internal Database to a Different Server .....	251
Terminology .....	251

Prerequisites .....	251
Preparing for migration .....	252
On OLD_SERVER .....	252
On NEW_SERVER .....	252
Migration tasks .....	253
Importing the IDB .....	253
Post Restore Tasks .....	254
Adding the NEW_SERVER as the Cell Manager .....	255
Changing the Cell Manager Name in the IDB .....	255
Next Steps .....	256
Troubleshooting .....	256
Upgrading the Cell Manager configured in HP Serviceguard .....	260
Upgrading the Cell Manager configured on Microsoft Cluster Server .....	264
<b>Chapter 5: Data Protector Licensing .....</b>	<b>269</b>
Overview .....	269
Traditional licensing .....	269
Capacity based licensing .....	270
New License Keys .....	270
Requesting new passwords for existing licenses .....	270
New License key introduced .....	271
License checking and reporting .....	271
Data Protector traditional licenses .....	271
Cell Manager related licenses .....	272
Backup targets .....	272
Used capacity calculation for applying to backup targets .....	273
The advanced backup to disk license .....	274
Examples for backup targets based on licensed capacity .....	276
Data Protector Functional Extensions .....	279
Capacity based license reports .....	279
Producing a license report on demand .....	281
Data Protector passwords .....	282
Obtaining and installing permanent passwords .....	283

Verifying the password .....	285
Finding the number of installed licenses .....	285
Moving licenses to another Cell Manager System .....	286
Centralized licensing .....	287
Data Protector 8.10 product structure and licenses .....	287
Password considerations .....	287
License migration to Data Protector 8.10 .....	288
Data Protector licensing forms .....	289
<b>Chapter 6: Troubleshooting installation and upgrade .....</b>	<b>291</b>
Name resolution problems when installing the Windows Cell Manager .....	291
Verifying DNS connections within Data Protector cell .....	292
Using the omnichck command .....	292
Troubleshooting common issues .....	293
Troubleshooting installation on UNIX systems .....	295
Troubleshooting installation on Red Hat 7 systems .....	297
Troubleshooting installation on Windows systems .....	298
Verifying Data Protector client installation .....	300
Troubleshooting upgrade .....	301
Troubleshooting remote upgrade on Windows systems .....	306
Manual process for local upgrade on UNIX systems .....	307
Using log files .....	307
Local installation .....	307
Remote installation .....	308
Data Protector log files .....	308
Creating installation execution traces .....	309
<b>Appendix A: Installing and upgrading using UNIX system native tools .....</b>	<b>311</b>
Installing on HP-UX and Linux systems using native tools .....	311
Installing a Cell Manager on HP-UX systems using swinstall .....	311
Installing the Cell Manager on Linux systems using rpm .....	312
Installing an Installation Server on HP-UX systems using swinstall .....	314
Installing an Installation Server on Linux systems using rpm .....	314
Installing the clients .....	317

Upgrading on HP-UX and Linux systems using native tools .....	317
Upgrading Data Protector on HP-UX systems using swinstall .....	317
Upgrading Data Protector on Linux systems using rpm .....	318
<b>Appendix B: System preparation and maintenance tasks .....</b>	<b>321</b>
Network configuration on UNIX systems .....	321
Checking the TCP/IP setup .....	321
Changing the default Data Protector ports .....	323
Changing the default Data Protector Inet port .....	323
Changing the default Data Protector IDB ports and user accounts on UNIX systems .....	324
Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation .....	325
Installing Data Protector on Microsoft Cluster Server with Veritas Volume Manager .....	327
Preparing a NIS server .....	327
Changing the Cell Manager name .....	328
Changing the hostname in Job Control Engine (JCE) database .....	335
<b>Appendix C: Device and media related tasks .....</b>	<b>339</b>
Using tape and robotics drivers on Windows systems .....	339
Creating device files (SCSI Addresses) on Windows systems .....	341
SCSI robotics configuration on HP-UX systems .....	342
Creating device files on HP-UX systems .....	346
Setting a SCSI controller's parameters .....	348
Finding the unused SCSI addresses on HP-UX systems .....	348
Finding the unused SCSI target IDs on Solaris systems .....	350
Updating the device and driver configuration on Solaris systems .....	350
Updating configuration files .....	350
Creating and checking device files .....	354
Finding unused SCSI target IDs on Windows systems .....	354
Setting SCSI IDs on an HP 330fx library .....	355
Connecting backup devices .....	356
Connecting an HP 24 standalone device .....	359
Connecting an HP DAT Autoloader .....	360
Connecting an HP DLT Library 28/48-Slot .....	361

Connecting a Seagate Viper 200 LTO Ultrium Tape Drive .....365

Appendix D: Command line changes after upgrading to Data Protector 8.10 ...367

Glossary .....389

Index .....430

We appreciate your feedback! .....447

# Chapter 1: Overview of the installation procedure

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

## Overview of the installation procedure

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

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

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

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

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

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

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

Client systems with applications and virtual environments that need to be backed up must have appropriate Data Protector integration agent components installed. The integration agent enables you to back up data from an application or virtual environment or restore it.

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

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

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

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

- Systems that will be used to access the Data Protector functionality through the user interface. These systems must have the User Interface component installed.
- Systems that will be backed up. These must have the Disk Agent component installed for filesystem backup and the relevant application agent component for online database integrations.
- Systems to which the backup devices will be connected. These must have a Media Agent component installed.
- One or more systems on which the Data Protector Installation Server will be installed. Two types of Installation Servers are available for remote software installation: one for UNIX clients and the other for Windows clients.

The choice of system for the Installation Server is independent of the Cell Manager and the systems on which the User Interface is installed. The Cell Manager and Installation Server can be installed on the same system or on different systems.

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

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

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

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

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

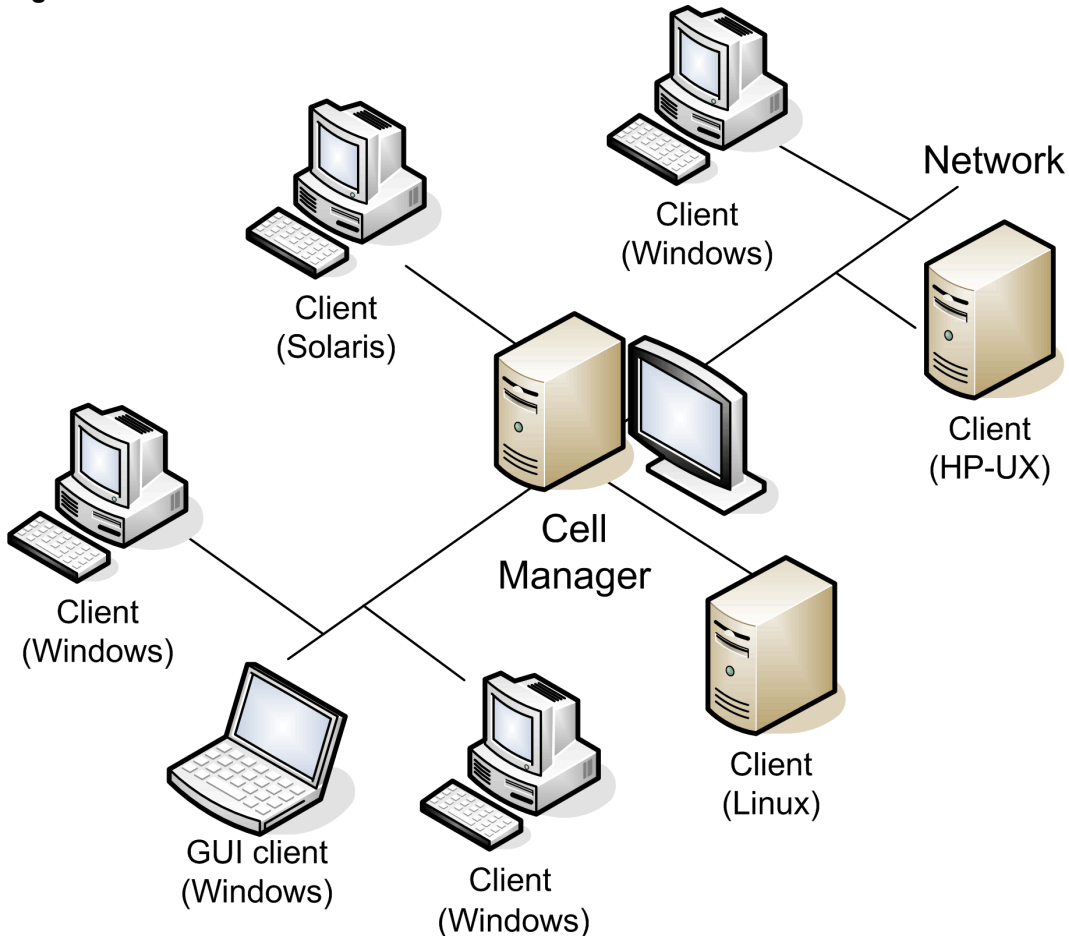
**Note:** You cannot remotely install a Data Protector client on a Windows system if an Installation Server has already been installed on this system. To install an Installation Server and client component(s) on the same system, you must perform a local client installation from the Data



Protector Windows installation DVD-ROM. In the Custom Setup window, select all desired client components and the Installation Server component.

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

**Figure 1: Data Protector Cell**



## The remote installation concept

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

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

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

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

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

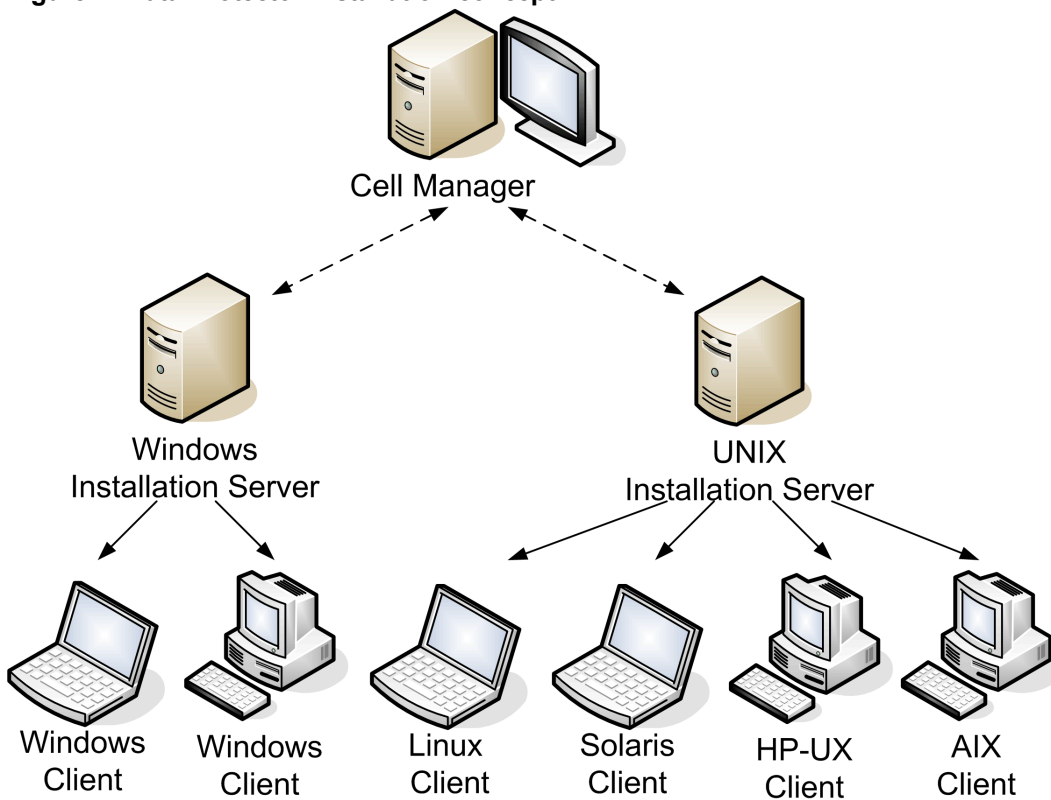
For UNIX operating systems on which remote installation is not supported, or if you do not install an Installation Server for UNIX, you can install UNIX clients locally, from the Data Protector UNIX installation DVD-ROM.

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

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

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

**Figure 2: Data Protector installation concept**



## Data Protector installation media

Data Protector supports various operating systems and several processor architectures. The software is delivered on either three DVD-ROMs (physical) or three ISO image files (electronic). ["Data Protector DVD-ROM/ISO image list"](#) lists the components found on the DVD-ROMs or ISO images.

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

**Table 1: Data Protector DVD-ROM/ISO image list**

DVD num.	DVD-ROM title/ISO image	Contents
1	Data Protector software 8.1 Windows  (TD586-15012.iso)	<ul style="list-style-type: none"><li>• Cell Manager and Installation Server for Windows 64-bit (AMD64/Intel EM64T) systems</li><li>• The complete set of English guides in the electronic PDF format (in the DOCS directory)</li><li>• Windows 64-bit clients</li><li>• HP OpenVMS clients (Alpha and Itanium systems)</li><li>• Product information</li><li>• HP software integration packages</li></ul>
2	Data Protector software 8.1 HP-UX  (TD586-15013.iso)	<ul style="list-style-type: none"><li>• Cell Manager, Installation Server, and clients for HP-UX systems</li><li>• Clients for other UNIX systems</li><li>• Clients for Mac OS X systems</li><li>• The complete set of English guides in the electronic PDF format (in the DOCS directory)</li><li>• HP software integration packages</li></ul>
3	Data Protector software 8.1 Linux  (TD586-15014.iso)	<ul style="list-style-type: none"><li>• Cell Manager, Installation Server, and clients for Linux systems</li><li>• Clients for other UNIX systems</li><li>• Clients for Mac OS X systems</li><li>• The complete set of English guides in the electronic PDF format (in the DOCS directory)</li><li>• HP software integration packages</li></ul>

## Choosing the Cell Manager system

The Cell Manager is the main system in a Data Protector cell. It manages the cell from one central point. The Cell Manager does the following:

- Runs the core Data Protector software.
- Hosts the Data Protector Internal Database (IDB) server.
- Collects and maintains data with information about Data Protector sessions.
- Runs the Session Managers that start and stop different types of Data Protector sessions and store related information into the IDB.

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

- Supported platforms

The Cell Manager can be installed on Windows, HP-UX, or Linux platforms.

For details on supported versions or releases of these platforms, see the latest support matrices at <http://support.openview.hp.com/selfsolve/manuals>.

- Reliability of the Cell Manager system

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

- Database growth and required disk space

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

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

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

**Note:** You do not have to use the Cell Manager as the user interface system. For example, you can have a UNIX Cell Manager system and the Data Protector user interface component installed on another system with a Windows platform.

### What's next?

To determine the minimum requirements for your future Cell Manager system, see "[Installing the Data Protector Cell Manager and Installation Servers](#)".

## Choosing the Data Protector user interface system

Data Protector provides two user interfaces: a graphical user interface (GUI) and a command-line interface (CLI). The GUI is available for Windows platforms, and the CLI is available for Windows, HP-UX, Solaris, and Linux platforms. Both user interfaces are provided by and are installed as a single Data Protector software component.

The system selected to control the cell will be used by a network administrator or a backup operator. However, in a large computer environment, it may be desirable to run the user interface on several systems, and in case of a heterogeneous environment, on various platforms.

For details on supported operating systems (releases, versions, editions) for the user interface, see the latest support matrices at <http://support.openview.hp.com/selfsolve/manuals>. For more information on local language support and usage of non-ASCII characters in file names, see the *HP Data Protector Help* index: “language settings, customizing”.

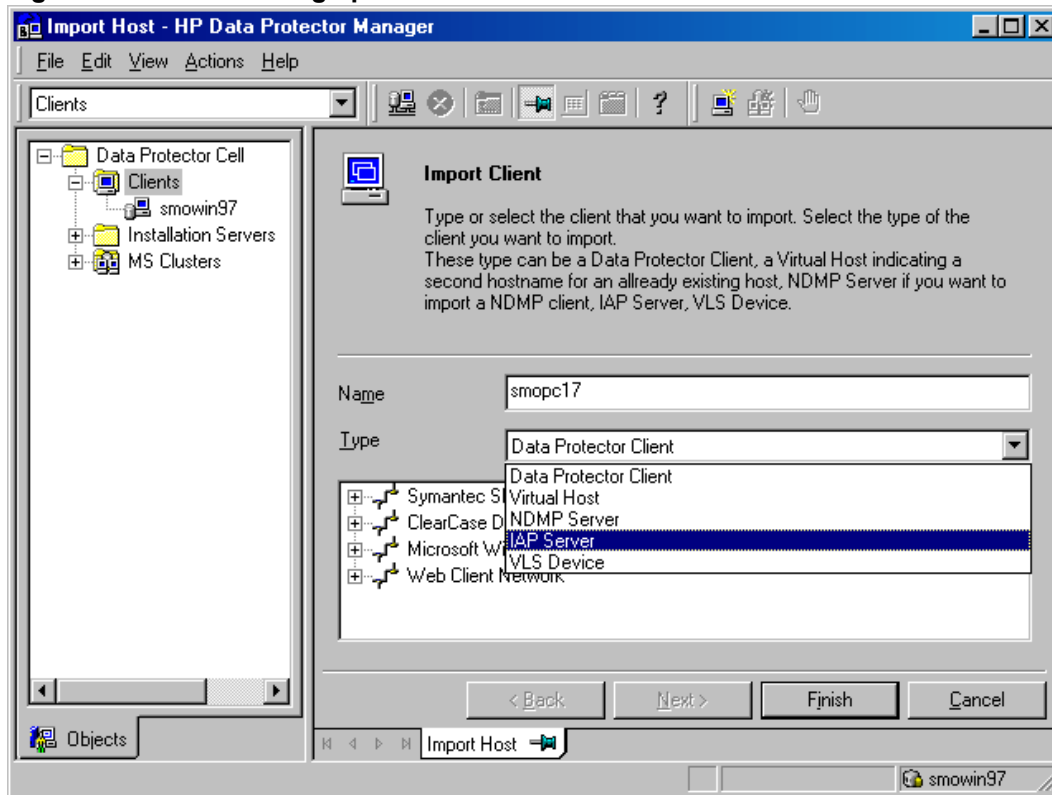
Once you have installed the user interface on a system in the cell, you can remotely access the Cell Manager from that system. You do not have to use the graphical user interface system on the Cell Manager.

## The Data Protector graphical user interface

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

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

**Figure 3: Data Protector graphical user interface**



See also [Data Protector graphical user interface](#) , which defines the most important areas of the Data Protector GUI.

## Chapter 2: Installing Data Protector on your network

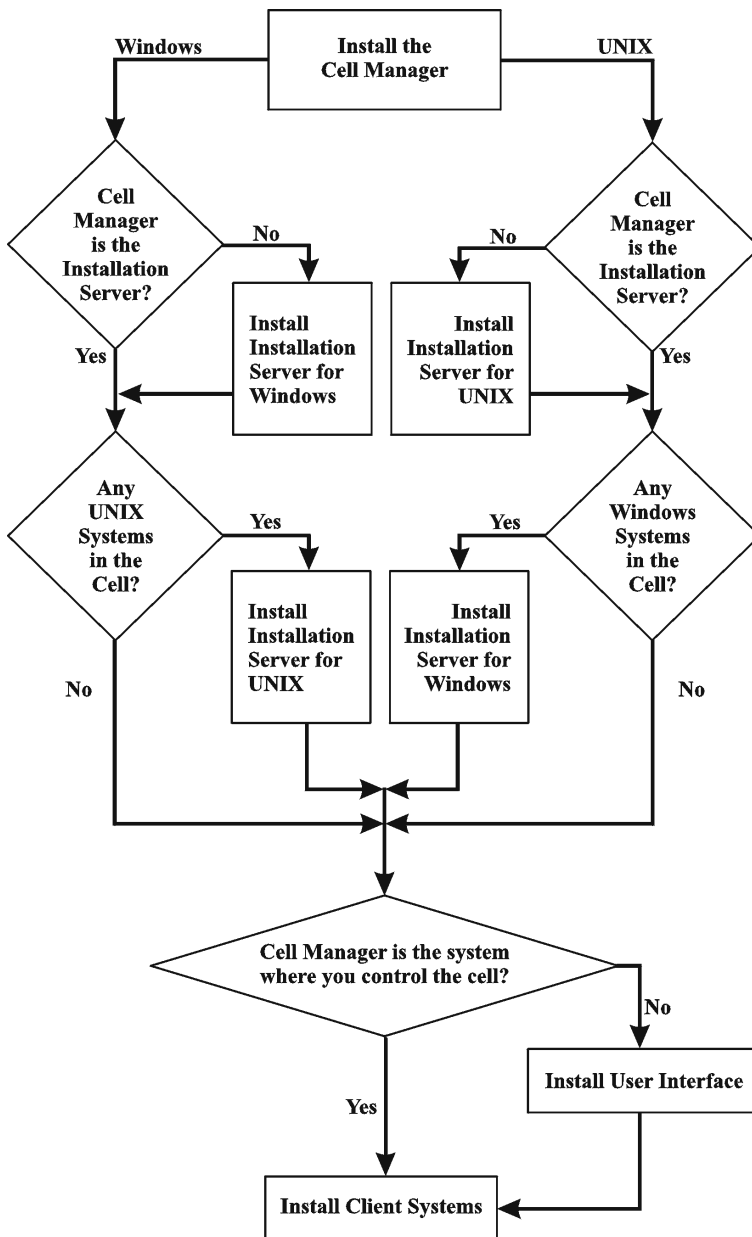
This chapter contains detailed instructions about:

- Installing the Data Protector Cell Manager and Installation Servers
- Installing the Data Protector clients
- Installing the Data Protector integration clients
- Installing the localized Data Protector documentation
- Installing the Data Protector Single Server Edition
- Installing the Data Protector web reporting
- Installing the Data Protector Cell Manager, Installation Servers, and clients on clusters: HP Serviceguard
- Installing the Data Protector Cell Manager and clients on clusters: Microsoft Cluster Server
- Installing the Data Protector clients on clusters: Veritas Cluster, IBM HACMP Cluster, Microsoft Hyper-V Cluster

### Installing the Data Protector Cell Manager and Installation Servers

For the flow of installation procedure, see " [Installation procedure](#) " .

**Figure 4: Installation procedure**



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

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

## Installing a UNIX Cell Manager

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



## Prerequisites

- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.
- The user account used for the installation must have administrative (root) privileges on the selected target system.
- Have the `glibc-x.xx-xx.e17.i686` installed (RHEL 6 version requires `glibc-x.xx-xx.e16.i686`). This is applicable for Red Hat 7 systems only.
- Have `net-tools` installed (some `net-tools` utilities are needed during installation). This is applicable for Red Hat 7 systems only.
- The system that will become the Cell Manager must:
  - Have a supported UNIX operating system installed. For a list of supported operating systems for the Cell Manager, see <http://support.openview.hp.com/selfsolve/manuals>.
  - Have access to a DVD-ROM drive or be able to mount an ISO image.
  - Have sufficient free disk space for the Data Protector Cell Manager software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*, chapter *Installation requirements*.

You can overcome free disk space shortage by installing Data Protector to linked directories. Before creating the links, see "[The installed directory structure on HP-UX and Linux systems](#)".

- Have sufficient free disk space for the Data Protector Internal Database (IDB). For details, see the *HP Data Protector Product Announcements, Software Notes, and References*, chapter *Installation requirements*. Note that the current IDB design allows the database binary files to be relocated if growth in database size makes it necessary.
- Have the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames.
- Recognize the Cell Manager system if using a NIS server. See "[Preparing a NIS server](#)".
- Have the following ports free:
  - 5555 — the default port for Data Protector communication
  - 7112 — the Internal Database Service port
  - 7113 — the Internal Database Connection Pooler (IDB CP) port
  - 7116 — the Application Server (HTTPS AS) port
  - 9999 — the Application Server management port

To change the default communication port number, see "[Changing the default Data Protector Inet port](#)".

To change the default IDB and Application Server ports, see "[Changing the default Data Protector IDB ports and user accounts on UNIX systems](#)".

- Support long filenames. To check if your filesystem supports long filenames, execute the `getconf NAME_MAX DirectoryPath` command.
- Have the `inetd` or `xinetd` daemon up and running.
- Have the user group `hdp` and the dedicated user account `hdp` in this user group configured to be used by Data Protector. To change the default user account, see ["Changing the default Data Protector IDB ports and user accounts on UNIX systems"](#) .
- Have the existing home folder configured for the `hdp` user otherwise some of the Data Protector services could fail to start.

### *Cluster-aware Cell Manager*

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

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

### *Recommendations*

- HP recommends to use large file support (LFS) on the file systems which store the Data Protector Internal Database and the DC binary files that are expected to grow larger than 2 GB.

## **Setting kernel parameters**

#### ***HP-UX systems:***

- Set the kernel parameter `shmmax` (maximum size of a shared memory segment) to at least 2.5 GB. To check the configuration, execute:

```
kccusage shmmax
```

- HP recommends to set the kernel parameter `maxdsiz` (max data segment size) or `maxdsiz_64` to at least 134217728 bytes (128 MB), and the kernel parameter `semnu` (maximum number of semaphore undo structures) to at least 4000.

After committing these changes, restart the system.

#### ***Linux systems:***

- Set the kernel parameter `shmmax` (maximum size of a shared memory segment) to at least 2.5 GB. To check the configuration, execute:

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

## Installation procedure

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

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

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

1. Insert and mount the appropriate UNIX installation DVD-ROM (for HP-UX or Linux) to a mount point or mount the ISO image directly.

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

Optionally, copy the following directories from the DVD-ROM to your local disk:

`LOCAL_INSTALL`

`platform_dir /DP_DEPOT`

Where `platform_dir` is:

<code>hpux</code>	for HP-UX systems
<code>linux_x86_64</code>	for Linux systems

2. Go to the `LOCAL_INSTALL` directory and execute:

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

For details on the `omnisetup.sh` command, see the *HP Data Protector Command Line Interface Reference*.

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

**Note:** The installation of Data Protector 8.10 on Red Hat 7 system fails. For more information, see ["Troubleshooting installation on Red Hat 7 systems"](#).

The installation of Data Protector 8.10 on HP-UX system creates unusable certificate that needs to be updated. For more information, see ["Troubleshooting installation on UNIX systems"](#).

## The installed directory structure on HP-UX and Linux systems

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

**Important:** To install Data Protector to linked directories, for instance:

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

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

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

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

/opt/omni/bin	User commands
/opt/omni/help/C	Help
/opt/omni/lbin	Administrative commands, command-line utilities
/opt/omni/sbin	Administrative commands, command-line utilities
/opt/omni/sbin/install	Installation scripts
/etc/opt/omni	Configuration data
/opt/omni/lib	Shared libraries for compression, data encoding, and device handling
/opt/omni/doc/C	Guides in the electronic PDF format
/var/opt/omni/log /var/opt/omni/server/log	Log files
/opt/omni/lib/nls/C	Message catalog files
/opt/omni/lib/man	Man pages
/var/opt/omni/tmp	Temporary files
/var/opt/omni/server/db80	IDB files  For details, see the <i>HP Data Protector Help</i> index: "IDB, location of directories".
/opt/omni/AppServer	HP Data Protector Application Server.
/opt/omni/idb	The HP Data Protector internal database.
/opt/omni/jre	The Java Runtime Environment for use with Data Protector.

## Configuring automatic startup and shutdown

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

The following files are automatically configured:

### HP-UX systems:

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

### Linux systems:

/etc/init.d/omni	A script with startup and shutdown procedures.
/etc/rcinit_level.d/K10omni	A link to the /etc/init.d/omni script that shuts down Data Protector.  Where <i>init_level</i> is 1 and 6.
/etc/rcinit_level.d/S90omni	A link to the /etc/init.d/omni script that starts up Data Protector.  Where <i>init_level</i> is 2,3,4, and 5.

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

### HP-UX systems:

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

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

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

<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. The MMD manages the device and media management operations.
<code>/opt/omni/sbin/kms</code>	The Data Protector Key Management Server (KMS) service runs on the Cell Manager and is started when the Cell Manager software is installed on the system. The KMS provides key management for the Data Protector encryption functionality.
<code>/opt/omni/idb/bin/postgres</code>	The Data Protector Internal Database Service (hdp-idb) is the service under which the IDB runs. The service is accessed locally on the Cell Manager by processes that need information from the internal database. This service is accessed remotely only for media management information about transfer from the IDB on the Cell Manager to the IDB on the Manager-of-Manager (MoM).
<code>/opt/omni/idb/bin/pgbouncer</code>	The Data Protector Internal Database Connection Pooler (hdp-idb-cp) service offers a pool of open connections to the hdp-idb which can be used on request instead of opening a new connection for every request, thus ensuring hdp-idb connection scalability. The service runs on the Cell Manager and is accessed only by local processes.
<code>/opt/omni/AppServer/bin/standalone.sh</code>	The Data Protector Application Server (hdp-as) service is used for connecting the GUI to the IDB through a HTTPS connection (web services). It runs on the Cell Manager and has a local connection to the hdp-idb-cp service.

## Setting environment variables

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

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

## What's next?

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

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

## Installing a Windows Cell Manager

### Prerequisites

- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.
- The user account used for the installation must:
  - Have administrative (Administrator) privileges on the selected target system.
  - Have network access user rights set in the Windows local security policy.
- The Data Protector Inet service by default runs under the Windows local user account SYSTEM. However, if for various reasons the Inet service runs under a Windows domain user account, you must additionally grant it the following Windows operating system Security Policy privileges:
  - Impersonate a client after authentication
  - Replace a process level token

For more information, see the *HP Data Protector Help* index: "Inet user impersonation".

- The system that will become the Cell Manager must:
  - Have a supported Windows operating system installed. For a list of supported operating systems for the Cell Manager, see <http://support.openview.hp.com/selfsolve/manuals>.
  - Have access to a DVD-ROM drive or be able to mount an ISO image.
  - Have sufficient free disk space for the Data Protector Cell Manager software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*, chapter *Installation requirements*.
  - Have sufficient free disk space for the Data Protector Internal Database (IDB). For details, see the *HP Data Protector Product Announcements, Software Notes, and References*, chapter *Installation requirements*.

- Have the Microsoft implementation of the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames. The computer name and the hostname must be the same.
- Have a static IP address assigned. 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 following ports free:
  - 5555 — the default port for Data Protector communication
  - 7112 — the Internal Database Service port
  - 7113 — the Internal Database Connection Pooler (IDB CP) port
  - 7116 — the Application Server (HTTPS AS) port
  - 9999 — the Application Server management port

You can change the IDB and Application Server service ports during installation. To change the default communication port number, see "[Changing the default Data Protector Inet port](#)".

### *Microsoft Terminal Services Client*

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

### *Recommendations*

- If you expect DC binary files to grow larger than 2 GB (their size is limited only by the file system settings), HP recommends to use the NTFS file system for their storage.

### *Cluster-aware Cell Manager*

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

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

## ***Installation procedure***

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

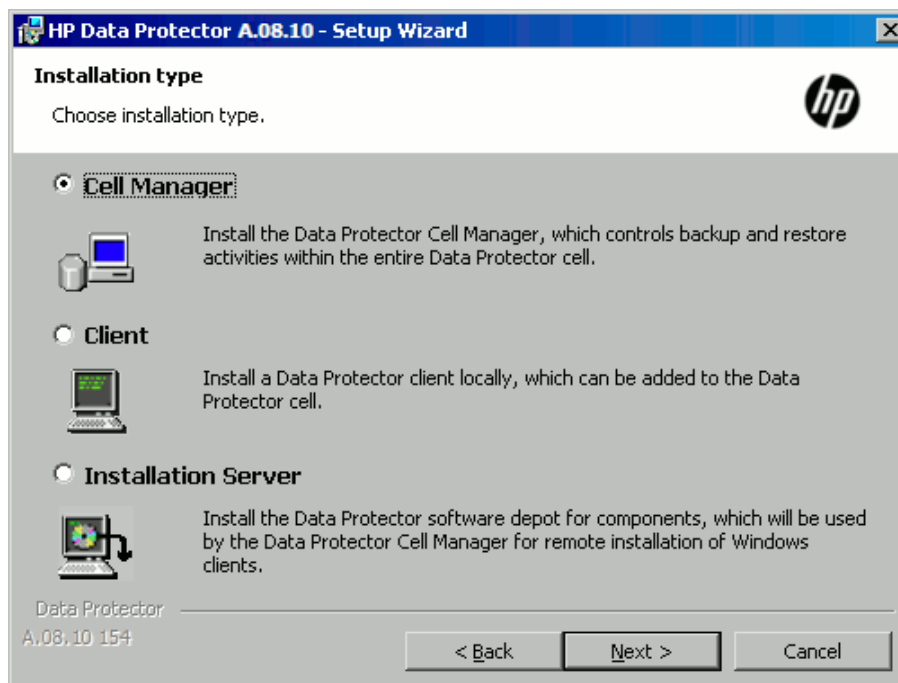


1. Insert the Windows installation DVD-ROM or mount the ISO image.

The User Account Control dialog is displayed. Click **Continue** to proceed with the installation.

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

**Figure 5: Selecting the installation type**



5. Provide the username and password for the account under which the Data Protector services will run.

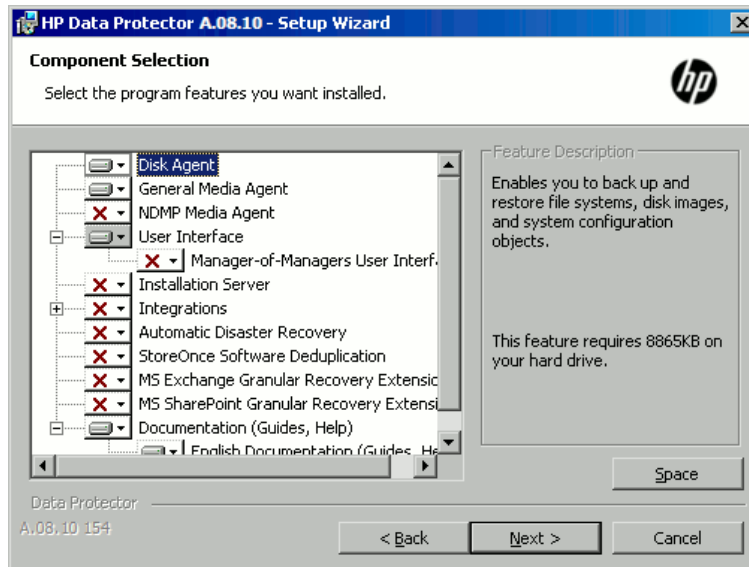
Click **Next** to continue.

6. Click **Next** to install Data Protector into the default installation folders.

Otherwise, click **Change** to open the Change Current Destination Folder or Change Current Program Data Destination Folder dialog box, and change the installation folder as needed. The path to the program data installation folder should not exceed 80 characters.

7. In the Component Selection page, select the components you want to install. For a list and descriptions of the Data Protector components, see ["Data Protector components"](#).

**Figure 6: Selecting software components**

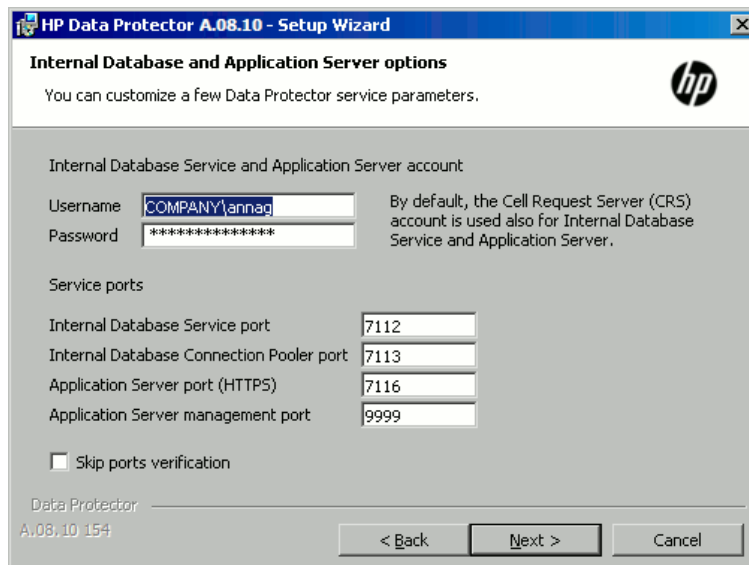


**Disk Agent**, **General Media Agent**, **User Interface**, and **Installation Server** are selected by default. Click **Next**.

8. Optionally, change the user account used by the Data Protector IDB and Application Server, and the ports used by these services.

Click **Next**.

**Figure 7: Changing the IDB and Application Server options**



9. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By

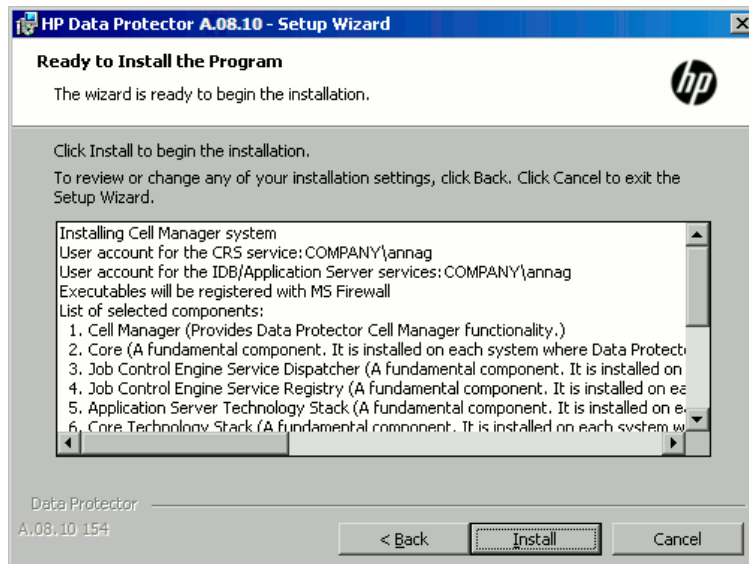
default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect the option. However, note that for proper functioning of Data Protector, the executables must be enabled.

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

Click **Next**.

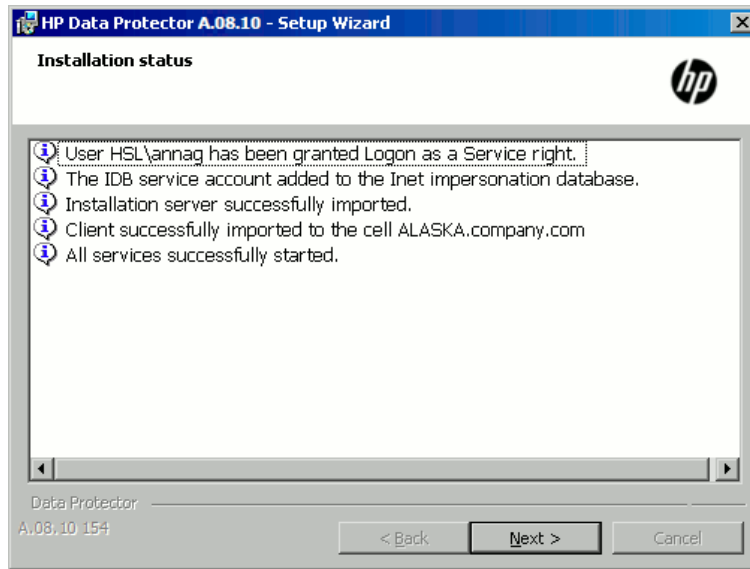
10. The component summary list is displayed. Click **Install** to start installing the selected components. This may take several minutes.

**Figure 8: Component summary list**



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

**Figure 9: Installation status page**



12. If you have installed the User Interface component, to start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

If you have installed the English Documentation (Guides, Help) component, to view the *HP Data Protector Product Announcements, Software Notes, and References* immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

Click **Finish**.

## ***After the installation***

The Cell Manager files are located in the *Data\_Protector\_home* directory and in *Data\_Protector\_program\_data*.

The software depot is located in the *Data\_Protector\_program\_data\Depot* directory.

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

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

The following processes are running on the Cell Manager system:

<code>crs.exe</code>	The Data Protector Cell Request Server (CRS) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The CRS starts and controls backup and restore sessions in the cell. It runs in the <i>Data_Protector_home\bin</i> directory.
----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

mmd.exe	The Data Protector Media Management Daemon (MMD) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The MMD manages the device and media management operations. It runs in the <i>Data_Protector_home\bin</i> directory.
omniinet.exe	The Data Protector client service that enables the Cell Manager to start agents on other systems. The Data Protector Inet service must run on all systems in the Data Protector cell. It runs in the <i>Data_Protector_home\bin</i> directory.
kms.exe	The Data Protector Key Management Server (KMS) service runs on the Cell Manager system and is started when the Cell Manager software is installed on the system. The KMS provides key management for the Data Protector encryption functionality. It runs in the <i>Data_Protector_home\bin</i> directory.
hdp-idb	The Data Protector Internal Database Service (hdp-idb) is the service under which the IDB runs. The service is accessed locally on the Cell Manager by processes that need information from the internal database. This service is accessed remotely only for media management information about transfer from the IDB on the Cell Manager to the IDB on the Manager-of-Manager (MoM).
hdp-idb-cp	The Data Protector Internal Database Connection Pooler (hdp-idb-cp) service offers a pool of open connections to the hdp-idb which can be used on request instead of opening a new connection for every request, thus ensuring hdp-idb connection scalability. The service runs on the Cell Manager and is accessed only by local processes.
hdp-as	The Data Protector Application Server (hdp-as) service is used for connecting the GUI to the IDB through a HTTPS connection (web services). It runs on the Cell Manager and has a local connection to the hdp-idb-cp service.

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

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

## Troubleshooting

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

This is the list of the requirements checked by Setup:

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

## What's next?

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

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

## Installing Installation Servers

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

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

**Note:** When using the Encrypted Control Communication (ECC) in a cell, ensure that ECC is enabled on the Installation Server also. Otherwise, the Installation Server will not communicate with the clients that use ECC.

## Installing Installation Servers for UNIX systems

### Prerequisites

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

- Have the HP-UX or Linux operating system installed. For details on supported operating systems for the Installation Server, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have the `inetd` or `xinetd` daemon up and running.
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.
- Have the port number 5555 (default) free. If this is not the case, see "[Changing the default Data Protector Inet port](#)".

- Have the TCP/IP protocol installed and running. The protocol must be able to resolve hostnames.
- Have enough disk space for the complete Data Protector software depot. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have a DVD-ROM drive or be able to mount ISO images.
- The Cell Manager in the Data Protector cell must be of the 8.10 version.

**Important:** To install Data Protector to linked directories, for instance:

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

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

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

## Installation procedure

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

1. Insert and mount the appropriate UNIX installation DVD-ROM or ISO image (for HP-UX or Linux) to a mount point.

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

Optionally, copy the following directories from the DVD-ROM to your local disk:

LOCAL\_INSTALL

*platform\_dir*/DP\_DEPOT

Where *platform\_dir* is:

hpux	for HP-UX systems
linux_x86_64	for Linux systems

2. Go to the LOCAL\_INSTALL directory and execute:

```
./omnisetup.sh -IS
```

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

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

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

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

### *What's next?*

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

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

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

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

## ***Installing an Installation Server for Windows systems***

### *Prerequisites*

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

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



## Limitations

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

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

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

## Installation procedure

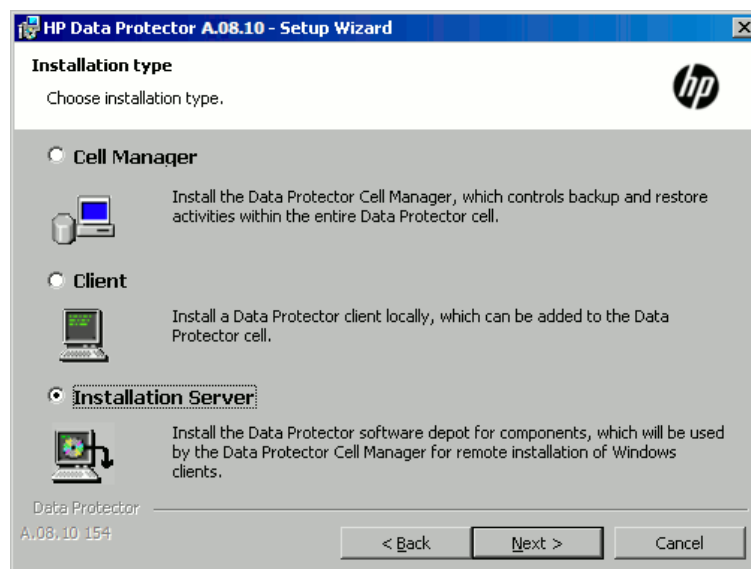
Follow these steps to install the Installation Server for Windows systems:

1. Insert the Windows installation DVD-ROM.

The User Account Control dialog is displayed. Click **Continue** to proceed with the installation.

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

**Figure 10: Selecting the installation type**



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

Otherwise, click **Change** to open the Change Current Destination Folder window and enter a new path.

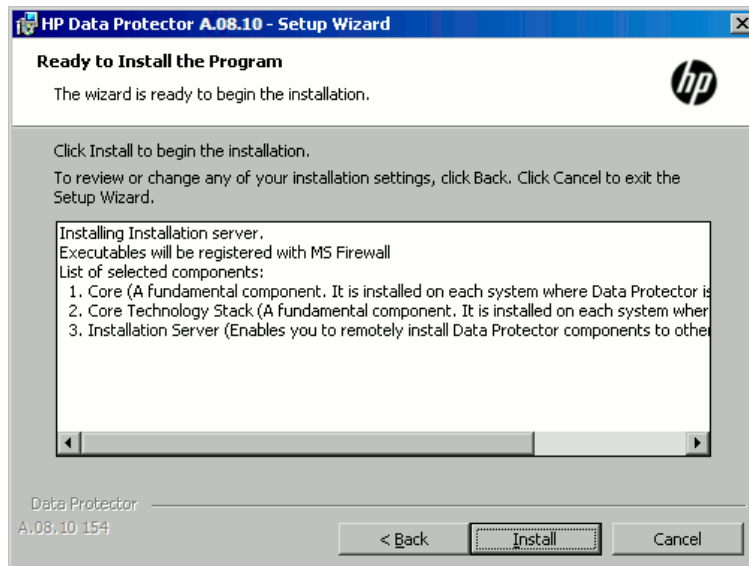
6. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports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

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

Click **Next**.

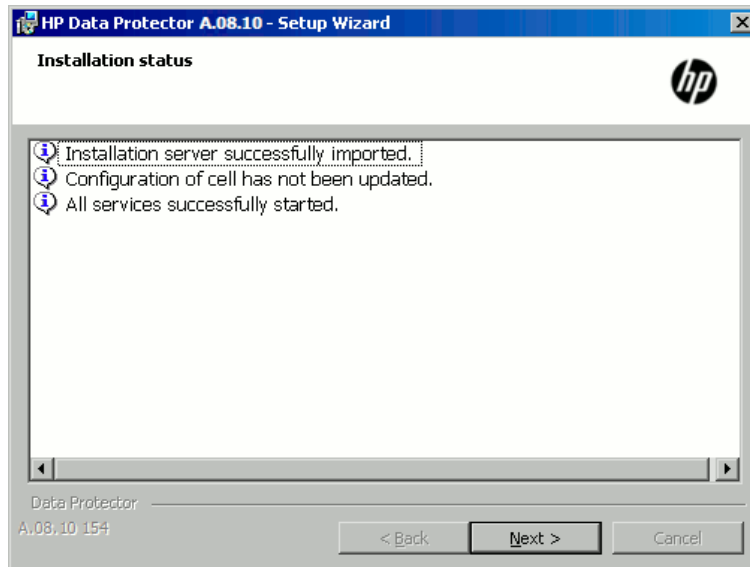
7. The component summary list is displayed. Click **Install** to start installing the selected components. This may take several minutes.

**Figure 11: Component selection summary page**



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

**Figure 12: Installation status page**



9. Click **Finish**.

As soon as the installation is finished, the software is, by default, installed in the directory *Data\_Protector\_program\_data\Depot*. The software is shared so that it can be accessed from the network.

### *What's next?*

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

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

## **Installing Data Protector clients**

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

For the list of Data Protector installation DVD-ROMs and ISO images, see ["Data Protector installation media"](#) .

**Note:** A Windows Installation Server targets a client's port 445 during a remote installation, while a HP-UX/Linux Installation Server targets a client's port 22 (secure remote install) or ports 512 / 514 (non-secure remote install). On the Installation Server side, ephemeral ports are used to make

connections to these target ports.

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

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

["Installing Data Protector clients"](#) lists Data Protector client systems with references to detailed descriptions.

**Table 2: Installing Data Protector client systems**

Client system	Installation type and reference
Windows	Remote and local installation; see <a href="#">"Installing Windows clients"</a> .
HP-UX	Remote and local installation; see <a href="#">"Installing HP-UX clients"</a> .
Solaris	Remote and local installation; see <a href="#">"Installing Solaris clients"</a> .
Linux	Remote and local installation; see <a href="#">"Installing Linux clients"</a> .
ESX Server	Remote and local installation; see <a href="#">"Installing ESX Server clients"</a> .
Mac OS X	Remote and local installation; see <a href="#">"Installing Mac OS X clients"</a> .
IBM AIX	Remote and local installation; see <a href="#">"Installing IBM AIX clients"</a> .
HP OpenVMS	Local installation; see <a href="#">"Installing HP OpenVMS clients"</a> .
other UNIX system	Local installation; see <a href="#">"Local installation on UNIX and Mac OS X systems"</a> .
DAS Media Agent client	Remote and local installation; see <a href="#">"Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library"</a> .
ACS Media Agent client	Remote and local installation; see <a href="#">"Installing a Media Agent to use the ADIC/GRAU Library or the StorageTek Library"</a> .

## Integrations

Data Protector integrations are software components that allow you to back up database applications with Data Protector. The systems running database applications are installed the same way as any Windows or UNIX client systems, provided that the appropriate software component has been selected (for example, the MS Exchange Integration component for backing up the Microsoft Exchange Server

database, Oracle Integration component for backing up an Oracle database, and so on). For the references, see ["Installing integrations"](#) .

**Table 3: Installing integrations**

Software application or disk array family	Reference
Microsoft Exchange Server	See <a href="#">"Microsoft Exchange Server clients"</a> .
Microsoft SQL Server	See <a href="#">"Microsoft SQL Server clients"</a> .
Microsoft SharePoint Server	See <a href="#">"Microsoft SharePoint Server clients"</a> .
Microsoft Volume Shadow Copy Service (VSS)	See <a href="#">"Microsoft Volume Shadow Copy Service clients"</a> .
Sybase Server	See <a href="#">"Sybase Server clients"</a> .
Informix Server	See <a href="#">"Informix Server clients"</a> .
SAP R/3	See <a href="#">"SAP R/3 clients"</a> .
SAP MaxDB	See <a href="#">"SAP MaxDB clients"</a> .
SAP HANA Appliance	See <a href="#">"SAP HANA Appliance clients"</a>
Oracle Server	See <a href="#">"Oracle Server clients"</a> .
IBM DB2 UDB	See <a href="#">"IBM DB2 UDB clients"</a> .
Lotus Notes/Domino Server	See <a href="#">"Lotus Notes/Domino Server clients"</a> .
VMware	See <a href="#">"VMware clients"</a> .
Microsoft Hyper-V	See <a href="#">"Microsoft Hyper-V clients"</a> .
Network Data Management Protocol (NDMP) Server	See <a href="#">"NDMP Server clients"</a> .
HP P4000 SAN Solutions	See <a href="#">"HP P4000 SAN Solutions clients"</a> .

Software application or disk array family	Reference
HP P6000 EVA Disk Array Family	See " <a href="#">HP P6000 EVA Disk Array Family clients</a> " .
HP P9000 XP Disk Array Family	See " <a href="#">HP P9000 XP Disk Array Family clients</a> " .
HP 3PAR StoreServ Storage	See " <a href="#">HP 3PAR StoreServ Storage clients</a> " .
EMC Symmetrix	See " <a href="#">EMC Symmetrix clients</a> " .

**Table 4: Other installations**

Installation	Reference
Integrated Archive Platform (IAP)	See " <a href="#">Installing the Data Protector integration clients</a> " .
Localized user interface	See <a href="#">Installing localized Data Protector user interface</a> .
Web reporting	See " <a href="#">Installing the Data Protector web reporting</a> " .
HP Serviceguard	See " <a href="#">Installing Data Protector on an HP Serviceguard</a> " .
Microsoft Cluster Server	See " <a href="#">Installing Data Protector on a Microsoft Cluster Server</a> " .
Veritas Cluster Server	See " <a href="#">Installing Data Protector clients on a Veritas Cluster</a> " .
IBM HACMP Cluster	See " <a href="#">Installing Data Protector on an IBM HACMP Cluster</a> " .
Microsoft Hyper-V cluster	See " <a href="#">Installing Data Protector on a Microsoft Hyper-V cluster</a> " .

## Data Protector components

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

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

User Interface	<p>The User Interface component includes the Data Protector graphical user interface on Windows systems and part of the command-line interface on Windows and UNIX systems. The software is needed to access the Data Protector Cell Manager and must be installed at least to the system that is used for managing the cell.</p> <p><b>Note:</b> Specific commands of the Data Protector command-line interface are included in other Data Protector components. For details, see the <i>HP Data Protector Command Line Interface Reference</i>.</p> <p>Before using the Data Protector User Interface in heterogeneous environments, see the <i>HP Data Protector Product Announcements, Software Notes, and References</i> for the limitations incurred.</p>
English Documentation (Guides, Help)	This is the Data Protector English language documentation file set.
French Documentation (Guides, Help)	This is the Data Protector French language documentation file set.
Japanese Documentation (Guides, Help)	This is the Data Protector Japanese language documentation file set.
Simplified Chinese Documentation (Guides, Help)	This is the Data Protector Simplified Chinese language documentation file set.
Manager-of-Managers User Interface	The Manager-of-Managers User Interface includes the Data Protector graphical user interface. The software is needed to access the Data Protector Manager-of-Managers functionality and control the multicell environment. The Manager-of-Managers User Interface and the Manager User Interface are available as a common application.
Disk Agent	The Disk Agent component must be installed on systems that have disks that will be backed up with Data Protector.
General Media Agent	The General Media Agent component must be installed on systems that have backup devices connected or have access to a library robotics and will be managed by Data Protector.
Automatic Disaster Recovery	The Automatic Disaster Recovery component must be installed on systems for which you want to enable recovery using any of the automatic disaster recovery methods and on systems where the DR CD ISO image for Enhanced Automated Disaster Recovery (EADR) or One Button Disaster Recovery (OBDP) will be prepared to provide automatic preparation for the disaster recovery.
SAP R/3 Integration	The SAP R/3 Integration component must be installed on systems that have an SAP R/3 database that will be backed up with Data Protector.

SAP MaxDB Integration	The SAP MaxDB Integration component must be installed on systems that have an SAP MaxDB database that will be backed up using Data Protector.
SAP HANA Integration	The SAP HANA Integration component must be installed on systems that represent or constitute an SAP HANA Appliance that you want to protect using Data Protector.
Oracle Integration	The Oracle Integration component must be installed on systems that have an Oracle database that will be backed up with Data Protector.
Virtual Environment Integration	The Virtual Environment Integration component must be installed on the systems which you will use as backup hosts to control the backup and restore of virtual machines using the Data Protector Virtual Environment integration.
DB2 Integration	The DB2 Integration component must be installed on all systems that have a DB2 Server that will be backed up with Data Protector.
Sybase Integration	The Sybase Integration component must be installed on systems that have a Sybase database that will be backed up with Data Protector.
Informix Integration	The Informix Integration component must be installed on systems that have an Informix Server database that will be backed up with Data Protector.
MS Exchange Integration	<p>The MS Exchange Integration component must be installed on Microsoft Exchange Server 2007 systems that you intend to back up using the Data Protector Microsoft Exchange Server 2007 integration or the Data Protector Microsoft Exchange Single Mailbox integration.</p> <p>It must also be installed on Microsoft Exchange Server 2010 systems that you intend to back up using the Data Protector Microsoft Exchange Single Mailbox integration.</p>
MS Exchange Server 2010+ Integration	The MS Exchange Server 2010+ Integration component must be installed on Microsoft Exchange Server 2010 or Microsoft Exchange Server 2013 systems that you intend to back up using the Data Protector Microsoft Exchange Server 2010 integration.
MS SQL Integration	The MS SQL Integration component must be installed on the systems that have an Microsoft SQL Server database which will be backed up with Data Protector.
MS SharePoint 2007/2010/2013 Integration	The MS SharePoint 2007/2010/2013 Integration component must be installed on Microsoft SharePoint Server 2007/2010/2013 systems that will be backed up with Data Protector.
MS Volume Shadow Copy Integration	The MS Volume Shadow Copy Integration component must be installed on the Windows Server systems where you want to run backups coordinated by Volume Shadow Copy Service.
HP P4000 Agent	The HP P4000 Agent component must be installed on both the application system and the backup system to integrate HP P4000 SAN Solutions with Data Protector.
HP P6000 / HP 3PAR SMI-S Agent	The HP P6000 / HP 3PAR SMI-S Agent component must be installed on both the application system and the backup system to integrate Data Protector with HP P6000 EVA Disk Array Family, or to integrate Data Protector with HP 3PAR StoreServ Storage.



HP P9000 XP Agent	The HP P9000 XP Agent component must be installed on both the application system and the backup system to integrate Data Protector with HP P9000 XP Disk Array Family.
HP 3PAR VSS Agent	The HP 3PAR VSS Agent component must be installed on both the application system and the backup system to integrate Data Protector with HP 3PAR StoreServ Storage in configurations where the application and backup systems are Windows systems and you want to use the Volume Shadow Copy Service to backup and restore your data.
EMC Symmetrix Agent	The EMC Symmetrix Agent component must be installed on both the application system and the backup system to integrate Data Protector with EMC Symmetrix.
NDMP Media Agent	The NDMP Media Agent component must be installed on all systems that will be backing up data to NDMP dedicated drives through an NDMP server.
IAP Deduplication Agent	The IAP Deduplication Agent component must be installed on systems that will perform backups directly to the IAP appliance using Data Protector.
Lotus Integration	The Lotus Integration component must be installed on all systems in the Data Protector cell that have Lotus Notes/Domino Server databases that you plan to back up with Data Protector.
MS Exchange Granular Recovery Extension	The Data Protector Granular Recovery Extension for Microsoft Exchange Server must be installed on each Microsoft Exchange Server system to enable the granular recovery feature. In a Microsoft Exchange Server Database Availability Group (DAG) environment, it must be installed on any of the Exchange Server systems in DAG.
MS SharePoint Granular Recovery Extension	The Data Protector Granular Recovery Extension for Microsoft SharePoint Server must be installed on the Microsoft SharePoint Server Central Administration system.
VMware Granular Recovery Extension Web Plug-In	The Data Protector VMware Granular Recovery Extension Web Plug-In component must be installed on the VMware Virtual Server system to enable the granular recovery feature of the VMware virtual machines. Only remote installation is supported.
VMware Granular Recovery Extension Agent	The Data Protector VMware Granular Recovery Extension Agent component must be installed on the mount proxy system to enable restore and granular recovery of the VMware virtual machines. Only remote installation is supported.

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

## Installing Windows clients

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

### Prerequisites

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

- Have sufficient disk space for the Data Protector client software. For details, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Have port number 5555 (default) free.
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.
- 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.
- Ensure that network access user rights are set under the Windows local security policy for the account performing the installation.

### Limitations

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

### Recommendations

- Prior to installing Data Protector 8.10, check if Microsoft Installer (MSI) 2.0 is installed on the system. If an earlier version is installed, it is recommended to upgrade it to the version 2.0 before starting the Data Protector installation. If you do not upgrade MSI beforehand, the Data Protector Setup Wizard automatically upgrades it to the required version. In this case, Data Protector informs you appropriately about the MSI upgrade.

If MSI is upgraded, it is highly recommended to restart the system.

### *Automatic disaster recovery*

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

### *Cluster-aware clients*

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

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

## **Local installation**

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

1. Insert the DVD-ROM or mount the ISO image.

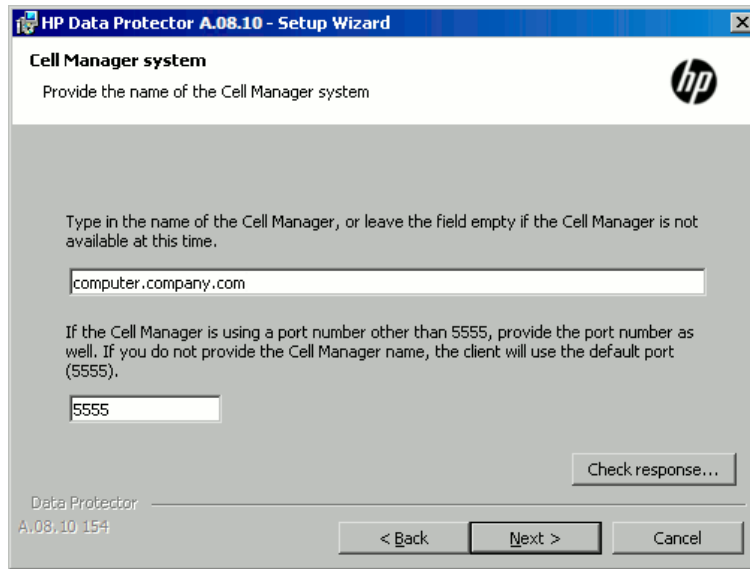
On Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, the User Account Control dialog box is displayed. Click **Continue** to proceed with the installation.

2. In the HP Data Protector window, select **Install Data Protector** to start the Data Protector Setup Wizard.
3. Follow the Setup Wizard and carefully read the license agreement. Click **Next** to continue, if you accept the terms of the agreement.
4. In the **Installation Type** page, select **Client**. For Itanium clients, the type is selected automatically.
5. Enter the name of the Cell Manager. See "[Choosing the Cell Manager](#)".

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

Click **Next**.

**Figure 13: Choosing the Cell Manager**



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

Otherwise, click **Change** to open the Change Current Destination Folder page and enter the path.

7. Select the Data Protector components that you want to install.

For information on other Data Protector components, see ["Data Protector components"](#) .

Click **Next**.

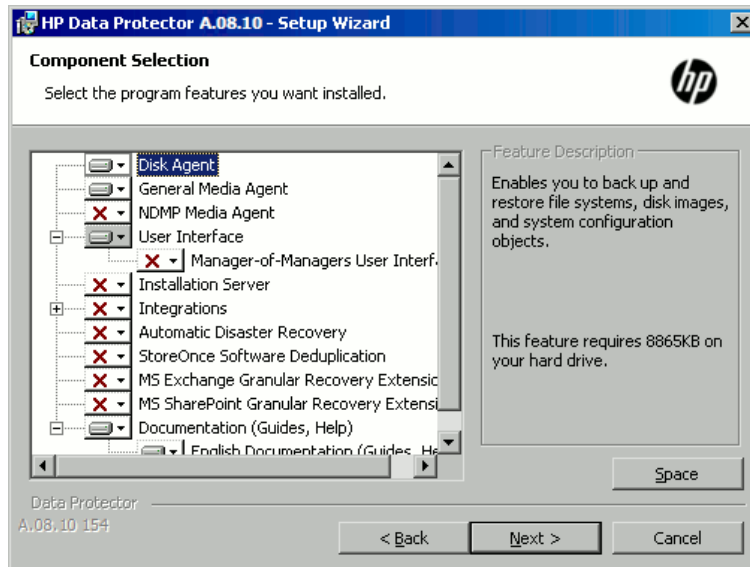
8. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports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

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

Click **Next**.

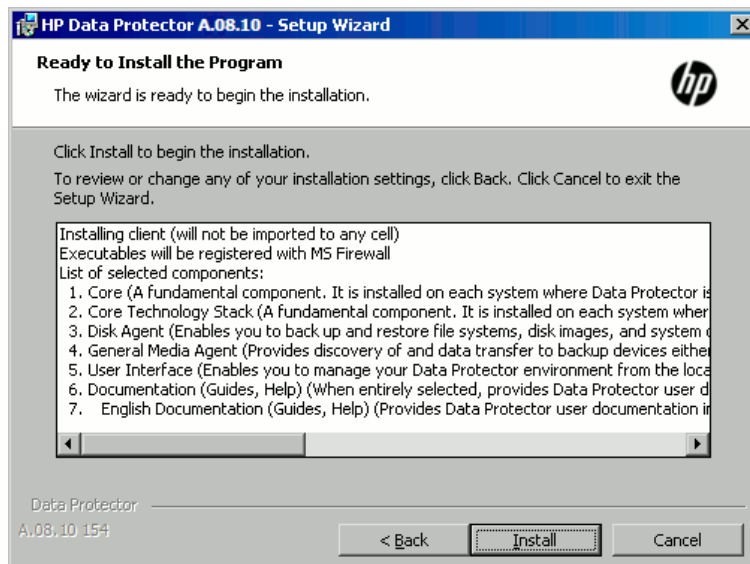
9. The component selection summary page is displayed. Click **Install** to install the selected components.

**Figure 14: Component selection summary page**



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

**Figure 15: Installation summary page**



11. If you have installed the User Interface component, to start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

If you have installed the English Documentation (Guides, Help) component, to view the *HP Data Protector Product Announcements, Software Notes, and References* immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

Click **Finish**.

## Connecting a backup device to Windows systems

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

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

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

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

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

- If the tape driver for your device is loaded:

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

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

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

- If the tape driver for your device is unloaded:

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

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

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

For loading or unloading the native tape driver for your device, see ["Using tape and robotics drivers on Windows systems"](#) .

For more information on creating a device filename, see ["Creating device files \(SCSI Addresses\) on Windows systems"](#) .

### *What's next?*

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

## **Installing HP-UX clients**

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

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

### *Prerequisites*

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX installed on your network. If not, for instructions see ["Installing the Data Protector Cell Manager and Installation Servers"](#) .
- You will need either *root* access or an account with *root* capabilities.
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.

### *Remote installation*

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

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

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

## Local installation

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

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

## Cluster-aware clients

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

## Checking the kernel configuration on HP-UX

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

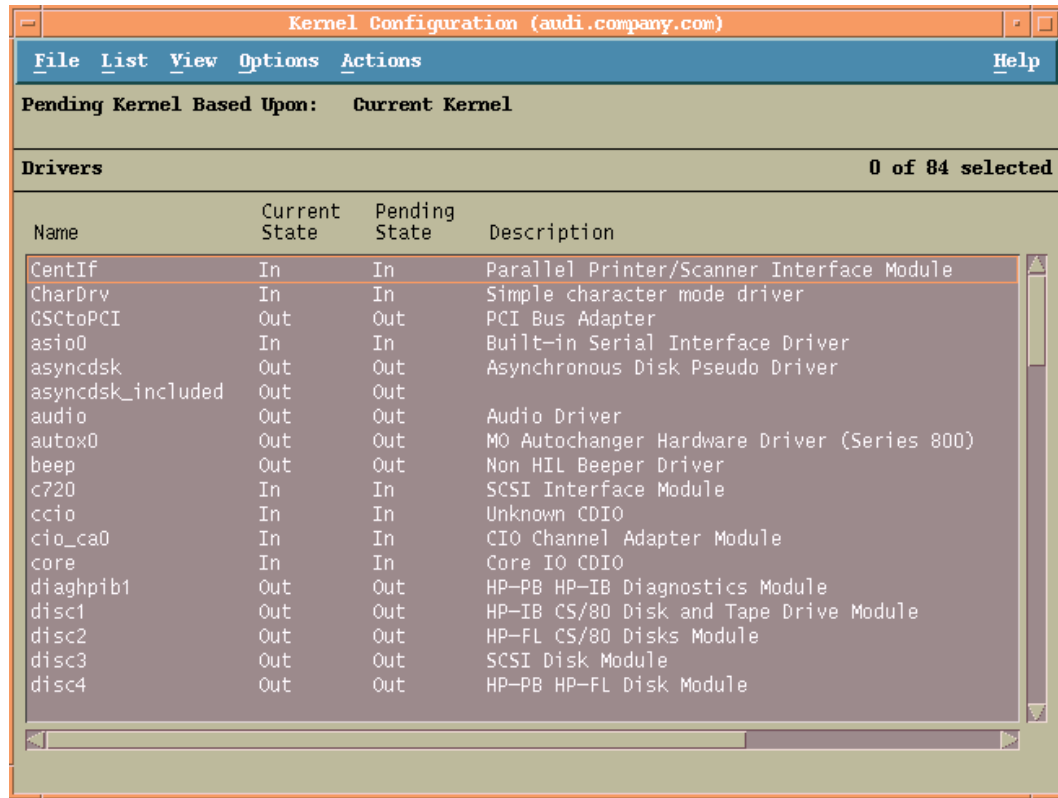
Follow this procedure to build the kernel configuration using the *HP System Administration Manager (SAM)* utility:

1. Log in as a root user, open the terminal and type `sam`.
2. In the **System Administration Manager** window, double-click **Kernel Configuration**, and then **Drivers**.
3. In the **Kernel Configuration** window, verify the following:
  - The drivers for the devices you will be using must be listed among the installed drivers. See ["Kernel configuration Window "](#) . If the driver you are looking for is not listed, you have to install it using the `/usr/sbin/swinstall` utility. For example:
    - A Tape Device Driver is required for tape devices and must be installed if you have connected a tape device to the system. For example, for generic SCSI tape drives, like DLT or LTO, the `stape` driver is used, and for DDS devices the `tape2` driver.
    - A SCSI Pass-Through driver named `sctl` or `spt`, or an autochanger robotics driver named `schgr` (depending on the hardware) is required to control robotics in Tape library devices.

For details, see ["SCSI robotics configuration on HP-UX systems"](#) .



**Figure 16: 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:
  - i. 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**.
  - ii. Click **Actions** and select **Create a New Kernel** to apply the changes, that is to build a **Pending Kernel** into the **Current Kernel**. The action requires a restart of the system.

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

## ***Connecting a backup device to HP-UX systems***

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

For more information, see ["Finding the unused SCSI addresses on HP-UX systems"](#).

2. Set the SCSI address on the device. Depending on the device type, this can be usually done with

switches on the device. For details, see the documentation that comes with the device.

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

3. Connect the device to the system, switch on the device, and then the computer, and wait until the boot process completes. The device files are usually created during the boot process.
4. Verify that the system correctly recognizes your new backup device. Use the `ioscan` utility:

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

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

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

## Installing Solaris clients

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

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

### Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network.  
For instructions, see "[Installing the Data Protector Cell Manager and Installation Servers](#)".
- To install a Solaris client, you will need either *root* access or an account with *root* capabilities.
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.

### Remote installation

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

**Note:** If you install the User Interface component, you should update your environment variables before using it. For more information, see "[Setting environment variables](#)".

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

**Important:** To install Data Protector to linked directories, for instance:

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

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

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

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

### *Local installation*

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

### *Cluster-aware clients*

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

## **Post-installation configuration**

### *Configuration files*

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

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

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

#### **Solaris (SPARC) systems:**

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

#### **Solaris (x86, x64) systems:**

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

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

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

```
tape-config-list =
```

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

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

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

```
tape-config-list =  
  
"HP      Ultrium 1-SCSI", "HP Ultrium 1-SCSI", "LTO-data",  
"HP      Ultrium 2-SCSI", "HP_LTO", "HP-LTO2",  
"DEC DLT2000", "Digital DLT2000", "DLT2k-data",  
"Quantum DLT4000", "Quantum DLT4000", "DLT4k-data",  
"QUANTUM DLT7000", "Quantum DLT7000", "DLT7k-data",  
"QUANTUM DLT8000", "Quantum DLT8000", "DLT8k-data",  
"HP C9264CB-VS80", "HP DLT vs80 DLTloader", "HP_data1"  
"QUANTUM SuperDLT1", "QUANTUM SuperDLT", "SDLT-data",  
"TANDBERGSuperDLT1", "TANDBERG SuperDLT", "SDL-data",  
"STK      9840", "STK 9840", "CLASS_9840";  
  
DLT2k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;  
DLT4k-data = 1,0x38,0,0x8639,4,0x17,0x18,0x80,0x81,3;  
DLT7k-data = 1,0x38,0,0x8639,4,0x82,0x83,0x84,0x85,3;  
DLT8k-data = 1,0x77,0,0x1D639,4,0x84,0x85,0x88,0x89,3;  
HP_data1 = 1,0x3a,0,0x8639,4,0x40,0x86,0x87,0x7f,0;  
LTO-data = 1,0x7a,0,0x1d679,4,0x00,0x00,0x00,0x40,3;  
HP-LTO2 = 1,0x7a,0,0xd639,4,0x00,0x00,0x00,0x42,3;  
SDLT-data = 1,0x79,0,0x8639,4,0x90,0x91,0x90,0x91,3;  
CLASS_9840 = 1,0x78,0,0x1d679,1,0x00,0;
```

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

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

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

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

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

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

**SCSI devices:**

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

**Fibre channel devices:**

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

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

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

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

- a. Copy the `sgen` module into the `/usr/kernel/drv/sparcv9` directory and the `sgen.conf` configuration file into the `/usr/kernel/drv` directory:

**32-bit Solaris systems:**

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

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

**64-bit Solaris systems:**

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

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

- b. 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.

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

**SCSI devices:**

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

**Fibre channel devices:**

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

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

- d. Install the driver on the system by entering the following command:

```
add_drv sgen
```

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

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

```
shutdown -i0
```

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

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

When you have finished, restart the system with:

```
ok boot -r
```

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

- i. Edit `/kernel/drv/st.conf` to set up the device parameters for using the assigned SCSI ports. For details, see the device documentation. Modify the `tape-config-list` parameter only if the tape device driver does not already support your device by default.
- ii. Edit `/kernel/drv/sgen.conf` to set up the device's drive parameters in order to use the assigned SCSI ports (refer to the appropriate device's documentation).
- iii. Edit `/usr/kernel/drv/sgen.conf` to set up the ADIC SCSI control device in order to use the assigned SCSI port 4. Add the following data for the ADIC SCSI Exchanger drive to the

/usr/kernel/drv/sst.conf file:

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

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

- a. Open the file /kernel/drv/sgen.conf.

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

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

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

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

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

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

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

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

```
shutdown -i0
```

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

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

When you have finished, restart the system with:

```
ok boot -r
```

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

- i. Edit /kernel/drv/st.conf to set up the device parameters for using the assigned SCSI ports. For details, see the device documentation. Modify the tape-config-list parameter only if the tape device driver does not already support your device by default.
- ii. Edit /kernel/drv/sgen.conf to set up the ADIC SCSI control device in order to use the assigned SCSI port 4. Add the following data for the ADIC SCSI Exchanger drive to the /kernel/drv/sgen.conf file:

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

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

## Connecting a backup device to a Solaris system

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

1. Create a reconfigure file:

```
touch /reconfigure
```

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

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

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

3. If your system is a Solaris (SPARC) system, switch the system back on and interrupt the startup process by pressing the Stop-A key.
4. Verify that the new device is recognized correctly by entering the `probe-scsi-all` command at the `ok` prompt:

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

Then, enter:

```
ok > go
```

to continue.

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

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

**When *sst* is used:**

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



**When sgen is used:**

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

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

```
echo "inq" | /opt/omni/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/0cbn` (not `/dev/rmt/0h`) for the tape drive and `/dev/rsst4` for the SCSI control device (picker).

### What's next?

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

## Installing Linux clients

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

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

### Prerequisites

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see "[Installing the Data Protector Cell Manager and Installation Servers](#)".
- The `rpm` utility must be installed and set up. Other packaging systems, for example, `deb`, are not supported.
- To install Data Protector components on a remote system, the following prerequisites must be met on the remote system:

- The `inetd` or `xinetd` service must be running or set up so that Data Protector is able to start it.
- Either the `ssh` or, if `ssh` is not installed, the `rexec` service must be enabled.
- Ensure that the kernel supports SCSI devices (modules `SCSI` support, `SCSI` tape support, `SCSI` generic support). The parameter `Probe all LUNa` on each `SCSI` device is optional.

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

- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.

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

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

### *Automatic disaster recovery*

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

### *HP Serviceguard cluster*

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

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

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

### *Novell Open Enterprise Server (OES)*

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

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

Note that the new Novell OES aware Disk Agent will be remotely installed to the client system during the upgrade.

- If you remove the Novell OES component from SLES, you have to reinstall the Data Protector client.

## Remote installation

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

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

## Troubleshooting remote installation

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

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

```
server_args = -h
```

For example:

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

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

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

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

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

It will enable administrative access from the Installation Server.

After you have installed Data Protector, you can remove the entry from the `-root/.rhosts` file, and the `-h` flag from the `/etc/xinetd.conf` (`/etc/inetd.conf` for Red Hat Enterprise Linux) file. Then repeat the `kill` command from the ["Terminate the inetd process with the HUP signal:"](#).

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

### *Local installation*

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

## ***Connecting a backup device to the Linux system***

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

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

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

3. Connect the device to the system, switch on the device, then switch on the computer, and wait until the boot process completes. The device files are created during the boot process.

On Red Hat Enterprise Linux systems, an application, Kudzu, is launched during the boot process when a new device is connected to the system. Press any key to start the application, and then click the Configure button.

4. To verify if the system correctly recognizes your new backup device, run `cat /proc/scsi/scsi` and then `dmesg |grep scsi`. The device files are listed for each connected backup device.

### ***Examples***

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

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

and for drives:

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

5. Device files are created in the `/dev` directory. To check if the links to the device files were created, execute:

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

For example:

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

The output of this command is:

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

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

### *What's next?*

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

## Installing ESX Server clients

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

## Installing Mac OS X clients

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

Only the Disk Agent (DA) is supported.

### *Prerequisites*

- For system requirements, disk space requirements, supported OS versions, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see ["Installing the Data Protector Cell Manager and Installation Servers"](#).
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.

### *Recommendation*

- If you increase the default block size, HP recommends to set the kernel parameter `kern.sysv.shmmax` (maximum size of a shared memory segment) to 32 MB.

### *Remote installation*

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

### *Local installation*

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

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

## **Installing IBM AIX clients**

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

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

### *Prerequisites*

- For system requirements, disk space requirements, supported platforms, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and Installation Server for UNIX already installed on your network. For instructions, see ["Installing the Data Protector Cell Manager and Installation Servers"](#).
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.
- Before installing the Disk Agent component, check that the port mapper is up and running on the selected system. In the `/etc/rc.tcpip` file, there must be the line that starts the port mapper:

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

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

### *IBM HACMP cluster*

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

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

### *Remote installation*

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

"Remote installation" .

### *Local installation*

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

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

## ***Connecting a backup device to an AIX client***

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

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

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

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

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

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

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

### *What's next?*

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

## **Installing HP OpenVMS clients**

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

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

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

For more OpenVMS specific information, see the *OpenVMS Release Notes* located in the default help document directory on OpenVMS, for example: `SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTES`.

## Prerequisites

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

- Make sure the HP TCP/IP transport protocol is installed and running.
- Set the TIMEZONE features of your system by executing the command `SYS$MANAGER:UTC$TIME_SETUP.COM`.
- Log in to the SYSTEM account of the OpenVMS system. Note that you must have appropriate permissions.
- Make sure that you have access to the Data Protector installation DVD-ROM or ISO image containing the HP OpenVMS client installation package.
- Reverse DNS lookup for host name resolution is required for all Data Protector components in the Data Protector cell.

## Installation

The installation procedure can be performed from the Data Protector Windows installation DVD-ROM or ISO image. 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 ["Run the following command:"](#) . To get the PCSI installation file, mount the installation DVD-ROM or ISO image on an OpenVMS Server and copy it to the desired location. You may also ftp the PCSI file from a Windows system.

2. Run the following command:

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

where *device:[directory]* is the location of the .PCSI installation file.

3. Verify the version of the kit by responding YES to the prompt:

```
The following product has been selected: HP AXPVMS DP A08.00-xx Layered Product Do  
you want to continue? [YES]
```

4. Choose the software components you wish to install. You may take the defaults and the Disk Agent, General Media Agent, and User Interface will be installed. You may also select each component individually.

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



### *Example*

```
HP IA64VMS DP A08.00-xx: HP OpenVMS IA64 Data Protector V8.00

COPYRIGHT HEWLETT-PACKARD COMPANY 2013

Do you want the defaults for all options? [YES] NO

Do you wish to install Disk Agent for this client node?

[YES] YES

Do you wish to install Media Agent for this client node?

[YES] YES

Do you wish to install Command Language Interface for this client node?

[YES] YES

Do you wish to install Oracle Integration Agent for this client node?

[YES] YES

Do you want to review the options?

[NO] YES

HP IA64VMS DP X08.00-xx: HP OpenVMS IA64 Data Protector V8.00 [Installed]

Do you wish to install Disk Agent for this client node?

YES

Do you wish to install Media Agent for this client node?

YES

Do you wish to install Command Language Interface for this client node?

YES

Do you wish to install Oracle Integration Agent for this client node?

[YES] YES

Are you satisfied with these options?

[YES] YES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0800
```

```
-XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
```

```
is not signed and therefore has no manifest file
```

To avoid the warning being issued, run the product install command using /OPTION=NOVALIDATE\_KIT.

### *Installation in a cluster environment*

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

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

### *Disk Agent configuration*

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

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

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

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

### *Example*

An OpenVMS file specification of:

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

must be specified to Data Protector in the form:

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

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

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

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

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

## *Media Agent configuration*

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

```
$ RUN SYS$SYSTEM:SYSMAN
```

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

where:

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

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

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

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

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

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

## *Media Agent in a cluster*

When dealing with devices attached to cluster systems:

1. Configure each tape device and tape library so that it can be accessed from each node.
2. Add the node name to the end of the device name to differentiate between the devices.

3. For tape devices, set a common Device Lock Name under Devices/Properties/Settings/Advanced/Other.

### Example

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

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

### Command-line interface

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

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

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

### Oracle integration

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

```
-key oracle8 -desc "Oracle Integration" -nlssset 159 -nlslId 12172 -flags 0x7 -ntpath  
"" -uxpath "" -version 8.10
```

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

### What's next?

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

## Remote installation

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

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

## Prerequisites

- For prerequisites and recommendations on the installation, see the section that describes the installation procedure for that particular client. The references are listed in " [Installing Data Protector client systems](#) " and in " [Installing integrations](#) " .
- For the information on supported platforms, Data Protector components, and for disk space requirements, see <http://support.openview.hp.com/selfsolve/manuals> and the *HP Data Protector Product Announcements, Software Notes, and References*.
- At this point, you should have the Cell Manager and the Installation Server(s) installed on your network.
- For a clean remote installation, the Installation Server for Windows must reside in a shared directory so that it is visible throughout the network.
- **Windows 2012:** To remotely install to a Windows 2012 system, complete one of the following steps:

Configure the domain user who is also the administrator of the remote host (`omniinetpasswd -inst_srv_user`) on the **Installation Server host**. Remote installation is started under this account and the connection to the remote host is established without any additional user intervention.

OR

Block the following services within firewall on the **remote host**.

- Remote Service Management (RPC)
- Remote Service Management (RPC-EPMAP)

OR

Switch off the RPC/TCP (client side) on the **Installation Server host**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
```

```
DWORD SCMApiConnectionParam = 0x80000000
```

Combine the SCMApiConnectionParam registry value with the mask value 0x80000000.

**Note:** A system restart is not required.

## Recommendations

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

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

**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.

- **Administrator Accounts:** To use local users who are members of the Administrators group on the remote host, where the remote host has UAC enabled, complete either of the following steps on the remote host:

#### Disable User Account Control (UAC)

**Note:** A system restart is required.

OR

#### Set the registry value:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

DWORD LocalAccountTokenFilterPolicy = 1

**Note:** A system restart is not required.

## Remote installation using secure shell

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

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

**Note:** Secure shell installation is supported on UNIX systems only.

### Setting up OpenSSH

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

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

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

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

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

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

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

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

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

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

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

```
ssh_install_directory /ssh/etc/ssh_config
```

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

- b. **On the client:**

```
ssh_install_directory /ssh/etc/sshd_config
```

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

Note that these two files must be in sync.

**Note:** The default SSH protocol version is SSH2.

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

```
ssh_install_directory /ssh/sbin/sshd
```

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

```
ssh root@client_host
```

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

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

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



## Setting up a keychain

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

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

### **HP-UX and Solaris systems:**

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

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

### **Linux systems:**

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

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

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

## What's next?

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

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

## Adding clients to the cell

### Adding clients to the cell

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

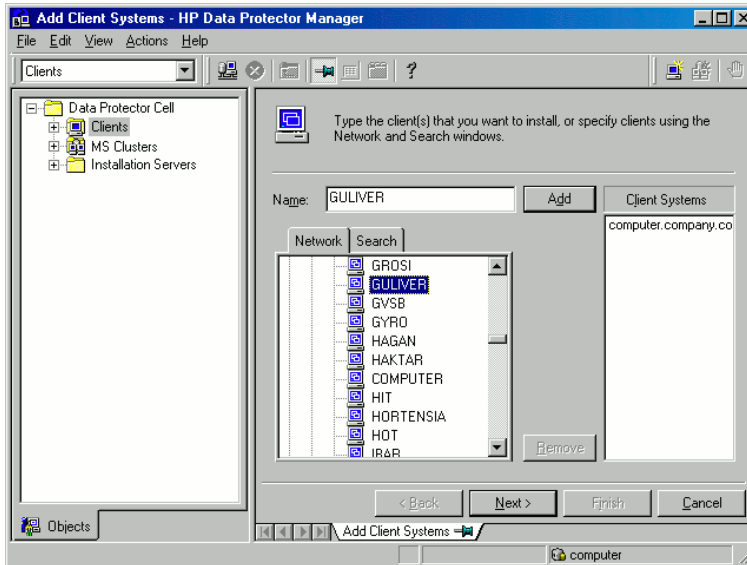
1. Start the Data Protector GUI by clicking **Start > Programs > HP Data Protector > Data Protector Manager**.

For details on the Data Protector graphical user interface, see "[The Data Protector graphical user interface](#)" and the *HP Data Protector Help*.

2. In the Data Protector Manager, switch to the **Clients** context.

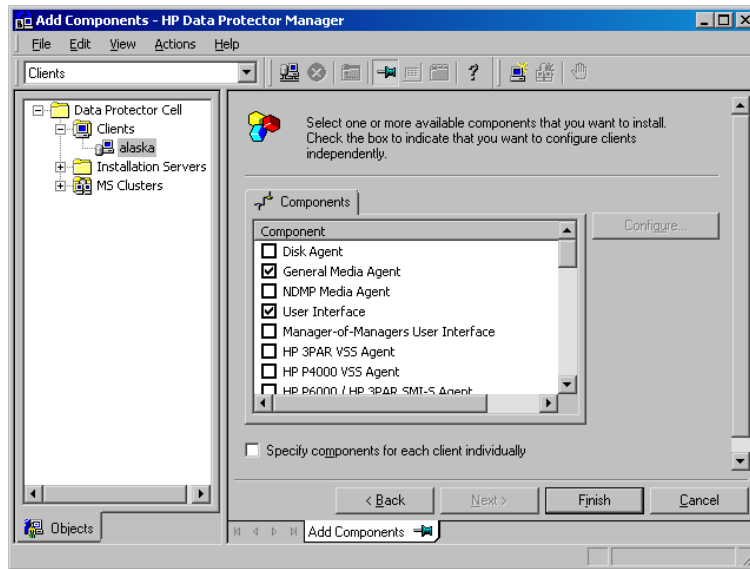
3. In the Scoping Pane, right-click **Clients** and click **Add Clients**.
4. If you have more than one Installation Server configured, select the platform of the clients you want to install (UNIX or Windows) and the Installation Server to be used for installing the clients. Click **Next**.
5. Type the names of the clients or search for the clients (on Windows GUI only) you want to install as shown in " [Selecting clients](#) ". Click **Next**.

**Figure 17: Selecting clients**



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

**Figure 18: Selecting components**



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

If you selected more than one client and you would like to install different components on each client, click **Specify components for each client individually** and then click **Next**. Select the components you want to install for each client independently.

Click **Finish** to start the installation.

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

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

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

## **Troubleshooting**

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

## **Adding components to clients**

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

## HP Serviceguard clients

In the HP Serviceguard cluster environment, make sure that the node to which you add the components is active.

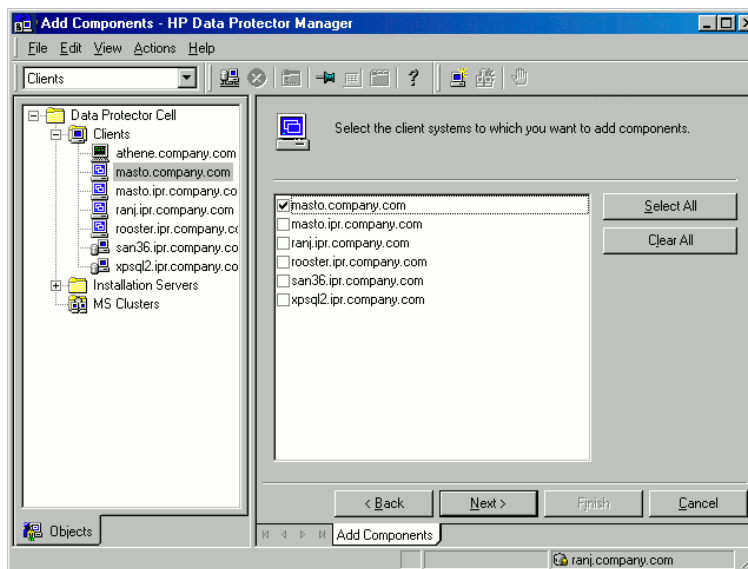
### Prerequisite

The corresponding Installation Server must be available.

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

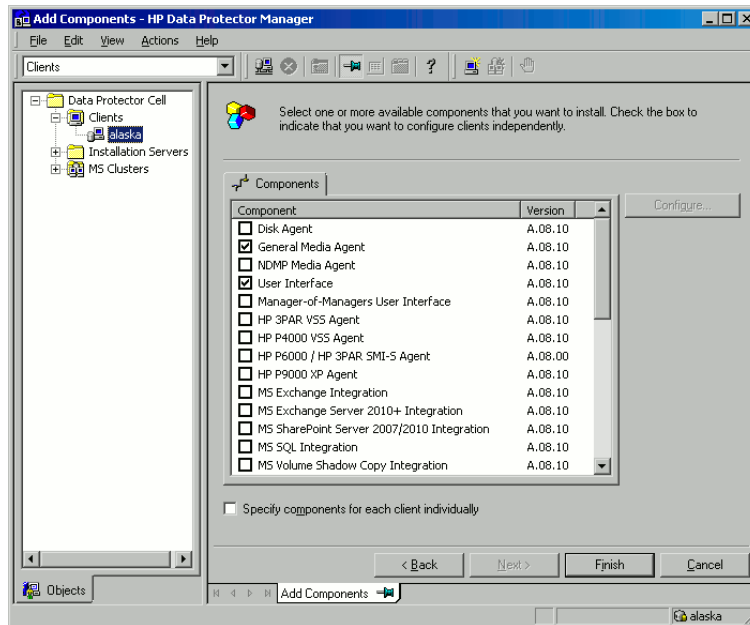
1. In the Data Protector Manager, switch to the **Clients** context.
2. In the Scoping Pane, expand Clients, right-click a client, and then click **Add Components**.
3. If you have more than one Installation Server configured, select the platform of the clients on which you want to install the components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

Figure 19: Selecting clients



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

**Figure 20: Selecting components**



If you selected more than one client and you want to install different components on each client, click **Specify components for each client individually** and then click **Next**. Select the components for each client independently.

Click **Finish** to start the installation.

## Local installation on UNIX and Mac OS X systems

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

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

### Prerequisites

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

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

## Procedure

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

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

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

2. From the *MountPoint*/LOCAL\_INSTALL directory execute the `omnisetup.sh` command.

The syntax of the command is as follows:

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

where:

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

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

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

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

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

**Table 5: Data Protector component codes**

Component code	Component
cc	User Interface
da	Disk Agent
ma	General Media Agent

Component code	Component
ndmp	NDMP Media Agent
informix	Informix Integration
lotus	Lotus Integration
oracle8	Oracle Integration
vmware	VMware Integration (Legacy)
vepa	Virtual Environment Integration
sybase	Sybase Integration
sap	SAP R/3 Integration
sapdb	SAP MaxDB Integration
saphana	SA HANA Integration
db2	DB2 Integration
emc	EMC Symmetrix Agent
smisa	HP P6000 / HP 3PAR SMI-S Agent
ssea	HPP9000 XP Agent
StoreOnceSoftware	StoreOnce Software Deduplication
autodr	Automatic Disaster Recovery
docs	English Documentation (Guides, Help)

### Example

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

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

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

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

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

### *Running the installation from the hard disk*

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

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

For example, if you copy installation packages to `/var/dp80`, the directories must be a subdirectory of `/var/dp62`:

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

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

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

For example:

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

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

### *What's next?*

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

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

Data Protector provides a dedicated ADIC/GRAU and StorageTek ACS library policies used to configure an ADIC/GRAU library or StorageTek ACS library as a Data Protector backup device. You need to install a Data Protector Media Agent (the General Media Agent or the NDMP Media Agent) on every system that will be physically connected to a drive in an ADIC/GRAU or StorageTek library. Also, for multihost configurations, you must install a Data Protector Media Agent on the systems that control the



ADIC/GRAU or StorageTek library robotics. Note that multihost configuration is a configuration where the library and drive are not connected to the same computer.

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

**Note:** You need special licenses that depend on the number of drives and slots used in the StorageTek library. For more information, see "[Data Protector Licensing](#)".

## Connecting library drives

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

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

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

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

## Preparing Data Protector clients to use the ADIC/GRAU Library

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

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

Each DAS client is identified with a unique client name (no spaces), for example DP\_C1. For example, the contents of the C:\DAS\ETC\CONFIG file should look like this:

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

2. On each Data Protector client with a Data Protector Media Agent installed that needs to access ADIC/GRAU DAS library robotics, edit the `omnirc` file and set the following options:

DAS_ CLIENT	A unique GRAU client name defined on the DAS server. For example, if the name of the client is "DP_C1", the appropriate line in the <code>omnirc</code> file is <code>DAS_CLIENT=DP_C1</code> .
DAS_ SERVER	The name of the DAS server.

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

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

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

```
OB2_ACIEJECTTOTAL = 0
```

**Note:** This applies to HP-UX and Windows.

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

## ***Installing a Media Agent to use the ADIC/GRAU Library***

### ***Prerequisites***

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

- The ADIC/GRAU library must be configured and running. See the documentation that comes with the ADIC/GRAU library.
- Data Protector must be installed and configured. See ["Installing the Data Protector Cell Manager and Installation Servers"](#).
- DAS server must be up and running.

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

- The following information must be obtained before you install a Media Agent:

- The hostname of the DAS Server (an application that runs on an OS/2 host).
- The list of available drives with the corresponding DAS name of the drive. The obtained drive names are to be used when configuring the ADIC/GRAU drives in Data Protector.

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

```
dasadmin listd2 client
```

```
dasadmin listd client
```

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

The `dasadmin` command can be called from the `C:\DAS\BIN` directory on the OS/2 host, or, if installed on other systems, from the directory where the DAS client software has been installed. On a UNIX client system, this directory is usually the `/usr/local/aci/bin` system directory.

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

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

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

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

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

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

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

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

For more information on SCSI addresses, see ["Connecting a backup device to Windows systems"](#).

## Installation

The installation procedure consists of the following steps:

1. Distribute a Media Agent component to clients, using the Data Protector graphical user interface and Installation Server. See ["Remote installation"](#) .
2. Install the ADIC/GRAU library:
  - On a Windows system, do the following:
    - i. 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.)
    - ii. Copy these three files to the `%SystemRoot%\system32` directory as well.
    - iii. 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.)
    - iv. In the Control Panel, go to `Administrative Tools`, `Services` and start `portinst` to install `portmapper`. The DAS client needs to be restarted to run the `portmapper` service.
    - v. After restarting the system, check if `portmapper` and both `rpc` services are running (in the Control Panel, go to **Administrative Tools**, **Services** and check the status of the services.
  - On an HP-UX system, copy the `libaci.sl` shared library into the `/opt/omni/lib` directory. You must have permissions to access this directory. Make sure that the shared library has read and execute permissions for everyone (root, group and others). The `libaci.sl` shared library is part of the DAS client software shipped with the ADIC/GRAU library. It can be found on the installation media.
  - On an AIX system, copy the `libaci.o` shared library into the `/usr/omni/lib` directory. You must have permissions to access this directory. Make sure that the shared library has read and execute permissions for everyone (root, group and others). The `libaci.o` shared library is part of the DAS client software shipped with the ADIC/GRAU library. It can be found on the installation media.

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

From the default Data Protector administrative commands location, execute the `devbra -dev` command to check whether the library drives are properly connected to your system.

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

### *What's next?*

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

## ***Preparing Data Protector clients to use the StorageTek Library***

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

- The StorageTek library must be configured and running. See the documentation that comes with the StorageTek library.
- Data Protector must be installed and configured. See ["Installing the Data Protector Cell Manager and Installation Servers"](#) .
- The following information must be obtained before you start installing a Media Agent software:
  - The *hostname* of the host where ACSLS is running.

- A list of ACS drive IDs that you want to use with Data Protector. The obtained drive IDs are to be used when configuring the StorageTek drives in Data Protector. To display the list, log in on the host where ACSLS is running and execute the following command:

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

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

```
ACSSA> query drive all
```

The format specification of an ACS drive must be the following:

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

- A list of available ACS CAP IDs and the ACS CAP format specification. To display the list, login on the host where ACSLS is running and execute the following command:

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

Enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

```
ACSSA> query cap all
```

The format specification of an ACS CAP must be the following:

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

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

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

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

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

For more information on SCSI addresses, see ["Connecting a backup device to Windows systems"](#) .

- Make sure that the drives that will be used for Data Protector are in the `online` state. If a drive is not in the `online` state, change the state with the following command on the ACSLS host: `vary drive drive_id online`
- Make sure that the CAPs that will be used for Data Protector are in the state `online` and in `manual` operating mode.

If a CAP is not in the `online` state, change the state using the following command:

```
vary cap cap_id online
```

If a CAP is not in `manual` operating mode, change the mode using the following command:

```
set cap manual cap_id
```

## ***Installing a Media Agent to use the StorageTek Library***

The installation procedure consists of the following steps:

1. Distribute a Media Agent component to clients using the Data Protector graphical user interface and Installation Server for UNIX systems. See ["Remote installation"](#) .
2. Start the ACS `ssi` daemon for every ACS client:

### **Windows systems:**

Install the `LibAttach` service. For details, see the ACS documentation. Make sure that during the configuration of `LibAttach` service the appropriate ACSLS hostname is entered. After successful configuration, the `LibAttach` services are started automatically and will be started automatically after every system restart as well.

### **HP-UX, Solaris, and Linux systems:**

Run the following command:

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

### **AIX systems:**

Run the following command:

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

**Note:** After you have installed the `LibAttach` service, check if the `libattach\bin` directory has been added to the system path automatically. If not, add it manually.

For more information on the `LibAttach` service, see the documentation that comes with the StorageTek library.

3. From the default Data Protector administrative commands location, execute the `devbra -dev`

command to check whether or not the library drives are properly connected to your system.

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

### *What's next?*

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

## Installing the Data Protector integration clients

Data Protector integrations are software components that allow you to run an online backup of the database applications, such as Oracle Server or Microsoft Exchange Server, with Data Protector. Data Protector ZDB integrations are software components that allow you to run zero downtime backup and instant recovery using disk arrays, such as HP P6000 EVA Disk Array Family.

The systems running database applications are called **integration clients**; the systems using ZDB disk arrays for backing up and storing data are called **ZDB integration clients**. Such clients are installed with the same installation procedure as any other clients on Windows or UNIX systems, provided that the appropriate software component has been selected (for example, MS Exchange Integration component for backing up the Microsoft Exchange Server database, HP P6000 / HP 3PAR SMI-S Agent component for ZDB and IR with HP P6000 EVA Disk Array Family or HP StoreServ Storage, and so on).

### *Prerequisites*

- For system requirements, disk space requirements, supported platforms, processors, and Data Protector components, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- You need a license to use the Data Protector integration with a database application (except for the VSS integration). For information about licensing, see "[Data Protector 8.10 product structure and licenses](#)".
- At this point, you should have the Cell Manager and Installation Server (optionally, for remote installation) already installed on your network. For instructions, see "[Installing the Data Protector Cell Manager and Installation Servers](#)".

Before starting the installation procedure, decide which other Data Protector software components you want to install on your client together with an integration component. For the list of the Data Protector software components and their descriptions, see "[Data Protector components](#)".

Note that in the cases stated below you need to install the following Data Protector components:

- The **Disk Agent** component to be able to back up filesystem data with Data Protector. You can use the Disk Agent for the following purposes:
  - To run a filesystem backup of important data that *cannot* be backed up using a database application backup.

- To run a filesystem test backup of a database application server (for example, Oracle Server or Microsoft SQL Server). You need to test a filesystem backup *before* configuring the Data Protector integration with a database application and resolve communication and other problems related to the application and Data Protector.
- To run zero downtime backup of filesystems or disk images.
- To restore from backup media to the application system on LAN in case of SAP R/3 ZDB integrations.
- The `User Interface` component to gain access to the Data Protector GUI and the Data Protector CLI on the Data Protector integration client.
- The `General Media Agent` component if you have backup devices connected to the Data Protector integration client. On Data Protector clients used to access an NDMP dedicated drive through the NDMP Server, the `NDMP Media Agent` is required.

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

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

- ["Microsoft Exchange Server clients"](#)
- ["Microsoft SQL Server clients"](#)
- ["Microsoft SharePoint Server clients"](#)
- ["Microsoft Volume Shadow Copy Service clients"](#)
- ["Sybase Server clients"](#)
- ["Informix Server clients"](#)
- ["SAP R/3 clients"](#)
- ["SAP MaxDB clients"](#)
- ["SAP HANA Appliance clients"](#)
- ["Oracle Server clients"](#)
- ["IBM DB2 UDB clients"](#)
- ["Lotus Notes/Domino Server clients"](#)
- ["VMware clients"](#)
- ["Microsoft Hyper-V clients"](#)
- ["NDMP Server clients"](#)



- ["HP P4000 SAN Solutions clients"](#)
- ["HP P6000 EVA Disk Array Family clients"](#)
- ["HP P9000 XP Disk Array Family clients"](#)
- ["HP 3PAR StoreServ Storage clients"](#)
- ["EMC Symmetrix clients"](#)

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

After the installation, also see the *HP Data Protector Integration Guide*, the *HP Data Protector Zero Downtime Backup Administrator's Guide*, or the *HP Data Protector Zero Downtime Backup Integration Guide* to configure Data Protector integration clients.

## Remote installation

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

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

## Local installation

If you do not have an Installation Server for the respective operating system installed in your environment, you have to perform local installation from the Windows, or from the UNIX installation DVD-ROM or ISO image (for HP-UX or Linux), depending on the platform you install a client to.

If you do not choose a Cell Manager during the installation, the client system has to be manually imported into the cell after the local installation. See ["Importing clients to a cell"](#).

## Installing cluster-aware integrations

The Data Protector cluster-aware integration clients must be installed locally, from the DVD-ROM or ISO image, on each cluster node. During the local client setup, install, in addition to the other client software components, the appropriate integration software components (such as Oracle Integration or HP P6000 / HP 3PAR SMI-S Agent).

You can also install a cluster-aware database application and a ZDB Agent on the Data Protector Cell Manager. Select the appropriate integration software component during the Cell Manager setup.

The installation procedure depends on a cluster environment where you install your integration client. See the clustering related sections corresponding to your operating system:

- ["Installing Data Protector on an HP Serviceguard"](#)
- ["Installing Data Protector on a Microsoft Cluster Server"](#)
- ["Installing Data Protector on a Microsoft Hyper-V cluster"](#)
- ["Installing Data Protector clients on a Veritas Cluster"](#)
- ["Installing Data Protector on an IBM HACMP Cluster"](#)

For more information on clustering, see the *HP Data Protector Help* index: "cluster, HP Serviceguard" and the *HP Data Protector Concepts Guide*.

### *What's next?*

When the installation has been completed, see the *HP Data Protector Integration Guide* for information on configuring the integration.

## **Microsoft Exchange Server clients**

Data Protector components that need to be installed on Microsoft Exchange Server systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- ["Data Protector Microsoft Exchange Server 2007 integration"](#)
- ["Data Protector Microsoft Exchange Server 2010 integration"](#)
- ["Data Protector Microsoft Exchange Server Single Mailbox integration"](#)
- ["Data Protector Microsoft Volume Shadow Copy Service integration"](#)
- ["Data Protector Granular Recovery Extension for Microsoft Exchange Server"](#)

### ***Data Protector Microsoft Exchange Server 2007 integration***

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

To be able to back up the Microsoft Exchange Server databases, install the *MS Exchange Integration* component to the Microsoft Exchange Server system.

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

### ***Data Protector Microsoft Exchange Server 2010 integration***

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

To be able to back up the Microsoft Exchange Server 2010 or the Microsoft Exchange Server 2013 databases, install the following Data Protector components to all the Microsoft Exchange Server systems:

- MS Exchange Server 2010+ Integration
- MS Volume Shadow Copy Integration
- The appropriate Data Protector disk array agent (if Microsoft Exchange Server data resides on a disk array)

**Note:** For VSS transportable backup sessions, the MS Volume Shadow Copy Integration component and the appropriate Data Protector disk array agent must also be installed on the backup systems.

In DAG environments, the DAG virtual system (host) must also be imported to the Data Protector cell. On how to import a client to a Data Protector Cell, see the *HP Data Protector Help* index: "importing, client systems".

- Because the Data Protector Microsoft Exchange Server 2010 integration is based on VSS technology, Data Protector automatically installs the MS Volume Shadow Copy Integration component when you install the MS Exchange Server 2010+ Integration component. If the MS Volume Shadow Copy Integration component is already installed, it is upgraded.
- If you remove the MS Exchange Server 2010+ Integration component from a system, the MS Volume Shadow Copy Integration component is not removed automatically. Also note that you cannot remove the MS Volume Shadow Copy Integration component from a system where the MS Exchange Server 2010+ Integration component is installed.

## ***Data Protector Microsoft Exchange Server Single Mailbox integration***

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

To be able to back up the Microsoft Exchange Server Mailbox and Public Folder items, install the MS Exchange Integration component on the Microsoft Exchange Server system. In a DAG environment, install the component on all Microsoft Exchange Server systems that are part of a DAG.

On Microsoft Exchange Server 2007 systems, you need to install an additional package to enable the functionality of the Data Protector Microsoft Exchange Single Mailbox integration. The package is named Microsoft Exchange Server MAPI Client and Collaboration Data Objects (ExchangeMapiCdo.EXE), and can be downloaded free of charge from the Microsoft web site <http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en>.

## ***Data Protector Microsoft Volume Shadow Copy Service integration***

See "[Microsoft Volume Shadow Copy Service clients](#)".

## ***Data Protector Granular Recovery Extension for Microsoft Exchange Server***

Use the Data Protector extension to be able to recover individual Microsoft Exchange Server mailbox items. Depending on the configuration of your Microsoft Exchange Server environment, install the corresponding Data Protector component on:

- single Microsoft Exchange Server system: this system
- multiple Microsoft Exchange Server systems: each Exchange Server system on which the Mailbox Server role is configured
- Microsoft Exchange Server Database Availability Group (DAG) environment: any of the Exchange Server systems in DAG

### ***Prerequisites***

- Install the following to the chosen Microsoft Exchange Server system:
  - The Data Protector MS Exchange Server 2010+ Integration component
  - The Data Protector User Interface component
  - All required non-Data Protector components

For details, see the installation chapter in the *HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server*.

- Keep the TCP/IP port 60000 (default) free on the chosen Microsoft Exchange Server system.

For instructions on how to locally or remotely install the Data Protector MS Exchange Granular Recovery Extension component, see the *HP Data Protector Help* index: “installing, client systems”.

## **Microsoft SQL Server clients**

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

To be able to back up the Microsoft SQL Server database, you need to select the MS SQL Integration component during the installation procedure.

## **Microsoft SharePoint Server clients**

Data Protector components that need to be installed in a Microsoft SharePoint Server environment vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- ["Data Protector Microsoft SharePoint Server 2007/2010/2013 integration"](#)
- ["Data Protector Microsoft SharePoint Server VSS based solution"](#)
- ["Data Protector Microsoft Volume Shadow Copy Service integration"](#)
- ["Data Protector Granular Recovery Extension for Microsoft SharePoint Server"](#)

## ***Data Protector Microsoft SharePoint Server 2007/2010/2013 integration***

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to back up Microsoft SharePoint Server objects, install the following Data Protector components:

- MS SharePoint 2007/2010/2013 Integration – on Microsoft SharePoint Server systems (Microsoft SQL Server systems are excluded)
- MS SQL Integration – on Microsoft SQL Server systems

**Note:** If a system has both the Microsoft SQL Server and Microsoft SharePoint Server installed, install both Data Protector components on it.

## ***Data Protector Microsoft SharePoint Server VSS based solution***

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to back up Microsoft SharePoint Server objects, install the following Data Protector components:

- MS Volume Shadow Copy Integration on the Microsoft SQL Server systems and the Microsoft SharePoint Server systems that have at least one of the following services enabled:

### ***Microsoft Office SharePoint Server 2007:***

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

### ***Microsoft SharePoint Server 2010:***

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

**Microsoft SharePoint Server 2013:**

- SharePoint Foundation Database
- SharePoint Server Search
- The Data Protector User Interface component on one of the Microsoft SharePoint Server systems with the Data Protector MS Volume Shadow Copy Integration component installed and on which you plan to configure and start a backup.

## ***Data Protector Microsoft Volume Shadow Copy Service integration***

See "[Microsoft Volume Shadow Copy Service clients](#)".

## ***Data Protector Granular Recovery Extension for Microsoft SharePoint Server***

It is assumed that your Microsoft SharePoint Server and related Microsoft SQL Server instances are up and running.

To be able to recover individual Microsoft SharePoint Server objects, install the MS SharePoint Granular Recovery Extension on the Microsoft SharePoint Server Central Administration system.

- When installing the component locally, the Data Protector installation wizard will display the MS SharePoint GRE options dialog box. Specify the Farm Administrator user name and password.
- To install this component remotely, select the MS SharePoint Granular Recovery Extension, click **Configure** and specify the Farm Administrator user name and password in the MS SharePoint GRE options dialog box.

- You can install the Granular Recovery Extension only to systems with Microsoft SharePoint Server installed.
- Ensure that the Data Protector components that are needed to back up Microsoft SharePoint Server data are also installed in the Microsoft SharePoint Server environment.

## **Microsoft Volume Shadow Copy Service clients**

To back up VSS writers or only the filesystem using VSS, install the following Data Protector software components on the application system (local backup) or on both the application and backup system (transportable backup):

- MS Volume Shadow Copy Integration.
- If you are using a disk array (with hardware providers) the appropriate disk array agent: HP P4000 Agent, HP P6000 / HP 3PAR SMI-S Agent, HP P9000 XP Agent, or HP 3PAR VSS Agent.

After you have installed the VSS integration, you need to resolve the source volumes on the application system if you will perform the ZDB-to-disk and ZDB-to-disk+tape sessions (instant recovery-enabled sessions). Run the resolve operation from any VSS client in the cell as follows:

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

However, if you do not resolve or fail to resolve the application system, it will be resolved automatically, as long as the OB2VSS\_DISABLE\_AUTO\_RESOLVE option in the `omnirc` file is set to 0 (default). In this case, the backup time for creating a replica is prolonged.

For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

## Sybase Server clients

It is assumed that your Sybase Backup Server is running.

For backing up the Sybase database, you need to select the following Data Protector component during the installation procedure:

- Sybase Integration - to be able to back up a Sybase database
- Disk Agent - install the Disk Agent for two reasons:
  - To run a filesystem backup of Sybase Backup Server. Make this backup *before* configuring your Data Protector Sybase integration and resolve all problems related to Sybase Backup Server and Data Protector.
  - To run a filesystem backup of important data that *cannot* be backed up using Sybase Backup Server.

## Informix Server clients

It is assumed that your Informix Server is up and running.

For backing up the Informix Server database, you need to select the following Data Protector component during the installation procedure:

- Informix Integration - to be able to back up an Informix Server database
- Disk Agent - install the Disk Agent for two reasons:
  - To run a filesystem backup of Informix Server. Make this backup *before* configuring your Data Protector Informix Server integration and resolve all problems related to Informix Server and Data Protector.
  - To run a filesystem backup of important Informix Server data (such as, ONCONFIG file, sqlhosts

file, ON-Bar emergency boot file, `oncfg_INFORMIXSERVER.SERVERNUM`, configuration files, and so on) that *cannot* be backed up using ON-Bar.

## IBM HACMP Cluster

If Informix Server is installed in the IBM HACMP cluster environment, install the Informix Integration component on all the cluster nodes.

## SAP R/3 clients

### Prerequisites

- Ensure that the following Oracle software is installed and configured:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 software
  - SQL\*Plus
- It is assumed that your SAP R/3 Database Server is up and running.

**Note:** The Data Protector SAP R/3 integration backup specifications are fully compatible with the previous version of Data Protector. Data Protector will run all backup specifications created by earlier Data Protector versions. You cannot use backup specifications created by the current version of Data Protector on older versions of Data Protector.

To be able to back up the SAP R/3 database, select the following components during the installation procedure:

- SAP R/3 Integration
- Disk Agent

Data Protector requires a Disk Agent to be installed on Backup Servers (clients with filesystem data to be backed up).

## SAP MaxDB clients

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

To be able to back up the SAP MaxDB database, you need to select the following Data Protector components during the installation procedure:

- SAP MaxDB Integration - to be able to run an integrated online backup of an SAP MaxDB database
- Disk Agent - to be able to run a filesystem backup of an SAP MaxDB database



## SAP HANA Appliance clients

To integrate Data Protector with your SAP HANA Appliance (SAP HANA), install the following Data Protector software components on the SAP HANA system:

- SAP HANA Integration

This component enables integrated backup of a complete SAP HANA database and the SAP HANA redo logs.

- Disk Agent

This component enables non-integrated backup of the SAP HANA configuration files using the Data Protector filesystem backup functionality. After a disaster, having a backup image of the SAP HANA configuration files available helps you more easily identify and restore your changes.

In case of a distributed SAP HANA environment, install the above components on each SAP HANA system that constitutes such environment.

## Oracle Server clients

It is assumed that your Oracle Server is up and running.

To be able to back up the Oracle database, you need to select the `Oracle Integration` component during the installation procedure.

### HP OpenVMS

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

```
-key oracle8 -desc "Oracle Integration" -nlssset 159 -nlslid 12172 -flags 0x7 -ntpath  
"" -uxpath "" -version 8.10
```

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

## IBM DB2 UDB clients

It is assumed that your DB2 Server is up and running.

To be able to back up the DB2 database, you need to select the `DB2 Integration` and the `Disk Agent` components during the installation procedure.

In a physically partitioned environment, install the `DB2 Integration` and `Disk Agent` components on every physical node (system) on which the database resides.

**Note:** Log in as user `root` to perform the installation.

## Lotus Notes/Domino Server clients

It is assumed that your Lotus Notes/Domino Server is up and running.

To be able to back up the Lotus Notes/Domino Server database, you need to select the `Lotus Integration` and the `Disk Agent` components during the installation procedure. You will need the `Disk Agent` component to be able to back up filesystem data with Data Protector in the following purposes:

- Backing up important data that *cannot* be backed up using Lotus Integration Agent. These are so called non-database files, which need to be backed up to provide a complete data protection solution for a Lotus Notes/Domino Server, such as `notes.ini`, `desktop.dsk`, all `*.id` files.
- Testing the filesystem backup to resolve communication and other problems related to the application and Data Protector.

## Lotus Domino Cluster

Install the `Lotus Integration` and the `Disk Agent` components on the Domino servers that will be used for backup, and, if you plan to restore Domino databases to other Domino servers containing replicas of these databases, install the components on these Domino servers as well.

## VMware clients

Data Protector components that need to be installed on VMware systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- ["Data Protector Virtual Environment integration"](#)
- ["Installing the Data Protector integration clients"](#)
- ["Data Protector Granular Recovery Extension for VMware vSphere"](#)

## Data Protector Virtual Environment integration

It is assumed that all systems on which you intend to install components are up and running.

On systems that should control backup and restore sessions (**backup hosts**), install the following Data Protector components:

- Virtual Environment Integration
- Disk Agent

**Note:**

- The `Disk Agent` component enables you to use the **Browse** button when restoring to a directory on the backup host. If the component is not installed, you must type the target directory yourself.
- The client that you intend to use as a backup host should *not* have the VMware Consolidated

Backup (VCB) software installed.

## ***Data Protector Granular Recovery Extension for VMware vSphere***

It is assumed that the Data Protector Virtual Environment integration is installed and configured as described in the *HP Data Protector Integration Guide for Virtualization Environments*. The virtual machines you plan to restore data to must have VMware tools 4.x or later installed.

### ***Limitations***

- Only remote installation of the Data Protector Granular Recovery Extension for VMware vSphere is supported.

### ***Installation procedure***

#### ***Mount proxy system:***

Remotely install the following Data Protector components to the mount proxy system:

- Virtual Environment Integration
- VMware Granular Recovery Extension Agent

For installation instructions, see the *HP Data Protector Help* index: “installing, client systems”.

**Note:** During the installation of the VMware Granular Recovery Extension Agent component on the mount proxy system, the user will be notified in the installation session output when the reboot of the target host must be performed to complete the installation.

#### ***vCenter Server (VirtualCenter Server):***

1. If no Data Protector component is installed on the vCenter Server, remotely install the Data Protector Disk Agent component to this system.
2. Import the vCenter Server to the Data Protector cell as a Data Protector client. For details, see the *HP Data Protector Help* index: “importing, client systems”.

Follow the steps:

- a. In the Import Client wizard, in the Type drop-down list, select **VMware vCenter**.
- b. In the Import Client wizard, specify the login credentials:
  - **Port** : Specify the port that VMware vSphere is using. By default, VMware vSphere uses the port 443.
  - **User name** and **Password**: Specify an operating system user account that has the following

VMware vSphere privileges:

**Web service root**

Optionally, change the web service entry point URI. Default: /sdk.

3. Follow the steps:

**vCenter Server 5.1:**

- To perform installation by using the automatic deployment feature of VMware Web Server:
  - i. In the VMware Web Server folder `installation_directory` (default path: `C:\Program Files\VMware\Infrastructure\tomcat`), in the `conf` subfolder, open the configuration file `server.xml`.
  - ii. In the Host node, change the value of the `autoDeploy` parameter from `false` to `true`.
  - iii. In the Control Panel, under Administrative Tools, open Services and restart the VMware VirtualCenter Management Webservices service.
  - iv. Remotely install the VMware Granular Extension Web Plug-In component to the vCenter Server.

- To perform installation without using the automatic deployment feature of VMware Web Server:
  - i. Remotely install the VMware Granular Extension Web Plug-In component to the vCenter Server.

The VMware GRE post-installation script will fail.

- ii. In the VMware Web Server folder `installation_directory`, in the `webapps` subfolder, extract the `VMwareGRE.war` file to a new directory named `VMwareGRE` (case sensitive).
- iii. From the `Data_Protector_home\bin` folder, execute:  

```
perl -I "..\lib\perl" vmwgre_wp.pl -install
```
- iv. In the Control Panel, under Administrative Tools, open Services and restart the VMware VirtualCenter Management Webservices service.

**Earlier vCenter Server versions:**

Remotely install the Data Protector VMware Granular Extension Web Plug-In component to the vCenter Server.

**Note:** If there is a post-installation script failure during the installation of the VMware Granular Extension Web Plug-In component, the cause of the failure is displayed in the session output.

## Microsoft Hyper-V clients

Data Protector components that need to be installed on Microsoft Hyper-V systems vary depending on the backup and restore solution you want to use. You can choose among the following solutions:

- ["Data Protector Virtual Environment integration"](#)
- ["Data Protector Microsoft Volume Shadow Copy Service integration"](#)

### ***Data Protector Virtual Environment integration***

It is assumed that all systems on which you intend to install components are up and running.

On systems that should control backup and restore sessions (**backup hosts**), install the following Data Protector components:

- Virtual Environment Integration
- MS Volume Shadow Copy Integration
- Disk Agent

**Note:** The Disk Agent component enables you to use the **Browse** button when restoring to a directory on the backup host. If the component is not installed, you must type the target directory yourself.

On Microsoft Hyper-V systems, install the following Data Protector component:

- MS Volume Shadow Copy Integration

**Note:** If your Microsoft Hyper-V systems are configured in a cluster, they must be installed as cluster-aware clients. For details, see ["Installing Data Protector on a Microsoft Hyper-V cluster"](#).

On backup systems (applicable for VSS transportable backups), install the following Data Protector component:

- MS Volume Shadow Copy Integration

**Note:** A *backup host* and a *backup system* are not one and the same system.

### ***Data Protector Microsoft Volume Shadow Copy Service integration***

For details on which components need to be installed on Microsoft Hyper-V systems, see ["Microsoft Volume Shadow Copy Service clients"](#).

## NDMP Server clients

It is assumed that your NDMP Server is up and running.

During the installation procedure, select the `NDMP Media Agent` and install it to all Data Protector clients accessing the NDMP dedicated drives.

**Note:** If a Data Protector client will not be used to access an NDMP dedicated drive through the NDMP Server, but it will be used only to control the robotics of the library, either the `NDMP Media Agent` or the `General Media Agent` can be installed on such a client.

Note that only one Media Agent can be installed on one Data Protector client.

## Oracle clients

### *Prerequisites*

- It is assumed that your Oracle Server is up and running.
- The following software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus
- The Oracle data files on the application system must be installed on the source volumes that will be replicated during backup.

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

- Oracle control file, online redo log files, and Oracle SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

By default, instant recovery is enabled for such configuration.

- Oracle control file, online redo log files, and Oracle SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

By default, instant recovery is *not* enabled for such configuration. You can enable instant recovery by setting the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR_omnirc` options. For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

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

### *Installation procedure*

- Install the following Data Protector software components:
  - Depending on the disk array used, HP P9000 XP Agent or HP P6000 / HP 3PAR SMI-S Agent – on both the application and backup systems.
  - Oracle Integration – on the application system only.

## **SAP R/3 clients**

### *Prerequisites*

- The following Oracle software must be installed on the application system.
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus
- If you plan to run SAP R/3 compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), correctly configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration). Note that if you want to use third-party backint software to stream data to tape, BRBACKUP must be started on the backup system.
- The database on the application system can be installed on disk images, logical volumes, or filesystems.
  - The Oracle datafiles *must* reside on a disk array.
  - Archived redo log files do not have to reside on the disk array.

**Note:** If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

- On UNIX systems, ensure that the following users exist on the application system:
  - oraORACLE\_SID with the primary group dba
  - ORACLE\_SID adm in the UNIX group sapsys
- The SAP R/3 software must be correctly installed on the application system.

The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

**Note:** The location of the directories is dependent on the environment (UNIX systems) or registry

(Windows system) variables. For more information, see the SAP R/3 documentation.

- `ORACLE_HOME /dbs` (UNIX systems)  
`ORACLE_HOME \database` (Windows systems) - the Oracle and SAP profiles)
- `ORACLE_HOME /bin` (UNIX systems)  
`ORACLE_HOME \bin` (Windows systems) - the Oracle binaries
- `SAPDATA_HOME /sapbackup` (UNIX systems)  
`SAPDATA_HOME \sapbackup` (Windows systems) - the SAPBACKUP directory with BRBACKUP log files
- `SAPDATA_HOME /saparch` (UNIX systems)  
`SAPDATA_HOME \saparch` (Windows systems) - the SAPARCH directory with BRARCHIVE log files
- `SAPDATA_HOME /sapreorg` (UNIX systems)  
`SAPDATA_HOME \sapreorg` (Windows systems)
- `SAPDATA_HOME /sapcheck` (UNIX systems)  
`SAPDATA_HOME \sapcheck` (Windows systems)
- `SAPDATA_HOME /saptrace` (UNIX systems)  
`SAPDATA_HOME \saptrace` (Windows systems)
- `/usr/sap/ORACLE_SID/SYS/exe/run` (UNIX systems)  
`c:\Oracle\ORACLE_SID\sys\exe\run` (Windows systems)

**Note:** If you plan to do instant recovery, ensure that the `sapbackup`, `saparch`, and `sapreorg` directories reside on different source volumes than the Oracle data files.

## UNIX systems

On UNIX systems, if the last six directories do not reside at the above specified destinations, create appropriate links to them.

On UNIX systems, the directory `/usr/sap/ORACLE_SID/SYS/exe/run` must be owned by the UNIX user `oraORACLE_SID`. The owner of the SAP R/3 files must be the UNIX user `oraORACLE_SID` and the UNIX group `dba` with `setuid` bit set (`chmod 4755 ...`). The exception is the file `BRRESTORE`, which must be owned by the UNIX user `ORACLE_SIDadm`.



### *UNIX example*

If `ORACLE_SID` is `PRO`, then the permissions inside the directory `/usr/sap/PRO/SYS/exe/run` should look like:

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive
-rwsr-xr-x 1 orapro dba 4750020 Apr 17 2011 brbackup
-rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011 brconnect
-rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011
brrestore
-rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

### *Installation procedure*

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
  - Depending on the disk array used, HP P9000 XP Agent or HP P6000 / HP 3PAR SMI-S Agent.
  - SAP R/3 Integration.

**Note:** You do not need to install SAP R/3 Integration on the backup system if you plan to run BRBACKUP only on the application system.

On Windows systems, the Data Protector software components must be installed using the SAP R/3 administrator user account, and this account must be included in the `ORA_DBA` or `ORA_SID_DBA` local group on the system where the SAP R/3 instance is running.

## **HP P4000 SAN Solutions clients**

To integrate HP P4000 SAN Solutions with Data Protector, install the following Data Protector software components on the application and backup systems:

- MS Volume Shadow Copy Integration
- HP P4000 Agent

To perform ZDB-to-disk+tape or ZDB-to-tape sessions, additionally install the following Data Protector software component on the backup system:

- General Media Agent

## **HP P6000 EVA Disk Array Family clients**

To integrate HP P6000 EVA Disk Array Family with Data Protector, install the following Data Protector software components on the application and backup systems:

- HP P6000 / HP 3PAR SMI-S Agent
- General Media Agent

Install the General Media Agent component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- Disk Agent

Install the Disk Agent component on the application and backup systems to run zero downtime backup of filesystems or disk images. Clients without the Disk Agent installed are not listed in the Application system and Backup system drop-down lists when creating a ZDB backup specification.

**Important:** On Microsoft Windows Server 2008 systems, two Windows Server 2008 hotfixes must be installed to enable normal operation of the Data Protector HP P6000 EVA Disk Array Family integration. You can download the required hotfix packages from the Microsoft websites <http://support.microsoft.com/kb/952790> and <http://support.microsoft.com/kb/971254>.

This additional requirement does not apply to Windows Server 2008 R2 systems.

### *Installing in a cluster*

You can install the HP P6000 EVA Disk Array Family integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

### *Integrating with other applications*

To install the HP P6000 EVA Disk Array Family integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the HP P6000 EVA Disk Array Family integration with Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, and Microsoft Volume Shadow Copy Service.

## ***HP P6000 EVA Disk Array Family integration with Oracle Server***

### *Prerequisites*

- The following software must be installed and configured on the application system and on the backup system for the backup set ZDB method:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus

The Oracle software on the backup system must be installed in the same directory as on the application system. The binaries should be identical to the binaries on the application system. You can achieve this either by copying the files and system environment from the application system to the backup system, or by a clean installation of the Oracle binaries on the backup system with the same installation parameters as on the application system.

- The Oracle datafiles on the application system must be installed on source volumes that will be replicated using the SMI-S agent you have installed.

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

- Oracle control file, online redo log files, and Oracle SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

By default, instant recovery is enabled for such configuration.

- Oracle control file, online redo log files, and Oracle SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

By default, instant recovery is *not* enabled for such configuration. You can enable instant recovery by setting the ZDB\_ORA\_INCLUDE\_CF\_OLF, ZDB\_ORA\_INCLUDE\_SPF, and ZDB\_ORA\_NO\_CHECKCONF\_IR omnirc options. For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

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

If some Oracle data files are installed on symbolic links, then these links have to be created on the backup system too.

### *Installation procedure*

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
  - HP P6000 / HP 3PAR SMI-S Agent – on both the application system and backup system
  - Oracle Integration – on both the application system and backup system

#### **Note:**

- The Data Protector Oracle Integration component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector Oracle Integration and HP P6000

/ HP 3PAR SMI-S Agent components on all the systems where the Oracle instances are running.

- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

## ***HP P6000 EVA Disk Array Family integration with SAP R/3***

### ***Prerequisites***

- The following Oracle software must be installed on the application system.
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or filesystems.
  - The Oracle datafiles *must* reside on a disk array.
  - For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
  - For *offline backup*, the control file and online redo logs *must* reside on a disk array.
  - Archived redo log files do not have to reside on a disk array.

If the Oracle control file, online redo logs, and Oracle SPFILE reside on the same LVM volume group or source volume as Oracle datafiles, set the Data Protector ZDB\_ORA\_NO\_CHECKCONF\_IR, ZDB\_ORA\_INCLUDE\_CF\_OLF, and ZDB\_ORA\_INCLUDE\_SPFomnirc options. Otherwise, you cannot run ZDB-to-disk and ZDB-to-disk+tape sessions. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

**Note:** If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

**UNIX systems:** If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX systems, ensure that the following users exist on the application system:
  - `oraORACLE_SID` with the primary group `dba`
  - `ORACLE_SID` `adm` in the UNIX group `sapsys`
- The SAP R/3 software must be correctly installed on the application system.

The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

**Note:** The location of the directories is dependent on the environment (UNIX systems) or registry (Windows system) variables. For more information, see the SAP R/3 documentation.

- `ORACLE_HOME /dbs` (UNIX systems) `ORACLE_HOME\database` (Windows systems) - the Oracle and SAP profiles)
- `ORACLE_HOME /bin` (UNIX systems) `ORACLE_HOME\bin` (Windows systems) - the Oracle binaries
- `SAPDATA_HOME /sapbackup` (UNIX systems) `SAPDATA_HOME\sapbackup` (Windows systems) - the SAPBACKUP directory with BRBACKUP log files
- `SAPDATA_HOME /saparch` (UNIX systems) `SAPDATA_HOME\saparch` (Windows systems) - the SAPARCH directory with BRARCHIVE log files
- `SAPDATA_HOME /sapreorg` (UNIX systems) `SAPDATA_HOME\sapreorg` (Windows systems)
- `SAPDATA_HOME /sapcheck` (UNIX systems) `SAPDATA_HOME\sapcheck` (Windows systems)
- `SAPDATA_HOME /saptrace` (UNIX systems) `SAPDATA_HOME\saptrace` (Windows systems)
- `/usr/sap/ORACLE_SID/SYS/exe/run` (UNIX systems)  
`c:\Oracle\ORACLE_SID\sys\exe\run` (Windows systems)

**Note:** If you plan to do instant recovery, ensure that the `sapbackup`, `saparch`, and `sapreorg` directories reside on different source volumes than the Oracle data files.

## UNIX systems

On UNIX systems, if the last six directories do not reside at the above specified destinations, create appropriate links to them.

On UNIX systems, the directory `/usr/sap/ORACLE_SID/SYS/exe/run` must be owned by the UNIX user `oraORACLE_SID`. The owner of the SAP R/3 files must be the UNIX user `oraORACLE_SID` and the UNIX group `dba` with `setuid` bit set (`chmod 4755 ...`). The exception is the file `BRRESTORE`, which must be owned by the UNIX user `ORACLE_SIDadm`.

### *UNIX example*

If `ORACLE_SID` is `PRO`, then the permissions inside the directory `/usr/sap/PRO/SYS/exe/run` should look like:

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive
-rwsr-xr-x 1 orapro dba 4750020 Apr 17 2011 brbackup
-rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011 brconnect
-rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore
-rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

### *Installation procedure*

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
  - HP P6000 / HP 3PAR SMI-S Agent
  - SAP R/3 Integration
  - Disk Agent

**Note:** You need to install SAP R/3 Integration on the backup system only if you plan to run SAP compliant ZDB sessions in which BRBACKUP is started on the backup system.

On Windows systems, the Data Protector software components must be installed using the SAP R/3 administrator user account, and this account must be included in the `ORA_DBA` or `ORA_SID_DBA` local group on the system where the SAP R/3 instance is running.

## ***HP P6000 EVA Disk Array Family integration with Microsoft Exchange Server***

### *Prerequisite*

The Microsoft Exchange Server database must be installed on the application system source volumes. The following objects must be located on the source volumes:

- Microsoft Information Store (MIS)
- optionally, Key Management Service (KMS)
- optionally, Site Replication Service (SRS)

To be able to back up transaction logs, disable Circular Logging on the Microsoft Exchange Server.

### *Installation procedure*

Install the following Data Protector software components:

- HP P6000 / HP 3PAR SMI-S Agent – on both the application and backup systems
- MS Exchange Integration – on the application system only

## **HP P6000 EVA Disk Array Family integration with Microsoft SQL Server**

### *Prerequisite*

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However, if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

### *Installation procedure*

Install the following Data Protector software components on both the application and the backup systems:

- HP P6000 / HP 3PAR SMI-S Agent – on both the application and backup systems
- MS SQL Integration – on the application system only

## **HP P9000 XP Disk Array Family clients**

To integrate HP P9000 XP Disk Array Family with Data Protector, install the following Data Protector software components on the application and backup systems:

- HP P9000 XP Agent
- General Media Agent

Install the General Media Agent component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- Disk Agent

Install the Disk Agent component on the application and backup systems to run zero downtime backup of filesystems or disk images. Clients without the Disk Agent installed are not listed in the Application system and Backup system drop-down lists when creating a ZDB backup specification.

**Important:** On Microsoft Windows Server 2008 systems, two Windows Server 2008 hotfixes must be installed to enable normal operation of the Data Protector HP P9000 XP Disk Array Family integration. You can download the required hotfix packages from the Microsoft websites <http://support.microsoft.com/kb/952790> and <http://support.microsoft.com/kb/971254>.

This additional requirement does not apply to Windows Server 2008 R2 systems.

### *Installing in a cluster*

You can install the HP P9000 XP Disk Array Family integration in a cluster environment. For the supported cluster configurations and specific installation requirements, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

### *Integrating with other applications*

To install the HP P9000 XP Disk Array Family integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the HP P9000 XP Disk Array Family integration with Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, and Microsoft Volume Shadow Copy Service.

## **HP P9000 XP Disk Array Family integration with Oracle Server**

### *Prerequisites*

- The following software must be installed and configured on the application system and on the backup system for the backup set ZDB method:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus

The Oracle software on the backup system must be installed in the same directory as on the application system. The binaries should be identical to the binaries on the application system. You can achieve this either by copying the files and system environment from the application system to the backup system, or by a clean installation of the Oracle binaries on the backup system with the same installation parameters as on the application system.

- The Oracle data files on the application system must be installed on HP P9000 XP Disk Array Family LDEVs that are mirrored to the backup system.

In case of the backup set method, if some Oracle data files are installed on symbolic links, then these links have to be created on the backup system too.

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

- Oracle control file, online redo log files, and Oracle SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

By default, instant recovery is enabled for such configuration.

- Oracle control file, online redo log files, and Oracle SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.



By default, instant recovery is *not* enabled for such configuration. You can enable instant recovery by setting the ZDB\_ORA\_INCLUDE\_CF\_OLF, ZDB\_ORA\_INCLUDE\_SPF, and ZDB\_ORA\_NO\_CHECKCONF\_IR omnirc options. For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

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

### *Installation procedure*

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
  - HP P9000 XP Agent – on both the application system and backup system
  - Oracle Integration – on both the application system and backup system

**Note:**

- The Data Protector Oracle Integration component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector Oracle Integration and HP P9000 XP Agent components on all the systems where the Oracle instances are running.
- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

## ***HP P9000 XP Disk Array Family integration with SAP R/3***

### *Prerequisites*

- The following Oracle software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or

filesystems.

- The Oracle datafiles *must* reside on a disk array.
- For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
- For *offline backup*, the control file and online redo logs *must* reside on a disk array.
- Archived redo log files do not have to reside on a disk array.

If the Oracle control file, online redo logs, and Oracle SPFILE reside on the same LVM volume group or source volume as Oracle datafiles, set the Data Protector ZDB\_ORA\_NO\_CHECKCONF\_IR, ZDB\_ORA\_INCLUDE\_CF\_OLF, and ZDB\_ORA\_INCLUDE\_SPFomnirc options. Otherwise, you cannot run ZDB-to-disk and ZDB-to-disk+tape sessions. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

**Note:** If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

**UNIX systems:** If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX systems, ensure that the following users exist on the application system:
  - oraORACLE\_SID with the primary group dba
  - ORACLE\_SID adm in the UNIX group sapsys
- The SAP R/3 software must be correctly installed on the application system.

The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

**Note:** The location of the directories is dependent on the environment (UNIX systems) or registry (Windows system) variables. For more information, see the SAP R/3 documentation.

- ORACLE\_HOME /dbs (UNIX systems)  
ORACLE\_HOME \database (Windows systems) - the Oracle and SAP R/3 profiles
- ORACLE\_HOME /bin or (UNIX systems)  
ORACLE\_HOME \bin (Windows systems) - the Oracle binaries
- SAPDATA\_HOME /sapbackup (UNIX systems)

`SAPDATA_HOME \sapbackup` (Windows systems) - the  
SAPBACKUP directory with BRBACKUP log files

- `SAPDATA_HOME /saparch` (UNIX systems)

`SAPDATA_HOME \saparch` (Windows systems) - the SAPARCH  
directory with BRARCHIVE log files

- `SAPDATA_HOME /sapreorg` (UNIX systems)

`SAPDATA_HOME \sapreorg` (Windows systems)

- `SAPDATA_HOME /sapcheck` (UNIX systems)

`SAPDATA_HOME \sapcheck` (Windows systems)

- `SAPDATA_HOME /saptrace` (UNIX systems)

`SAPDATA_HOME \saptrace` (Windows systems)

- `/usr/sap/ORACLE_SID/SYS/exe/run` (UNIX systems)

`c:\Oracle\ORACLE_SID\sys\exe\run` (Windows systems)

**Note:** If you plan to do instant recovery, ensure that the `sapbackup`, `saparch`, and `sapreorg` directories reside on different source volumes than the Oracle data files.

## UNIX systems

On UNIX systems, if the last six directories do not reside at the above specified destinations, create appropriate links to them.

On UNIX systems, the directory `/usr/sap/ORACLE_SID/SYS/exe/run` must be owned by the UNIX user `oraORACLE_SID`. The owner of the SAP R/3 files must be the UNIX user `oraORACLE_SID` and the UNIX group `dba` with `setuid` bit set (`chmod 4755 ...`). The exception is the file `BRRESTORE`, which must be owned by the UNIX user `ORACLE_SIDadm`.

## UNIX example

If `ORACLE_SID` is `PRO`, then the permissions inside the directory `/usr/sap/PRO/SYS/exe/run` should look like:

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive
-rwsr-xr-x 1 orapro dba 4750020 Apr 17 2011 brbackup
-rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011 brconnect
-rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011
brrestore
-rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

### *Installation procedure*

1. Install SAP R/3 BRTOOLS on the application system.
2. Install the following Data Protector software components on both the application system and backup system:
  - HP P9000 XP Agent
  - SAP R/3 Integration
  - Disk Agent

**Note:** You need to install SAP R/3 Integration on the backup system only if you plan to run SAP compliant ZDB sessions in which BRBACKUP is started on the backup system.

On Windows systems, the Data Protector software components must be installed using the SAP R/3 administrator user account, and this account must be included in the ORA\_DBA or ORA\_SID\_DBA local group on the system where the SAP R/3 instance is running.

## ***HP P9000 XP Disk Array Family integration with Microsoft Exchange Server***

### *Prerequisite*

The Microsoft Exchange Server database must be installed on the application system on the HP P9000 XP Disk Array Family volumes (LDEVs), which are mirrored to the backup system. The mirroring can be HP BC P9000 XP or HP CA P9000 XP and the database installed on a filesystem. The following objects must be located on volumes that are mirrored:

- Microsoft Information Store (MIS)
- optionally, Key Management Service (KMS)
- optionally, Site Replication Service (SRS)

To be able to back up transaction logs, disable Circular Logging on the Microsoft Exchange Server.

### *Installation procedure*

Install the following Data Protector software components:

- HP P9000 XP Agent – on both the application and the backup system
- MS Exchange Integration – on the application system only

## **HP P9000 XP Disk Array Family integration with Microsoft SQL Server**

### ***Prerequisite***

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However, if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

### ***Installation procedure***

Install the following Data Protector software components on both the application and the backup systems:

- HP P9000 XP Agent
- MS SQL Integration

## **HP 3PAR StoreServ Storage clients**

To integrate HP 3PAR StoreServ Storage with Data Protector, install the following Data Protector software components on the application and backup systems:

- HP P6000 / HP 3PAR SMI-S Agent

For backing up and restoring objects using the Volume Shadow Copy Service, you also need the following components:

- MS Volume Shadow Copy Integration
- HP 3PAR VSS Agent

Regardless of the operating system, to perform ZDB-to-disk+tape or ZDB-to-tape sessions, additionally install the following Data Protector software component on the backup system:

- General Media Agent

## **EMC Symmetrix clients**

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

- EMC Symmetrix Agent (SYMA)

Before remotely installing the EMC Symmetrix Agent component, install the following two EMC components:

- EMC Solution Enabler
- EMC Symmetrix TimeFinder or EMC Symmetrix Remote Data Facility (SRDF) microcode and license.

- General Media Agent

Install the General Media Agent component on the backup system to back up the bulk data. Install it on the application system to back up archive logs or to perform a restore to the application system.

- Disk Agent

Install the Disk Agent component on the application and backup systems to run disk image and filesystem ZDB. Clients without Disk Agent installed are not listed in the Application system and Backup system drop-down lists when creating a ZDB backup specification.

### *Installing in a cluster*

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

### *Integrating with other applications*

To install the EMC Symmetrix integration with a database application, install the Data Protector component specific for the particular integration to the application and backup systems and perform the installation tasks specific for this integration. You can install the EMC Symmetrix integration with Oracle and SAP R/3.

## **EMC Symmetrix Integration with Oracle**

### *Prerequisites*

- The following software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net services
  - SQL\*Plus
- The Oracle database files used by the application system must be installed on EMC Symmetrix devices which are mirrored to the backup system.

The database can be installed on disk images, logical volumes or filesystems. The following Oracle files have to be mirrored:

- Datafiles
- Control file

- Online redo log files

The archive redo log files have to reside on non-mirrored disks.

### *Installation procedure*

Perform the following installation tasks:

1. Install the Oracle recovery catalog database. Preferably, install it on a separate system, on non-mirrored disks. Leave the recovery catalog unregistered. For details on how to install the database, see the Oracle documentation.
2. Install the following Data Protector software components:
  - EMC Symmetrix Agent – on both the application system and backup system
  - Oracle Integration – on both the application system and backup system

#### **Note:**

- The Data Protector Oracle Integration component on the backup system is needed only for the backup set ZDB method. It is not needed for the proxy-copy ZDB method.
- In a RAC cluster environment, the Oracle application database is accessed by multiple Oracle instances. Therefore, install the Data Protector Oracle Integration and EMC Symmetrix Agent components on all the systems where the Oracle instances are running.
- If you installed the Oracle recovery catalog database on a separate system, you do not need to install any Data Protector software components there.

## ***EMC Symmetrix Integration with SAP R/3***

### *Prerequisites*

- The following Oracle software must be installed and configured on the application system:
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 software
  - SQL\*Plus
- If you plan to run SAP compliant ZDB sessions (BRBACKUP started on the backup system and not on the application system), configure the backup system. For details, see the SAP database guide for Oracle (split mirror backup, software configuration).
- The database on the application system can be installed on disk images, logical volumes, or filesystems.

- The Oracle datafiles *must* reside on a disk array.
- For *online backup*, the control file and online redo logs do not have to reside on a disk array. *Online* SAP compliant ZDB sessions are an exception, for which the control file must reside on a disk array.
- For *offline backup*, the control file and online redo logs *must* reside on a disk array.
- The archived redo log files do not have to reside on a disk array.

**Note:** If some of the Oracle data files are installed on symbolic links, create the links on the backup system too.

**UNIX systems:** If the Oracle database is installed on raw partitions (rawdisk or raw logical volumes), ensure that the volume/disk group names on the application system and backup system are identical.

- On UNIX systems, ensure that the following users exist on the application system:
  - oraORACLE\_SID with the primary group dba
  - ORACLE\_SID adm in the UNIX group sapsys
- The SAP R/3 software must be correctly installed on the application system.

The following is a list of standard directories that must be installed on the application system after installing SAP R/3:

**Note:** The location of the directories depends on the environment variables. For more information, see the SAP R/3 documentation.

- ORACLE\_HOME /dbs - the Oracle and SAP R/3 profiles
- ORACLE\_HOME /bin - the Oracle binaries
- SAPDATA\_HOME /sapbackup - the SAPBACKUP directory with BRBACKUP log files
- SAPDATA\_HOME /saparch - the SAPARCH directory with BRARCHIVE log files
- SAPDATA\_HOME /sapreorg
- SAPDATA\_HOME /sapcheck
- SAPDATA\_HOME /saptrace
- /usr/sap/ORACLE\_SID/SYS/exe/run



**Note:** If you plan to do instant recovery, ensure that the `sapbackup`, `saparch`, and `sapreorg` directories reside on different source volumes than the Oracle data files.

If the last six directories do not reside at the above specified destinations, create appropriate links to them.

The directory `/usr/sap/ORACLE_SID/SYS/exe/run` must be owned by the UNIX user `oraORACLE_SID`. The owner of the SAP R/3 files must be the UNIX user `oraORACLE_SID` and the UNIX group `dba` with `setuid` bit set (`chmod 4755 ...`). The exception is the file `BRRESTORE`, which must be owned by the UNIX user `ORACLE_SIDadm`.

### Example

If `ORACLE_SID` is `PRO`, then the permissions inside the directory `/usr/sap/PRO/SYS/exe/run` should look like:

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive
-rwsr-xr-x 1 orapro dba 4750020 Apr 17 2011 brbackup
-rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011 brconnect
-rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011 brrestore
-rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

### Installation procedure

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

**Note:** You need to install SAP R/3 Integration on the backup system only if you plan to run SAP compliant ZDB sessions in which `BRBACKUP` is started on the backup system.

## EMC Symmetrix Integration with Microsoft SQL Server

### Prerequisite

Microsoft SQL Server has to be installed on the application system. User databases *must* reside on the disk array source volumes, while system databases can be installed anywhere. However, if the system databases are also installed on the disk array, they *must* be installed on *different* source volumes than user databases.

### *Installation procedure*

Install the following Data Protector software components on both the application and the backup systems:

- EMC Symmetrix Agent
- MS SQL Integration

## **Installing the Data Protector Single Server Edition**

The Single Server Edition (SSE) of Data Protector is designed for small environments where backups run on only one device connected to a Cell Manager. It is available for supported Windows and for HP-UX platforms.

To install the Cell Manager and (optionally) Installation Server, follow the instructions in ["Installing the Data Protector Cell Manager and Installation Servers"](#).

### *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.
- Adding extension products is not supported with SSE.
- Clustering is not supported with SSE.
- Disaster Recovery is not supported with SSE.

The number of Windows clients is not limited.

For supported devices, see the *HP Data Protector Product Announcements, Software Notes, and References*.

## **Limitations of SSE for HP-UX**

- SSE supports backups to only one device concurrently, connected to a single Cell Manager.
- One 10-slot DDS autochanger only is supported.
- On a UNIX Cell Manager, you cannot back up servers - only UNIX clients, Windows clients and Solaris clients.

- Adding extension products is not supported with SSE.
- Clustering is not supported with SSE.

The number of clients (UNIX, Windows) is not limited.

For supported devices, see the *HP Data Protector Product Announcements, Software Notes, and References*.

### *Installing a password*

For the step-by-step instructions on how to install a password on the Cell Manager, see "[Data Protector passwords](#)".

## Installing the Data Protector web reporting

Data Protector Web Reporting is installed with other Data Protector components by default, and as such, you can use it locally from your system.

You can also install it on a Web server and in that way make it available on other systems which do not need to have any of the Data Protector software components installed.

### *Prerequisites*

To use Data Protector Web Reporting on your system, see the *HP Data Protector Product Announcements, Software Notes, and References* for prerequisites and limitations.

### *Installation*

To install Data Protector Web Reporting to a Web server, do the following:

1. Copy the following Data Protector Java reporting files to the server. The server does not have to be a Data Protector client. On systems with the Data Protector User Interface component installed, the files are located in the following directory:

#### **Windows systems:**

`Data_Protector_home\java\bin`

#### **UNIX systems:**

`/opt/omni/java/bin`

2. Open the `WebReporting.html` file in your browser to access the Data Protector Web Reporting.

You must make the file available to the users of the Web reporting in the full URL form. For example, you can put a link to this file from your Intranet site.

**Tip:** By default, no password is needed to use Data Protector Web Reporting. It is strongly recommended to set password on Cell Manager and in that way restrict the access to the Web reporting. For the procedure, see the *HP Data Protector Help* index: "Web reports, limiting access

to”.

### *What's next?*

When the installation has been completed, see the *HP Data Protector Help* index: “Web reporting interface, configuring notifications” for more information on configuration issues and creating your own reports.

## **Installing Data Protector on an HP Serviceguard**

Data Protector supports HP Serviceguard (HP SG) for HP-UX and Linux. For details on supported operating system versions, see the *HP Data Protector Product Announcements, Software Notes, and References*.

If your Cell Manager is to be cluster-aware, note that the virtual server IP address should be used for licenses.

## **Installing a cluster-aware Cell Manager**

### *Prerequisites*

Before you install a Data Protector Cell Manager on HP 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 HP Serviceguard installed and must be configured as cluster members.
- Data Protector Cell Manager, with recommended patches, and all other Data Protector software components for the integrations you want to have in the cluster, must be installed on the Primary node and each of the Secondary nodes.

The installation procedure is standard procedure for installing the Cell Manager system. See ["Installing the Data Protector Cell Manager and Installation Servers"](#).

- The user group `hdp` and the dedicated user account `hdp` must have the same IDs on both nodes.
- Users with the same user ID must exist on all nodes in the cluster.
- Users must be members of the same group, having the same group ID on both nodes.
- A home directory must be present for the users.

### *What's next?*

When the installation has been completed, you must configure the installed Primary Cell Manager and the Secondary Cell Manager(s), and the Cell Manager package. For more information on configuring HP Serviceguard with Data Protector, see the *HP Data Protector Help* index: “cluster, HP Serviceguard”.

## Installing an Installation Server on cluster nodes

You can install the Installation Server on a secondary HP Serviceguard node and use it for remote installation. "[Installing Installation Servers for UNIX systems](#)".

## Installing cluster-aware clients

**Important:** The Data Protector cluster-aware clients must be installed on all the cluster nodes.

The installation procedure is standard procedure for installing Data Protector on an UNIX client. For detailed instructions, see "[Installing HP-UX clients](#)" and "[Installing Linux clients](#)".

### *What's next?*

When the installation has been completed, you must import the virtual server (the hostname specified in the cluster package) to the Data Protector cell. See "[Importing a cluster-aware client to a cell](#)".

For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuration".

## Installing Data Protector on a Microsoft Cluster Server

For supported operating systems for Microsoft Cluster Server integration, see the latest support matrices at <http://support.openview.hp.com/selfsolve/manuals>.

**Note:** If your Cell Manager is to be cluster-aware, the Cell Manager's virtual server IP address should be used for licenses.

## Installing a cluster-aware Cell Manager

### *Prerequisites*

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

- Clustering functionality must be installed properly on all cluster nodes. For example, you must be able to move groups from one to another node as many times as needed, without problems with shared disks.
- Make sure resources with the following names do not exist on the cluster:

OBVS\_MCRS, OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, OBVS\_HPDP\_IDB\_CP, and OmniBack\_Share

Data Protector uses these names for the Data Protector virtual server. If such resources exist, delete or rename them.

This can be done as follows:

- a. Click **Start > Programs > Administrative Tools > Cluster Administrator**.
  - b. Check the resource list and delete or rename these resources, if necessary.
- At least one group in the cluster should have a file cluster resource defined. Data Protector will install some of its data files in this file cluster resource under a specific folder.

**Windows Server 2008, Windows Server 2012:** Data files are installed on the *File Server* resource under the shared folder selected by the user at installation.

**Other Windows systems:** Data files are installed on the *File Share* resource under the folder specified when the file cluster resource was created.

For instructions on how to define a file cluster resource, see the cluster-specific documentation. Note that the file share name of the file cluster resource cannot be *OmniBack*.

- If the virtual server does not exist in the same group as the file cluster resource, create a new virtual server using a free registered IP address and associate a network name with it.
- The file cluster resource where Data Protector is to be installed must have the *IP Address*, *Network Name*, and *Physical Disk* set among the file cluster resource dependencies. This ensures that the Data Protector cluster group can run on any node independently of any other group.
- Ensure that only the cluster administrator has access to shared folder of the file cluster resource, and they should have full access to it.
- Data Protector is installed on the same location (drive and path name) on all cluster nodes. Ensure that these locations are free.
- If you start the cluster-aware Cell Manager installation from a network share, you must have access to this share from all cluster nodes.
- Ensure no other Microsoft Installer-based installations are running on any cluster node.
- Each system (node) of the cluster should be running and functioning properly.
- To enable installation of the cluster-aware Data ProtectorCell Manager on a server cluster with Microsoft Cluster Service (MSCS) running on Windows Server 2008 or Windows Server 2012, perform the procedure described in ["Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation"](#).

## Considerations

- Setup must be started under the cluster service account on the system (node) where the file cluster resource is active, so that shared folder of the file cluster resource can be accessed directly. The

resource owner (the system where the resource is active) can be determined using Cluster Administrator.

- To properly install and configure cluster-aware Data ProtectorCell Manager, a domain account with the following user rights must be provided during installation:
  - Administrator rights on the Cell Manager system
  - Cluster Administrator rights within the cluster
  - Password Never Expires
  - Logon as a service
  - User Cannot Change Password
  - All logon hours are allowed

**Important:** An account with administrator rights on all the cluster systems (nodes) is required for Microsoft Cluster Server installation. You should use this account to install Data Protector as well. Failing to do so results in Data Protector services running in the ordinary instead of the cluster-aware mode.

- The Windows domain user account that is used for the Inet service must additionally be given the following Windows operating system Security Policy privileges on all cluster nodes:
  - Impersonate a client after authentication
  - Replace a process level token

See the *HP Data Protector Help* index: "Inet user impersonation".

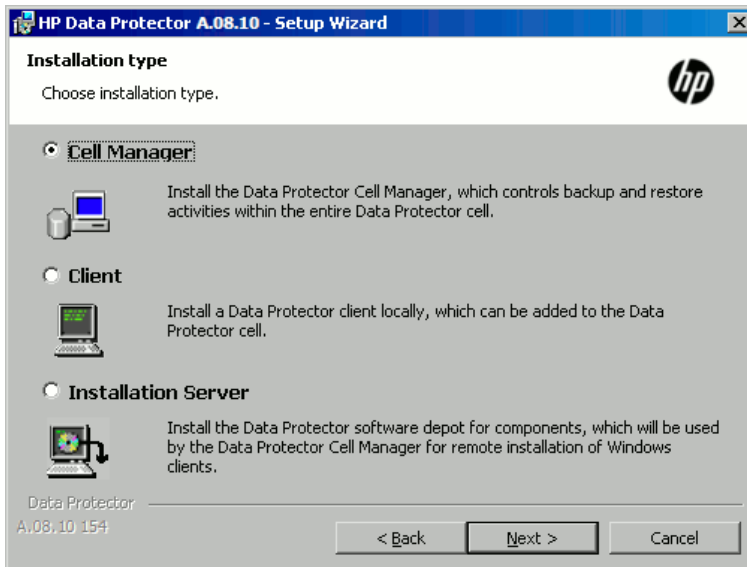
### *Local installation procedure*

The cluster-aware Data Protector Cell Manager must be installed locally, from the DVD-ROM or ISO image. Perform the following:

1. Insert the Windows installation DVD-ROM or mount the ISO image.

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

**Figure 21: Selecting the installation type**

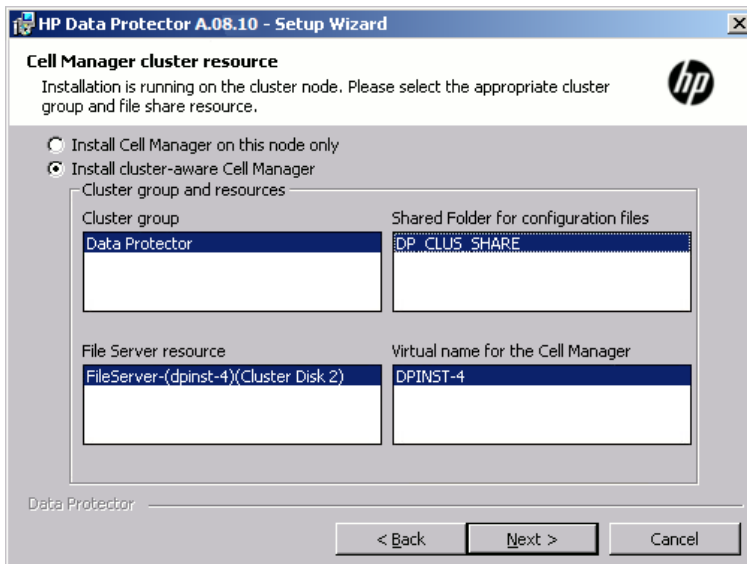


5. Setup automatically detects that it is running in a cluster environment. Select **Install cluster-aware Cell Manager** to enable a cluster setup.

Select the cluster group, the virtual hostname, and the file cluster resource on which Data Protector shared files and the database will reside.

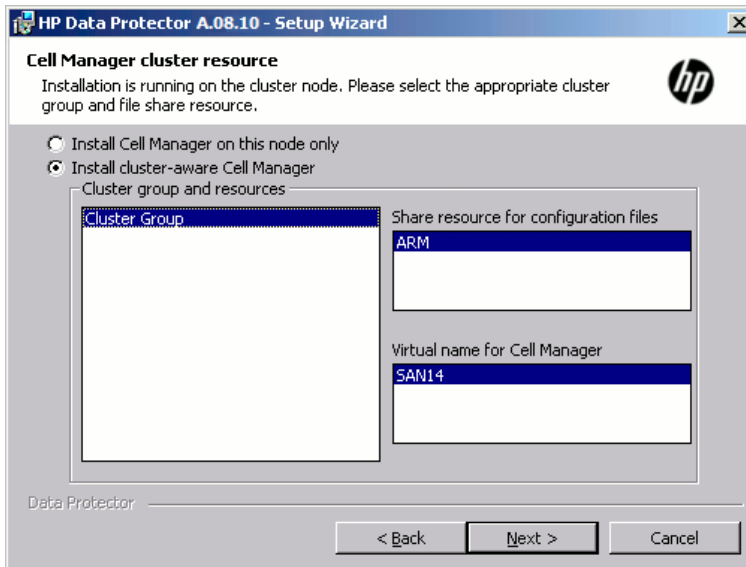
**Note:** If you select **Install Cell Manager on this node only**, the Cell Manager will *not* be cluster aware. See ["Installing a Windows Cell Manager"](#) .

**Figure 22: Selecting the cluster resource on Windows Server 2008**



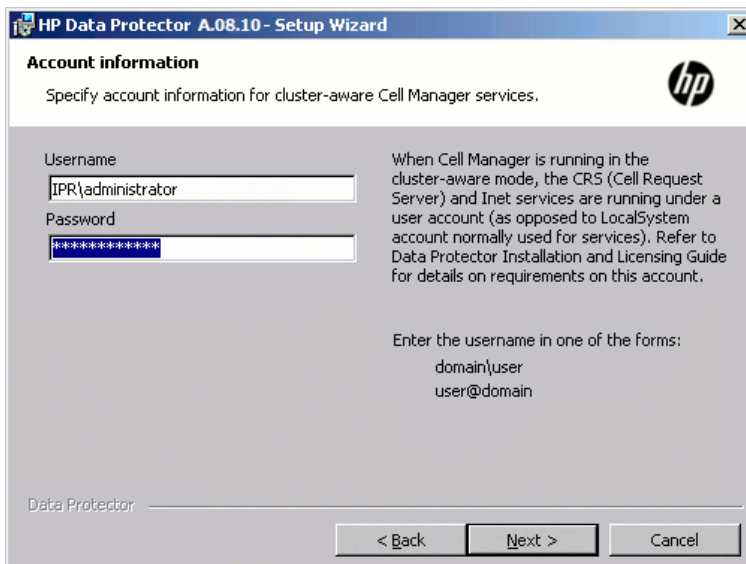


**Figure 23: Selecting the cluster resource on other Windows systems**



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

**Figure 24: Entering the account information**



7. Click **Next** to install Data Protector into the default installation folders.

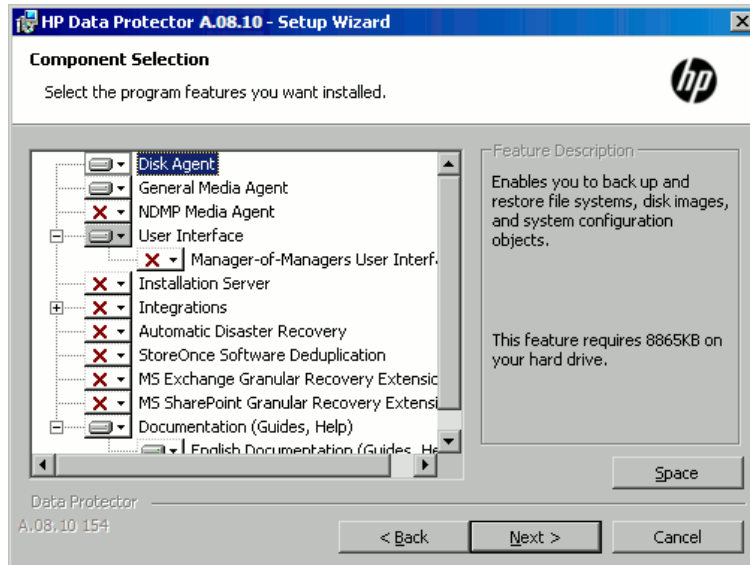
Otherwise, click **Change** to open the Change Current Destination Folder or Change Current Program Data Destination Folder dialog box, and change the installation folder as needed. Path to the program data installation folder should not exceed 80 characters.

8. In the Component Selection window, select the components you want to install on all cluster nodes and cluster virtual servers. Click **Next**.

The MS Cluster Support files are installed automatically.

The selected components will be installed on all the cluster nodes.

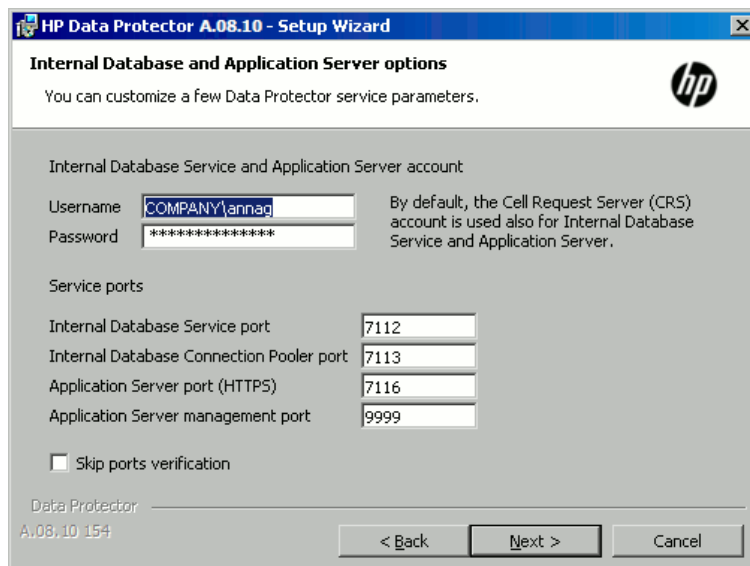
**Figure 25: Component selection page**



9. Optionally, change the user account or the ports used by the Data Protector services Internal Database Service and Application Server.

Click **Next**.

**Figure 26: Changing the IDB and Application Server options**



10. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration

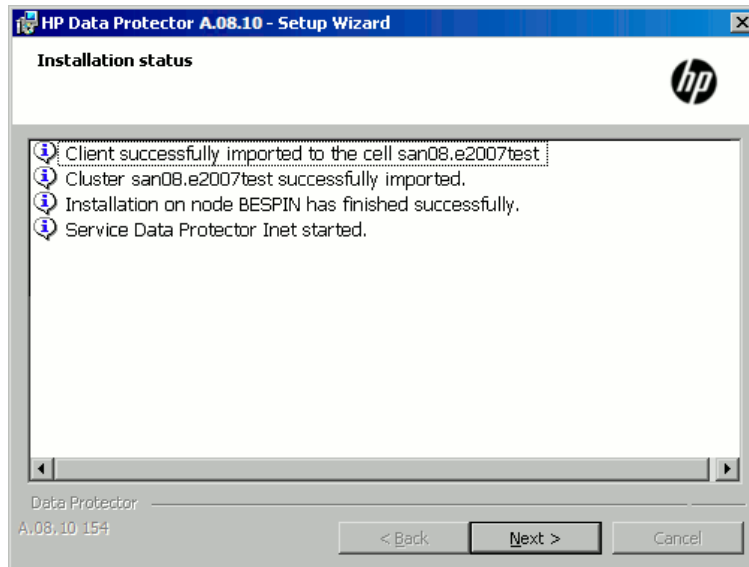
page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the selected option is **Initially, enable newly registered Data Protector binaries to open ports as needed**. If you do not want to enable Data Protector to open ports at the moment, deselect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

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

Click **Next**.

11. The component selection summary page is displayed. Click **Install**.
12. The Installation setup page is displayed. Click **Next**.

**Figure 27: Installation status page**



13. If you have installed the User Interface component, to start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

If you have installed the English Documentation (Guides, Help) component, to view the *HP Data Protector Product Announcements, Software Notes, and References* immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

14. Click **Finish** to complete the installation.

## ***Installing a cluster-aware Cell Manager for Windows 2012 and Windows 2012 R2 clusters***

### ***To install a cluster-aware Cell Manager***

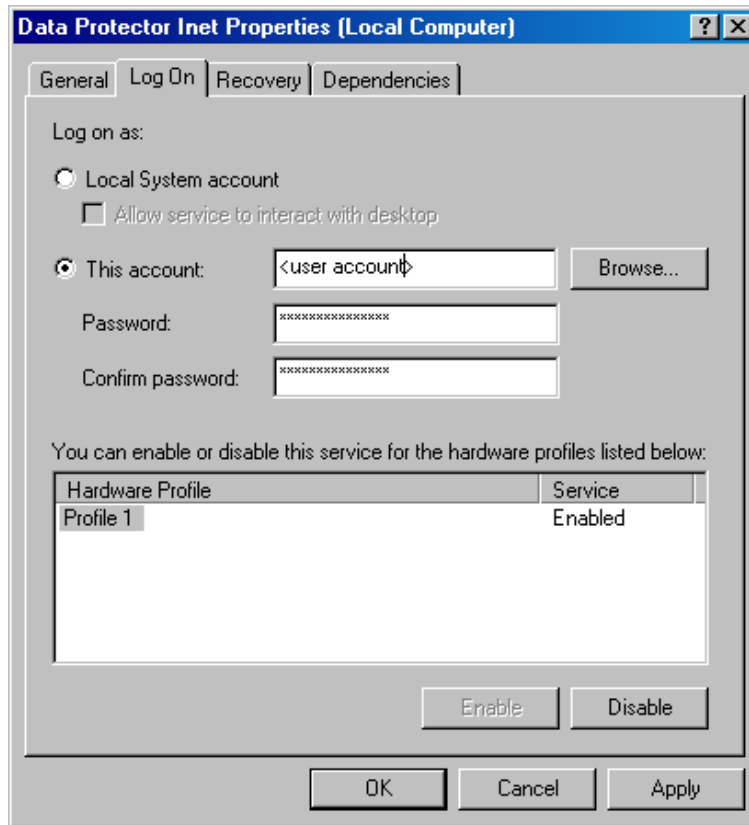
1. Install the Data Protector 8.10 Installation Server on a machine that is not a part of the cluster.
2. Apply the latest patch on it. The depot in ‘\DP\_Program\_data\Depot’ of the Installation Server can be used to install the cluster-aware Cell Manager in Windows 2012 and 2012 R2 systems.
3. Copy the depot to any of the cluster nodes and start the installation from the local disk.
4. Alternatively, access the depot using a network share and start the installation from the share. For this step, you need to consider the following:
  - The installation server should be in the same domain as the cluster.
  - Administrative (hidden) shares (\\hostname or IP address of IS\c\$\...) should not be used, because in some cases, they will not be accessible from other cluster nodes. Therefore, normal paths (\\hostname or IP address of IS\depot) should be used and it should be shared with all the cluster nodes.
  - The cluster nodes should be able to connect to the normal net path without any password.
  - Normal net path should be accessible from a browser without providing the credentials. If prompted for credentials, enter them and select Remember Credentials.

### ***Checking the installation***

When the setup procedure has been completed, you can check whether or not the Data Protector software has been properly installed. Proceed as follows:

1. Check if the Cluster service account is assigned to the Data Protector Inet service on each cluster node. Make sure the same user is also added to the Data Protector admin user group. The logon account type should be set to This account as shown in "[Data Protector user account](#)".

**Figure 28: Data Protector user account**



2. Execute the following command:

```
omnirsh host INFO_CLUS
```

where *host* is the name of the cluster virtual server (case-sensitive). The output should list the names of the systems within the cluster and the name of virtual server. If the output returns 0 "NONE", Data Protector is not installed in the cluster-aware mode.

3. Start the Data Protector GUI, select the **Clients** context, and then click **MS Clusters**. See the newly installed systems listed in the Results Area.

### *Data Protector Inet and CRS services*

If needed, change the accounts under which the Data Protector Inet and CRS services are running.

## **Installing cluster-aware clients**

### *Prerequisites*

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

- Clustering functionality must be installed properly on all cluster nodes. For example, you must be able to move groups from one to another node as many times as needed, without problems with shared disks.
- Each system of the cluster should be running and functioning properly.
- To enable installation of the cluster-aware Data Protector client on a server cluster with Microsoft Cluster Service (MSCS) running on Windows Server 2008 or Windows Server 2012, perform the procedure described in ["Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation"](#).

### Local installation procedure

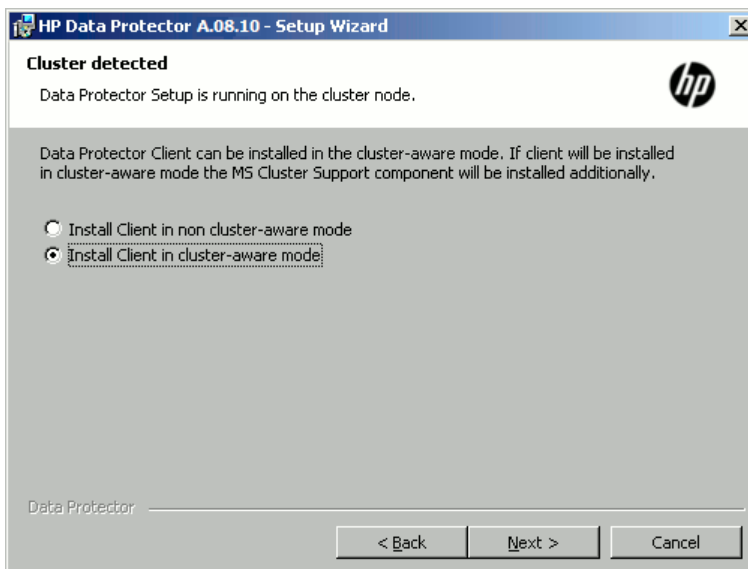
The cluster-aware Data Protector clients must be installed locally, from the DVD-ROM or ISO image, on each cluster node. The cluster nodes (Data Protector cluster clients) are imported to the specified cell during the installation process. You need to import the virtual server name afterwards.

The cluster Administrator account is required to perform the installation. Apart from that, the cluster client setup is the same as for the ordinary Windows client setup. The MS Cluster Support files are installed automatically.

For information on how to locally install a Data Protector Windows client system, see ["Installing Windows clients"](#).

The Data Protector installation reports that a cluster was detected. Select **Install client in cluster-aware mode**.

**Figure 29: Selecting cluster-aware installation mode**



If you are installing the Data Protector Oracle integration, the setup procedure must be performed on all cluster nodes and on the virtual server of the Oracle resource group.

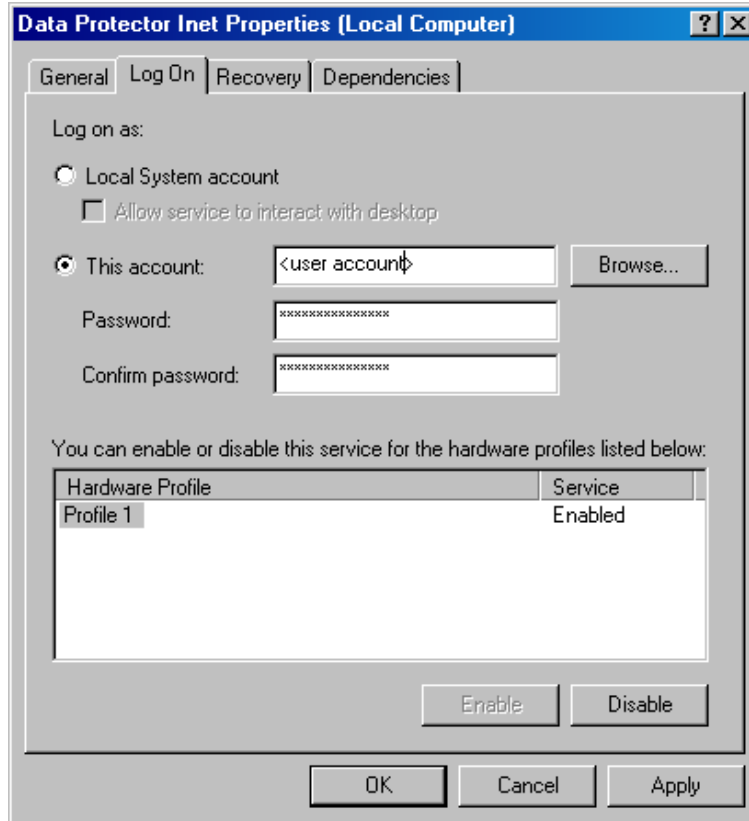
**Note:** You can import a cluster-aware client to the Data Protector cell that is managed using either the standard Cell Manager or the cluster-aware Cell Manager.

## Checking the installation

When the setup procedure has been completed, you can check whether or not the Data Protector software has been properly installed. Proceed as follows:

1. Check if the Cluster service account is assigned to the Data Protector Inet service on each cluster node. Make sure the same user is also added to the Data Protector admin user group. The logon account type should be set to **This account** as shown in ["Data Protector user account"](#).

**Figure 30: Data Protector user account**



2. Execute:

```
omnirsh host INFO_CLUS
```

where *host* is the name of the cluster client system. The output should return the name of the cluster-aware client system. If the output returns 0 "NONE", Data Protector is not installed in the cluster-aware mode.

## Veritas Volume Manager

If you have Veritas Volume Manager installed on the cluster, additional steps are required after you have completed the installation of Data Protector on Microsoft Cluster Server. For the additional steps to be performed, see ["Installing Data Protector on Microsoft Cluster Server with Veritas Volume Manager"](#).

### *What's next?*

When the installation has been completed, you must import the virtual server hostname (cluster-aware application) to the Data Protector cell. See ["Importing a cluster-aware client to a cell"](#).

For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuring".

### *Changing the Inet and CRS accounts*

If needed, change the accounts under which the Data Protector Inet and CRS services are running.

## Installing Data Protector clients on a Veritas Cluster

Data Protector clients can be installed on Veritas Cluster nodes, with a Cell Manager outside of the cluster. Using this configuration, backup of the local disks is supported.

In order to back up shared disks or cluster-aware applications, the virtual server IP address should be used for licenses.

**Important:** For Data Protector, cluster-aware backups with failover are not supported.

## Installing cluster-aware clients

The installation procedure is standard procedure for installing Data Protector on a Solaris client system. For detailed instructions, see ["Installing Solaris clients"](#).

### *What's next?*

When the installation has been completed:

- To back up the virtual server, you should import it into the cell.
- To back up the physical nodes, you should also import them into the cell.

See ["Importing a cluster-aware client to a cell"](#). For more information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuring".

## Installing Data Protector on an IBM HACMP Cluster

Data Protector supports IBM High Availability Cluster Multi-Processing for AIX.

**Important:** Install the Data Protector Disk Agent component on all the cluster nodes.

## Installing cluster-aware clients

To install Data Protector components on a cluster node, use the standard procedure for installing Data Protector on UNIX systems. For details, see ["Remote installation"](#) or ["Local installation on UNIX and Mac OS X systems"](#).



### *What's next?*

After the installation, import the cluster nodes and the virtual server (virtual environment package IP address) to the Data Protector cell. See ["Importing a cluster-aware client to a cell"](#) .

For information on how to configure backup devices, media pools, or any additional Data Protector configuration tasks, see the *HP Data Protector Help* index: "configuration".

## **Installing Data Protector on a Microsoft Hyper-V cluster**

Installing Data Protector on Microsoft Hyper-V systems that are configured in a cluster using the Microsoft Failover Clustering feature is similar to installing Data Protector on Microsoft Cluster Server; Microsoft Hyper-V systems must become Data Protector cluster-aware clients. For details, see ["Installing Data Protector on a Microsoft Cluster Server"](#) .

**Note:** Once the Microsoft Hyper-V systems become cluster-aware clients, you can install any additional Data Protector components on them remotely, using the Data Protector Installation Server.



## Chapter 3: Maintaining the installation

This chapter describes the procedures most frequently performed to modify the configuration of your backup environment. The following sections provide information about:

- How and when to use maintenance mode
- How to import clients to a cell using the graphical user interface
- How to import an Installation Server to a cell using the graphical user interface
- How to import clusters/virtual servers using the graphical user interface
- How to export clients using the graphical user interface
- How to ensure security using the graphical user interface
- How to configure LDAP for user authentication in Data Protector
- How and when to use the Certificate Generation Utility
- How to manage Data Protector patch bundles and identify the installed Data Protector patches
- How to uninstall Data Protector software
- How to add or remove Data Protector software components

### Data Protector maintenance mode

Maintenance tasks on Cell Manager, during which the write operations to the Internal Database should be prevented, require Data Protector to enter maintenance mode. Such tasks include upgrading the Data Protector installation, installing patches and critical fixes, upgrading hardware or the operating system. Maintenance mode is required only for certain procedures described in this chapter, but is as well applicable for tasks described elsewhere throughout the documentation.

The process of entering maintenance mode automatically initiates a series of tasks, such as stopping the scheduler, renaming the backup specification directories, aborting the running processes and freeing up locked resources. Maintenance mode is supported in individual cells, as well as in MoM and cluster environments.

### Initiating maintenance mode

Maintenance mode can be initiated by the users with administrative rights via the command line interface. To initiate the maintenance mode, execute:

In an individual cell:

```
omnisv -maintenance [GracefulTime]
```

In a MoM environment:

```
omnisv -maintenance -mom
```

Running sessions are instructed by the Cell Manager to stop all at once, while the cells in a MoM environment enter the maintenance mode one by one.

To customize the way Cell Manager enters the maintenance mode, modify the appropriate global options. The `MaintenanceModeGracefulTime` option reflects the seconds given to the Data Protector services to abort the running sessions, while the `MaintenanceModeShutdownTime` option reflects the seconds to wait for the sessions to abort. The default value for both options is 300. If the *GracefulTime* option is used, it overrides the `MaintenanceModeGracefulTime` global option. In case a restore session is still running after this option is exceeded, maintenance mode initiation fails.

In case any cell in MoM environment fails to enter the maintenance, the mode is reverted.

To check if Data Protector is running in maintenance mode, see the status of CRS service by executing `omnisv -status`, or check the GUI status bar. Note that the GUI can only reliably indicate the maintenance mode when connecting to the Cell Manager, which may sometimes result in the status bar indicating the maintenance mode even after the Cell Manager has been switched back to normal mode.

During the maintenance mode, Cell Manager rejects all operations that write data to the Internal Database, such as creating new devices, backup and restore sessions or their previews, purge, copy and consolidation sessions.

In cluster environments, only manual cluster related activities can be performed while the maintenance mode is active, such as shutting down cluster packages, stopping the Data Protector services, or manual volume mounting.

All read-only IDB operations are allowed while the maintenance mode is active. Data Protector services are all up and running. Only users with administrative Data Protector user rights can connect to the cell or MoM while the Cell Manager is in maintenance mode.

## Quitting maintenance mode

To quit the maintenance mode on Cell Manager using the CLI, execute:

- In an individual cell:

```
omnisv -maintenance -stop
```

- In a MoM environment:

```
omnisv -maintenance -mom_stop
```

While in a MoM environment, an individual cell cannot quit the maintenance mode. MoM maintenance can only be invoked from MoM Server.

To quit maintenance mode using the GUI:

1. In the Context List select **Clients**.
2. In the **Actions** menu click **Stop Maintenance Mode**.

After the normal mode is resumed, you can restart aborted and rejected sessions, as they have been logged in the `maintenance.log` file, located at the default Data Protector log files directory.

The following two examples show `maintenance.log` entries for aborted and rejected sessions:

```
10.5.2013 10:52:45 OMNISV.2492.9936  
["/cli/omnisv/omnisv.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2  
Session was aborted - graceful period expired!  
session id:      2013/05/10-8  
session type:    0  
datalist:        large_backup  
start date:      2013-05-10 10:52:45  
owned by:        JOHN.JOHNSON@company.com
```

```
10.5.2013 10:48:45 CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $ $Date:: 2013-  
03-22 18:00:03":142] X.99.01 b2  
CRS is in maintenance mode - session rejected  
session id:      R-2013/05/10-200  
session type:    dbsm  
session desc:    Database  
start date:      2013-05-10 10:48:45  
owned by:        .@ pid=0
```

Sessions are logged as aborted when they attempted to start while the maintenance mode was active. To run aborted sessions afterwards:

1. In the Context List, click **Internal Database**
2. In the Scoping Pane, expand **Sessions**.
3. Right-click a session, and select **Restart Failed Objects** from the context menu

Sessions are logged as rejected when they attempted to start while the Cell Manager was entering the maintenance mode. To run rejected session afterwards, restart each session manually.

## 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 HP OpenVMS and Windows XP Home Edition, that were installed locally from the installation DVD-ROM or ISO image must be imported to the cell after the installation. **Importing** means manually adding a system to a cell after the Data Protector software has been installed. When added to a Data Protector cell, the system becomes a Data Protector client. Once the system is a member of the cell, information about the new client is written to the IDB, which is located on the Cell Manager.

A client can only be a member of one cell. If you wish to move a client to a different cell, you first *export* it from its current cell and then *import* it to the new cell. For the procedure on how to export clients, see ["Exporting clients from a cell"](#).

**Important:** After you have installed Data Protector clients and imported them to a cell, it is highly

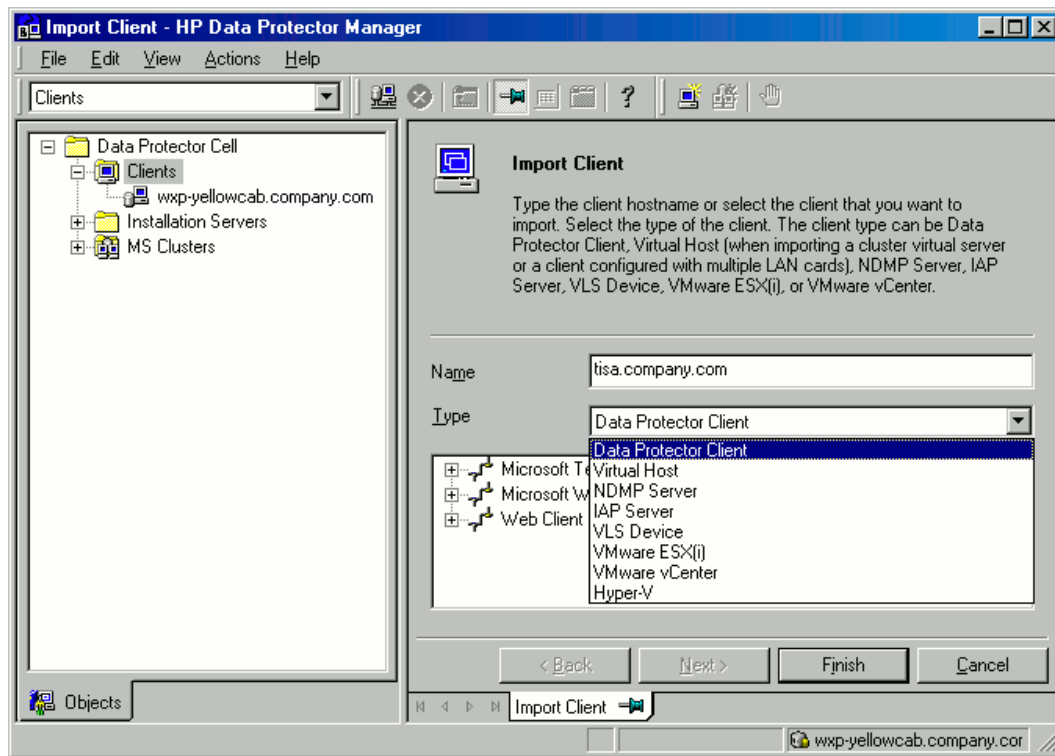
recommended to protect the clients from access by unwanted cell authorities. See ["Securing clients"](#) .

### How to import?

You import a client system using the graphical user interface by performing the following steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Import Client**.
3. Type the name of the client or browse the network to select the client (on Windows GUI only) you want to import. See [" Importing a client to the cell "](#) .

**Figure 31: Importing a client to the cell**



If you are importing a client configured with multiple LAN cards, select the **Virtual Host** option. With this option you must import all names of the same system.

If you are importing an NDMP client, select the **NDMP Server** option and click **Next**. Specify the information about the NDMP Server.

If you are importing an HP OpenVMS client, type the TCP/IP name of the OpenVMS client in the Name text box.

If you are importing a VLS device, select the **VLS Device** option and click **Next**. Specify the information about the VLS device.

If you are importing a Microsoft Exchange Server DAG virtual host for the Data Protector Microsoft Exchange Server 2010 integration, select **Virtual Host**.

If you are importing a client for the Data Protector Virtual Environment integration, select either **VMware ESX(i)** for a standalone VMware ESX(i) Server system, **VMware vCenter** for a VMware vCenter Server system, or **Hyper-V** for a Microsoft Hyper-V system. Click **Next** and specify login credentials.

Click **Finish** to import the client.

The name of the imported client is displayed in the Results Area.

## Importing an Installation Server to a cell

### *When to add?*

An Installation Server must be added to a cell in the following circumstances:

- If it is installed as an independent UNIX Installation Server, for example, it is not installed on a Cell Manager.

In this case, it will not be possible to remotely install any clients within a cell until the Installation Server has been added to that cell.

- If it is installed on a Cell Manager, but you also want to use it to perform remote installations in another cell. It must then be added to the other cell (using the GUI connected to the Cell Manager of the other cell).

Unlike a client, an Installation Server can be a member of more than one cell. Therefore it does not have to be deleted (exported) from one cell before it can be added (imported) to another cell.

### *How to add?*

The process for importing an Installation Server is similar to that for importing a client. The task is performed using the Data Protector GUI (connected to the Cell Manager of the cell to which the Installation Server is to be added) by performing the following steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Installation Servers**, and then click **Import Installation Server** to start the wizard. See "[Importing a client to the cell](#)".
3. Enter or select the name of the system that you want to import. Click **Finish** to import the Installation Server.

## Importing a cluster-aware client to a cell

After you have locally installed the Data Protector software on a cluster-aware client, import the virtual server representing the cluster-aware client to the Data Protector cell.

## Prerequisites

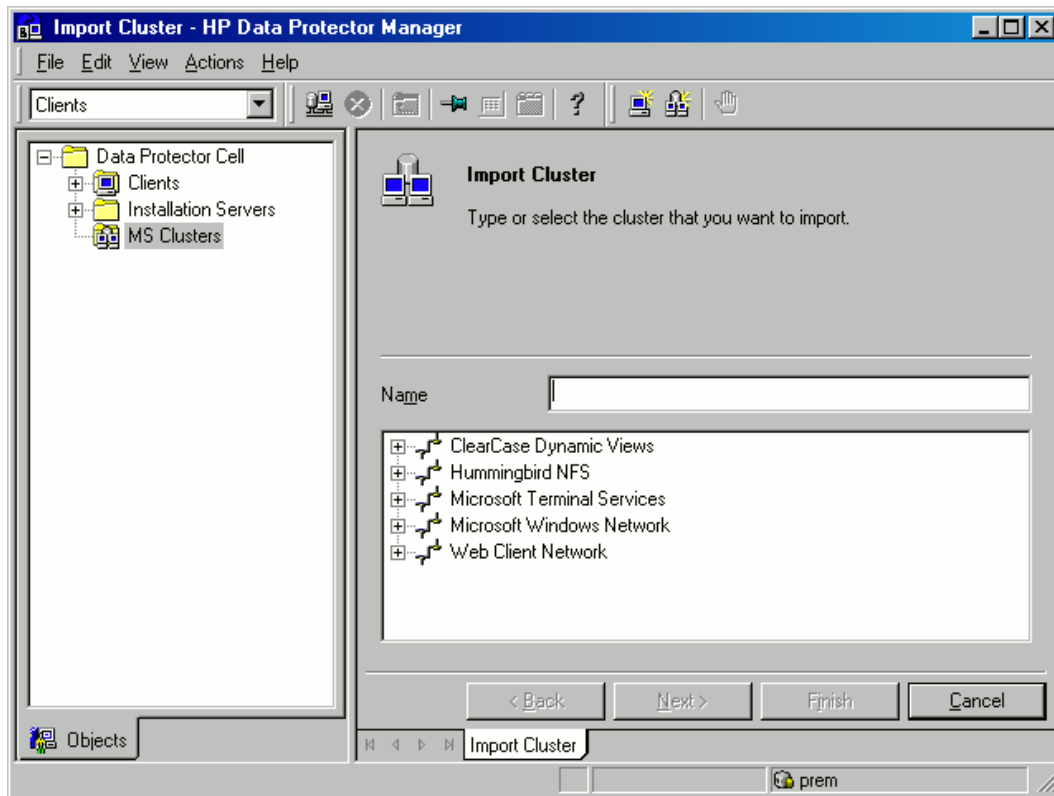
- Data Protector must be installed on all cluster nodes.
- All cluster packages must be running within the cluster.

## Microsoft Cluster Server

To import a Microsoft Cluster Server client to the Data Protector cell, proceed as follows:

1. In the Data Protector Manager, switch to the Clients context.
2. In the scoping pane, right-click **MS Clusters** and click **Import Cluster**.
3. Type the name of the virtual server representing the cluster client to be imported or browse the network to select the virtual server. See "[Importing a Microsoft Cluster Server client to a cell](#)".

**Figure 32: Importing a Microsoft Cluster Server client to a cell**



4. Click **Finish** to import the cluster client.

**Tip:** To import a specific cluster node or a virtual server, right click its cluster in the Scoping Pane and click **Import Cluster Node** or **Import Cluster Virtual Server**.



## Other clusters

### Procedure

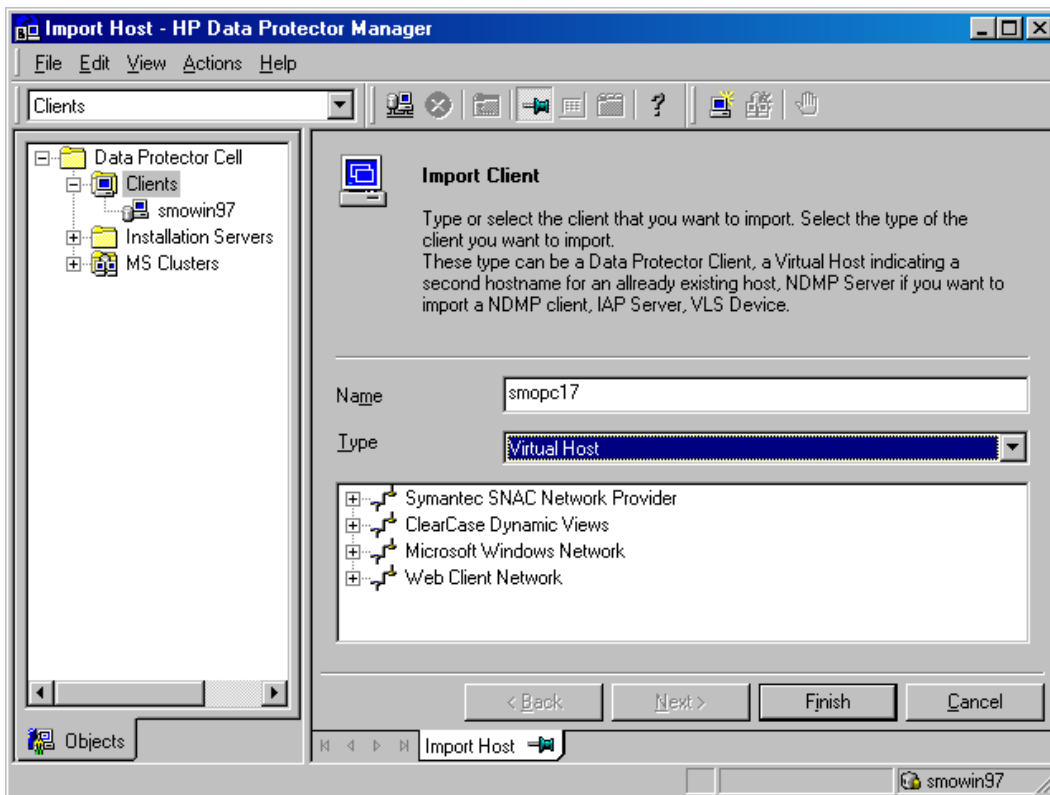
To import an HP Serviceguard, Veritas, or IBM HACMP Cluster client to the Data Protector cell, proceed as follows:

1. In the Data Protector Manager, switch to the Clients context.
2. In the Scoping Pane, right-click **Clients** and click **Import Client**.
3. Type the hostname of the virtual server as specified in the application cluster package, or browse the network to select the virtual server (on Windows GUI only) you want to import.

Select the **Virtual Host** option to indicate that this is a cluster virtual server. See "[Importing an HP Serviceguard or Veritas client to a cell](#)".

4. Click **Finish** to import the virtual server.

**Figure 33: Importing an HP Serviceguard or Veritas client to a cell**



**Tip:** To configure backups of data on the local disks of the cluster nodes, you need to import the cluster nodes representing the Data Protector clients. For the procedure, see "[Importing clients to a cell](#)".

## Exporting clients from a cell

**Exporting** a client from a Data Protector cell means removing its references from the IDB on the Cell Manager without uninstalling the software from the client. This can be done using the Data Protector GUI.

You may want to use the export functionality if you:

- Want to move a client to another cell
- Want to remove a client from the Data Protector cell configuration which is no longer part of the network
- Want to resolve problems related to licensing

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

### *Prerequisites*

Before you export a client, check the following:

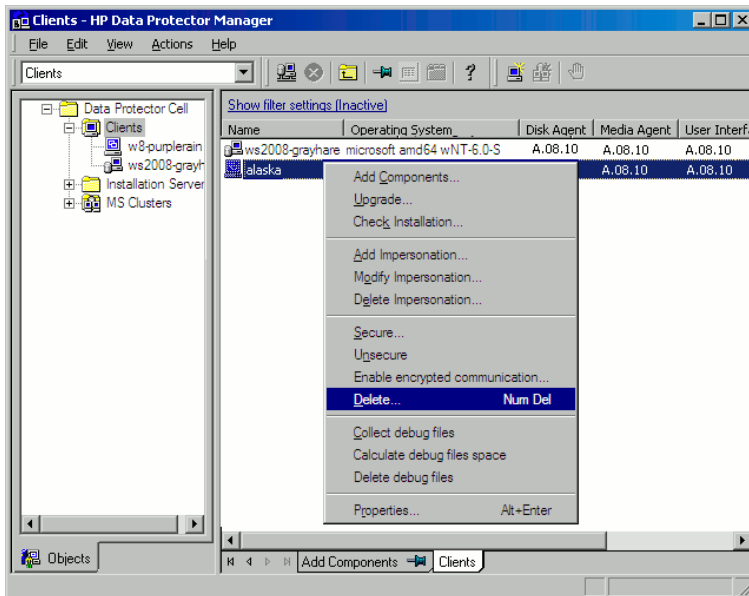
- All the occurrences of the client have been removed from backup specifications. Otherwise, Data Protector will try to back up unknown clients and this part of the backup specification will fail. For instructions on how to modify backup specifications, see the *HP Data Protector Help* index: "modifying, backup specification".
- The client does not have any connected and configured backup devices or disk arrays. Once the system is exported, Data Protector can no longer use its backup devices or disk arrays in the original cell.

### *How to export?*

You export a client using the Data Protector GUI by performing these steps:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, click **Clients**, right-click the client system that you want to export, and then click **Delete**. See "[Exporting a client system](#)".

**Figure 34: Exporting a client system**



3. You will be asked whether you want to uninstall Data Protector software as well. Click **No** to export the client, and then click **Finish**.

The client will be removed from the list in the Results Area.

**Note:** You cannot export or delete a Data Protector client if the Cell Manager is installed on the same system as the client you would like to export. However, you can export the clients from systems where only the client and Installation Server are installed. In this case, Installation Server is also removed from the cell.

### *Microsoft Cluster Server clients*

To export a Microsoft Cluster Server client from the Data Protector cell, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **MS Clusters**, right-click the cluster client that you want to export, and then click **Delete**.
3. You are asked if you also want to uninstall the Data Protector software. Click **No** to only export the cluster client.

The cluster client will be removed from the list in the Results Area.

**Tip:** To export a specific cluster node or a virtual server, right-click the cluster node or virtual server in the Scoping Pane and click **Delete**.

## Security considerations

This section describes the security elements of Data Protector. It describes the advanced settings that can be used to enhance the security of Data Protector with prerequisites and considerations that have to be taken into account.

Since enhancing security in an entire environment requires additional effort, many security features cannot be enabled by default.

The considerations described in this chapter apply not only when the security settings are changed, but must also be followed when configuring new users, adding clients, configuring application agents, or making any other changes these considerations apply to. Any changes in the security settings can have cell-wide implications and should be carefully planned.

## Security layers

Security has to be planned, tested and implemented on different security-critical layers to ensure the secure operation of Data Protector. Such layers are Data Protector clients, Cell Manager, and users. This section explains how to configure security on each of these layers.

### *Client security*

Data Protector agents installed on clients in the cell provide numerous powerful capabilities, like access to all the data on the system. It is important that these capabilities are available only to the processes running on **cell authorities** (Cell Manager and Installation Server), and that all other requests are rejected.

Before securing clients, it is important to determine a list of trusted hosts. This list must include:

- Cell Manager
- Relevant Installation Servers
- For some clients also a list of clients that will access the robotics remotely.

**Important:** The list must contain all possible hostnames (or IP addresses) where connections can come from. Multiple hostnames may be needed if any of the above clients is multihomed (has multiple network adapters and/or multiple IP addresses) or is a cluster.

If the DNS configuration in the cell is not uniform, additional considerations may apply. For more information, see "[Securing clients](#)".

While it may not always be necessary to secure each and every client in the cell, it is important that the computers that other clients will trust are secured themselves:

- Cell Manager / Manager-of-Managers
- Installation Servers
- Media Agent clients

**Note:** User interface clients do not need to be added to the list of trusted clients. Depending on the user rights, you can either use the GUI to access the complete Data Protector functionality or to access only specific contexts.

## Data Protector users

Consider the following important aspects when configuring Data Protector users:

- Some user rights are very powerful. For example, the `User configuration` and `Clients configuration` user rights enable the user to change the security settings. `Restore to other clients` user right is also very powerful, especially if (but not only if) combined with either the `Back up as root` or `Restore as root` user right.
- Even less powerful user rights bear an inherent risk associated with them. Data Protector can be configured to restrict certain user rights to reduce these risks. These settings are described later on in this chapter. See also "[Start backup specification user right](#)".
- Data Protector comes with only a few predefined user groups. It is recommended to define specific groups for each type of user in the Data Protector environment to minimize the set of rights assigned to them.
- In addition to assigning user rights by user group membership, you may want to further restrict actions of certain user groups to only specific systems of the Data Protector cell. You can implement this policy by configuring the `user_restrictions` file. For more information, see the *HP Data Protector Help*.
- The configuration of users is connected with user validation (see "[Strict hostname checking](#)"). Enhanced validation can be worthless without careful user configuration and the other way round - even the most careful user configuration can be worked around without the enhanced validation.
- It is important that there are no "weak" users in the Data Protector user list.

**Note:** The host part of a user specification is the strong part (especially with the enhanced validation), while user and group parts cannot be verified reliably. Any user with powerful user rights should be configured for the specific client they will use for Data Protector administration. If multiple clients are used, an entry should be added for each client, rather than specifying such a user as `user, group, <Any>`. Non-trusted users should not be allowed to log on to any of those systems.

For details on configuring users, see the *HP Data Protector Help* index: "configuring, users".

## Cell Manager security

Cell Manager security is important because the Cell Manager has access to all clients and all data in the cell.

Security of the Cell Manager can be enhanced via the strict hostname checking functionality. However, it is important that the Cell Manager is also secured as a client and that Data Protector users are configured carefully.

While it may not always be necessary to secure each and every client in the cell, it is important that the computers that other clients will trust are secured themselves. These are besides the Cell Manager also the Installation Server and Media Agent clients.

Security of a Cell Manager and subsequently all clients in the Data Protector cell can be additionally enhanced by enabling encrypted control communication.

For details, see the ["Strict hostname checking"](#) , ["Securing clients"](#) , and ["Security considerations"](#) .

## Other security aspects

There are also some other security related aspects you should consider:

- Users should not have access to any of the trusted clients (Cell Manager, Installation Servers, MA, and robotics clients). Even granting anonymous log on or ftp access could introduce a serious risk to overall security.
- Media and tape libraries (and the clients they are connected to) must be physically protected from unauthorized or untrusted personnel.
- During backup, restore, object or media copying, object consolidation or object verification, data is generally transferred via network. If sufficient separation from the untrusted network cannot be achieved with network segmentation, use locally attached devices, Data Protector encryption techniques, or a custom encoding library. Note that after changing the encoding library, you should perform a full backup.
- In addition, enabling encrypted control communication in a Data Protector cell helps preventing unauthorized access to your system and enhances security.

For other security related aspects, see the *HP Data Protector Help* and the *HP Data Protector Concepts Guide*.

## Securing clients

After you have installed Data Protector clients and imported them to a cell, it is highly recommended to protect the clients from access by unwanted clients.

Data Protector allows you to specify from which cell authorities (Cell Manager, MoM, and Installation Servers) a client will accept requests on the Data Protector port 5555. Consequently, other computers will not be able to access such a client. See ["Client security"](#) .

**Note:** Clients that will access library robotics remotely should be added to the cell authorities list for the library robotics clients.

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

### Consider exceptional situations

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

- A cell authority has several LAN cards and several IP addresses/client names.
- The Cell Manager is cluster-aware.
- A tape library has robotics configured on a separate (or dedicated) system.

Data Protector lets you specify not only one but a list of systems that are explicitly authorized to connect as a cell authority to the client. To avoid failure, prepare in advance such a list of all possible valid client names for alternate cell authorities.

The list should include:

- All additional client names (for all LAN cards) of the cell authority.
- Client names of all cluster nodes where the Cell Manager might failover, as well as a cluster virtual server hostname.
- The target system name to which a cell authority will be moved in case of a total hardware failure of the cell authority. This target system has to be defined in the disaster recovery strategy.
- For clients that are allowed to access a client that controls the robotics of a library, all clients that use the drives of that library.

The concept of allowing and denying access can be applied to all systems with Data Protector installed. For example, you can allow or deny access of Cell Managers to clients, Cell Managers to Cell Managers, Installation Servers to clients, or clients to clients.

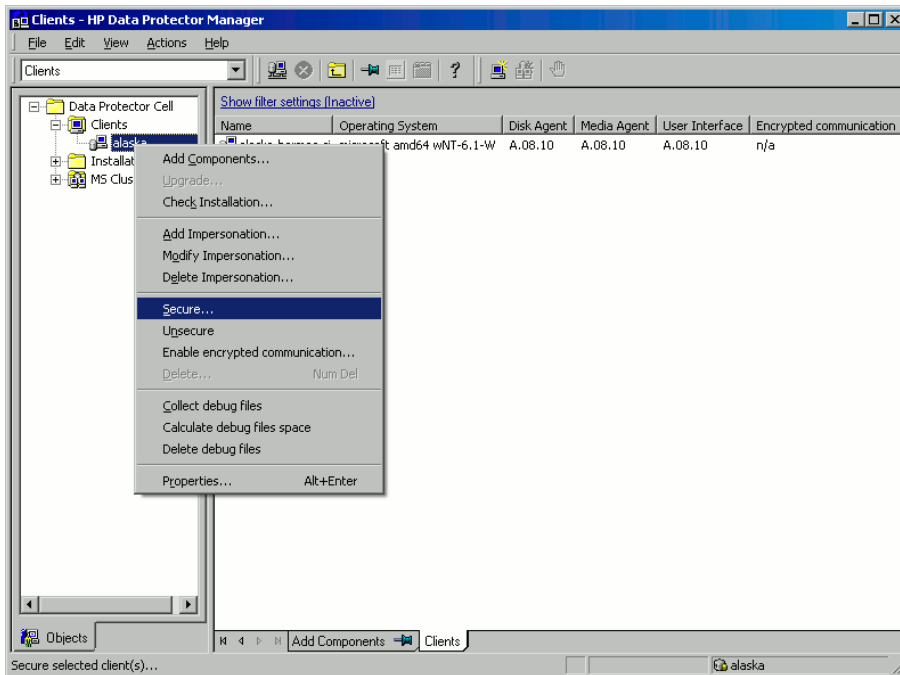
**Note:** If an Installation Server residing on a system other than the Cell Manager is not added to the list of allowed clients, it will not have access to a secured client. In this case, the operations dependent on the Installation Server (such as checking installation, adding components and removing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

### *How to secure a client*

To enable verification of a cell authority on the client side (secure a client), perform the following steps in the Data Protector GUI:

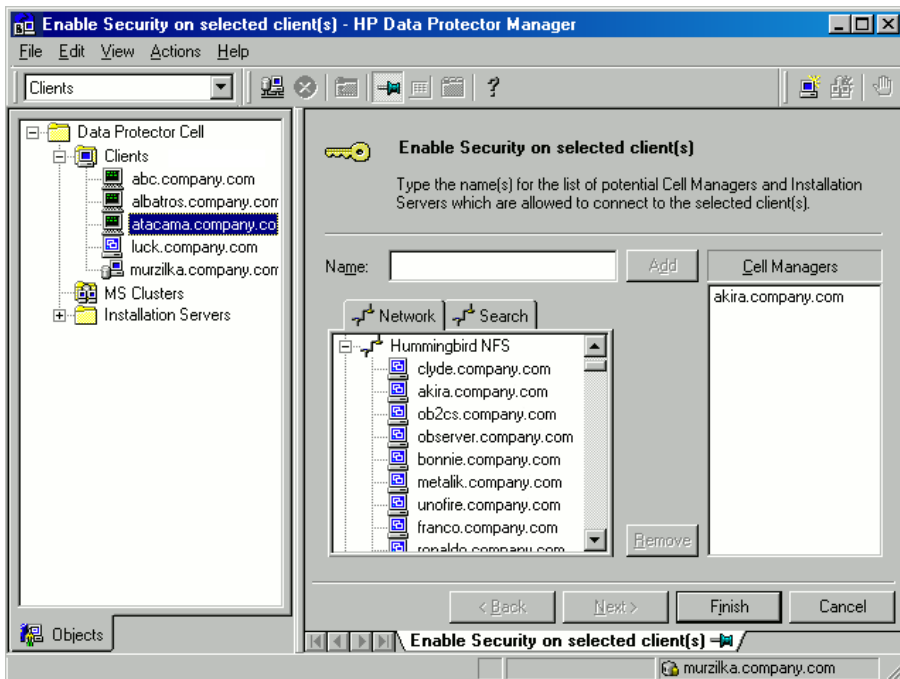
1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand Clients, right-click the client(s) you want to secure, and click **Secure**. See "[Securing a client](#)".

**Figure 35: Securing a client**



3. Type the names of the systems that will be allowed to access the selected client(s) or search for the systems using the Network tab (on Windows systems only) or Search tab. Click **Add** to add each system to the list. See " [Enabling security on selected client\(s\)](#) " .

**Figure 36: Enabling security on selected client(s)**





The Cell Manager is automatically provided with access and added to the list of trusted clients. You cannot exclude the Cell Manager from the list.

4. Click **Finish** to add the selected systems to the `allow_hosts` file.

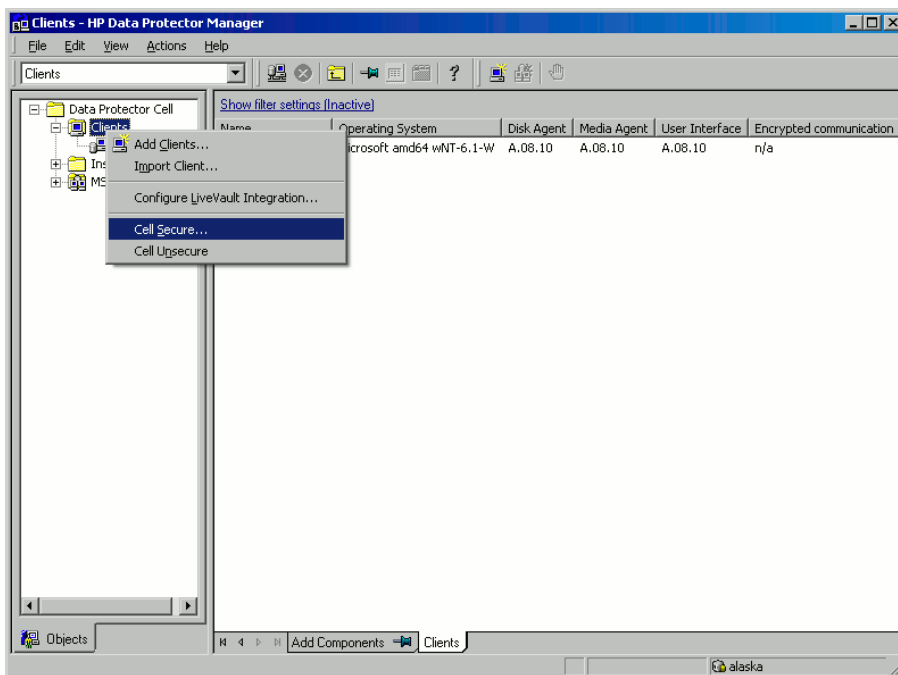
### *What happens?*

Clients will verify the source for each request from other clients and allow only those requests received from clients selected in the Enable Security on selected client(s) window. These clients are listed in the `allow_hosts` file. If a request is denied, the event is logged to the `inet.log` file residing in the default Data Protector log files directory.

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

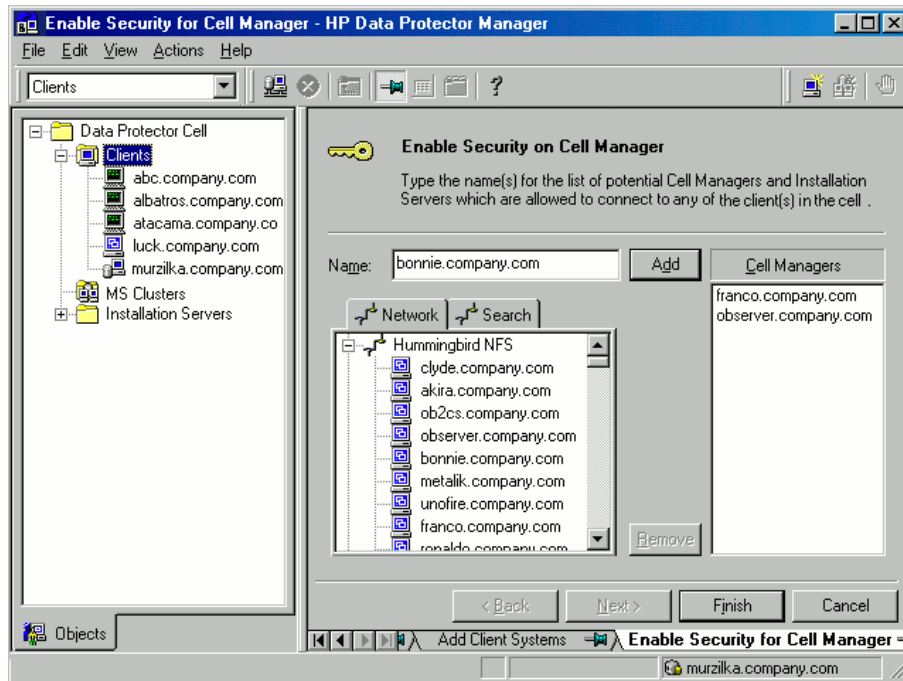
1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Cell Secure**. See "[Securing a cell](#)".

**Figure 37: Securing a cell**



3. Type the names of the systems that will be allowed to access all clients in the cell or search for the systems using the Network (on Windows GUI only) or Search tabs. Click **Add** to add each system to the list. See "[Enabling security for all clients in the cell](#)".

**Figure 38: Enabling security for all clients in the cell**



4. Click **Finish** to add the selected systems to the `allow_hosts` file.

### *What happens?*

Clients will verify the source of each request and allow only those requests received from clients selected in the Enable Security on Cell Manager window. These clients are listed in the `allow_hosts` file. If a request is denied, the event is logged to the `inet.log` file residing in the default Data Protector log files directory.

When you secure an entire cell, all clients residing in this cell at the time are secured. When you add new clients to the cell, you should also secure them.

### *How to remove security*

To remove security from the selected system(s), perform the following steps in the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click the client(s) from which you want to remove security and click **Unsecure**.
3. Click **Yes** to confirm that you allow access to the selected client(s).

To remove security from all the clients in the cell, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Cell Unsecure**.

3. Click **Yes** to confirm that you allow access to all client(s) in your cell.

## ***The allow\_hosts and deny\_hosts files***

When you secure a client, the client names of the systems allowed to access a client are written to the `allow_hosts` file. You can also explicitly deny access to a client from certain computers by adding their names to the `deny_hosts` file. These files are located in the default Data Protector client configuration directory.

Specify each client name in a separate line.

**Note:** If you accidentally lock out a client, you can manually edit (or delete) the `allow_hosts` file on this client.

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

## ***Excessive logging to the inet.log file***

If the clients are not secured and the Cell Manager is configured in the HP Serviceguard environment or has multiple names or IP numbers, the `inet.log` file may contain many entries of the following type:

A request 0 came from host *name.company.com* which is not a Cell Manager of this client.

This happens because the client, which is not secured, recognizes only the primary hostname of the Cell Manager. Requests from any other clients are allowed, but logged to the `inet.log` file.

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

Securing clients can be used as a workaround to prevent unnecessary entries in `inet.log` files. However, all possible client names for the Cell Manager should be listed in the `allow_hosts` file on each client. This enables access to the client also in case of a failover.

If this workaround is for any reason not possible in your environment, you can secure the clients and specify `*` as an IP address range for the systems you want to allow access. This means that your clients will accept requests from all systems (any IP address) and will practically not be secured, but you will still resolve the excessive logging issue.

## **Strict hostname checking**

By default, the Cell Manager uses a relatively simple method for validating users. It uses the hostname as known by the client where a user interface or an application agent is started. This method is easier to configure and it provides a reasonable level of security in environments where security is considered as “advisory” (for example, malicious attacks are not expected).

The strict hostname checking setting on the other hand, provides enhanced validation of users. The validation uses the hostname as it is resolved by the Cell Manager using the reverse DNS lookup from the IP obtained from the connection. This imposes the following limitations and considerations:

## *Limitations*

- IP based validation of users can only be as strong as the anti-spoof protection in the network. The security designer must determine whether the existing network provides a sufficient degree of anti-spoof safety for the particular security requirements. Anti-spoof protection can be added by segmenting the network with firewalls, routers, VPN, and such.
- The separation of users within a certain client is not as strong as the separation between clients. In a high security environment, one must not mix regular and powerful users within the same client.
- Hosts that are used in user specifications cannot be configured to use DHCP, unless they are bound to a fixed IP and configured in the DNS.

Be aware of the limitations in order to correctly assess the degree of safety that can be achieved with the strict hostname checking.

## *Hostname resolution*

The hostname that Data Protector uses for validation may differ between the default user validation and strict hostname checking in the following situations:

- Reverse DNS lookup returns a different hostname. This can be either intentional or can indicate misconfiguration of either the client or the reverse DNS table.
- The client is multihomed (has multiple network adapters and/or multiple IP addresses). Whether this consideration applies to a specific multihomed client, depends on its role in the network and on the way it is configured in the DNS.
- The client is a cluster.

The nature of checks that are enabled with this setting may require reconfiguration of Data Protector users. Existing specifications of Data Protector users must be checked to see if they could be affected by any of the above reasons. Depending on the situation, existing specifications may need to be changed or new specifications added to account for all the possible IPs from which the connections can come.

Note that users have to be reconfigured also when reverting back to the default user validation, if you had to modify user specifications when you enabled the strict hostname checking. It is therefore recommended to decide which user validation you would like to use and keep using it.

A prerequisite for a reliable reverse DNS lookup is a secure DNS server. You must prevent physical access and log on to all unauthorized personnel.

By configuring users with IPs instead of hostnames, you can avoid some DNS related validation problems, but such configuration is more difficult to maintain.

## *Requirements*

The enhanced validation does not automatically grant access for certain internal connections. Therefore, when this validation is used, a new user must be added for each of the following:

- Any application agent (OB2BAR) on Windows clients. For Windows clients, it is required to add the user SYSTEM, NT AUTHORITY, *client* for each client where an application agent is installed. Note that if Inet on a certain client is configured to use a specific account, this account must have already been

configured. For more information, see the *HP Data Protector Help* index: “strict hostname checking”.

- If you are using Web Reporting, user `java`, `applet`, *Hostname* must be added for every hostname from where Web Reporting will be used. Note that for full Web Reporting functionality the users must be in the `admin` group. Therefore, these clients must be trusted. Also, before making any data or functionality of Web Reporting available to other users (for example, via a web server), consider the security implications of making such data generally available.

For detailed information on user configuration, see the *HP Data Protector Help* index: “configuring, users”.

## Enabling the feature

To enable the strict hostname checking, set the `StrictSecurityFlags` global option to `0x0001`.

For more information about the global options, see the *HP Data Protector Troubleshooting Guide*.

## Managing encrypted control communication

Data Protector encrypted control communication helps in preventing unauthorized access to clients in Data Protector Cell Managers. Using the Data Protector GUI or the CLI, you can remotely enable encrypted control communication for all clients in the Data Protector cell.

## Considerations

- StoreOnce Software may fail if the certificate key length is 512 bits or less when the encrypted control communication is enabled. Therefore, use a certificate that has a key length of more than 512 bits.

**Note:** When using the Encrypted Control Communication (ECC) in a cell, ensure that ECC is enabled on the Installation Server also. Otherwise, the Installation Server will not communicate with the clients that use ECC.

## Enabling encrypted control communication

You can enable encrypted control communication on the following:

In a cell: This includes the Cell Manager and individual clients. You do not need to enable encrypted control communication on all clients.

In a MoM environment: This includes all cells that are a part of the MoM environment.

**Note:** Ensure that the Universal Standard Time (UST) is the same on all clients in the cell and the Cell Manager.

### Enabling encrypted control communication for all clients in the cell, using the CLI:

Execute the following command: `omnicc -encryption -enable -all`

If encrypted control communication has been disabled on the Cell Manager, then it is not possible to enable encrypted control communication for a client in a cell.

To enable encrypted communication only on the Cell Manager, run:

```
omnicc -encryption -enable <CellManager_name>
```

To enable encrypted communication on the Cell Manager (if it has not yet been enabled) and all clients in the cell, run:

```
omnicc -encryption -enable -all
```

For details, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

### ***Enabling encrypted control communication for all cells in a MoM environment, using the CLI:***

It is recommended that you first disable encrypted control communication on all the Cell Managers (including the clients of the Cell Managers) before importing them to the MoM environment, otherwise the Cell Managers cannot communicate and the creation of the MoM environment will not complete. After creating the MoM environment, proceed to enable encrypted control communication in the MoM environment.

Enabling MoM encryption only works:

1. If all the Cell Managers are upgraded to the latest patch. Some clients in Cell Managers can be older, but disabling will not work in this case.
2. If the MoM server and the other Cell Managers can connect and communicate:
  - Encrypted control communication has not been enabled on the MoM server and all the other Cell Managers
  - or
  - Encrypted control communication has been enabled with Data Protector generated certificates on the MoM server and on some or all of the Cell Managers, which are a part of the MoM environment. Additionally, trust has been established between the MoM server and member servers.

#### **Establishing trust**

To enable encrypted control communication without disabling the earlier encrypted control communication, the MoM server has to be able to communicate with the other (member) servers. Before MoM can be created, trust has to be established between the MoM server and the member servers.

**Note:** Save the initial state of the files so that you can revert the changes in case of an error.

To establish trust between the Cell Managers, do the following:

1. Get the CA certificate for MoM server.
  - a. On the MoM server, open the MoM server trusted certificates file `Data_Protector_program_data/config/client/config` and find the line `trusted_certificates_file=`

For example, trusted\_certificates\_  
file='C:\ProgramData\OmniBack\config\client\certificates\<CMhostname>\_  
cacert.pem';

- b. Open the file client\certificates\<CMhostname>\_cacert.pem file in a text editor (unless it has been modified, the standard file name format is <CMhostname>\_cacert.pem ) and copy its contents (MoM server CA certificate).

2. Get the CA certificate for server1.

- a. On server 1 open the server 1 trusted certificates file Data\_Protector\_program\_data/config/client/config and find the line trusted\_certificates\_file=

For example, trusted\_certificates\_  
file='C:\ProgramData\OmniBack\config\client\certificates\<CMhostname>\_  
cacert.pem'

- b. Open the file client\certificates\<CMhostname>\_cacert.pem file in a text editor (unless it has been modified, the standard file name format is <CMhostname>\_cacert.pem ) and copy its contents (server 1 CA certificate).

3. Edit both trusted certificate files '<CMhostname>\_cacert.pem' to include all the certificates that exist on each server that needs to be trusted. In this example, the MoM Server and Server1 need to establish trust with each other.

- a. On the MoM server, open the MoM server trusted certificates file and include the server 1 CA certificate to the file.
- b. On server 1, open the server 1 trusted certificates file and include the MoM server CA certificate to the file.

4. If there are more servers (server 2) and so on. Repeat steps 2 and 3 for every server, to be added to the MoM environment.

The Cell Manager trusted certificate file is initially a copy of Data\_Protector\_program\_data/config/server/certificates/<CMhostname>\_cacert.pem

To enable encrypted control communication, in the MoM environment run omnicc -encryption -enable\_mom{CSHostname1 [CSHostName2...] [-all]} [-recreate\_cert]

For more details, see the omnicc command in the *HP Data Protector Command Line Interface Reference*.

**Enabling encrypted control communication for all clients in the cell, using the GUI:**

**Note:** You must first enable encrypted control communication on a Cell Manager then on the clients in the cell.

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.

3. Right-click the client that you want to modify and select **Enable encrypted control communication**. In case of multiple clients, select one or more clients for which you want to enable encrypted control communication.

**Note:** If you select enable encrypted communication option for a client whose Cell Manager is not yet encrypted, you are prompted with a message “You can change encrypted communication configuration only from a client with encrypted communication enabled or the Cell Manager” and the options on that page become unavailable.

4. In the Connection tab, the **Encrypted control communication** option is selected by default.
5. Select **Use Existing certificates**, if you need to use the existing certificates on the Cell Manager.
6. Click **Apply** to save the changes.

**Note:** You can also enable encrypted control communication in the following scenarios:  
Adding or importing: clients to a cell.  
Editing the Properties of a client or Cell Manager.

### *Enabling encrypted control communication with manual distribution of certificates and keys*

You can enable encrypted control communication between the clients in the Data Protector cell using the custom keys and certificates.

This section provides details on manual distribution of certificates and keys.

**Note:** Follow the manual steps carefully to avoid Data Protector communication issues.

## ***Enabling encrypted control communication with manual distribution of certificates and keys***

You can enable encrypted control communication between the clients in the Data Protector cell using the custom keys and certificates.

This section provides details on manual distribution of certificates and keys.

**Note:** Follow the manual steps carefully to avoid Data Protector communication issues.

### *Encrypted control communication with manual distribution of certificates*

This section covers details on enabling encrypted control communication by manually distributing certificates, instead of using the Data Protector distribution of certificates.

#### **Considerations**



- Store certificates and keys in PEM format without any password.
- Do not use existing certificate names for new certificates.

The certificate naming convention is as follows:

<CMhost>\_cacert-C.pem for the Certificate authority PEM file.

<host>\_key-C.pem for the Host private key PEM file.

<host>\_cert-C.pem for the Host certificate PEM file.

**Note:** This is a sample of the certificate naming convention, which can be changed based on user preferences.

To enable encrypted control communication starting with the Cell Manager, perform the following steps:

1. Place certificates in the following certificate directory on the client:

Windows 7, Windows Server 2008, and later:

Data\_Protector\_program\_data\Config\client\certificates

Older Windows systems:

Data\_Protector\_home\Config\client\certificates

HP-UX and Linux systems:

/etc/opt/omni/client/certificates

Other UNIX systems:

/usr/omni/client/certificates

2. Create a config file with the following:

```
encryption={  
  enabled=1;  
  certificate_chain_file='<client certificate directory>/<host>_cert-C.pem';  
  private_key_file='<client certificate directory>/<host>_key-C.pem';  
  trusted_certificates_file='<client certificate directory>/<CMhost>_cacert-C.pem';  
};
```

The created config file must be placed in the following directory:

Windows 7, Windows Server 2008, and later:

Data\_Protector\_program\_data\Config\client\config

Older Windows systems:

Data\_Protector\_home\Config\client\config

HP-UX and Linux systems:

/etc/opt/omni/client/config

Other UNIX systems:

/usr/omni/client/config

3. Create or modify the config file in the Server directory on the Cell Manager of the client.

Perform the following steps:

- a. Create or search for the following config file in the Server directory:

Windows 7, Windows Server 2008 and later:

Data\_Protector\_program\_data\Config\Server\config

HP-UX and Linux systems:

/etc/opt/omni/server/config

- b. Add or modify the following host configuration entry:

```
<host>={  
  encryption={  
    enabled=1;  
    certificate_chain_file='<client certificate directory>/<host>_cert-C.pem';  
    private_key_file='<client certificate directory>/<host>_key-C.pem';  
    trusted_certificates_file='<client certificate directory>/<CMhost>_cacert-C.pem';  
  };  
};
```

**Note:** The host configuration file entry details are used by the Data Protector GUI.

4. After the encrypted control communication is enabled on the Cell Manager, the clients that connect to

the Cell Manager requires a trusted certificate or needs to be added to the security exception list. You can add all the clients that needs to contact the Cell Manager to the security exception list by editing the config file in the Server directory as follows:

```
<client1>={  
encryption={  
exception=1;  
};  
};
```

(OR)

You can add the client to the exception list by issuing the following command:

```
omnicc -encryption -add_exception <client1>
```

5. Upload the PEM files into the following server certificate directory to view the certificate content in the Clients context in the Data Protector GUI:

Windows 7, Windows Server 2008 and later:

Data\_Protector\_program\_data\Config\Server\certificates

HP-UX and Linux systems:

/etc/opt/omni/server/certificates

**Note:** In the Data Protector GUI client context, a lock icon is displayed on the host. The flag -encryption in cell\_info file handles this lock functionality.

To add the lock, perform the following steps:

- a. Navigate to the following cell directory:

Windows 7, Windows Server 2008 and later:

Data\_Protector\_program\_data\Config\Server\cell\cell\_info

HP-UX and Linux systems:

/etc/opt/omni/server/cell/cell\_info

**Note:** The cell\_info file lists all clients.

- b. Modify the line in the cell\_info file for the client with encrypted control communication

enabled by adding `-encryption 1` as shown:

```
-host "computer.company.com" -os "gpl i686 linux-2.6.18-8.el5" -core  
A.08.10 -da A.08.10 -ma A.08.10 -encryption 1
```

6. Repeat steps 1, 2, 3, and 5 for clients you want to enable secure communication.

**Note:** If Encrypted Control Communication (ECC) is applied on hosts with Physical and Virtual clients, the ECC certificates are applicable for both clients.

**Important:**

- It is recommended to use the user generated keys and certificates instead of the default HP Data Protector certificate `hdpcert.pem`.
- Remote clients must consider the manual steps for distribution of certificates and keys, instead of enabling encrypted control communication from the Data Protector GUI or CLI.

For more information, see ["Enabling encrypted control communication with manual distribution of certificates and keys"](#).

### *What happens?*

Encryption is enabled on a per-client basis, which means that encryption is either enabled or disabled for all control communication with the selected client.

### *How to add a client to the Security Exceptions list*

Clients that for some reason are not supposed to communicate confidentially can be placed in a Cell Manager exception list, which allows particular clients to communicate in non-encrypted mode.

To add a client to the Security Exceptions list, perform the following steps in the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
3. Click the Cell Manager that you want to modify.
4. Type the names of the systems that will be added to the Security Exceptions list in the cell or search for systems using the **Network** (on Windows GUI only) or **Search** tabs.
5. Click **Add** to add systems to the list, then click **Apply** to save the changes.

### *The server configuration file*

The clients that are accepted in a plain text mode are written to the server configuration file, located on the Cell Manager in the directory:

**Windows systems:** `Data_Protector_program_data\Config\server\config`

**HP-UX and Linux systems:** `/etc/opt/omni/server/config`

To remove a system from the Security Exceptions list, perform steps 1 to 4 and click **Remove**, then click **Apply** to save the changes.

## Encrypted control communication with user-created certificates

This section is applicable for users who want to generate the certificates themselves.

### Encrypted control communication with certificates created manually

The earlier versions of Data Protector did not create certificates automatically, you had to create the certificates and point Data Protector to the certificate files.

If you generate the certificates manually, then you have to place the certificates in the following certificates directory on the Cell Manager :

Windows: `Data_Protector_program_data\Omniback\Config\Server\certificates` ;

UNIX: `/etc/opt/omni/server/certificates` directory.

In addition, the certificates have to comply with the following naming convention.

`<computer.company.com>_cert.pem` for the certificate

`<computer.company.com >_key.pem` for the private key

`<CellManager.company.com>_cacert.pem` for the trusted certificate

When you enable encryption (while adding / importing / editing properties of a client or a Cell Manager), these certificates are used by Data Protector. When encryption is enabled, ensure that you select the **Use existing certificates** option from the Data Protector GUI otherwise the existing certificates will get overwritten.

Note that you can also generate the certificates to be used for encrypted control communication, using the script `omnigencert.pl` and then select **Use existing certificates** option from the Data Protector GUI. This enables faster encryption of the clients.

To create the certificates for encrypted control communication use the script `omnigencert.pl` , and run:

```
omnigencert.pl -pem_client -user_id <computer.company.com> [-recreate]
```

The `-recreate` option overwrites the existing certificates, if they exist.

**Note:** The `omnigencert.pl` script can also be used for generating certificates for other purposes.

### Encrypted control communication with certificates created automatically

If you need to generate certificates automatically, and as per your specification, then you can create a Perl script file `gencert.pl` and place it in the following location:

**ws:** `%Data_Protector_home%\bin`

**UNIX:** `/opt/omni/lbin`

Data Protector starts using the `gencert.pl` instead of the `omnigencert.pl` script after it is added to the specified folder. You can enable encryption using the Data Protector GUI or CLI. This `gencert.pl` script must comply with the following certificate naming conventions:

`<computer.company.com>_cert.pem` for the certificate

`<computer.company.com >_key.pem` for the private key

`<CellManager.company.com>_cacert.pem` for the trusted certificate

The `gencert.pl` script should be able to accept the following parameters:

```
gencert.pl-pem_client -user_id <computer.company.com> [-recreate]
```

### Replacing CA certificates in an encrypted control communication environment

It is possible to replace certificates with the ones signed by a different CA. If you need to replace the CA and the certificates in the cell you must perform the following steps:

1. Concatenate the CA certificates:

Copy the new CA certificate to the following path:

- Windows - `Data_Protector_program_data\Omniback\Config\Server\certificates` and
- UNIX - `/etc/opt/omni/server/certificates`

To update all the clients in the cell to also trust this new CA, run the following command:

```
omnicc -encryption -update_trust -all -trust newCA.pem
```

2. Recreate the certificates:

You can recreate the certificates either manually or use Data Protector to trigger certificate generation. Data Protector triggers `omnigencert.pl` or `gencert.pl` (if it exists) for creating certificates when you run the following command:

```
omnicc -encryption -enable -all -recreate_cert
```

3. Update the clients to trust only the new CA:

```
omnicc -encryption -update_trust -all -trust newCA.pem -replace
```

## Selecting TLS version

To configure the TLS versions, execute the following `omnicc` command:

```
omnicc -encryption -encr_param <hosts> -tls_min <min_ver> -tls_max <max_ver>
```

This command specifies both minimum and maximum versions of TLS. The default range after the installation is TLSv1 to TLSv1.1.

By default, Data Protector uses TLSv1.1 for Encrypted Control Communication. TLSv1 is the default minimum version supported to support communication with previous versions of Data Protector binaries. Binaries prior to 8.16 supported only TLSv1.

**Note:** From 8.16 onwards, the list of certificates do not contain private keys (\*\_key.pem) as they are no longer available on the Cell Manager.

When setting the range of minimum and maximum TLS versions, ensure that a common version is available for all the pairs of systems and Data Protector processes that communicate. If there is no overlap between the two clients, then the connection between them cannot be established.

The maximum version of TLS is TLS1.2. To enable TLS1.2 for a host, use the following command:

```
omnicc -encryption -encr_param <hostname> -tls_max TLS1.2
```

**Note:** The file hdpcert.pem is not suitable for TLS1.2 version.

When using the hdpcert.pem or similar short certificate, update the encryption before setting TLS1.2. It is recommended to switch to the Data Protector generated certificates. This can be done by disabling the old encrypted control communication and enabling it again. This causes the certificates to be newly generated by Data Protector.

The <ssl/> element with protocol attribute defines the allowed versions of TLS protocol. The default value is comma-separated list of three versions:

protocol = **TLSv1,TLSv1.1,TLSv1.2**

For Windows: c:\ProgramData\OmniBack\Config\Server\AppServer\standalone.xml

For Linux: /etc/opt/omni/server/AppServer/standalone.xml

## Disabling encrypted control communication

You can disable encrypted control communication:

- In a cell: This includes the Cell Manager and clients
- In a MoM environment: This includes all Cell Managers in a MoM environment.

**Note:** You can change encrypted communication configuration only from a client with encrypted communication enabled or from the Cell Manager.

### Disabling encrypted control communication, using the CLI:

- In a cell, run: `omnicc -encryption -disable -all`
- In a MoM environment, run: `omnicc -encryption -disable_mom -all`
- On a specific client, run: `omnicc -encryption -disable <client_name>`
- On multiple clients, run: `omnicc -encryption -disable{Hostname1 [HostName2 ...] | -all}`

For more details, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

### Disabling encrypted control communication for multiple clients, using the GUI:

1. In the Clients context, select a client or multiple clients.
2. Right-click the selection and select **Disable Encrypted Communication**.

The Disable encrypted control communication page appears. All the clients are selected.

3. Click **Finish** to disable encrypted control communication for the clients.

#### **Disabling encrypted control communication for each client, using the GUI:**

1. In the Clients context, select a client.
2. Right-click the selection and select **Properties**.
3. In the **Connection** tab deselect the **Encrypted control communication** option.
4. Click **Apply**.

**Note:** You can also disable encrypted control communication in the following scenarios:  
Adding or importing: Clients to a cell.  
Editing the Properties of a client and Cell Manager.

#### **Disabling encrypted communication when the Cell Manager is cluster-aware**

This section is relevant only if the Cell Manager is configured in a non-Microsoft cluster.

To illustrate how to disable encrypted communication in such an environment, we will use this example:

The Cell Manager consists of the following systems:

- cm1.company.com (cluster node 1)
- cm2.company.com (cluster node 2)
- cmvs.company.com (cluster virtual server)

The clients are:

- cl1.company.com
- cl2.company.com
- cl3.company.com

To disable encrypted control communication:

1. Ensure that all cluster nodes are online.
2. Disable encrypted communication on all clients in the cell that are not part of the Cell Manager cluster. Run:

```
omnicc -encryption -disable cl1.company.com cl2.company.com cl3.company.com
```



**Tip:** If you have a Windows client with GUI installed, use the Disable Encrypted Communication wizard in the GUI. Select all clients in the cell by clicking the **Select All** button and then deselect all systems that are part of the Cell Manager cluster, including the Cell Manager cluster virtual server.

This comes useful if you have many clients in the cell.

3. On the active Cell Manager node, run the following command to disable encrypted communication on all the remaining cluster Cell Manager nodes:

```
omnicc -encryption -disable cm1.company.com cm2.company.com cmvs.company.com
```

**Note:** If the command fails to disable encrypted communication on all nodes in the cluster, run the command once again.

### Disabling encrypted communication manually

To disable encrypted control communication in a whole cell manually, delete the `config` file that is located in the `client` directory on each client in the cell, including the Cell Manager.

Windows systems: `<Data_Protector_program_data>\Config\client`

UNIX systems: `/etc/opt/omni/client`

To disable encrypted control communication on an individual client:

1. Delete the `config` file on the client.
2. On the Cell Manager, modify the `config` file that is located in the `server` directory:

Windows Cell Manager: `<Data_Protector_program_data>\Config\Server\`

UNIX Cell Manager: `/etc/opt/omni/server`

Delete the section related to the client and replace it with:

```
<client.company.com>={  
  encryption={  
    exception=1;  
  };  
};
```

## Viewing certificate expiration date in Data Protector GUI

To view the duration from when the certificates are valid using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients** . All clients are displayed.
3. Select a Cell Manager host.

You get to view the General tab details.

4. Select the **Certificates** tab.

You get to view the list of all certificates and their valid from and to dates.

**Note:** From Data Protector 8.16 onwards, the private keys are generated on the client. If there exists any old private keys of the clients that were created prior to Data Protector 8.16, only those private keys are displayed until recreated.

## Upgrading an encrypted environment

By default, after upgrading to the latest patch, changes made to the encrypted control communication functionality do not affect the existing environment. You can choose from the following options to maintain the existing encrypted environment:

### Option 1

Remove the encryption from the entire cell and enable encryption in the cell in the new way (recommended). See [Enabling encrypted control communication](#).

### Option 2

Keep the existing certificates on the clients and maintain the environment using the `omnicc` command:

```
omnicc -encryption -enable {Hostname1 [HostName2 ...] | -all} [-cert Cert [-key Key]]  
[-trust TrustedCerts]
```

In this method, it is not possible to configure encrypted control communication using the GUI. Also, the clients will not be encrypted automatically after import. You can encrypt the clients after importing them using the CLI.

For details, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

**Note:** With the earlier method of enabling encrypted control communication, if certificates were not specified, then using the command line `omnicc -encryption -enable` defaulted to `hdpdcert.pem`. With the new approach, the default mechanism is for Data Protector to generate the certificates. To enable encrypted control communication with `hdpdcert.pem`, the certificate has to be specified:  
`omnicc -encryption -enable <host> -cert hdpdcert.pem -key hdpdcert.pem -trust hdpdcert.pem`

## What happens

Encrypted control communication is enabled on a per-client basis, which means that encryption control communication is either enabled or disabled for all control communication with the selected client.

## How to add a client to the Security Exceptions list

Clients that for some reason are not supposed to communicate confidentially can be placed in a Cell Manager exception list, which allows particular clients to communicate in non-encrypted mode.

To add a client to the Security Exceptions list

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
3. Click the Cell Manager that you want to modify.
4. Type the names of the systems that will be added to the Security Exceptions list in the cell or search for systems using the **Network** (on Windows GUI only) or **Search** tabs.
5. Click **Add** to add systems to the list, then click **Apply** to save the changes.

The server configuration file

The clients that are accepted in a plain text mode are written to the server configuration file, located on the Cell Manager in the directory:

**Windows systems:** `Data_Protector_program_data\Config\server\config`

**HP-UX and Linux systems:** `/etc/opt/omni/server/config`

To remove a system from the Security Exceptions list, perform steps 1 to 4 and click **Remove**, then click **Apply** to save the changes.

## Start backup specification user right

For general information about the Data Protector users and user rights, see the *HP Data Protector Help* index: "users".

The Start backup specification user right alone does not enable a user to use the Backup context in the GUI. The user is allowed to start a backup specification from the command line by using the omnib with the -datalist option.

**Note:** By combining the Start Backup Specification with the Start Backup user rights, a user is allowed to see the configured backup specifications in the GUI and is able to start a backup specification or an interactive backup.

Allowing users to perform interactive backups may not always be desired. To allow interactive backups only for users who also have the right to save a backup specification, set the `StrictSecurityFlags` global option to `0x0200`.

For more information on the global options, see the *HP Data Protector Troubleshooting Guide*.

## Hiding the contents of backup specifications

In a high security environment, the contents of saved backup specifications may be considered to be sensitive or even confidential information. Data Protector can be configured to hide the contents of backup specifications for all users, except for those who have the `Save backup specification` user right. To do so, set the `StrictSecurityFlags` global option to `0x0400`.

For more information about the global options, see the *HP Data Protector Troubleshooting Guide*.

## Host trusts

The host trusts functionality reduces the need to grant the `Restore to other clients` user right to users when they only need to restore the data from one client to another within a limited number of clients. You can define groups of hosts that will trust each other with the data.

Host trusts are typically used in the following situations:

- For clients in a cluster (nodes and virtual server).
- If the hostname of a client is changed and the data from the old backup objects needs to be restored.
- If there is a mismatch between the client hostname and backup objects due to DNS issues.
- If a user owns several clients and needs to restore the data from one client to another.
- When migrating data from one host to another.

### Configuration

To configure host trusts, on the Cell Manager, create the file `Data_Protector_program_data\Config\Server\cell\host_trusts` (Windows systems) or `/etc/opt/omni/server/cell/host_trusts` (UNIX systems).

The groups of hosts that trust each other are defined as lists of hostnames enclosed in curly brackets. For example:

### Example

```
GROUP="cluster.domain.com"
{
    cluster.domain.com
    node1.domain.com
    node2.domain.com
}
GROUP="Bajo"
{
    computer.domain.com
    anothercomputer.domain.com
}
```

## Monitoring security events

If you encounter problems using Data Protector, you can use the information in the log files to determine your problem. For example, logged events can help you to determine misconfigured users or clients.

### *Client security events*

Client security events are logged in the `inet.log` file on every client in the cell in the default Data Protector log files directory.

### *Cell Manager security events*

Cell Manager security events are logged in the `security.log` file residing in the default Data Protector server log files directory.

## User authentication and LDAP

Authentication and authorization of Data Protector as an enterprise system should be connected to the enterprise user management infrastructure. This connection allows users and groups configured in a corporate user directory to be granted access to Data Protector services.

User authentication is performed over secure connections, and Lightweight Directory Access Protocol (LDAP) is used as the underlying technology. Consequently, users can use their corporate credentials to access Data Protector services and are not required to maintain separate passwords. In addition, administrators or operators can be maintained as groups in the corporate directory, adhering to established authorization and approval processes.

LDAP integration is configured in a security domain of Data Protector's embedded application server (JBoss) using Java Authentication and Authorization Service (JAAS) login modules. An optional LDAP login module provides LDAP authentication and authorization services, which are mapped to Data Protector permissions by a mandatory Data Protector Login Module. If LDAP integration is not configured, then Data Protector works just as it did in previous releases.

Data Protector uses the login modules in an login module stack to authenticate users. When a user connects to the Cell Manager using the Data Protector GUI, user authentication is performed by the following login modules:

1. LDAP Login Module: Authenticates user credentials, such as username and password, against an existing LDAP server. See [Initializing and Configuring the LDAP Login Module](#).
2. Data Protector Login Module: Authenticates user credentials against the Data Protector user list and the Web access password. See [Granting Data Protector Permissions to LDAP Users or Groups](#).
3. After performing all the steps necessary to complete LDAP initialization and configuration, you can also check the configuration. See [Checking the LDAP Configuration](#).

**Note:** Whenever a user or client is configured in Data Protector to allow the CLI access in the classic way, the Data Protector GUI does not use the LDAP feature.

## Initializing and configuring the LDAP login module

The LDAP login module is located in the security domain of JBoss Application Server, which is installed with Data Protector. The LDAP login module must be initialized and configured prior to the first use of the LDAP security feature.

1. Initializing the LDAP Login Module.
2. Configuring the LDAP Login Module.

### *Initializing the LDAP login module*

To initialize the LDAP login module, use the `jboss-cli` utility, which is also installed with Data Protector

1. The `jboss-cli` utility is located in: `%Data_Protector_home%/AppServer/bin`. Execute the following command:

- **Windows:** `jboss-cli.bat --file=ldapinit.cli`
- **UNIX:** `jboss-cli.sh --file=ldapinit.cli`

This command creates an LDAP login module in JBoss configuration and populates this new login module with default values. The default values generated by the command line within the `standalone.xml` configuration file:

```
<security-domain name="hdp-domain">
  <authentication>
    <login-module code="LdapExtended" flag="optional">
      <module-option name="java.naming.factory.initial"
        value="com.sun.jndi.ldap.LdapCtxFactory"/>
      <module-option name="java.naming.security.authentication" value="simple"/>
      <module-option name="roleFilter" value="(member={1})"/>
      <module-option name="roleAttributeID" value="memberOf"/>
      <module-option name="roleNameAttributeID" value="distinguishedName"/>
      <module-option name="roleAttributeIsDN" value="true"/>
      <module-option name="searchScope" value="SUBTREE_SCOPE"/>
      <module-option name="allowEmptyPasswords" value="true"/>
      <module-option name="password-stacking" value="useFirstPass"/>
    </login-module>
    <login-module code="com.hp.im.dp.cell.auth.DploginModule" flag="required">
      <module-option name="password-stacking" value="useFirstPass"/>
    </login-module>
  </authentication>
</security-domain>
```

```
</authentication>  
</security-domain>
```

2. To access the JBoss admin console, located on the Cell Manager, from a remote client, enable the remote access to the JBoss admin console. To do this, use a text editor and change the bind address of the management interface from 127.0.0.1 to 0.0.0.0 in the interfaces section of the standalone.xml file:

```
<interfaces>  
  <interface name="management">  
    <inet-address value="${jboss.bind.address.management:0.0.0.0}"/>  
  </interface>  
  <interface name="public">  
    <inet-address value="0.0.0.0"/>  
  </interface>  
  <interface name="unsecure">  
    <inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"/>  
  </interface>  
</interfaces>
```

3. Restart the Data Protector services:

```
omnisv stop  
omnisv start
```

## Configuring the LDAP login module

To configure the LDAP login module, use the web-based admin console of JBoss Application Server, which gets installed together with Data Protector. Proceed as follows:

1. To access the JBoss admin console, create a JBoss user. To create a JBoss user, run the add-user utility:
  - **Windows:** add-user.bat located in %Data\_Protector\_home%/AppServer/bin
  - **UNIX:** add-user.sh located in /opt/omni/AppServer/bin
2. Provide inputs for the following parameters:
  - **Type of user to add:** Select Management User.
  - **Realm:** Leave this field blank, as the default value ManagementRealm is selected by the utility.

- **Username:** Add a username.
  - **Password:** Add a password.
3. To access the JBoss admin console, use a browser and open the URL: <http://cell-manager-name:9990/console>
  4. In the Authentication screen, specify the **Username** and **Password** created using the add-user utility.
  5. Click **Log In**. JBoss Application Server admin console appears.
  6. In the JBoss admin console, select the **Profile** tab.
  7. In the **Profile** tab, expand the **Security** node and then click **Security Domains**.
  8. From the list of registered security domains, click **View** for hdp-domain. The following login modules are defined for the security domain, hdp-domain:
    - LdapExtended
    - Com.hp.im.dp.cell.auth.DpLoginModule
  9. Select the **LdapExtended** module.
  10. From the Details section, click the **Module Options** tab. All of the pre-configured module options are listed in the **Module Options** tab.
  11. To customize and use the LDAP login module, you need to add additional Module Options. Click **Add** and specify the **Name** and **Value** for each module option. See the following table for more information:

Module Option	Name	Value	Description
Provider URL	java.naming.provider.url	Specify the URL of the LDAP server in the following format: ldap://<server>:<port>	A standard property name
Base Context Distinguished Name (DN)	baseCtxDN	Specify the DN of the LDAP location that contains the users.	The fixed DN of the context from where you start the user search



Module Option	Name	Value	Description
Base Filter	baseFilter	Specify the attribute in the LDAP setup that matches the user's login name in the following format: (<user-login-name-attribute>={0}) where <user-login-name-attribute> needs to be replaced by the corresponding LDAP attribute name.	A search filter used to locate the context of the user to authenticate
Roles Context DN	rolesCtxDN	Specify the DN of the LDAP location that contains the user groups.	The fixed DN of the context to search for user groups
Bind DN	bindDN	Specify the DN of an LDAP user that is used by the login module to perform the initial LDAP bind. You must have the required permission to search the LDAP location of the users and groups to obtain the users and their groups. These locations are defined in the baseCtxDN and rolesCtxDN module options.	The DN used to bind against the LDAP server for the user and roles queries. This is a DN with read/search permissions on the baseCtxDN and rolesCtxDN values
Bind Credential	bindCredential	Specify the password for the LDAP user provided in the BindDN module option.	The password for the bindDN.

For more information on other Module Options, visit the following URLs:

- <https://community.jboss.org/wiki/LdapExtLoginModule>
- [http://technet.microsoft.com/en-us/library/cc773354\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx)

12. The changes will take effect when you reload JBoss Application Server configuration. To reload the configuration, use the `jboss-cli` utility located in: `%Data_Protector_home%/AppServer/bin`.

13. Execute the following command:

- **Windows:** `jboss-cli.bat -c :reload`
- **UNIX:** `jboss-cli.sh -c :reload`

**Note:** When configuring the LDAP Login Module in MoM environments, ensure that you perform the steps described above on every Cell Manager. Every Cell Manager in the MoM environment needs to have the same configuration for the LDAP login module.

## Granting Data Protector permissions to LDAP users or groups

LDAP users can connect to a Cell Manager only if they are granted the Data Protector permissions. After configuring the LDAP login module, you can grant the LDAP users the required Data Protector permissions.

To grant the Data Protector permissions, proceed as follows:

1. Start the Data Protector GUI and grant Data Protector permissions to the LDAP users or groups.
  - Add LDAP users to Data Protector user groups.
  - Add LDAP groups to Data Protector user groups.
2. Log In using LDAP credentials.

### *Adding LDAP users to user groups*

To add LDAP users to Data Protector user groups, proceed as follows:

1. In the Context List, click **Users**.
2. In the Scoping Pane, expand **Users** and right-click the user group to which you want to add the LDAP user(s).
3. Click **Add/Delete Users** to open the wizard.
4. In the **Manual** tab of the Add/Delete Users dialog box, provide the following details:
  - **Type:** Select LDAP.
  - **Name:** Specify the LDAP user in the LDAP user principal name format.
  - **Entity:** Enter LDAP User.
  - **Description:** This is optional.
5. Click **Finish** to exit the wizard.

### *Adding LDAP groups to user groups*

To add LDAP groups to Data Protector user groups, proceed as follows:

1. In the Context List, click **Users**.
2. In the Scoping Pane, expand **Users** and right-click the user group to which you want to add the LDAP group.
3. Click **Add/Delete Users** to open the wizard.
4. In the **Manual** tab of the Add/Delete Users dialog box, provide the following details:
  - **Type**: Select LDAP.
  - **Name**: Specify the LDAP group name in the Distinguished Name (DN) format.
  - **Entity**: Enter LDAP Group.
  - **Description**: This is optional.
5. Click **Finish** to exit the wizard.

**Note:** An LDAP user is automatically granted the same permission level as the LDAP group this user belongs to.

## Logging in using LDAP credentials

To log in using your LDAP credentials, proceed as follows:

1. Start the Data Protector GUI and connect to a Cell Manager.
2. In the LDAP Authentication screen, provide the LDAP credentials to access Data Protector. The LDAP user can belong to any available Data Protector user group.

## Checking the LDAP configuration

The following procedure explains how to check if the user rights are set correctly for a specific LDAP user or group by querying the Data Protector login provider service `getDpAc1` from a web browser.

To obtain the Data Protector Access Control List (ACL) for a specific user, proceed as follows:

1. Connect to the Data Protector login provider web service using a browser.
2. The browser may prompt you to accept the server certificate. Click **Accept** to confirm the request.
3. A dialog box appears, prompting you to provide login credentials. Provide a valid LDAP user name and password that was configured using Data Protector. See [Configuring the LDAP login module](#).
4. The browser returns the following Access Control List (ACL): `https://<server>:7116/dp-loginprovider/restws/dp-ac1`
5. Use the ACL to check if the assigned rights match the Data Protector user rights specified for the corresponding Data Protector user group.

## Certificate Generation Utility

The X.509 certificate generation utility—`omnigencert.pl`—generates the Certificate Authority (CA), server, and client certificates. It is responsible for the following tasks:

- Setting up a single-level root CA
- Generating CA, server, and client certificates
- Creating the necessary directory structure for storing keys, certificates, configuration, and keystore files
- Storing the generated certificates in predefined locations on the CM
- Generating the properties files of web service roles

**Note:** The `omnigencert.pl` utility can be run only by the Administrator user (Windows) or the root user (UNIX).

The `omnigencert.pl` utility is developed as a script and gets installed along with the Cell Manager (CM) installation kit. As part of the CM installation, the script is run for the first time, and the certificates are generated and stored in predefined locations.

The `omnigencert.pl` script exists in the following location:

**Windows:** `%Data_Protector_home%\bin`

**Unix:** `/opt/omni/sbin`

If required, the Data Protector administrators can run this utility any time after the installation to regenerate certificates using the new keys pair or the new CA setup. However, it is not mandatory to use the certificates generated by this utility for the certificate-based authentication. Instead, you can use an existing CA setup for generating the necessary certificates.

## Syntax

This utility is executed initially by the installer as part of Cell Manager installation and the necessary certificates are generated and stored at predefined locations.

The use of this utility is restricted to administrators and is also used to regenerate certificates using new keys pair even including new CA setup. The 'Administrator' user on Windows platform and 'root' user on UNIX platform can execute this script.

The `omnigencert.pl` script exists in the following location:

**Windows:** `%Data_Protector_home%\bin`

**Unix:** `/opt/omni/sbin`

You can run the `omnigencert.pl` utility using the following syntax and options:

## Usage

`[-no_ca_setup]`  
`[-server_id ServerIdentityName]`  
`[-user_ID UserIdentityName]`  
`[-store_password KeystorePassword]`  
`[-cert_expire CertificateExpireInDays]`  
`[-ca_dn CertificateAuthorityDistinguishedName]`  
`[-server_dn ServerDistinguishedName]`  
`[-client_dn ClientDistinguishedName]`  
`[-server_san]`

The `omnigencert.pl` utility supports multiple options, which provide flexibility while generating certificates. If no options are specified, the utility uses default values for generating the certificates.

The `omnigencert.pl` utility supports the following options:

Option	Description
<code>-no_ca_setup</code>	Generates the client and server certificates for an existing CA setup. This option is invalid if a CA setup does not exist.
<code>-server_id</code>	Specifies the value for the Common Name (CN) entity in the Distinguished Name (DN) section of the server certificate. The default value for this option is the CM Fully Qualified Domain Name (FQDN).
<code>-user_id</code>	Specifies the value for the CN entity in the DN section of the client certificate. The default value for this option is WebService User.
<code>-store_password</code>	Defines the password for the keystore or truststore, where the server and client certificates, including their keys, are stored. If this option is not provided, the default password is used for creating stores.
<code>-cert_expire</code>	Defines the expiry of the generated certificate in days. The default value for this option is 8760 days (24 years).

Option	Description
-ca_dn	Defines the DN string for the CA. The DN format is as follows: "CN=<value>, O=<value>, ST=<value>, C=<value>" CN = Common Name, O=Organization Name, ST=State Name, C=Country Name. The default values for the O, ST, and C parameters are as follows: CN = CA <FDQN name of CM server> O = HEWLETT-PACKARD ST = CA C= US
-server_dn	Defines the DN string for the server certificate. The DN format is as follows: "CN=<value>, O=<value>, ST=<value>, C=<value>" CN = Common Name, O=Organization Name, ST=State Name, C=Country Name. The default values for the O, ST, and C parameters are as follows: CN = <FDQN name of CM server> O = HEWLETT-PACKARD ST = CA C= US
-client_dn	Defines the DN string for the client or user certificate. The DN format is as follows: "CN=<value>, O=<value>, ST=<value>, C=<value>" CN = Common Name, O=Organization Name, ST=State Name, C=Country Name. The default values for the O, ST, and C parameters are as follows: CN = WebService User O = HEWLETT-PACKARD ST = CA C= US

Option	Description
-server_san	<p>Specifies the Subject Alternative Names (SAN) in the server certificate. However, the generated server certificate, during the installation of a Cell Manager, has entries of type DNS in the SAN section. These SAN entries are generated automatically based on the available IP numbers in the Cell Manager. To override default auto-generation of SAN entries in the server certificate, specify this option while generating certificates using the certificate generation utility.</p> <p>The DNS and IP types of SAN entries are supported.</p> <p>The format of value for this option is as follows: santype:value, santype:value</p> <p>Each SAN entry is separated by comma (',') and it contains 2 parts; 1) SAN type, 2) value of the SAN type.</p> <p><b>Examples:</b></p> <p>dns:iwf1112056.dprdn.hp.com, dns:iwf1113456.dprnd.hp.com</p> <p>ip:15.218.1.100, ip:15.218.1.200, ip:15.218.1.155</p> <p>dns:iwf1112056.dprnd.hp.com, ip:15.218.1.100</p>

**Note:** The utility does not support the following combinations for options: -server\_id and -server\_dn, -user\_id and -client\_dn, and -no\_ca\_setup and -ca\_dn

## Examples

The following sections list sample commands for running the `omnigencert.pl` utility on Windows and UNIX.

The `omnigencert.pl` script exists in the following location:

**Windows:** %Data\_Protector\_home%\bin

**Unix:** /opt/omni/sbin

### *Windows and Unix Commands*

<b>Task</b>	<b>Windows Command</b>	<b>Unix Command</b>
To set up CA and to generate CA, client, and server certificates using default values	%Data_Protector_home%\bin\perl.exe omnigencert.pl	/opt/omni/bin/perl omnigencert.pl



Task	Windows Command	Unix Command
To set up CA and to generate CA, client, and server certificates using specified common name values	<pre>%Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id &lt;value&gt; -user_ id &lt;value&gt;</pre>	<pre>/opt/omni/bin/perl omnigencert.pl - server_id &lt;value&gt; -user_id &lt;value&gt;</pre>

Task	Windows Command	Unix Command
To set up CA and to generate CA, client, and server certificates using specified store password	%Data_Protector_home%\bin\perl.exe omnigencert.pl -store_password <value>	/opt/omni/bin/perl omnigencert.pl -store_password <value>

Task	Windows Command	Unix Command
To set up CA and to generate CA, client, and server certificates using specified certificate expiry days	%Data_Protector_home%\bin\perl.exe omnigencert.pl -cert_expire <value>	/opt/omni/bin/perl omnigencert.pl -cert_expire <value>

Task	Windows Command	Unix Command
To generate the client and server certificates using an existing CA setup (which is created as part of the installation) using default values	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup	/opt/omni/bin/perl omnigencert.pl -no_ca_setup

Task	Windows Command	Unix Command
To set up CA and to generate CA, client, and server certificates using specified DNS	%Data_Protector_home%\bin\perl.exe omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn <value>

Task	Windows Command	Unix Command
To generate the client and server certificates using an existing CA setup using specified DNS	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl - no_ca_setup -server_dn <value> - client_dn <value>

Task	Windows Command	Unix Command
To generate client and server certificates using an existing CA certificate in the SG-CLUSTER environment	<ol style="list-style-type: none"> <li>1. Retrieve the existing keystore password from &lt;DP_DATA_DIR&gt;\Config\client\components\webservice.properties.</li> <li>2. Retrieve the <b>PGOSUSER</b> value from &lt;DP_DATA_DIR&gt;\server\idb\idb.config.</li> <li>3. Run the omnigencert.pl utility with the cluster virtual system name as follows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_id cm_virtual_name.domain.com -user_id hdpd_so_user -store_password existing_keystor_passwd</li> </ol>	<ol style="list-style-type: none"> <li>1. Retrieve the existing keystore password from /etc/opt/omni/client/components/webservice.properties.</li> <li>2. Retrieve the <b>PGOSUSER</b> value from /etc/opt/omni/server/idb/idb.config.</li> <li>3. Run the omnigencert.pl utility with the cluster virtual system name as follows: /opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_id cm_virtual_name.domain.com -user_id hdpd_so_user -store_password existing_keystor_passwd</li> </ol>

Task	Windows Command	Unix Command
To generate CA, client, and server certificates in the SG-CLUSTER environment	<ol style="list-style-type: none"> <li>1. Retrieve the existing keystore password from &lt;DP_DATA_DIR&gt;\Config\client\components\webservice.properties.</li> <li>2. Retrieve the <b>PGOSUSER</b> value from &lt;DP_DATA_DIR&gt;\server\idb\idb.config.</li> <li>3. Run the omnigencert.pl utility with the cluster virtual system name as follows: %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hdpd_so_user -store_password existing_keystor_passwd</li> </ol>	<ol style="list-style-type: none"> <li>1. Retrieve the existing keystore password from /etc/opt/omni/client/components/webservice.properties.</li> <li>2. Retrieve the <b>PGOSUSER</b> value from /etc/opt/omni/server/idb/idb.config.</li> <li>3. Run the omnigencert.pl utility with the cluster virtual system name as follows: /opt/omni/bin/perl omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hdpd_so_user -store_password existing_keystor_passwd</li> </ol>



Task	Windows Command	Unix Command
To generate a server certificate with SAN entries of type DNS for a specific Cell Manager server.	<pre>%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn iwf11160123.dprnd.hp.com -server_san "dns:iwf11160123.dprnd.hp.com,dns:iwf1116 0123.dp.hp.com"</pre>	<pre>/opt/omni/bin/perl omnigencert.pl - no_ca_setup -server_dn iwf11160123.dprnd.hp.com -server_ san "dns:iwf11160123.dprnd.hp.com,dns:i wf11160123.dp.hp.com"</pre>

Task	Windows Command	Unix Command
To generate a server certificate with SAN entries of type IP for a specific Cell Manager server.	<pre>%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn 15.218.1.100 -server_san "ip:15.218.1.100,ip:15.218.1.101,ip:15.21 8.1.125,ip:15.218.1.116"</pre>	<pre>/opt/omni/bin/perl omnigencert.pl - no_ca_setup -server_dn 15.218.1.100 -server_san "ip:15.218.1.100,ip:15.218.1.101,ip :15.218.1.125,ip:15.218.1.116"</pre>

Task	Windows Command	Unix Command
To generate a server certificate with SAN entries of types DNS and IP for a specific Cell Manager server.	<pre>%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn iwf111206.dprnd.hp.com -server_san "dns:iwf111206.dprnd.hp.com, iwf111206.hp.com,ip:15.218.1.100,ip:15.21 8.1.101,ip:15.218.1.125,ip:15.218.1.116"</pre>	<pre>/opt/omni/bin/perl omnigencert.pl - no_ca_setup -server_dn iwf111206.dprnd.hp.com -server_san "dns:iwf111206.dprnd.hp.com, iwf111206.hp.com,ip:15.218.1.100,ip :15.218.1.101,ip:15.218.1.125,ip:15 .218.1.116"</pre>

## Directory Structure

The following sections list the directories where certificates are stored.

Windows Directory	Unix Directory	Description
ProgramData\Omniback\Config\Server\certificates	/etc/opt/omni/server/certificates	Contains the CA certificate file, cacert.pem, which contains the CA public key.
ProgramData\Omniback\Config\Server\certificates\ca	/etc/opt/omni/server/certificates /ca	Contains the configuration, input, and other files necessary for the CA functioning.
ProgramData\Omniback\Config\Server\certificates\ca\keys	/etc/opt/omni/server/certificates /ca/keys	Contains the CA private key file, cakey.pem.
ProgramData\Omniback\Config\Server\certificates\server	/etc/opt/omni/server/certificates /server	Contains two kinds of stores: keystore and truststore. These stores are created by the Java utility, keytool, for protecting server certificates and its keys. These stores are protected by the store password. It contains the following stores:  ca.truststore  server.keystore  server.truststore

Windows Directory	Unix Directory	Description
ProgramData\Omniback\Config\Server\certificates\client	/etc/opt/omni/server/certificates /client	<p>Contains two kinds of stores: keystore and truststore. These stores are created by the Java utility, keytool, for protecting client certificates and its keys. These stores are protected by the store password. It contains the following stores:</p> <ul style="list-style-type: none"> <li>• client.keystore</li> <li>• client.truststore</li> </ul>
ProgramData\Omniback\Config\Server\AppServer	/etc/opt/omni/server/AppServer	<p>Contains the properties files created by this utility. This directory contains other files apart from the following properties files:</p> <ul style="list-style-type: none"> <li>• jce-webservice-roles.properties</li> <li>• dp-webservice-roles.properties</li> </ul>

## Overwriting existing certificates

To overwrite existing certificates—generated by the utility as part of the CM installation—with the certificates generated by an existing CA setup, you can use one of the following options:

- Overwriting certificates in existing keystore and truststore files
- Overwriting certificates by creating new keystore and truststore files

**Note:** After regenerating certificates or using new certificates, you must restart the Data Protector services on the CM. You must do this before performing any operation that uses certificates, as restarting the services ensures that new certificates are in effect.

## Overwriting certificates in existing keystore and truststore files

To overwrite certificates in existing keystore and truststore files, complete the following tasks:

- Replace existing server and client store files
- Replace the CA certificate
- Update the Distinguished Name(DN) string

## *Replacing existing server and client store files*

To replace existing server and client store files, proceed as follows:

1. Retrieve the keystore and truststore files' store password from the `webservice.properties` and `standalone.xml` configuration files, located in:

### **Windows**

- `ProgramData\OmniBack\Config\client\components\webservice.properties`
- `ProgramData\OmniBack\Config\server\AppServer\standalone.xml`

### **UNIX**

- `/etc/opt/omni/client/components/webservice.properties`
- `/etc/opt/omni/server/AppServer/standalone.xml`

2. Remove all entries from the existing server and client store files, `server.keystore`, `server.truststore`, `client.keystore`, and `client.truststore`, located in:

### **Server**

- Windows: ProgramData\Omniback\Config\Server\certificates\server
- Unix: /etc/opt/omni/server/certificates/server

#### **Client**

- Windows: ProgramData\Omniback\Config\Server\certificates\client
- UNIX: /etc/opt/omni/server/certificates/client

To make these changes, you can use the Java keytool utility, located in:

**Windows:** Program Files\Omniback\jre\bin

**UNIX:** /opt/omni/jre/bin

3. Import the generated certificates into the following stores using the Java keytool utility:

- Server and CA certificates into `server.keystore`
- CA and Client certificate into `server.truststore`
- CA certificate into `ca.truststore`
- Client and CA certificates into `client.keystore`
- CA and Server certificate into `client.truststore`

## ***Replacing the CA certificate***

To replace the existing CA certificate, proceed as follows:

1. Note the permissions of the existing CA certificate file `cacert.pem`, located in:
  - **Windows:** ProgramData\Omniback\Config\Server\certificates
  - **UNIX:** /etc/opt/omni/server/certificates
2. Replace the existing CA certificate `cacert.pem` file with the generated CA certificate.

## ***Updating the distinguished name (DN) string***

Replace the existing Distinguished Name (DN) string in the `jce-webservice-roles.properties` and `dp-webservice-roles.properties` files with the DN string used for the client certificate. These files are located in:

**Windows:** ProgramData\Omniback\Config\Server\AppServer

**UNIX:** /etc/opt/omni/server/AppServer

**Note:** In the DN string, precede spaces and “=” characters with the backslash (\) character.

## Overwriting certificates by creating new keystore and truststore files

To overwrite certificates in new keystore and truststore files, complete the following tasks:

- Replace existing server and client store files
- Replace the CA certificate
- Update the Distinguished Name (DN) string
- Update the configuration file with the stores password

**Note:** You must retain the password for server and client stores.

### *Replacing existing server and client store files*

To replace existing server and client store files, proceed as follows:

1. Note the permissions of the existing server and client store files, `server.keystore`, `server.truststore`, `client.keystore`, and `client.truststore`, located in:

#### **Server**

- Windows: `ProgramData\Omniback\Config\Server\certificates\server`
- UNIX: `/etc/opt/omni/server/certificates/server`

#### **Client**

- Windows: `ProgramData\Omniback\Config\Server\certificates\client`
- UNIX: `/etc/opt/omni/server/certificates/client`

2. Remove the server and client store files.
3. Create stores with the same file names and permissions.
4. Import the generated certificates into the following stores using the Java keytool utility:
  - Server and CA certificates into `server.keystore`
  - CA and Client certificate into `server.truststore`
  - CA certificate into `ca.truststore`
  - Client and CA certificates into `client.keystore`
  - CA and Server certificate into `client.truststore`



**Note:** The Java keytool utility is located at Windows: Program Files\Omniback\jre\bin and UNIX: /opt/omni/jre/bin.

## ***Replacing the CA certificate***

To replace the existing CA certificate, proceed as follows:

1. Note the permissions of the existing CA certificate file, `cacert.pem`, located in:

### **Windows**

`ProgramData\Omniback\Config\Server\certificates`

### **UNIX**

`/etc/opt/omni/server/certificates`

2. Replace the existing CA certificate file, `cacert.pem`, with the generated CA certificate.

## ***Updating the distinguished Name (DN) string***

Replace the existing Distinguished Name (DN) string in the `jce-webservice-roles.properties` and `dp-webservice-roles.properties` files with the DN string used for the client certificate. These files are located in:

### **Windows**

`ProgramData\Omniback\Config\Server\AppServer`

### **UNIX**

`/etc/opt/omni/server/AppServer`

**Note:** In the DN string, precede spaces and “=” characters with the backslash (\) character.

## ***Updating the configuration file with the stores password***

To update the configuration file with the stores password, proceed as follows:

**Note:** This task is required only if new stores are created with a new password.

1. Update the `webservice.properties` and `standalone.xml` configuration files with the store password used while creating store files, such as `server.keystore`, `server.truststore`, `ca.truststore`, `client.keystore`, and `client.truststore`.

The configuration files are located in:

### **Windows**

• `ProgramData\OmniBack\Config\client\components\webservice.properties`

- ProgramData\OmniBack\Config\server\AppServer\standalone.xml

## UNIX

- /etc/opt/omni/client/components/webservice.properties

- /etc/opt/omni/server/AppServer/standalone.xml

2. In the standalone.xml file, update the stores password (highlighted in bold):

```
<ssl name="ssl" password="M6.p0ino06L3w" certificate-key-  
file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"  
verify-client="want" ca-certificate-  
file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-  
password="M6.p0ino06L3w"/>
```

3. In the webservice.properties file, update the password (highlighted in bold):

```
<jsse keystore-password="M6.p0ino06L3w" keystore-  
url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-  
password="M6.p0ino06L3w" truststore-  
url="/etc/opt/omni/server/certificates/server/server.truststore"/>
```

```
<jsse keystore-password="M6.p0ino06L3w" keystore-  
url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-  
password="M6.p0ino06L3w" truststore-  
url="/etc/opt/omni/server/certificates/server/server.truststore"/>
```

```
<ssl name="ssl" password="M6.p0ino06L3w" certificate-key-  
file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"  
verify-client="want" ca-certificate-  
file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-  
password="M6.p0ino06L3w"/>
```

## Managing Data Protector patches

Data Protector patches are provided through HP support and can be downloaded from the HP support website. Data Protector provides individual patches and patch bundles.

## Installing patches

Cell Manager patches can be installed locally. However, in order to patch clients, Installation Server is required. Once the Installation Server is patched, you can then patch clients remotely.

**Note:** When using the Encrypted Control Communication (ECC) in a cell, ensure that ECC is enabled on the Installation Server also. Otherwise, the Installation Server will not communicate with the clients that use ECC.

**Important:** On HP-UX systems, before patching the Cell Manager with a Cell Manager (CS) patch, stop the Data Protector services using the Data Protector `omnisv` command, and start them again after the patching process completes.

If individual patches are included into a patch bundle, you can only install the whole bundle. For details, see the installation instructions provided with the patch.

To verify which patches are installed on the system, you can use the Data Protector GUI or CLI. See ["Verifying which Data Protector patches are installed"](#)

## Installing and removing Data Protector patch bundles

If Data Protector is already installed on your system, you can also install a Data Protector patch bundle (a set of Data Protector patches) on this system.

To install a Data Protector patch bundle on UNIX systems, you can use the `omnisetup.sh` script. On Windows systems, a patch bundle installation is provided as an executable file.

You can also remove the patch bundle. After removing the patch bundle, the last Data Protector release version remains on the system. For details, see the installation instructions provided with the patch bundle.

### *Installing and removing Data Protector patch bundles on UNIX systems*

To install a Data Protector patch bundle, use the `omnisetup.sh` command provided in the tar archive together with the patch bundle files. Use the `-bundleadd` option. For example:

```
omnisetup.sh -bundleadd b701
```

You can install a Data Protector patch bundle only on the Installation Server and the Cell Manager. If the installation fails or you stopped it, you can continue with the installation and install the rest of the patches (supported with Linux systems only), rollback the installed patches to the previous patch level, or exit the installation without installing all patches.

To remove the Data Protector patch bundle, use the `omnisetup.sh -bundlerem` command. For example:

```
omnisetup.sh -bundlerem b701
```

For details, see the installation instructions provided with the patch or patch bundle.

### *Installing and removing Data Protector patch bundles on Windows systems*

A Data Protector patch bundle for Windows is provided as an executable file (for example, `DPWINBDL_00701.exe`). You can install a Data Protector patch bundle on the Installation Server, the Cell Manager, or the client system.

To install the patch bundle on a Windows system, execute the `BundleName.exe` command, for example:

```
DPWINBDL_00701.exe
```

The command recognizes, which components are installed on the system and upgrades them to the latest patch.

To remove the Data Protector patch bundle, use the `remove_patch.bat` command located at the default Data Protector commands location in the `utils` directory .

`remove_patch`*BundleNameDPInstallationDepot* where *DPInstallationDepot* is the location from which Data Protector (not the patch bundle) was installed. For example, to remove the patch bundle `b701`, where Data Protector was installed from `D:\WINDOWS_OTHER`, execute:

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

You can remove a Data Protector patch bundle from the Installation Server, the Cell Manager, or the client system.

**Note:** On Windows systems, it is also possible to remove individual patches using the `remove_patch.bat` command. However make sure that if you do not remove the `CORE` patch until other individual patches are still installed on the system. Otherwise, you will not be able to remove other individual patches later.

## Verifying which Data Protector patches are installed

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

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

### Prerequisites

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

### Limitations

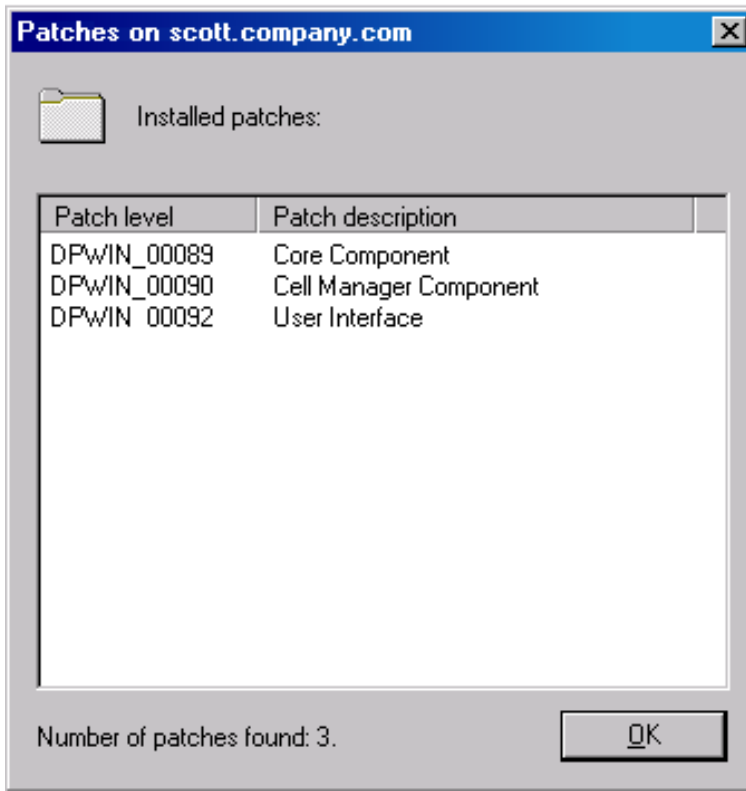
- Patch verification can check which patches are installed on systems within the same cell only.

## Verifying Data Protector patches using the GUI

To verify which patches are installed on a particular client using the Data Protector GUI, follow the below procedure:

1. In the Context List, select **Clients**.
2. In the Scoping Pane, expand **Clients** and select a system in the cell for which you want to verify the patches installed.
3. In the Results Area, click **Patches** to open the **Patches on** window.

**Figure 39: Verifying patches installed**



If there are patches found on the system, the verification returns the level and the description of each patch and the number of the patches installed.

If there are no Data Protector patches on the system, the verification returns an empty list.

If the system verified is not a member of the cell, is unavailable, or an error occurs, the verification reports an error message.

4. Click **OK** to close the window.

## ***Verifying Data Protector Patches Using the CLI***

To verify which patches are installed on a particular client using the Data Protector CLI, execute the `omnicheck -patches -host hostname` command, where the *hostname* is the name of the system to be verified.

For more information on the `omnicheck` command, see the `omnicheck` man page.

## **Uninstalling Data Protector software**

If your system configuration changes, you may want to uninstall the Data Protector software from the system or remove some software components.

Uninstalling is removing all the Data Protector software components from the system, including *all* references to this system from the IDB on the Cell Manager computer. However, by default, the Data Protector configuration data remains on the system because you may need this data in the future upgrade of Data Protector. To remove the configuration data after uninstalling the Data Protector software, delete the directories where Data Protector was installed.

If you have some other data in the directory where Data Protector is installed, make sure you copied this data to another location before uninstalling Data Protector. Otherwise, the data will be removed during the uninstallation process.

Uninstalling the Data Protector software from a cell consists of the following steps:

1. Uninstalling the Data Protector client software using the GUI. See "[Uninstalling a Data Protector client](#)".
2. Uninstalling Data Protector Cell Manager and Installation Server. See "[Uninstalling the Cell Manager and Installation Server](#)".

You can also uninstall Data Protector software components without uninstalling the Cell Manager or client. See "[Changing Data Protector software components](#)".

On UNIX, you can also manually remove the Data Protector software. See "[Manual removal of Data Protector software on UNIX](#)".

## Prerequisites

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

- Make sure that all references to the computer are removed from the backup specifications. Otherwise, Data Protector will try to back up unknown systems and this part of the backup specification will fail. For instructions on how to modify backup specifications, see the *HP Data Protector Help* index: "modifying, backup specification".
- Make sure that no backup devices or disk arrays are connected and configured on the system that you want to uninstall. Once the system is exported, Data Protector can no longer use its backup devices or disk arrays in the original cell.

## Uninstalling a Data Protector client

**Note:** The remote uninstallation procedure requires the Installation Server to be installed for the platforms from which you are uninstalling the Data Protector software.

You uninstall a client remotely by performing these steps in the Data Protector GUI:

1. In the Context List, switch to the **Clients** context.
2. In the Scoping Pane, expand **Clients**, right-click the client you want to uninstall, and then click **Delete**. You will be asked whether you want to uninstall the Data Protector software as well.
3. Click **Yes** to uninstall all the software components from the client, and then click **Finish**.

The client will be removed from the list in the Results Area and the Data Protector software will be deleted from its hard disk.

Note that the Data Protector configuration data remains on the client system. To remove the configuration data, delete the directories where Data Protector was installed.

### *Cluster clients*

If you have cluster aware clients in your Data Protector environment and you want to uninstall them, you must do this locally. The procedure is the same as for uninstalling Cell Manager or Installation Server. See "[Uninstalling the Cell Manager and Installation Server](#)".

The cluster client will be removed from the list in the Results Area and the Data Protector software will be deleted from its hard disk.

### *TruCluster*

To uninstall TruCluster clients, export the virtual node first. Then uninstall Data Protector clients from the node(s).

### *HPOpenVMS 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](#)".

If asked whether you want to uninstall the Data Protector software as well, select **No**.

2. To delete the actual Data Protector client software, log in to the SYSTEM account on the OpenVMS client and execute the following command: `$ PRODUCT REMOVE DP`. Respond to the prompt with YES.

**Important:** This will shut down the Data Protector service and delete all the directories, files, and accounts associated with Data Protector on the OpenVMS system.

## **Uninstalling the Cell Manager and Installation Server**

This section describes the procedure of uninstalling the Data Protector Cell Manager and Installation Server software from Windows, HP-UX and Linux systems.

### ***Uninstalling from Windows systems***

#### *Uninstalling from a Microsoft server cluster*

To uninstall Data Protector software from a Windows system, follow these steps:

1. Make sure you have terminated all Data Protector sessions and exited the GUI.
2. In Windows Control Panel, click **Add/Remove Programs**.
3. Depending on whether you want to leave the configuration data on the system or not, different actions apply:

**Important:** If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, during the installation choose the option that will remove the configuration data.

- To uninstall Data Protector and leave the Data Protector configuration data on the system, select **HP Data Protector 8.10** and click **Remove**.
  - To uninstall Data Protector and remove the Data Protector configuration data, select **HP Data Protector 8.10**, click **Change** and then **Next**. In the Program Maintenance dialog box, select **Remove**. Select **Permanently remove the configuration data** and click **Next**.
4. When uninstalling is completed, click **Finish** to exit the wizard.

## Uninstalling from HP-UX systems

The Cell Manager for HP-UX is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `swremove` utility.

**Important:** If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, after the uninstallation remove the remaining Data Protector directories from your system.

### Prerequisites

- Remove any installed Data Protector patch bundles using the `omnisetup.sh -bundlerem` command. See ["Installing and removing Data Protector patch bundles on UNIX systems"](#).

### Procedure

Before you start uninstalling Data Protector software, shut down Data Protector processes running on the Cell Manager and/or Installation Server system:

1. Log in as root and execute the `omnisv -stop`.
2. Enter the `ps -ef | grep omni` command to verify whether or not all the processes have been shut



down. There should be no Data Protector processes listed after executing `ps -ef | grep omni`.

If you have any Data Protector processes running, stop them using the `kill process_ID` command before you proceed with uninstalling.

3. Run `/usr/sbin/swremove DATA-PROTECTOR` to uninstall Data Protector software.
4. The HP AutoPass utility is not removed during the Data Protector uninstallation. You can manually remove it by running the `/usr/sbin/swremove HPOVLIC` command as the user root.

To remove the remaining Data Protector directories from your system, see ["Manual removal of Data Protector software on UNIX"](#).

## ***Uninstalling the Cell Manager and/or Installation Server configured on HP Serviceguard***

If your Cell Manager and/or Installation Server is configured on an HP 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 PackageName
```

where *PackageName* 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. Dismount 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.

4. Remove the soft links:

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

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

5. Remove the backup directories:

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

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

6. Remove the Data Protector directory with its contents:

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

7. Remove the directories in the shared filesystem:

```
rm -rf shared_disk/etc_opt_omni
```

```
rm -rf shared_disk/var_opt_omni
```

For example:

```
rm -rf /omni_shared/etc_opt_omni
```

```
rm -rf /omni_shared/etc_opt_omni
```

8. Dismount 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 Linux systems

### Prerequisites

- Remove any installed Data Protector patch bundles using the `omnisetup.sh -bundlerem` command. See ["Installing and removing Data Protector patch bundles on UNIX systems"](#).

### Cell Manager

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

**Important:** If you leave the Data Protector configuration data on the system after the uninstallation, and you later install a lower version of the Data Protector Cell Manager than the uninstalled version was, note that the configuration data will be unusable.

To successfully install a lower version, after the uninstallation remove the remaining Data Protector directories from your system.

To uninstall the Data Protector Cell Manager, proceed as follows:

- Make sure you have terminated all Data Protector sessions and exited the graphical user interface.
- Enter the `rpm -qa | grep OB2` command to list all the Data Protector components installed on the Cell Manager.

The components associated with the Cell Manager are as follows:

OB2-CORE	Data Protector Core software.
OB2-TS-CORE	Data Protector Core Technology Stack Libraries
OB2-CC	Cell Console software. This contains the command-line interface.
OB2-TS-CS	Cell Manager Technology Stack Libraries.
OB2-TS-JRE	Java Runtime Environment for use with Data Protector.
OB2-TS-AS	Data Protector Application Server
OB2-WS	Data Protector Web Services
OB2-JCE-DISPATCHER	Job Control Engine Dispatcher
OB2-JCE-SERVICEREGISTRY	Job Control Engine Service Registry
OB2-CS	Cell Manager software.

OB2-DA	Disk Agent software. This is required, otherwise it is not possible to back up the IDB.
OB2-MA	The General Media Agent software. This is required to attach a backup device to the Cell Manager.
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the <i>HP Data Protector Help</i> in the WebHelp format.

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

**Note:** To leave any other Data Protector components installed, you must leave the OB2-CORE component installed, since it is a dependency for other components.

3. In reverse order to the sequence in which they were installed, remove the components mentioned in the previous step using the `rpm -e package name` command and follow the prompts.

## Installation Server

The Installation Server for UNIX on Linux is always installed locally, using the `omnisetup.sh` command. Therefore, it must be uninstalled locally, using the `rpm` utility.

To uninstall the Data Protector Installation Server, proceed as follows:

1. Make sure you have terminated all Data Protector sessions and exited the GUI.
2. Enter the `rpm -qa | grep OB2` command to list all the Data Protector components and remote installation packages stored on the Installation Server system.

The components and remote installation packages associated with the Installation Server are as follows:

OB2-CORE	Data Protector Core software. Note that this is already installed, if you are installing the Installation Server on the Cell Manager system.
OB2-TS-CORE	Data Protector Core Technology Stack Libraries.
OB2-CORE-IS	Installation Server Core software.
OB2-CFP	Common Installation Server Core software for all UNIX platforms.

OB2-TS-CFP	Common Installation Server Technology Stack software for all UNIX platforms
OB2-DAP	Disk Agent remote installation packages for all UNIX systems.
OB2-MAP	Media Agent remote installation packages for all UNIX systems.
OB2-NDMPP	The NDMP Media Agent component.
OB2-CCP	Cell Console remote installation packages for all UNIX systems.

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

For a complete list of components and their dependencies, see ["Data Protector software component dependencies on Linux"](#).

**Note:** To leave any other Data Protector components installed, you must leave the OB2-CORE component installed, since it is a dependency for other components.

3. In reverse order to the sequence in which they were installed, remove the components mentioned in the previous step using the `rpm -e package name` command and follow the prompts.

## Manual removal of Data Protector software on UNIX

Before uninstalling a UNIX client, you should export it from the cell. For procedure, see ["Exporting clients from a cell"](#).

### 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.

### *Linux systems*

To manually remove files from a Linux system, delete them from the following directories and then delete the directories using the `rm` command:

```
rm -fr /var/opt/omni  
rm -fr /etc/opt/omni  
rm -fr /opt/omni
```

### *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 and Mac OS X systems*

Delete the files from the following directory and then delete the directories using the `rm` command:

```
rm -fr /usr/omni
```

## Changing Data Protector software components

This section describes the procedure for removing and adding Data Protector software components from or to Windows, HP-UX, Solaris, and Linux systems. For the list of supported Data Protector components for a particular operating system, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Data Protector software components can be added on the Cell Manager or on a client using the Data Protector GUI. You perform the remote installation of selected components using the Installation Server functionality. For the detailed procedure, see "[Remote installation](#)".

The Data Protector components can be removed locally on the Cell Manager, an Installation Server, or a client.

## On Windows systems

To add or remove the Data Protector software components on a Windows system, follow the steps below:

1. In the Windows Control Panel, click **Add or Remove Programs**.
2. Select **HP Data Protector 8.10** and click **Change**.
3. Click **Next**.
4. In the Program Maintenance window, click **Modify** and then **Next**.

5. In the Custom Setup window, select the components you want to add and/or unselect the software components you want to remove. Click **Next**.
6. Click **Install** to start the installing or removing the software components.
7. When the installation is completed, click **Finish**.

### *Cluster-aware clients*

If you are changing the Data Protector software components on the cluster-aware clients, it must be done locally, from the DVD-ROM, on each cluster node. After that, the virtual server hostname has to be manually imported to the Data Protector cell using the GUI.

## **On HP-UX systems**

You can add new components using the Installation Server functionality.

To remove components, use the `swremove` command.

### *Procedure*

Perform the following procedure to remove Data Protector software components:

1. Log in as `root` and run the `swremove` command.
2. Double-click **B6960MA**, **DATA-PROTECTOR**, and then **OB2-CM** to display a list of the Data Protector components.
3. Select the components you want to remove.
4. In the **Actions** menu, click **Mark for Remove** to mark the components you want to remove.
5. When the components you want to remove are marked, click **Remove** in the **Actions** menu, and then click **OK**.

**Note:** When you mark the Data Protector components you want to remove, and if the remaining components cannot operate properly, the **Dependency Message Dialog** box appears with a list of dependent components.

### *Oracle Server specifics*

After uninstalling the Data Protector Oracle Server integration on an Oracle Server system, the Oracle Server software is still linked to the Data Protector Database Library. You have to remove this link, otherwise the Oracle Server cannot be started after removing the integration. For more information, see the *HP Data Protector Integration Guide for Oracle and SAP*.

## **On Linux systems**

You can add new components using the Installation Server functionality. On Linux systems, some Data Protector components depend on each other and cannot operate properly, if you remove one of them. The



table below presents the components and their dependencies on each other.

**Table 6: Data Protector software component dependencies on Linux**

Components	Depend on
<b>Cell Manager</b>	
OB2-CC, OB2-DA, OB2-MA, OB2-DOCS	OB2-CORE, OB2-TS-CORE
OB2-CS	OB2-CORE, OB2-TS-CORE, OB2-CC
OB2-TS-CS, OB2-TS-JRE, OB2-TS-AS, OB2-WS, OB2-JCE-DISPATCHER, OB2-JCE-SERVICEREGISTRY	OB2-CORE, OB2-TS-CORE, OB2-CC
<b>Installation Server</b>	
OB2-CORE-IS	OB2-CORE
OB2-CF-P, OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

## Procedure

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

1. Make sure you terminated all Data Protector sessions and exited the GUI.
2. Enter the command `rpm | grep OB2` to list all the Data Protector components installed.
3. In reverse order to the sequence in which they were installed, remove the components mentioned in Step 2 using the `rpm -e package name` command and follow the prompts.

## On other UNIX systems

When manually removing components from a Data Protector client on a UNIX system other than HP-UX or Linux, update the `omni_info` file in `/usr/omni/bin/install`.

For each of the removed components, remove the associated component version string from the `omni_info` file.

If you are only removing components from a Data Protector client and have not exported the client from the cell, you will need to update the cell configuration in the `cell_info` file (on the Cell Manager). This can be done by executing the following command on a system in the cell with the Cell Console installed:

```
omnicc -update_host HostName
```

# Chapter 4: Upgrading to Data Protector 8.10

This chapter provides instructions for performing Data Protector upgrade and migration tasks.

## Upgrade overview

### *Before you begin*

Before upgrading an existing product version to Data Protector 8.10, consider the following:

- For information about supported and discontinued platforms and versions, see the latest support matrices at <http://support.openview.hp.com/selfsolve/manuals> and the *HP Data Protector Product Announcements, Software Notes, and References*.

On platforms on which the Cell Manager is no longer supported, first migrate the Cell Manager to a supported platform and then upgrade to Data Protector 8.10. For details, see "[Migrating the Cell Manager to a different platform](#)".

As an unsupported functional area, the Data Protector Java graphical user interface is not supplied in Data Protector 8.10. If there are UNIX systems in your Data Protector cell that have the Data Protector Java graphical user interface installed, during the cell upgrade process, you need to choose other systems that will take the role of Data Protector graphical user interface clients. These clients should run on operating systems supported by the original (native) Data Protector graphical user interface.

- License passwords issued for releases prior to Data Protector 8.10 will no longer work with this version.

You need to have a valid active support agreement in place in order to be eligible for new license passwords according to the type and quantity of licenses listed in your support agreement.

Before you start the upgrade, check the quantity and type of license keys installed in your Data Protector environment and compare it to the quantity and type of licenses listed in your support agreement.

If you have fewer or different licenses listed in your support agreement than actually installed in your environment, you should not start the upgrade. Otherwise you risk that your Data Protector environment is no longer operational due to missing license keys. Instead, contact your HP sales representative or HP partner first to determine what steps are needed to close the gap in the licensed functionality covered by the support contract and the actual licenses currently in use with Data Protector versions older than 8.10.

For details about licensing, see "[Data Protector Licensing](#)".

- Data Protector 8.00 introduced a new Internal Database (IDB) to address scalability needs in enterprise environments, resulting in changes in the IDB structure, system requirements (disk space, user rights, and so on), and platform support. If you are upgrading from Data Protector 6.20 or 7.00, check the requirements in the *HP Data Protector Product Announcements, Software Notes, and*

*References and ["Installing a UNIX Cell Manager"](#) .*

- After the upgrade, the Cell Manager, and Installation Server must have the same Data Protector version installed. Although older Data Protector Disk Agent and Media Agent versions are supported in the same cell, it is highly recommended that the clients also have the same version of Data Protector components installed.

For constraints imposed by older Disk Agent and Media Agent versions after an upgrade, see the *HP Data Protector Product Announcements, Software Notes, and References*.

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

### *Prerequisites*

- Perform a backup of the existing Cell Manager system and the Internal Database (IDB).
- If you are upgrading from Data Protector 6.20 or 7.00, note that the new IDB requires more disk space due to format changes. Before upgrading, make sure you have enough free space available. See ["IDB conversion duration and changes in IDB size and structure"](#) .
- If you are upgrading from Data Protector 6.20 or 7.00, in order to allow the upgrade process to export the IDB, the existing Data Protector installation must be functional and the IDB services or at least the Raima Database Server (RDS) service must be up and running.

### *Limitations*

- The upgrade to Data Protector 8.10 is only supported for Data Protector Data Protector 6.20, Data Protector 7.00, and Data Protector 8.00.
- A backup of the Internal Database, created with Data Protector 6.20 or 7.00, cannot be restored with Data Protector 8.10.

After upgrading the Cell Manager, back up the Internal Database before you continue using Data Protector.

- Changing the Cell Manager platform during the upgrade is not supported. Upgrades are only supported on the same Cell Manager platform (HP-UX to HP-UX, Linux to Linux, and Windows to Windows).

If your platform is discontinued, migrate the Cell Manager to a supported platform first and then upgrade to the new version. See ["Migrating the Cell Manager to a different platform"](#) .

## **Support for earlier agent versions**

Wherever possible, Data Protector components on all clients in a Data Protector cell should be upgraded to version 8.10 during the regular upgrade process. This ensures that customers can benefit from the full feature set of Data Protector 8.10 on all systems in a cell.

Nevertheless, Disk Agent and Media Agent components of an earlier Data Protector version (6.20, 7.00, or 8.00) are supported in a 8.10 cell with the following constraints:

- The earlier product version is still supported by HP as an independent product. To check the announced end-of-support dates for HP products, see the webpage <http://support.openview.hp.com/encore/products.jsp>.
- Support is limited to the feature set of the earlier Data Protector version.
- If you are performing operations involving clients on different systems, all agents of the same type (for example Media Agents) must be of the same version.
- Earlier Media Agent component versions are not supported in combination with NDMP servers.
- A file system backup can be sourced from multiple Disk Agents with different versions and the Backup Server deduplication is supported with different versions of the Media Agent. The Disk and Media agent versions could be lower than or equal to the Cell Manager version. However, the source deduplication requires the same versions of Disk Agents and Media Agents, which can be lower than or equal to the Cell Manager version.
- For the Data ProtectorStoreOnce Software store, the Disk Agent and Media Agent must be the same version. However, this version can be lower than or equal to the Cell Manager version.
- If one Data Protector component on a client is upgraded to 8.10, all other components have to be upgraded to 8.10 as well.

If you encounter problems establishing a connection with agents of an earlier product version, consider upgrading to 8.10 as the first resolution step.

**Note:** Media Agents (8.0x and earlier clients) used as gateways are not compatible with the StoreOnce Software (SOS) server (8.1x or later).

Compatibility issues exists between the following:

- Clients before 7.03 and 7.03 server.
- 7.03 client and SOS server versions (8.0x and later).

## Upgrade sequence

To upgrade your cell from the earlier versions of the product to Data Protector 8.10, proceed as follows:

1. Upgrade the Cell Manager and Installation Server to Data Protector 8.10. The steps are different for UNIX and Windows platforms.

You must first upgrade the Cell Manager in the current cell before you can upgrade the Installation Server.

2. Upgrade the GUI clients.
3. Upgrade the clients that have an online application integration installed, such as Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server, and other.

4. Upgrade the clients that have a Data Protector Media Agent (MA) installed. You can perform backups as soon as MA is upgraded on all MA clients of the same platform as the Cell Manager.
5. HP recommends that you upgrade the clients that have the Data Protector Disk Agent (DA) installed within the next two weeks.
6. Optionally, if you are upgrading from Data Protector 6.20 or 7.00, migrate the Detail Catalog Binary Files (DCBF).

**Note:** The Data Protector Internal Database changed in Data Protector 8.00 and is automatically migrated during the upgrade, except for the Detail Catalog Binary Files (DCBF). Because a migration of DC Binary Files is time consuming, HP recommends to perform it after you upgrade the entire cell. For details, see "[Migrating the Detail Catalog Binary Files \(DCBF\)](#)".

### *Upgrading in a MoM environment*

To upgrade your MoM environment to Data Protector 8.10, 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, but other MoM functionality is not available. Note that device sharing between the Data Protector 8.10 MoM cell and the cells with earlier versions of the product installed is not supported. During the upgrade in a MoM environment, none of the Cell Managers in the MoM environment should be operational.

## **Upgrading from Data Protector 6.20, 7.00, and 8.00**

The Data Protector 6.20, 7.00, and 8.00 release versions can be directly upgraded to Data Protector 8.10 for UNIX and Windows platforms.

### *Licenses*

The existing Data Protector 6.20, 7.00, and 8.00 license keys need to be updated. Existing license keys will not work anymore with Data Protector 8.10. Licensing. For details about licensing, see "[Data Protector Licensing](#)".

### *Before you begin*

Before you begin with the upgrade, see "[Upgrade overview](#)" for information on limitations and the upgrade sequence.

## **Upgrading the UNIX Cell Manager and Installation Server**

### *Prerequisites*

- A POSIX shell (sh) is required for the installation.
- You must have root permissions to perform the upgrade.

If the HP-UX or Linux Installation Server is installed together with the Cell Manager, it is upgraded automatically when the `omnisetup.sh` command is executed.

If the HP-UX or Linux Installation Server is installed on a separate system, see ["Upgrading an Installation Server"](#) .

## Upgrading a Cell Manager

The HP-UX or Linux Cell Manager is upgraded automatically when the `omnisetup.sh` command is executed.

On HP-UX, this command directly upgrades the installed components using the `swinstall` utility. On Linux, this command directly upgrades the installed components using the `rpm` utility.

If the Installation Server is installed with client components, it will be removed by the `omnisetup.sh` command. In this case, install a new Installation Server depot using the `omnisetup.sh -IS` command, and then re-import the upgraded Installation Server. For details, see ["Importing an Installation Server to a cell"](#) .

### HP Serviceguard

The upgrade procedure for the Cell Manager, configured on HP SG differs from the upgrade procedure for the Cell Manager not running in the HP SG environment. The detailed steps you need to follow are described in ["Upgrading the Cell Manager configured in HP Serviceguard"](#) .

### Preparing the environment

#### HP-UX systems:

- Set the kernel parameter `shmmax` (maximum size of a shared memory segment) to at least 2.5 GB. To check the configuration, execute:

```
kcsusage shmmax
```

- HP recommends to set the kernel parameter `maxdsiz_64` (max data segment size) to at least 134217728 bytes (128 MB), and the kernel parameter `semnu` (number of semaphore undo structures) to at least 256. After committing these changes, recompile the kernel and restart the system.

#### Linux systems:

- Set the kernel parameter `shmmax` (maximum size of a shared memory segment) to at least 2.5 GB. To check the configuration, execute:

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

### Upgrade procedure

To upgrade the HP-UX or Linux Cell Manager to Data Protector 8.10, follow the procedure described below:

1. Insert and mount the appropriate UNIX installation DVD-ROM or ISO image (for HP-UX or Linux) to a mount point.

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

- Optionally, copy the following directories from the DVD-ROM or ISO image to your local disk:

LOCAL\_INSTALL

*platform\_dir*/DP\_DEPOT

Where *platform\_dir* is:

hpux	for HP-UX systems
linux_x86_64	for Linux systems

2. Go to the LOCAL\_INSTALL directory on the DVD-ROM, ISO image, or local directory and execute:

```
./omnisetup.sh
```

After the 6.20, 7.00, or 8.00 version of Data Protector is detected, the upgrade procedure is automatically started. To perform a clean installation (the database of previous version will be deleted), uninstall the old version and restart the installation.

For details about installation, see ["Installing a UNIX Cell Manager"](#) and ["Installing Installation Servers for UNIX systems"](#).

As soon as the procedure is completed, you can start using Data Protector.

For the description of the `omnisetup.sh` command, see the README file located in the *Mount\_point*/LOCAL\_INSTALL directory on the DVD-ROM or ISO image, or the *HP Data Protector Command Line Interface Reference* located in the *Mount\_point*/DOCS/C/MAN directory on the DVD-ROM or ISO image.

### What's next?

- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See ["Checking configuration changes"](#).
- You must manually adjust the library capacity (VTLCAPACITY) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade to Data Protector 8.10 by default set to 1 TB. See ["Checking configuration changes"](#).
- On HP-UX 11.31 (Itanium) and SUSE Linux Enterprise Server (x86-64) the maximum size of database files can exceed the default maximum size of 2 GB. Consequently, during an upgrade to Data Protector 8.10 a warning message is displayed with an advice to adjust the maximum size of database files. This adjustment should be done after the upgrade, as it may take a significant amount of time, depending on the database size. See ["Troubleshooting upgrade"](#).

## Upgrading an Installation Server

The HP-UX or Linux Installation Server is upgraded automatically when the `omnisetup.sh` command is executed.



On HP-UX, this command directly upgrades the installed components and stored remote installation packages using the `swinstall` utility. On Linux, this command directly upgrades the installed components and stored remote installation packages using the `rpm` utility.

If the Installation Server is installed with client components, it will be removed by the `omnisetup.sh` command. In this case, install a new Installation Server depot using the `omnisetup.sh -IS` command, and then re-import the upgraded Installation Server. For details, see ["Importing an Installation Server to a cell"](#).

**Important:** You cannot upgrade the Installation Server unless you upgraded the Cell Manager first.

## Upgrade procedure

To upgrade the HP-UX or Linux Installation Server to Data Protector 8.10, follow the procedure described below:

1. Insert and mount the appropriate UNIX installation DVD-ROM or ISO image (for HP-UX or Linux) to a mount point.

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

- Optionally, copy the following directories from the DVD-ROM or ISO image to your local disk:

`LOCAL_INSTALL`

`platform_dir/DP_DEPOT`

Where `platform_dir` is:

<code>hpux</code>	for HP-UX systems
<code>linux_x86_64</code>	for Linux systems

2. Go to the `LOCAL_INSTALL` directory on the DVD-ROM, ISO image, or local directory and execute:

```
./omnisetup.sh
```

As soon as the procedure is completed, you can start using Data Protector.

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

## What's next?

Once the Installation Server system is upgraded, check if you have to apply any modifications to your configuration files. See ["Checking configuration changes"](#).

## Upgrading the Windows Cell Manager and Installation Server

When the previous version of Data Protector is detected, the same component set as installed is assumed by the operating system (without obsolete components). The installed components are removed and the new components are installed as for a new (clean) installation.

The Windows Installation Server is upgraded automatically during the upgrade procedure if it is installed on the same system as the Cell Manager. The old Installation Server depot is removed and if the Installation Server component is selected during the installation, the new Installation Server depot is copied to its place.

If the Installation Server is installed together with the Data Protector client, and this client is upgraded remotely (using the Data Protector GUI), the Installation Server is upgraded as well.

**Important:** Re-import the upgraded Installation Server after the installation procedure has finished. For details, see ["Importing an Installation Server to a cell"](#).

### Considerations

- **Microsoft Cluster Server**

The upgrade procedure for the Cell Manager, running in the Microsoft Cluster Server environment, is different from the upgrade procedure for the Cell Manager not configured for use with Microsoft Cluster Server. The detailed steps you need to follow are described in ["Upgrading the Cell Manager configured on Microsoft Cluster Server"](#).

- You cannot upgrade Data Protector directly if the installation path:
  - contains non-ASCII characters
  - contains the characters "@" or "#"
  - contains a directory that ends with the character "!"
  - is longer than 80 characters.

For workarounds, see ["Upgrading to Data Protector 8.10 fails if the previous version of the product is installed in a long path"](#) and ["Upgrading to Data Protector 8.10 fails if the previous version of the product is installed in a path with unsupported characters"](#).

### Upgrade procedure

To upgrade the Windows Cell Manager and Installation Server to Data Protector 8.10, follow the procedure described below:

1. Insert the Windows installation DVD-ROM or mount the ISO image and run the `\Windows\x8664\setup.exe` command. Setup detects the old Data Protector installation. Click **Next** to start the upgrade.

2. In the **Component Selection** page, the components previously installed on the system are selected. Note that you can change the component set by selecting or deselecting additional components. For a description of selected components, see the next step of the wizard. Click **Next**.
3. Optionally, change the user account or the ports used by the Data Protector services Internal Database Service and Application Server.

Click **Next**. For details on these services, see ["After the installation"](#) .

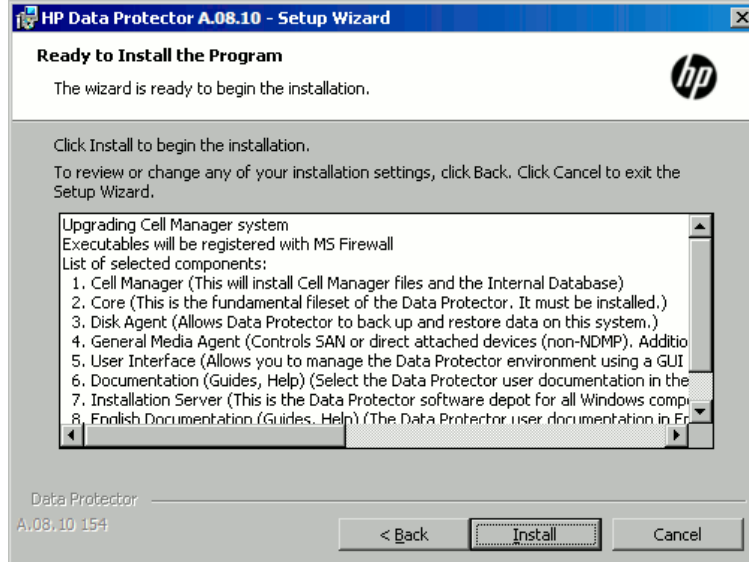
4. If Data Protector detects Windows Firewall on your system, the Windows Firewall configuration page is displayed. Data Protector setup will register all necessary Data Protector executables. By default, the **Initially, enable newly registered Data Protector binaries to open ports as needed** option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

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

Click **Next**.

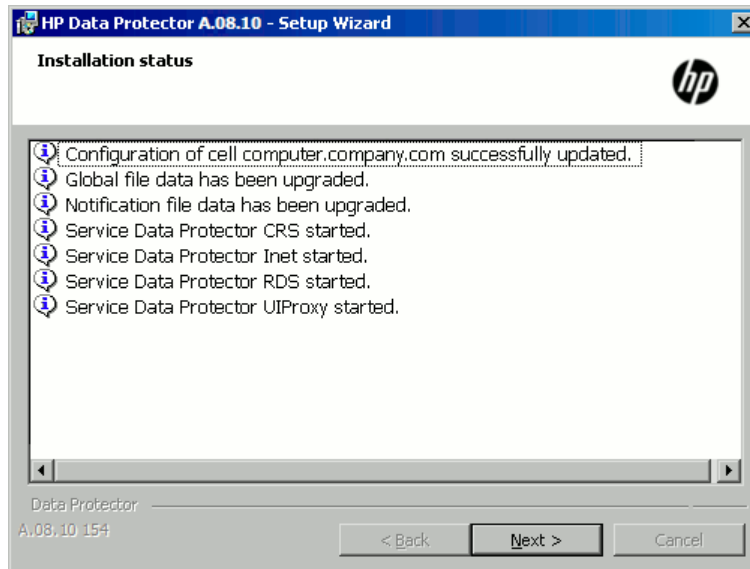
5. The component summary list is displayed. Click **Install** to perform the upgrade.

**Figure 40: Component selection summary page**



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

**Figure 41: Installation status page**



7. This step is performed only for a Cell Manager upgrade. If the Installation Server installed on a client other than the Cell Manager is being upgraded, this step does not occur.

If the User Interface component has been upgraded or newly installed, to start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

If the English Documentation (Guides, Help) component has been upgraded or newly installed, to view the *HP Data Protector Product Announcements, Software Notes, and References* immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

8. Click **Finish**.
9. Restart the services by executing `omnisv -start` command.

As soon as the procedure is completed, you can start using Data Protector.

### *What's next?*

- Once the Cell Manager and Installation Server systems are upgraded, check if you have to apply any modifications to your configuration files. See ["Checking configuration changes"](#).
- You must manually adjust the library capacity (VTLCAPACITY) of a virtual tape library, which was created with a previous version of Data Protector, and is after the upgrade to Data Protector 8.10 by default set to 1 TB. See ["Checking configuration changes"](#).

## Checking configuration changes

### Global options file

During the upgrade, the contents of the *old* global options file are merged with the contents of the *new* (default) global options file on the Cell Manager, located at:

**Windows systems:** `Data_Protector_program_data\NewConfig\Server\Options`

**UNIX systems:** `/opt/omni/newconfig/etc/opt/omni/server/options`

The *merged* file `global` resides at the same location on the Cell Manager as the old one and is used by the upgraded version of the product. The *old* global options file is renamed to `global.1`, `global.2`, and so on, depending on the number of upgrades performed.

The following applies when the merged file is created:

- Global options that were active (uncommented) in the old file remain active in the merged file. The following comment, stating that the value of the option was copied from the old file, is added to the merged file:

```
Option=Value
# Data Protector 8.10
# This value was automatically copied from previous version.
```

- Global options that are not used anymore, are commented (made inactive) in the merged file and added the following comment stating that the option is no longer in use:

```
#Option=Value
# Data Protector 8.10
# This value is no longer in use.
```

- Global options with values, not supported anymore, are commented (made inactive) in the merged file. The following comment is added, containing a template line (*DefaultValue*) and stating the previous value of this option:

```
# Option=DefaultValue
# Data Protector 8.10
# This variable cannot be transferred automatically.
# The previous setting was:
# Option=Value
```

- Comments are not transferred to the newly merged file.

Descriptions of the new options are in the merged global options file. For more information about the global options use, see the *HP Data Protector Troubleshooting Guide*.

### Manual steps

The following list summarizes the steps you must perform manually once the upgrade procedure has successfully completed:

- Omnirc options

After upgrading the Cell Manager and Installation Server systems, you may want to edit the `omnirc` file. For instructions, see section *How to use omnirc options?* in the *HP Data Protector Troubleshooting Guide* and in the *HP Data Protector Help*.

- Command line

You may need to make adjustments for your scripts that invoke Data Protector commands:

- For a general list of newly introduced commands, commands that have been changed or are provided with extended functionality, and commands that are no longer available in Data Protector 8.10, see ["Command line changes after upgrading to Data Protector 8.10"](#). For command usage synopses, see the *HP Data Protector Command Line Interface Reference* or the corresponding man pages.
- In Data Protector 8.10, the `omnidbrestore` command is replaced with the extended `omniofflr` command that provides the same functionality. Until you replace the `omnidbrestore` command lines with the `omniofflr` command lines, you can use the script `omnidbrestore.pl` that is supplied for your convenience. It recognizes the same set of options as `omniofflr`. Invocations of the script should be in the following format where `OMNIOFFLR_OPTIONS` are `omniofflr` command options without the `-idb` option:

**Windows systems:**

```
perl omnidbrestore.pl OMNIOFFLR_OPTIONS
```

**UNIX systems:**

```
omnidbrestore.pl OMNIOFFLR_OPTIONS
```

- Verify that the `hosts` file contains the fully qualified domain names (FQDNs) in the `computer.company.com` format. If needed, update the file accordingly. The file resides at the following location:

**Windows systems:** `%SystemRoot%\system32\drivers\etc\`

**UNIX systems:** `/etc/hosts`

- Changed default block size of backup devices

Pay attention to an increased default block size for physical backup devices and other device types in device configuration wizard of Data Protector 8.10. Specific use cases, for example, object copying, object mirroring, and object consolidation, require careful selection of backup device block sizes. Devices configured with the default block size in Data Protector 8.10 may not meet such use case requirements when used in conjunction with devices configured with the default block size in an earlier product version.

## *Non-converted Internal Database parts after an upgrade from Data Protector 6.20 or 7.00*

To ensure an efficient upgrade, the Data Protector 8.10 upgrade process does not automatically upgrade (convert) specific parts of the Internal Database to the new format. The non-converted parts are nevertheless actively used in the new product version. Files constituting these IDB parts are located in the following directory:

**Windows systems:** `Data_Protector_program_data\db40`

**UNIX systems:** `/var/opt/omni/server/db40`

The directory continues to be used in Data Protector 8.10 until either of the following happens:

- Catalog protection expires for all backup data that was referenced in the DCBF of the earlier product version at the time of upgrade.
- You trigger migration of the legacy DCBF to the new format using the `omnimigrate.pl` command.

For more information, see ["Migrating the Detail Catalog Binary Files \(DCBF\)"](#).

**Caution:** The above-mentioned directory should not be manually removed. Failing to do so may result in a data loss.

### *What's next?*

Once the Cell Manager and Installation Servers are installed and all required modifications implemented, HP recommends that you distribute the software to clients. See ["Upgrading the clients"](#).

## **Internal database changes after upgrade from Data Protector 6.20 or 7.00**

Data Protector 8.00 introduced a new Internal database (IDB) which differs significantly from the IDB in Data Protector version 7.00 or earlier. This includes changes in the IDB structure, size, and operation. As a result, you may also need to migrate some parts of the IDB after the conversion.

### ***Migrating the Detail Catalog Binary Files (DCBF)***

After the upgrade, Data Protector is fully operational. However, all objects whose catalogs are still protected and were backed up prior to the upgrade still have their catalogs stored in the old format. When catalogs expire, the old DC Binary Files are automatically deleted (through daily maintenance tasks). Old database files are however kept as long as there are any filenames in any of the old catalogs files which are protected and continue to occupy disk space.

Data Protector helps you to identify the protected media, objects, and sessions that still need the old DC Binary Files and IDB files, and the amount of space they occupy, and writes a report (warning) to the Event log. You can also execute the report manually from the CLI:

```
omnimigrate.pl -report_old_catalog [media | sessions | objects]
```

Catalogs for permanently protected objects, media, and sessions will not expire and must be migrated manually.

**Tip:** The migration process can take a significant amount of time. Therefore, HP recommends that you wait until most of your old media expire and you trigger the migration only for permanently protected media.

To migrate the catalog files, execute:

```
omnimigrate.pl -start_catalog_migration
```

For the conversion duration and space requirement estimates, see ["IDB conversion duration and changes in IDB size and structure"](#).

**Important:** After you finish the upgrade, back up the IDB. The old IDB backups cannot be used with Data Protector 8.10.

## ***IDB conversion duration and changes in IDB size and structure***

During the upgrade process, the IDB is converted to the new format. The conversion duration depends on the size and complexity of the existing database as well as on the performance of your hardware. Note that the examples given below may differ in your environment.

### ***IDB size after IDB migration***

The size of the new IDB depends on the size of the original IDB and its structure; therefore it is not possible to exactly predict the new size. During tests, 1 GB tended to be sufficient for medium sized databases. The installation will check for an additional 1 GB of available space and display a warning if this space is not available. If you are migrating large databases, you will likely need more free space.

### ***Detailed Catalog Binary Files migration***

The DCBF format in Data Protector 8.10 is changed and the DCBFs now contain the file version information. Additionally, the space requirements for the new DCBFs change as well.

The DCBF size increases because the filenames are now stored in the DCBF, therefore it is not possible to exactly predict the new size. However, a rough guideline is an increase of approximately four times. Some example conversions are listed in the following table:

<b>Old DCBF size</b>	24 MB	48.4 MB	97.3 MB
<b>Upgrade duration (minutes:seconds)</b>	1:51	3:33	6:13
<b>New DCBF size</b>	90.6 MB	181 MB	417 MB

### ***Serverless Integrations Binary Files migration***

During the upgrade process, data contained in the Serverless Integrations Binary Files (SIBF) is moved to the Catalog Database (CDB) part of the IDB, and becomes its integral part. Thus, the SIBF part of the IDB is no longer used, and the following IDB installation directories are not present in Data Protector 8.10:



**Windows systems:** `Data_Protector_program_data\server\db80\meta`

**UNIX systems:** `/var/opt/omni/server/db80/meta`

## ***Importing legacy NDMP media***

Ownership of objects backed up from UNIX file systems and stored on NDMP media was incorrectly handled in Data Protector versions earlier than 8.10. When legacy NDMP media are imported to Data Protector 8.10, ownership flags of such objects are set to 0 0 (owner, group), since the original ownership information is missing.

## ***Ordinal numbers in session IDs***

Due to an increased limit on a specific backup session concurrency metric in Data Protector 8.10, session IDs may contain 5-digit ordinal numbers. Additionally, in the Data Protector debug messages, ordinal numbers lower than 10 000 are padded with zeroes. For example, the first backup session run on 1 January 2013 is logged with the ID 2013/01/01-0001 in the debug files.

You may need to revise and possibly adapt scripts that you have been using in conjunction with Data Protector to consider the above changes.

## **Upgrading the clients**

### ***Upgrade sequence***

For information about the sequence in which the client upgrade is performed, see ["Upgrade overview"](#) .

On platforms where remote installation is supported, HP recommends that you upgrade the clients remotely.

### ***Upgrading clients remotely***

For the procedure on how to upgrade the clients using the Installation Server, see ["Remote installation"](#) . On UNIX systems, you must upgrade the already present components before you add new components. After new components are added, the components from previous versions are not displayed by Data Protector. In this case, you have to reinstall them.

### ***Upgrading clients locally***

If you do not have an Installation Server installed on your network, or if for some reason you cannot distribute the Data Protector software to a client system, Data Protector clients can be upgraded locally.

To upgrade Windows clients locally, see ["Installing Windows clients"](#) .

To upgrade UNIX clients locally, see ["Local installation on UNIX and Mac OS X systems"](#) .

## ***Upgrade-related operating system specifics***

### ***Upgrading Windows, HP-UX, and Linux clients***

During an upgrade to Data Protector 8.10, the enhanced incremental backup database is not migrated to the new release version. The old enhanced incremental backup repository is deleted from the directory *Data\_Protector\_home\enhincrd\MountPoint* (Windows systems) or */var/opt/omni/enhincrd* (UNIX systems). During the first full backup after the client upgrade, a new repository is created at the same location. Ensure the type if your first backup performed after the upgrade is full.

### ***Upgrading Linux clients***

If the *xinetd* service is used instead of *inetd*, the */etc/xinetd.d/omni* file is *not* replaced and thus the settings remain unchanged. To check if the *xinetd* service is running, run the following command:

```
ps -e | grep xinetd
```

To replace your settings with the default Data Protector settings or to replace a corrupted file, remove the file and remotely upgrade any Data Protector software component from the Data Protector GUI. The */etc/xinetd.d/omni* file is then installed with the default settings.

**Important:** By replacing the */etc/xinetd.d/omni* file, your modifications are lost. To retain your modifications, create a backup copy in advance and manually transfer the settings to the newly installed file after the upgrade.

### ***Upgrading Solaris 8 to Solaris 9 systems***

Starting with Data Protector 7.00, upgrading the operating system on the Data Protector Disk Agent clients from Solaris 8 to Solaris 9 is no longer supported.

If you still have Disk Agent (DA) of an earlier Data Protector version installed on Solaris 8, to upgrade the operating system to Solaris 9, follow instructions in the corresponding section of the *HP Data Protector Installation and Licensing Guide* of the earlier product version.

### ***Upgrading clients configured on HP Serviceguard***

If you are upgrading the client that uses HP Serviceguard, and if the Data Protector integration component to be upgraded is installed on the same node as the Cell Manager, first upgrade the physical nodes, and then perform the following:

1. Export the virtual host by executing:

```
omnicc -export_host virtual_hostname
```

2. Re-import the virtual host by executing:

```
omnicc -import_host virtual_hostname -virtual
```

### ***Upgrading integration clients***

If you are upgrading a Data Protector client that has the integration installed (such as the integration for Oracle, SAP R/3, Microsoft Volume Shadow Copy Service, or HP P6000 EVA Disk Array Family, the Automatic Disaster Recovery module, the integration for Microsoft Exchange Server, Microsoft SQL

Server, HP P9000 XP Disk Array Family, or EMC Symmetrix, and so on), follow the steps described in sections below to successfully perform the upgrade:

- For instructions on how to upgrade the Oracle integration, see ["Upgrading the Oracle integration"](#) .
- For instructions on how to upgrade the SAP R/3 integration, see ["Upgrading the SAP R/3 integration"](#) .
- For instructions on how to upgrade the Microsoft Volume Shadow Copy Service integration, see ["Upgrading the Microsoft Volume Shadow Copy Service integration"](#) .
- For instructions on how to upgrade the HP P6000 EVA Disk Array Family integration, see ["Upgrading the HP P6000 EVA Disk Array Family integration"](#) .
- For instructions on how to upgrade the Virtual Environment integration, see ["Upgrading the Virtual Environment integration"](#) .
- For instructions on how to upgrade the Microsoft Exchange Server, Microsoft SQL Server, HP P9000 XP Disk Array Family, or EMC Symmetrix integration, or any other integration, see ["Upgrading other integrations"](#) .

## ***Upgrading the Oracle integration***

The clients that have the Oracle integration installed are upgraded either locally, by running the `omnisetup.sh -install oracle8` command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, by remotely installing the Oracle integration agent to the client using the Data Protector GUI. Note that on UNIX, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-install oracle8` option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

### ***User root is no longer required***

On UNIX clients, the Data Protector Oracle Server integration no longer configures, checks the configuration of, and browses Oracle databases under the user `root`. Now, these operations run under the operating system user account that you specify in a backup specification. Therefore, you can safely remove the user `root` from the Data Protector user group.

**Note:** For ZDB and instant recovery sessions, the user `root` is still required.

After the upgrade, it is also recommended to perform a configuration check for each Oracle database, during which Data Protector copies the operating system user account (backup owner) from the backup specification to the corresponding Data Protector Oracle database configuration file.

If the configuration check is not performed, the configuration file is not updated. In such cases, during restore, Data Protector browses Oracle databases under the backup owner of the last backup session. If such a backup session has not been created in the last three months, the `root` user is used as the last option.

## ***Configuring an Oracle instance for instant recovery***

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you must either reconfigure the Oracle instance or set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options. See the *HP Data Protector Zero Downtime Backup Integration Guide*.

## ***Oracle ASM configurations using HP P6000 EVA Disk Array Family or HP 3PAR StoreServ Storage***

To enable support for creation of consistent replicas of the Oracle Server data on P6000 EVA Array or in HP 3PAR StoreServ Storage configurations in which Automatic Storage Management (ASM) is used, you need to upgrade both Data Protector components, the Oracle Integration and the HP P6000 / HP 3PAR SMI-S Agent, on the application system as well as on the backup system.

## ***Upgrading the SAP R/3 integration***

The clients that have the SAP R/3 integration installed are upgraded either locally, by executing the `omnisetup.sh -install sap` command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, by remotely installing the SAP R/3 integration agent to the client using the Data Protector GUI. Note that on UNIX, if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-install sap` option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

## ***SAP compliant ZDB sessions***

SAP standards recommend that BRBACKUP is started on the backup system during ZDB sessions (SAP compliant ZDB sessions). Data Protector 8.10 enables you to comply with these standards. First, configure the backup system as described in the SAP guide for Oracle (split mirror backup, software configuration) and install the Data Protector SAP R/3 Integration component on the backup system. Then, configure Data Protector for SAP compliant ZDB sessions as described in the *HP Data Protector Zero Downtime Backup Integration Guide*.

## ***Configuring an Oracle instance for instant recovery***

If the control files, recovery catalogs, or archive redo logs are located on the same volume group (if LVM is used) or source volume as the database files, you have three options:

- Reconfigure the Oracle instance.
- Set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options.
- Configure Data Protector to start BRBACKUP on the backup system (SAP compliant ZDB sessions).

For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

## ***Upgrading the Microsoft Volume Shadow Copy Service integration***

### ***Instant recovery-enabled backup sessions after upgrading from HP Data Protector HP Data Protector 6.20, Data Protector 7.00, and Data Protector 8.00***

After you upgraded the VSS integration from an older version of Data Protector, you need to resolve the source volumes on the application system if you will perform the ZDB-to-disk and ZDB-to-disk+tape sessions. Otherwise, the ZDB-to-disk sessions will fail and ZDB-to-disk+tape session will complete only with backups to tape not leaving the replicas on the disk array. Execute the resolve operation from any VSS client in the cell as follows:

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

For more information, see the *HP Data Protector Zero Downtime Backup Integration Guide*.

## ***Upgrading the HP P6000 EVA Disk Array Family integration***

### ***Considerations***

- When upgrading a pre-6.20 version of Data Protector to Data Protector 8.10, note that the *Loose* snapshot policy for replica creation on P6000 EVA Array was no longer supported starting with the Data Protector version 6.20. The *Strict* snapshot policy is implied for all ZDB sessions involving this disk array. After the upgrade, when a ZDB session using the *Loose* snapshot policy is run, a warning is reported and the *Strict* snapshot policy is used instead, but the ZDB backup specification itself is not updated. To avoid such warnings, you need to manually update such ZDB backup specifications.

To manually update a ZDB backup specification to use the now implicit *Strict* snapshot policy, open the backup specification in the Data Protector GUI, change any of its options and change it back, and finally save the backup specification by clicking **Apply**.

For information on snapshot policies for replica creation on P6000 EVA Array, see the *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Help*.

## ***Upgrading the Virtual Environment integration***

When upgrading the Data Protector Virtual Environment integration component from the Data Protector version 6.20 or earlier, run the following command after the new version has been installed on the corresponding clients:

```
vepa_util.exe --upgrade-cell_info
```

This is needed due to a change in password encoding in the `cell_info` file. It will re-encode the passwords used by the Virtual Environment integration, first creating a `cell_info.bak` file.

## Upgrading other integrations

If the Data Protector client has the Microsoft Exchange Server, Microsoft SQL Server, HP P9000 XP Disk Array Family, or EMC Symmetrix integration, or any other integration installed, upgrade such client either locally, using the `omnisetup.sh -installcomponent_list` command (UNIX systems) or the `setup.exe` command (Windows systems), or remotely, using the Data Protector GUI. For a list of the Data Protector component codes, see ["Local installation on UNIX and Mac OS X systems"](#). Note that if you are upgrading the client that does not reside on the Cell Manager, you do not need to specify the `-installcomponent_list` option. In this case, the setup will select the same components as installed on the system before the upgrade without issuing a prompt.

## Upgrading in a MoM environment

You can upgrade a MoM Environment sequentially. However, note the following limitations:

### Limitations

- You cannot use **distributed file media format** with your file libraries until all Cell Managers have been upgraded to Data Protector 8.10.

To upgrade your MoM environment to Data Protector 8.10, proceed as follows:

1. Upgrade the MoM Manager/CMMDB Server to Data Protector 8.10.

During the upgrade, Cell Managers in a MoM environment must not be operational. After the upgrade, the MoM Manager can still work with the old Cell Managers.

2. Upgrade each client Cell Manager in a MoM environment.

For the upgrade procedure, see ["Upgrading the UNIX Cell Manager and Installation Server"](#) and ["Upgrading the Windows Cell Manager and Installation Server"](#).

3. Upgrade clients with configured devices.
4. Upgrade clients with application integrations.

After this part of the upgrade is finished, you can backup and restore filesystems and integrations with the Data Protector 8.10 MoM GUI.

## Upgrading from the Single Server Edition

You can perform the upgrade from one of the following:

- From earlier versions of the Single Server Edition (SSE) to Data Protector 8.10 Single Server Edition. For details, see ["Upgrading from earlier versions of SSE to Data Protector 8.10 SSE"](#).
- From Data Protector 8.10 Single Server Edition to Data Protector 8.10. For details, see ["Upgrading from Data Protector 8.10 SSE to Data Protector 8.10"](#).

## Upgrading from earlier versions of SSE to Data Protector 8.10 SSE

The upgrade procedure from earlier versions of SSE to Data Protector 8.10 SSE is the same as the upgrade procedure from earlier versions of Data Protector to Data Protector 8.10. For the information, see ["Upgrading from Data Protector 6.20, 7.00, and 8.00"](#).

## Upgrading from Data Protector 8.10 SSE to Data Protector 8.10

### *Licenses*

You need to have a license to perform the upgrade from Data Protector 8.10 Single Server Edition to Data Protector 8.10. For details about licensing, see ["Data Protector Licensing"](#).

The upgrade from Data Protector 8.10 Single Server Edition to Data Protector 8.10 is offered for two possible scenarios:

- If you have the Data Protector Single Server Edition installed on one system (Cell Manager) only. See ["Upgrading the Cell Manager"](#).
- If you have the Data Protector Single Server Edition installed on multiple systems and you want to merge these cells. See ["Upgrading from multiple installations"](#).

**Note:** To upgrade from a previous version of the Single Server Edition to a full Data Protector installation, first upgrade your Single Server Edition to the full installation of the same version level. To upgrade this full installation to Data Protector 8.10, see ["Upgrading from Data Protector 6.20, 7.00, and 8.00"](#).

### *Upgrading the Cell Manager*

To upgrade the Single Server Edition Cell Manager, do the following:

1. Remove the Single Server Edition license:

#### ***Windows systems:***

```
del Data_Protector_program_data\Config\server\Cell\lic.dat
```

#### ***UNIX systems:***

```
rm /etc/opt/omni/server/cell/lic.dat
```

2. Start the Data Protector GUI and add a permanent password.

## Upgrading from multiple installations

To upgrade the Data Protector Single Server Edition installed on multiple systems, proceed as follows:

1. Select one of the existing Single Server Edition systems to be the new Cell Manager. See ["Choosing the Cell Manager system"](#).
2. Upgrade the selected Cell Manager by performing the following:
  - a. Remove the Single Server Edition license:  

```
del Data_Protector_program_data\Config\server\Cell\lic.dat (on Windows systems)
```

```
rm /etc/opt/omni/server/cell/lic.dat (on UNIX systems)
```
  - b. Start the Data Protector GUI and add a permanent password.
3. Import the other Single Server Edition systems into the newly created Cell Manager system as clients using the GUI.
4. Uninstall the Data Protector Single Server Edition from the other systems. See .
5. Import the media to the new Cell Manager.

For information about importing media, see the *HP Data Protector Help* index: "importing, media".

## Migrating the Cell Manager to a different platform

### Migration from PA-RISC HP-UX systems to Intel Itanium HP-UX systems

Data Protector 8.10 no longer supports PA-RISC architecture based HP-UX 11.11/11.23 systems as a Cell Manager platform. Therefore, you must migrate Cell Manager from a PA-RISC architecture based HP-UX 11.11/11.23 system to an HP-UX 11.23/11.31 system for the Intel Itanium 2 architecture before the upgrade.

For the migration procedure, see the *HP Data Protector Installation and Licensing Guide* of the appropriate product version.

### Migrating from 32-bit/64-bit Windows to 64-bit Windows/Windows Server 2008 or Windows Server 2012

Data Protector 8.10 no longer supports 32-bit Windows systems as a Cell Manager platform. Therefore, you must migrate the Cell Manager to a 64-bit Windows system before you start the upgrade procedure to Data Protector 8.10. For the migration procedure, see the *HP Data Protector Installation and Licensing Guide* from the appropriate product version.



## Migrating from Solaris to Linux

This section describes the procedure for migrating your existing Cell Manager from a Solaris system to a Linux system.

**Important:** Data Protector 8.10 no longer supports Solaris as a Cell Manager platform. Therefore, you must migrate the Cell Manager to a new platform before you start the upgrade procedure to Data Protector 8.10, using the installed Data Protector version.

### Procedure

1. Using your existing Data Protector installation, export all media catalogs on the current Cell Manager:
  - a. In the Context List, click **Devices & Media**.
  - b. In the Scoping Pane, expand **Media** and then expand **Pools**.
  - c. Expand the media pool with the media whose catalog you want to copy.
  - d. Select and right-click the media and click **Copy Catalog to File**.
  - e. Specify the output directory for the MCF files, which will contain media-related catalog data.
  - f. Click **Finish** to start copying and exit the wizard. For details, see the *HP Data Protector Help* topic *Copying the Catalog Media Data to the MCF File*.
2. Install Data Protector on the Linux system that will become the new Cell Manager. For details, see ["Installing a UNIX Cell Manager"](#).
3. If you changed the default Data Protector Inet port on the old Cell Manager, set the same Inet port also on the new Cell Manager. See ["Changing the default Data Protector Inet port"](#).
4. Import the MCF files to the new Cell Manager:
  - a. In the Context List, click **Devices & Media**.
  - b. In the Scoping Pane, expand **Media**, right-click **Pools**, and click **Import Catalog from MCF File** to open the wizard.
  - c. Specify MCF files you want to import.
  - d. Specify additional options for the session: by default, the **Import to original pool if possible** option is selected. Select the **Import Copy as Original option**.
  - e. Click **Finish** to start importing and exit the wizard.

For details, see the *HP Data Protector Help* topic *Importing the Catalog Media Data from the MCF Files*.

5. Configure the licenses on the new Cell Manager. See ["Data Protector 8.10 product structure and licenses"](#) .
6. Additional steps are required if the following is true:
  - Your cell is a part of the MoM environment. See ["MoM specifics"](#) .
  - Your cell works across a firewall. Reconfigure all firewall related settings on the new Cell Manager. See the *HP Data Protector Help* index: "firewall environments".
  - You want to have an Installation Server on your new Cell Manager. See ["Installation Server specifics"](#) .

After the migration is done, you can upgrade Data Protector.

## ***MoM specifics***

If the new Cell Manager will be configured in the MoM, additional steps are required after the basic migration procedure has been completed. The required steps depend on the configuration of the MoM for the old and new Cell Managers in your environment. The supported combinations are:

- The old Cell Manager was a MoM client; the new Cell Manager will be a MoM client of the same MoM Manager.

Perform the following steps:

- a. On the MoM Manager, export the old Cell Manager from the MoM Manager cell and import the new Cell Manager. See the *HP Data Protector Help* index: "client systems exporting".
  - b. Add the MoM administrator to the users list on the new Cell Manager. See the *HP Data Protector Help* index: "MoM administrator, adding".
- The old Cell Manager was a MoM Manager; the new Cell Manager will be a MoM Manager.

If the old MoM Manager was the only client in the MoM, no action is necessary. Otherwise, perform the following steps:

- a. On the old MoM Manager (the old Cell Manager), export all MoM clients.
- b. On the new MoM Manager (the new Cell Manager), import all MoM clients.
- c. Add the MoM administrator to the users list on all MoM clients.

## ***Installation Server specifics***

The migration of the Installation Server is not done as part of the Cell Manager migration. If Installation Server is installed on your old Cell Manager, it will not be migrated to the new Cell Manager and will stay the Installation Server for your cell.

To use the new Cell Manager also as an Installation Server, install the Installation Server component on the new Cell Manager after the migration and import it in the cell. See the *HP Data Protector Help* index: "Installation Server".

## Migrating a Windows Cell Manager Internal Database to a Different Server

The following scenario is an example of migrating an Internal Database (IDB) from one Windows Cell Manager server to another.

### Terminology

The following terminology is used in this scenario.

- **OLD\_SERVER.** The source Cell Manager from which the IDB will be moved.
- **NEW\_SERVER.** The destination Cell Manager to which the IDB will be moved.

### Prerequisites

- When using command line arguments, substitute the fully qualified domain name for OLD\_SERVER and NEW\_SERVER.
- If the OLD\_SERVER is running on Windows 2008, the NEW\_SERVER may run either Windows 2008 or Windows 2012.
- If the OLD\_SERVER is running on Windows 2012, the NEW\_SERVER must be running on Windows 2012.
- Both servers must have the same version of Data Protector installed on the Cell Manager.
- If the NEW\_SERVER has a different IP address than the OLD\_SERVER, you must move your licenses to the new IP address by contacting the HP Password Center (<http://webware.hp.com>).
- On the NEW\_SERVER you must be able to import the media that contains the full IDB backup from the OLD\_SERVER.
  - If the IDB backup is on a physical tape, you must configure a tape drive or library on the NEW\_SERVER and ensure that the tape is accessible.
  - If the IDB backup is on a file library backup device, you may need to export the file library from the OLD\_SERVER and import it to the NEW\_SERVER. For more information, see "[On NEW\\_SERVER](#)".
- The configuration, logs, and database files are stored under the *Data\_Protector\_program\_data* directory, usually C:\ProgramData\Omniback.

If you have installed to a different location, take note of the location for later use.

## Preparing for migration

Before you begin the migration, there are several tasks that must be performed on the OLD\_SERVER and the NEW\_SERVER to prepare them for the migration of the IDB.

### On OLD\_SERVER

- Run an extended database consistency check on the existing IDB on the OLD\_SERVER to validate data consistency prior to the migration.
- Perform a full backup of the existing IDB.

#### *Running an extended database consistency check*

1. Run `omnidbcheck -extended`.

This command validates data consistency in the following areas:

- Database connection
- Database and schema consistency
- Datafiles and media consistency

If any inconsistencies are detected, ensure that you first fix those problems and then perform the migration.

#### *Performing a full backup of the IDB on OLD\_SERVER*

For more information on performing a full backup of the IDB, see the *HP Data Protector Help*.

### On NEW\_SERVER

- Save a copy of the `cell_info` file, found in the *Data\_Protector\_program\_data* directory, usually `C:\ProgramData\Omniback\Config\Server\cell\cell_info`. This file will be used later.

#### *Using omnidownload and omniupload to transfer information about a file library*

1. On the OLD\_SERVER, use `omnidownload-library Library` to download information about the file library from the Data Protector IDB to an ASCII file.

For example, for an IDB backup to a file library named "FL1" use the command as follows:

```
omnidownload -library FL1 -file "C:\tmp\FL1.txt"
```

2. Copy the `omnidownload` output file to the NEW\_SERVER.

For example, copy to `C:\tmp\FL1.txt`.

3. On the NEW\_SERVER, use `omniupload -create_library <filename>.txt` to upload the library file and create a new backup device on NEW\_SERVER.

```
omniupload -create_library "C:\tmp\FL1.txt"
```

4. Import the media from the new backup device on NEW\_SERVER.

For details on commands, see the *HP Data Protector Command Line Interface Reference*. For details on importing media, see the *HP Data Protector Help*.

## Migration tasks

### *Prerequisite for Linux:*

- If the IDB is restored to a new host or Cell Manager, the user and group ID must be the same as the original Cell Manager.

Use the following commands to change the user and group ID on new host before installing the Data Protector:

- To determine the ID for `hdpd` user and group on the original host, use `cat /etc/passwd`.
- To set user and group ID on the new host, use:

```
usermod -u <NEWID> <LOGIN>
```

```
groupmod -g <NEWID> <GROUP>
```

```
usermod -g <GROUP> <LOGIN>
```

## Importing the IDB

### *To import the IDB on the NEW\_SERVER*

1. Once the media is imported, ensure that you can see the IDB backup session in the Data Protector GUI.
2. Create a new directory to be used for the restored IDB.

For example, create a directory at the following location:

```
C:\ProgramData\Omniback\server\db80_restore\idb
```

**Note:** You cannot restore the IDB from OLD\_SERVER to the same location on NEW\_SERVER, because it is in use.

3. In the Data Protector GUI Context List, click **Restore**.

4. In the Scoping Pane, expand **Restore Objects**, and then expand **Internal Database**.
5. Expand the OLD\_SERVER item, and click **Internal Database**.
  - a. On the Internal Database property page, to restore the basic Internal Database parts:
    - i. Select the **Restore Internal Database** option.
    - ii. Specify the temporary port to be used for the Internal Database Service during the restore, and the restore location as C:\ProgramData\OmniBack\server\db80\_restore\idb.
    - iii. Select **Restore catalog binary files** to restore the DCBF part of the IDB, and select the **Restore to original location** option.
  - b. On the Configuration Files property page:

*On Windows system:*

- i. Select **Restore to original location**.

**Note:** Ensure that the **Restore configuration files** option is checked.

- ii. Select Keep most recent from the **File conflict handling** list.

*On UNIX system:*

See ["IDB restore fails at the end of a restore process"](#) .

- c. Click **Restore** to start the restore of the IDB.

During restore, you might see the following error message along with few others; which can be ignored:

```
[Major] From: OB2BAR_POSTGRES_BAR@mrou77.usa.hp.com "DPIDB" Time: 10/9/2014
10:35:29 PM The OS reported error while accessing
C:/ProgramData/OmniBack/config/server/certificates: [80] The file exists.
```

- d. When the restore has completed, stop and start the Data Protector services.

```
omnisrv -stop
omnisrv -start
```

**Note:** If you encounter any issues after completing the IDB restore session, see [Troubleshooting](#).

## Post Restore Tasks

Perform the following post-restore tasks.

1. Run `omnidbutil -show_db_files` to ensure that the restored files exist in the directory created in Step 3 of ["Importing the IDB"](#) .
2. Add the NEW\_SERVER as the Cell Manager. See ["Adding the NEW\\_SERVER as the Cell Manager"](#)
3. Optionally, change the Cell Manager name in the IDB. See ["Changing the Cell Manager Name in the IDB"](#) .
4. Run `omnidbcheck -extended` to verify the consistency of the restored IDB. See ["Running an extended database consistency check "](#) .

## ***Adding the NEW\_SERVER as the Cell Manager***

*To add the NEW\_SERVER as the Cell Manager*

1. In the Data Protector GUI Context List, click **Clients**.
2. Delete the OLD\_SERVER item.
3. Import the NEW\_SERVER and ensure that it is shown as the Cell Manager.

*If the steps above do not work*

1. In a text editor, open the `cell_info` file that you saved in ["Preparing for migration"](#) .
2. Copy the line containing the host name of the NEW\_SERVER to your paste buffer.
3. Edit the `cell_info` file.
  - a. Add the entry for the NEW\_SERVER from your paste buffer.
  - b. Remove the entry for the OLD\_SERVER and save the `cell_info` file.
4. Restart the GUI.

## ***Changing the Cell Manager Name in the IDB***

If the NEW\_SERVER has a different host name than the OLD\_SERVER, you must change the Cell Manager name in the IDB.

For example, the OLD\_SERVER name is `oldcm.company.com` and the NEW\_SERVER name is `newcm.company.com`.

*On the NEW\_SERVER*

1. Run `omnidbutil -show_cell_name` to display which Cell Manager owns the IDB.

For example

```
> omnidbutil -show_cell_name  
Catalog database owner: "oldcm.company.com"
```

2. Run `-change_cell_name OldHost` to change the ownership of the IDB to the `NEW_SERVER`.

For example

```
> omnidbutil -change_cell_name oldcm.company.com  
This action will change ownership of libraries, devices, media pools and media.  
Are you sure [y/n]? y  
DONE!
```

## Next Steps

1. Migrate your clients to the `NEW_SERVER` by running the `omnicc` command.

Run the `omnicc -update_all -force_cs` command to update the version and installed components information in the `NEW_SERVER` `cell_info` configuration file for all clients in the cell.

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

2. Create a new IDB backup specification for the `NEW_SERVER` because the original one is configured to use the `OLD_SERVER`.

For more information, see the *HP Data Protector Help*.

3. Navigate to the Internal Database and check, if any sessions are in running state. If any, run the `omnidbutil -clear` command.
4. Stop and start the Data Protector services.

```
omnisrv -stop
```

```
omnisrv -start
```

## Troubleshooting

### *Problem*

**After completing the IDB restore operation, connecting from the Data Protector GUI to the Cell Manager fails**

After completing a restore operation, connecting from the GUI to the Cell Manager fails with the error:

```
A server error has occurred. Reported error message:  
couldn't connect to host.
```

The `hdpd-as` service process is not listening on port 7116.



## Action

1. Verify the listening port as 7116 by opening a command window and running the netstat command.

```
c:\> netstat -ban | findstr 7116 | findstr LISTEN
```

If the netstat command returns results, the listening port is properly configured.

If the netstat command does not return any results the port is improperly configured, for example:

```
c:\> netstat -ban | findstr 7116 | findstr LISTEN
c:\>
```

2. Take a backup of /etc/opt/omni/server/AppServer/standalone.xml file.

3. Replace all keystore and truststore passwords in /etc/opt/omni/server/AppServer/standalone.xml with ones stored in /etc/opt/omni/client/components/webservice.properties.

Navigate to the C:\ProgramData\OmniBack\Config\client\components directory and in webservice.properties file search for the following lines of code:

```
keystorePassword=jones7XE7EJjHzZ
truststorePassword=jones7XE7EJjHzZ
```

4. Take note of the keystore password for later use.
5. Open standalone.xml file in a text editor and search for the lines that contain keystore-password, such as:

```
<jsse keystore-password="JypjEnc0.9aG1"
keystoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.key
store"

truststore-password="JypjEnc0.9aG1"
truststoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.t
ruststore"/>
```

6. Replace all instances of keystore and truststore passwords in the standalone.xml file with the keystore password from the webservice.properties file from [Step 4](#) and save the file.
7. In a command window, navigate to C:\Program Files\OmniBack\bin.
8. Regenerate the certificate using the following command:

```
perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
where the <keystore-password> is the password noted in Step 4.
```

9. Stop and start the Data Protector services.

```
omnisrv -stop
```

```
omnisrv -start
```

10. Attempt to connect to the Cell Manager again.

### *Problem*

**After completing the IDB restore operation, connecting from the Data Protector GUI to the Cell Manager fails with SSL errors**

After completing a restore operation, connecting from the GUI to the Cell Manager fails with the error:

A server error has occurred. Reported error message:  
SSL peer certificate or SSH remote was not OK.

### *Action*

1. Navigate to the C:\ProgramData\OmniBack\Config\client\components directory and open the webservice.properties file:

```
# global property file for all components
jce-serviceregistry.URL = https://newcm.company.com:7116/jce-
serviceregistry/restws
```

```
keystorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client.key
store
```

```
truststorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client.t
ruststore
keystorePassword=jones7XE7EJjHzZ
truststorePassword=jones7XE7EJjHzZ
```

2. Take note of the keystorePassword and the truststorePassword.
3. In a command window, navigate to C:\Program Files\OmniBack\bin.
4. Regenerate the certificate using the following command:

```
perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
```

where the <keystore-password> is the password noted in Step 2.

5. Stop and start the Data Protector services.

```
omnisrv -stop
omnisrv -start
```

6. Attempt to connect to the Cell Manager again.

### *Problem*

**During an IDB backup, the IDB cannot be put into backup mode and fails**

During an IDB backup, the Session Messages display an error:

```
[Critical] From: OB2BAR_POSTGRES_BAR@oldcm.company.com "DPIDB" Time: 10/10/2014  
12:19:51 PM
```

Putting the Internal Database into the backup mode failed

### Action

1. Navigate to C:\ProgramData\OmniBack\Config\Server\idb and made a copy of the idb.config file as a backup.
2. In a text editor, open the idb.config file and search for PGOSUSER.

For example

```
PGOSUSER='OLD_SERVER\Administrator';
```

3. If the server name is not correct, edit it to the NEW\_SERVER name.

For example

```
PGOSUSER='NEW_SERVER\Administrator';
```

4. Stop and start the Data Protector services.

```
omnisrv -stop
```

```
omnisrv -start
```

5. Attempt the IDB backup again.

### Problem

#### IDB restore fails at the end of a restore process

IDB restore fails at the end of restore process with the message:

```
cannot execute omnidbutil -clear command
```

### Action

This could happen under the following circumstances in a HP-UX cell manager: When restoring to a different cell manager or on the same cell manager, but postgres passwords have changed after the backup session was restored or after a fresh cell manager installation.

**Note:** In a Linux environment, restore will complete successfully. This is because Linux mostly uses Operating System authentication on databases in contrast to HP-UX, which uses password authorization and in this case passwords files are not restored correctly. However the workaround should be applied in the Linux environment too, to have the correct password files.

1. Restore only the configuration files to another location <restore-conf> up to the point in time you are planning to restore the whole IDB.

2. Restore the whole IDB but don't choose to restore DCBFs or else restore the whole DCBFs to the original location.
3. Save a backup of `/etc/otp/omni/server/idb/idb.config` to `idb.config.bkp`
4. Perform file copies from the `<restore-conf>` location to the original location:
  - a. `cp <restore-conf>/etc/opt/omni/server/idb/idb.config /etc/opt/omni/server/idb/idb.config`
  - b. `cp <restore-conf>/etc/opt/omni/server/idb/ulist /etc/opt/omni/server/idb/ulist`
  - c. `cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml /etc/opt/omni/server/AppServer/standalone.xml`
5. Modify the following fields in `idb.config` to point to the correct location (correct locations are stored in `idb.config.bkp`)
  - a. `PGDATA_PG='/space/restore1/pg';`
  - b. `PGDATA_IDB='/space/restore1/idb';`
  - c. `PGDATA_JCE='/space/restore1/jce';`
  - d. `PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;`
6. Stop and start Data Protector services.
  - a. `run omniv stop` (this could take a while)
  - b. `run omniv start`
  - c. `run omnibutil -clear`

## Upgrading the Cell Manager configured in HP Serviceguard

During an upgrade procedure, only the database is upgraded, and the previous version of the product is removed. Data Protector 8.10 is installed with the default selection of agents, and other agents are removed. 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.

### *Prerequisites*

- The Data Protector services on the HP Serviceguard secondary node(s) should not be running.

This ensures the upgrade uses the IDB exported during the upgrade of the primary node and avoids an additional IDB export.

The upgrade procedure from 6.20, 7.00, Data Protector 8.00 consists of upgrading the primary and secondary nodes. Follow instructions in the order they are presented in the sections below.

### *Primary node*

Log on to the primary node and perform the procedure:

1. Stop the old Data Protector package by running the `cmhaltpkg PackageName` command (where *PackageName* is the name of the cluster package). For example:

```
cmhaltpkg ob2cl
```

2. Activate the volume group in exclusive mode:

```
vgchange -a e -q y VGName
```

For example:

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

3. Mount the logical volume to the shared disk:

```
mount LVPathSharedDisk
```

The *LVPath* parameter is the path name of the logical volume, and *SharedDisk* is the mount point or a shared directory. For example:

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

4. Start the Data Protector services:

```
omnisv -start
```

5. Upgrade the Cell Manager by following the instructions in the section "[Upgrading the UNIX Cell Manager and Installation Server](#)". Some steps are different depending on the product version you are upgrading from.

6. Stop the Data Protector services:

```
omnisv -stop
```

7. Dismount the shared disk:

```
umount SharedDisk
```

For example:

```
umount /omni_shared
```

8. Deactivate the volume group:

```
vgchange -a n VGName
```

For example:

```
vgchange -a n /dev/vg_ob2cm
```

### Secondary node

Log on to the secondary node and perform the procedure:

1. Activate the volume group in exclusive mode:

```
vgchange -a e -q y VGName
```

2. Mount the logical volume to the shared disk:

```
mount LVPPathSharedDisk
```

3. Upgrade the Cell Manager by following the instructions in the section "[Upgrading the UNIX Cell Manager and Installation Server](#)". Some steps are different depending on the product version you are upgrading from.
4. Rename the `csfailover.sh` and `mafailover.ksh` startup scripts in the `/etc/opt/omni/server/sg` directory (for example, to `csfailover_DP70.sh` and `mafailover_DP70.ksh`) and copy the new `csfailover.sh` and the `mafailover.ksh` scripts from the `/opt/omni/newconfig/etc/opt/omni/server/sg` directory to the `/etc/opt/omni/server/sg` directory.

If you customized your old startup scripts, reimplement the changes also in the new startup scripts.

5. Stop the Data Protector services:

```
omnisv -stop
```

6. Dismount the shared disk:

```
umount SharedDisk
```

7. Deactivate the volume group:

```
vgchange -a n VGName
```

### Primary node

Log on to the primary node again and perform the procedure:

1. Start the Data Protector package:

```
cmrunpkg PackageName
```

2. Configure the Cell Manager. Make sure not to be positioned in the `/etc/opt/omni` or `/var/opt/omni` directory or their subdirectories when running the script. Make also sure to have no mounted

subdirectories in the `/etc/opt/omni` or `/var/opt/omni`. Execute:

```
/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
```

3. Stop the Data Protector package:

```
cmhaltpkg PackageName
```

### *Secondary node*

Log on to the secondary node again and perform the procedure:

1. Start the Data Protector package:

```
cmrunpkg PackageName
```

2. Configure the Cell Manager. Make sure not to be positioned in the `/etc/opt/omni` or `/var/opt/omni` directory or their subdirectories when running the script. Ensure no subdirectories are mounted in the `/etc/opt/omni` or `/var/opt/omni` directory. Execute:

```
/opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
```

3. Stop the Data Protector package:

```
cmhaltpkg PackageName
```

### *Primary node*

Log on to the primary node once again and perform the procedure:

1. Start the Data Protector package:

```
cmrunpkg PackageName
```

Make sure that the package switching and switching for nodes options are enabled.

2. Re-import the virtual host:

```
omnicc -import_host VirtualHostname -virtual
```

3. Change the Cell Manager name in the IDB:

```
omnidbutil -change_cell_name
```

4. If you have the Installation Server in the same package as the Cell Manager, import the Installation Server virtual hostname:

```
omnicc -import_is VirtualHostname
```

**Note:** All requests coming from the Cell Managers are logged in the `/var/opt/omni/log/inet.log` file on the Data Protector clients. To prevent unnecessary log entries, secure the clients. See

"[Security considerations](#)" for information on how to secure a cell.

## Upgrading the Cell Manager configured on Microsoft Cluster Server

The upgrade of 6.20, 7.00, or 8.00 Cell Manager to Data Protector 8.10 on Microsoft Cluster Server (MSCS) is performed locally, from the Windows installation DVD-ROM or ISO image.

### *Prerequisites*

- The upgrade option is supported only if the previously installed Data Protector software is the Cell Manager installed in cluster-aware mode. If a system in the cluster has the Data Protector software installed as non-cluster-aware, you need to uninstall it prior to starting the setup.

### *Upgrade procedure*

To perform the upgrade, proceed as follows:

1. Insert the Windows installation DVD-ROM or mount the ISO image and run \Windows\_Other\x8664\setup.exe. It is recommended to start the setup on the currently active virtual server node.

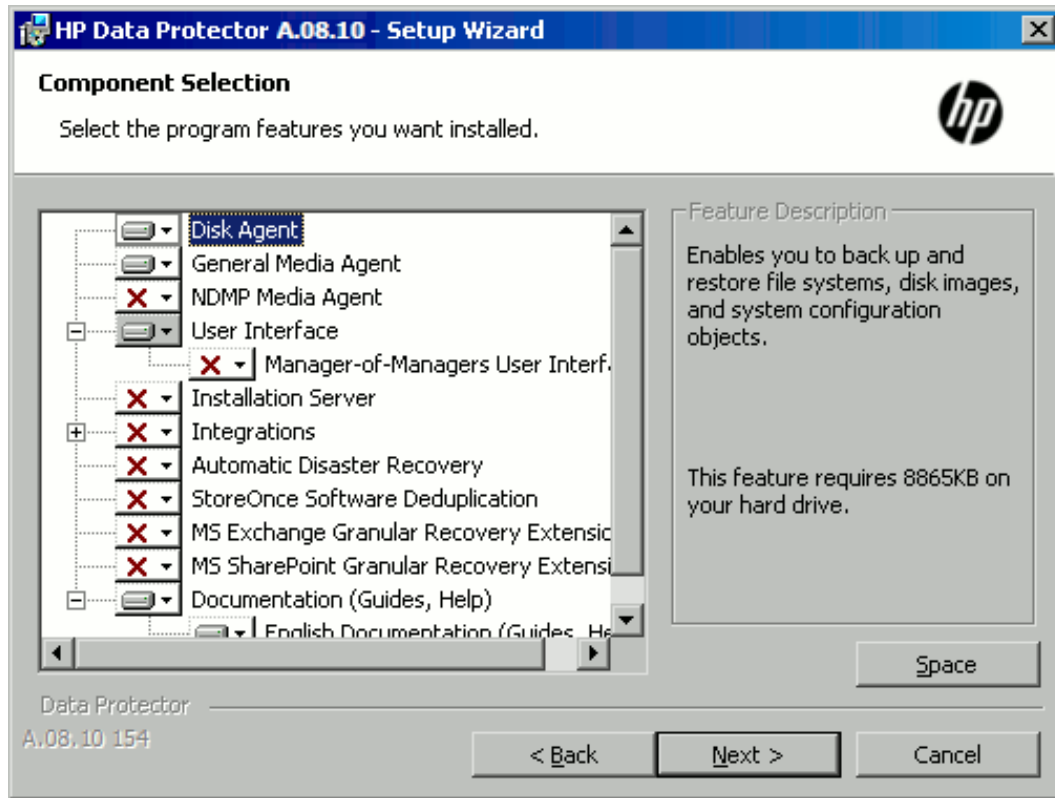
Setup automatically detects the old version of the product and prompts you to upgrade it to Data Protector 8.10.

Click **Next** to continue.

2. Data Protector automatically selects the components that were installed.



**Figure 42: Selecting the components**



Click **Next**.

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

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

Click **Next**.

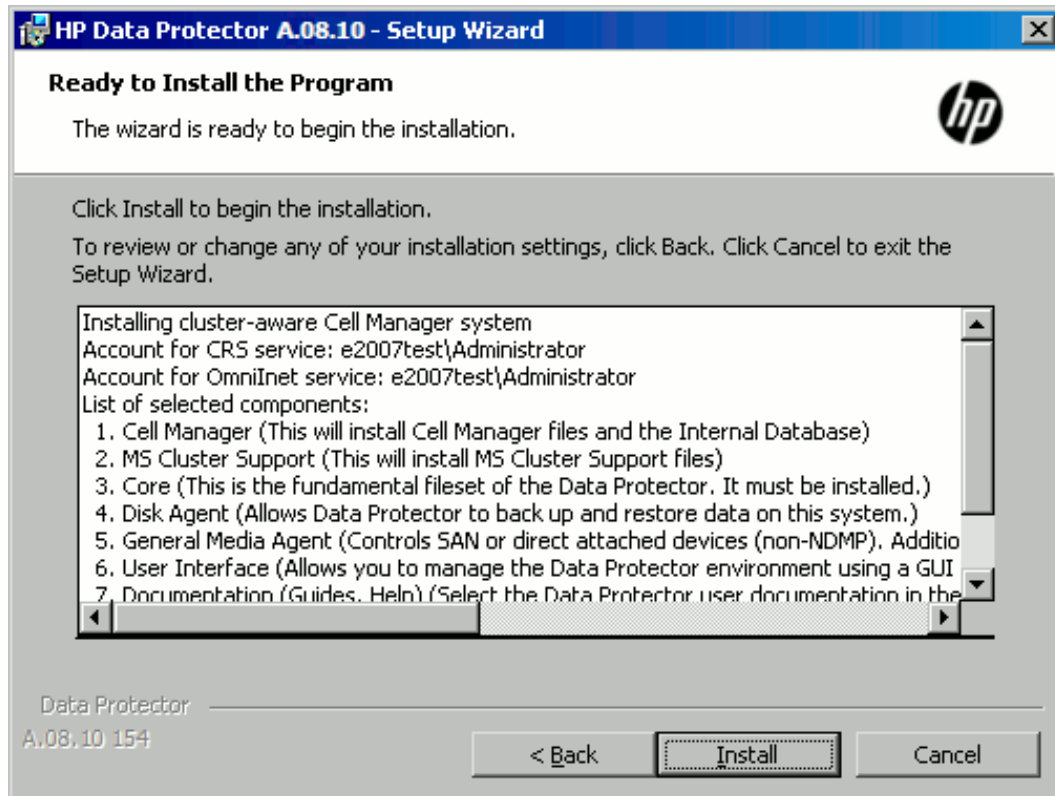
4. Optionally, change the user account used by the Data Protector IDB and HTTPS Application Server and the ports used by these services.

Click **Next**.

5. The component selection summary list is displayed. Click **Install** to perform the upgrade.

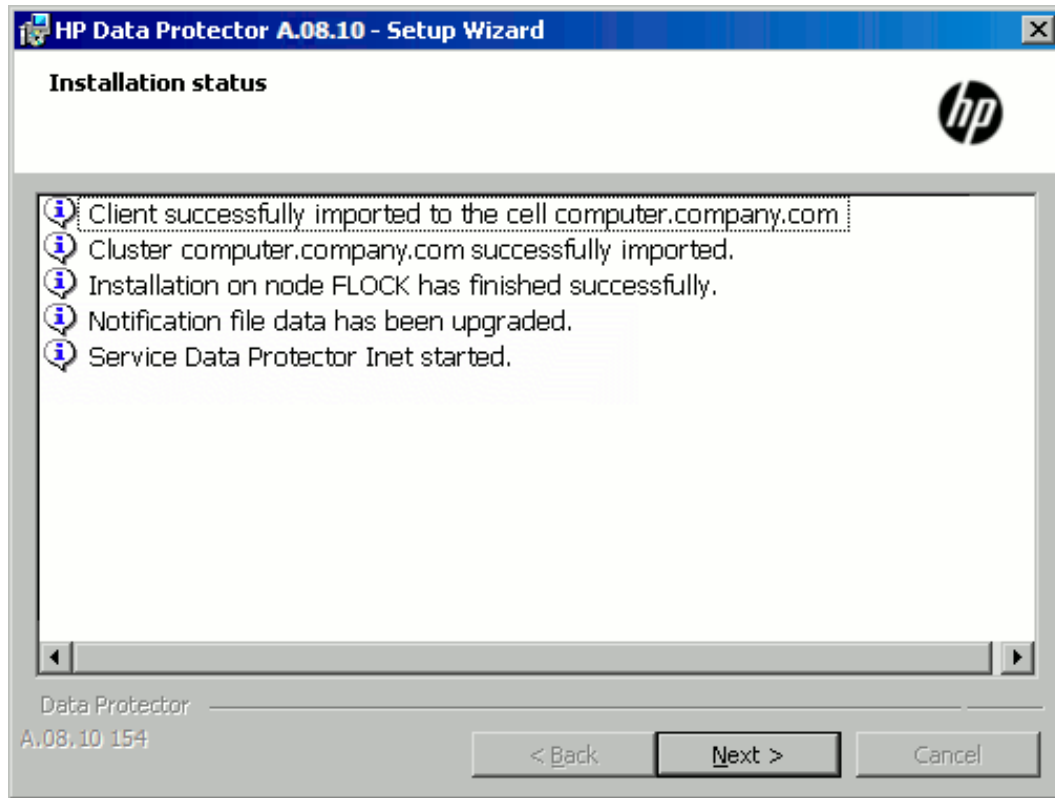
Note that after the upgrade, every node has the same component set.

**Figure 43: Component selection summary page**



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

**Figure 44: Installation status page**



7. If the User Interface component has been upgraded or newly installed, to start using the Data Protector GUI immediately after setup, select **Launch Data Protector GUI**.

If the English Documentation (Guides, Help) component has been upgraded or newly installed, to view the *HP Data Protector Product Announcements, Software Notes, and References* immediately after setup, select **Open the Product Announcements, Software Notes, and References**.

Click **Finish**.

**Note:** If you are upgrading cluster-aware clients, first upgrade every cluster node separately, and then re-import the virtual server. The remote upgrade is not supported.



# Chapter 5: Data Protector Licensing

This chapter contains information about:

- New license keys introduced
- Data Protector license checking and reporting
- Obtaining and installing Data Protector passwords
- Data Protector product structure and licenses

## Overview

HP Data Protector 8.10 supports two licensing schemes:

- Traditional licensing based on features and backup targets
- Capacity based licensing

## Traditional licensing

Data Protector supports essentially three different backup targets (snapshot, disk, and tape). Depending on which one used, you would license one or all targets as they also can be combined. In addition you can control the performance of the backup by parallelizing use of targets.

The Data Protector software product structure and traditional licensing model consists of three main categories:

- The Starter Packs: A management server (Cell Manager) is supported on HP-UX, Windows and Linux.
- Backup targets such as tape drive or jukebox licenses, referred to as Drive Extensions, for one drive, advanced backup to disk and Zero Downtime Backup both licensed by capacity
- 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, encryption, Instant Recovery, NDMP, and Granular Recovery Extension.

**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. The *Starter Pack* and *Drive extensions and Library extensions* passwords are bound to the Cell Manager and are valid for the entire Data Protector cell. Clients do not require any license for file system or disk image backups. Licenses of the *Functional Extensions* category either apply only to a specific client that is protected or cover the entire cell, depending on the license type.

## Capacity based licensing

The capacity based product structure is based on the volume of primary data protected by HP Data Protector and includes unlimited use of enterprise protection features. The capacity is measured in "Front End Terabytes" or Front End TB. The total amount of Front End Terabytes is defined as the aggregate amount of data from all systems being backed up. Per system it is measured as the largest full (that is, the total amount of source data protected). The licensing in this product structure is perpetual that covers all existing or new server, storage, apps, and so on.

The following features are included in the capacity based license:

- Cell Managers and Manager of Managers
- Tape Drives and Libraries
- Online Backup and Granular Recovery Extensions
- Zero Downtime Backup and Instant Recovery
- Advanced Backup to Disk and NDMP

The following licenses are not included in this product structure and must be ordered separately:

- Software encryption

You can find details about the product structure and licensing model in the document "*HP Data Protector software, Worldwide*" (PDF format) at <http://www.hp.com/go/dataprotector> by selecting the tab labeled **Resources** under **QuickSpecs**.

## New License Keys

### Requesting new passwords for existing licenses

If you are an existing Data Protector customer, in order to upgrade your old license passwords to version 8.10 of Data Protector, you have to have a valid active support agreement in place, covering the quantity and types of licenses you have in use.

Once you have received the new license keys, you should compare them to the quantity and type of license keys installed in your Data Protector environment. You should upgrade the software the software only after you have verified that you are in possession of enough valid HP Data Protector 8.10-based license keys.

If you have received fewer or different new license keys than there are actually installed in your Data Protector environment, you should not upgrade to Data Protector 8.10. Otherwise you risk that your Data Protector environment is no longer operational due to missing license keys.

Instead, you should contact your HP sales representative or HP partner first to determine what steps are needed to close the gap in the licensed functionality covered by your support contract and the actual licenses currently in use with Data Protector versions earlier than 8.10.

## New License key introduced

All old passwords (for versions earlier than 8.00, ovkey3-based) and Data Protector 8.00 (ovkey4 based) passwords are no longer valid and not recognized by HP Data Protector 8.10. For this version of Data Protector you have to request new license keys or passwords. For newly purchased licenses, you need to select the product version “8.10” when requesting a password. A password generated for HP Data Protector 8.10 will not work with any previous version of Data Protector.

After the upgrade, HP Data Protector 8.10 will run with a 60 days Instant-On password. The behavior will be identical to a fresh installation with an Instant-On password.

**Important:** As soon as *at least one new license key* for HP Data Protector 8.10 has been installed, the Instant-On password will be turned off and only installed valid keys will be recognized.

The activation of the instant-on passwords after the upgrade can be done only once.

**Tip:** After upgrade, existing licenses are still reported as invalid alongside the new (Instant-On) ones. To avoid that, rename (but do not delete) the file `lic.dat`:

**Windows systems:** Go to the directory `Data_Protector_program_data\Config\server\Cell` and rename the file:

```
ren lic.dat lic.bak
```

**UNIX systems:** Go to the directory `/etc/opt/omni/server/cell` and move the file:

```
mv lic.dat lic.bak
```

## License checking and reporting

Data Protector licenses are checked and if missing, reported during various Data Protector operations, for example:

- As a part of the Data Protector checking and maintenance mechanism, the licenses are checked and, if missing, reported in the Data Protector Event Log. The Data Protector Event Log is located on the Cell Manager in `Data_Protector_program_data\log\server\Ob2EventLog.txt` (Windows systems) or `/var/opt/omni/server/log/Ob2EventLog.txt` (UNIX systems). For more information on Data Protector checking and maintenance mechanism, see the *HP Data Protector Help* index: “Event Log, Data Protector”.
- When the Data Protector GUI is launched, if there are any missing licenses reported in the Data Protector Event Log, an Event Log notification is displayed. For more information on Data Protector Event Log, see the *HP Data Protector Help* index: “Event Log, Data Protector”.
- When a Data Protector session is started, the licenses are checked and, if missing, reported.

## Data Protector traditional licenses

Data Protector traditional licenses are with regard to their characteristics grouped as follows:

- Cell Manager related licenses
- Backup target related licenses (examples: tape drive or jukebox licenses, referred to as Drive Extensions, for one drive, advanced backup to disk and Zero Downtime Backup both licensed by capacity)
- Functional Extensions related licenses

## ***Cell Manager related licenses***

The Data Protector Cell Manager related licenses are:

- Starter packs
- Manager-of-Managers Extension
- Single Server Edition

When a certain Data Protector component, such as the Cell Manager (included in the Starter Pack) or the Manager-of-Managers (MoM) is present in the cell, only the presence of the required basic or special license is checked.

## ***Backup targets***

*For the following backup targets, Data Protector checks the number of configured items against the number of entity based licenses:*

- Library extension for one library with 61-250 slots and for one library with unlimited slots
- Drive extension for SAN / all platforms and Drive extension for Windows / Linux

The presence and number of the required entity based licenses is checked if any of the items that are the subject of the source based licenses is configured in the cell. If there are less licenses than configured items, Data Protector issues a notification.

When a backup device is configured in a SAN environment for several Data Protector clients, multipath functionality must be used for Data Protector to recognize it as a single backup device.

*The following backup targets are licensed by capacity:*

- UNIX Zero Downtime Backup for 1 TB and 10 TB
- UNIX Instant Recovery for 1 TB and 10 TB
- Linux Zero Downtime Backup for 1 TB and 10 TB
- Linux Instant Recovery for 1 TB and 10 TB
- Windows Zero Downtime Backup for 1 TB and 10 TB



- Windows Instant Recovery for 1 TB and 10 TB
- Direct Backup using NDMP for 1 TB and 10 TB
- Advanced backup to disk for 1 TB, 10 TB, and 100 TB

When a license for a backup target that is based on capacity (other than the advanced backup to disk license) is being checked, the amount of *total* disk space on logical units that have been backed up is compared to the capacity of licenses installed. For the advanced backup to disk license, see "[The advanced backup to disk license](#)"

License checking is done in such a way as not to prevent you from performing instant recovery or a backup even if you have run out of licensed capacity. In these circumstances a warning message appears during the backup session informing you that you have exceeded your licensed capacity.

Capacity of used disks is calculated based on historical information gathered during each ZDB backup session. The time interval taken into account is twenty-four hours. Data Protector calculates used disk capacity based on the disks that were used in all sessions in the last twenty-four hours and compares the calculated capacity with the licensed capacity.

If a license violation occurs, a warning message is issued during the backup. In addition, the license reporting tool is run daily and writes a notification to the Data Protector Event Log if the licensed capacity is exceeded.

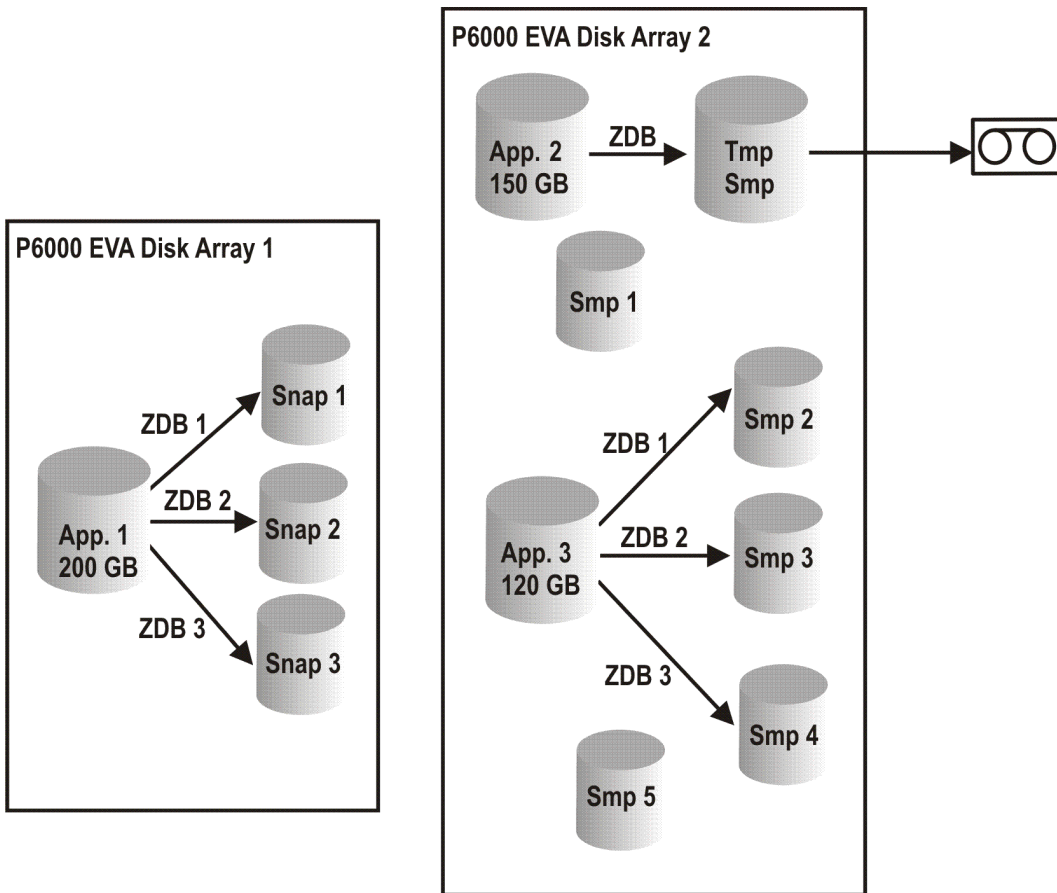
## ***Used capacity calculation for applying to backup targets***

The used capacity calculation calculates the licensed capacity of each disk array used in the past twenty-four hours. Disks used two or more times in the specified time interval are only counted once. Disk array units are identified by their identification numbers taken from each array. The use of array identification numbers means that it is possible to know when an array has already been counted.

If a ZDB backup has been run that includes instant recovery, the original unit's total capacity is calculated both for ZDB used capacity per disk array, and in addition, that used for instant recovery capacity per disk array.

For example, imagine a scenario where there are two P6000 EVA disk arrays. On one array there is a single disk (App.1) with a capacity of 200 GB being used for data protection. An instant recovery option is included with each backup session which are triggered three times a day. Three replicas at a time are kept, these are rotated for instant recovery purposes. On the second disk array there are two disks (App.2 and App.3) with capacities of 150 GB and 120 GB respectively. Backup is run once a day on App.2 disk and the snapshot is deleted after the data is moved to tape. On App.3, backup is run three times a day and five different replicas are rotated for instant recovery. See "[Used capacity calculation scenario](#)".

**Figure 45: Used capacity calculation scenario**



The calculation for ZDB used capacity counts all disks used in backup sessions in the last twenty-four hours  $200 \text{ GB (App. 1)} + 150 \text{ GB (App. 2)} + 120 \text{ GB (App. 3)} = 470 \text{ GB}$ .

Calculations for instant recovery used capacity count source capacity for ZDB sessions that left data for instant recovery purposes. The same disk is only counted once  $200 \text{ GB (App. 1)} + 120 \text{ GB (App. 3)} = 320 \text{ GB}$ .

## ***The advanced backup to disk license***

The advanced backup to disk license is required to back up to a Data Protector file library and can be used for a virtual tape library (VTL) instead of drive licenses.

- Usable native capacity of a Data Protector file library is the available size on disk for the file library, as reported by the filesystem.
  - Virtual full backups and the incremental backups that will be consolidated into a synthetic full or virtual full backup must be stored in the Data Protector file library, which requires this license.
- If Data Protector is using the VTL exclusively, it is recommended to license a quantity matching the physical capacity of the VTL, also referred as usable native capacity.

- Usable native capacity of a virtual tape library (VTL) is the size on disk of the virtual tape library consumed by all protected HP Data Protector backups as reported by the VTL.
- For each VTL, you can choose whether to use the backup to disk or tape drive licensing model. Within one VTL, both concepts must not be mixed.
- If the VTL has a built-in capability to migrate backup data from the disk cache to another disk or tape, the migrated storage capacity needs to be fully licensed. No drive and library licenses are required for the tape library exclusively controlled by the VTL, but ***the used capacity of all tapes in the physical tape library needs to be licensed***. However, this is not applicable if Data Protector object copy functionality has been used to migrate the backup data to another disk or tape.
- By default, Data Protector treats VTL devices as ordinary libraries (such as SCSI II libraries) and does not utilize capacity based licensing. To enable capacity based licensing, the device must be marked as a VTL during the device configuration.

For more information on how to configure a VTL via the graphical user interface (GUI), see the *HP Data Protector Help* index: “virtual tape library”. For more information on how to configure a VTL via the command-line interface (CLI), see the following ["Example"](#).

- In case of central licensing with the Manager-of-Manager (MoM), you need to assign at minimum 1 TB to each cell using the advanced backup to disk functionality.

**Note:** Data Protector cannot report the required amount of licenses due to the missing instrumentation and interfaces of today's Virtual Tape Libraries and some files servers hosting the Data Protector file library. It is your responsibility to license the capacity consistently with the licensing definitions.

### Example

If you configure a virtual tape library named “VTL\_2011” via the command-line interface (CLI) by using the `omniupload` command, you must specify the estimated library capacity in the configuration file for the string `VTLCAPACITY`. This estimated value consequently adds up to used licenses capacity for advanced backup to disk in the license checker report.

**Note:** The estimated virtual library capacity consumption value (`VTLCAPACITY`) in terabytes (TB) must be an integer to avoid the error message “Invalid VTL capacity specified”.

In the configuration file named “libVTL.txt” in the directory “C:\Temp” type the estimated library capacity, for example 11 and execute:

```
omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt
```

To verify library configuration, execute:

```
omnidownload -library VTL_2011  
  
#omnidownload -library VTL_2011  
NAME "VTL2011"  
DESCRIPTION ""
```

```
HOST computer.company.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 11
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
    "SCSI repository"
MGMTCONSOLEURL ""
```

The license checker reports the license capacity in use, which is the sum of used space on disk for the file library (FL) and the estimated size of disk space on a virtual tape library. For example, you are using 2 TB of the disk space by backing up with the FL and 10 TB of disk capacity on the VTL. The total capacity in use is 12 TB. If there are only 5 TB licenses capacity installed, you get a notification that you need additional 7 Advanced Backup to disk for 1 TB licenses.

```
#omnicc -check_licenses -detail
-----
License Category           : Advanced Backup to disk for 1 TB
Licenses Capacity Installed : 5 TB
Licenses Capacity In Use   : 12.0 TB
Add. Licenses Capacity Required: 7 TB

Summary
-----
Description                                     Licenses Needed
Advanced Backup to disk for 1 TB                  7
```

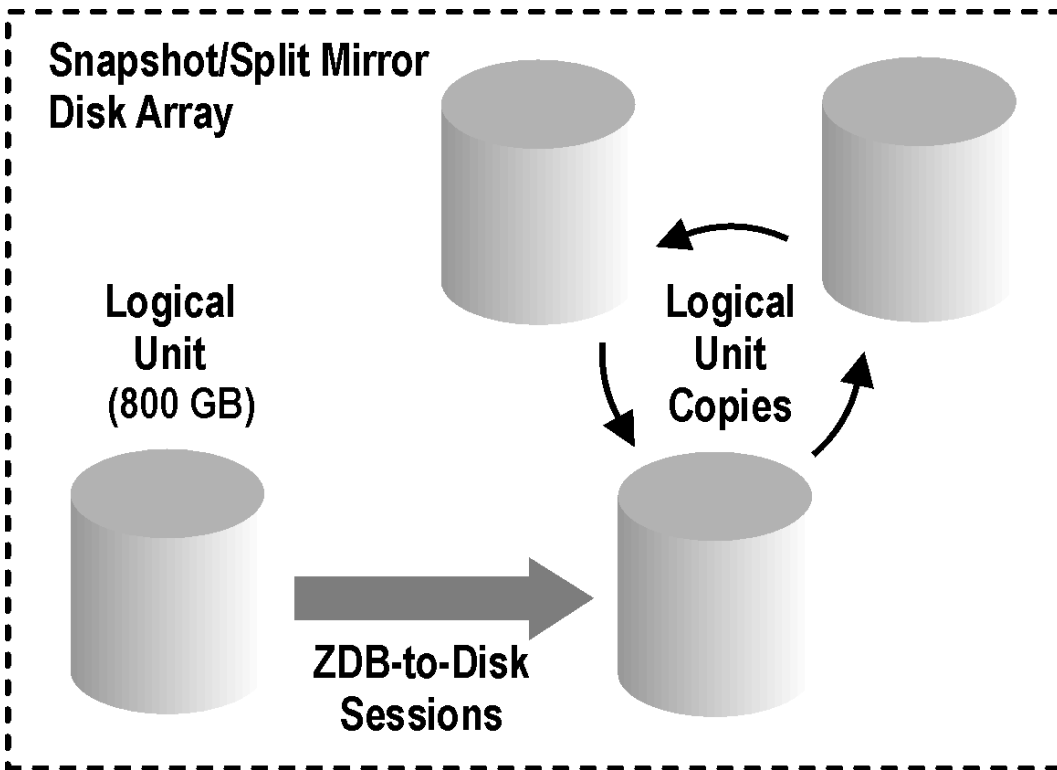
## ***Examples for backup targets based on licensed capacity***

This section provides examples of how capacity based licensing is calculated.

### ***Example 1***

"[ZDB-to-disk sessions](#)" shows a situation where data from one 800 GB logical unit is backed up three times a day in a ZDB-to-disk session.

Figure 46: ZDB-to-disk sessions



Three split mirror or snapshot copies (replicas) are rotated and kept for the purpose of instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk sessions:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$  for the “Zero Downtime Backup for 1 TB” license.

Three replicas of the same 800 GB logical unit are kept for the purpose of instant recovery. Note that it is the capacity of source volumes and not the capacity of replica that is the subject of the license:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$  for the “Instant Recovery for 1 TB” license.

One “Zero Downtime Backup for 1 TB” license and one “Instant Recovery for 1 TB” license are sufficient for this situation.

### Example 2

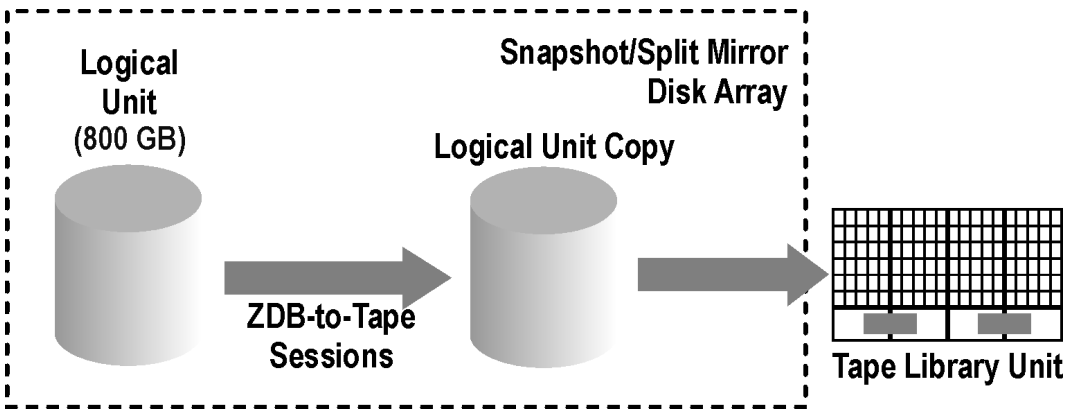
" [ZDB-to-tape sessions](#) " shows a situation where data from one 800 GB logical unit is backed up twice a day in a ZDB-to-tape session. Split mirror or snapshot copies (replicas) are, therefore, not kept for instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk sessions:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$  for the “Zero Downtime Backup for 1 TB license.

One “Zero Downtime Backup for 1 TB” license is sufficient.

Figure 47: ZDB-to-tape sessions



### Example 3

"ZDB-to-disk+tape sessions" shows a situation where data from one 800 GB logical unit is backed up three times a day in a ZDB-to-disk+tape session. Five split mirror or snapshot copies (replicas) are rotated and kept for the purpose of instant recovery. The capacity based licensing is calculated as follows:

One 800 GB logical unit is used for ZDB-to-disk+tape sessions:

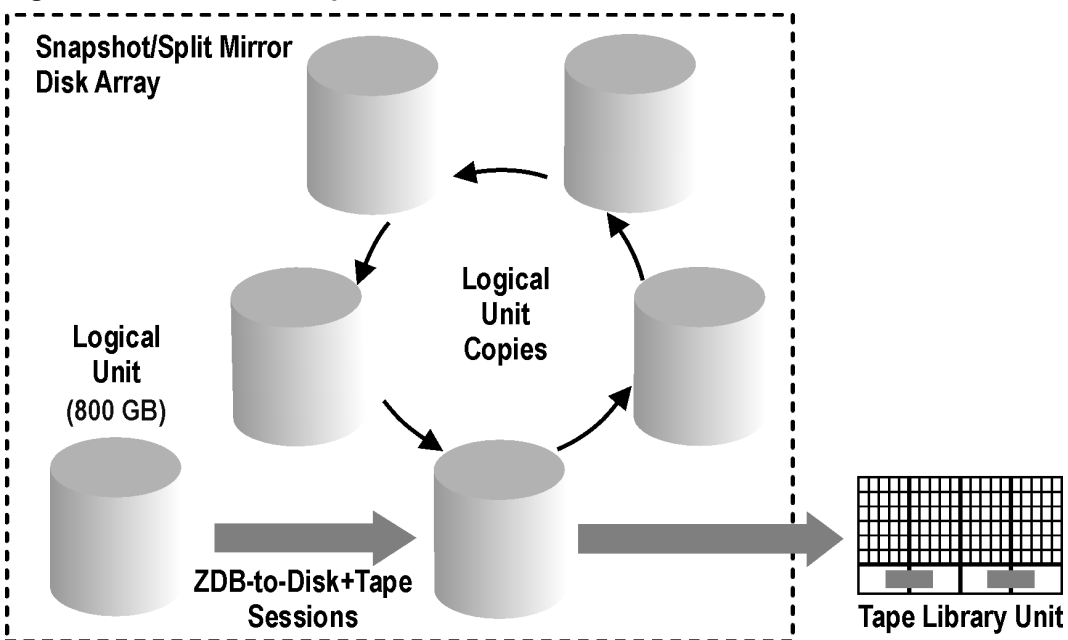
$1 \times 800 \text{ GB} = 0.8 \text{ TB}$  for the "Zero Downtime Backup for 1 TB" license.

Five replicas of the same 800 GB logical unit are kept for the purpose of instant recovery. Note that it is the capacity of source volumes and not the capacity of replica that is the subject of the license:

$1 \times 800 \text{ GB} = 0.8 \text{ TB}$  for the "Instant Recovery for 1 TB" license.

One "Zero Downtime Backup for 1 TB" license and one "Instant Recovery for 1 TB" license are sufficient.

Figure 48: ZDB-to-disk+tape sessions



### Example 4

One 200 GB logical unit, one 500 GB logical unit, one 120 GB logical unit, and one 300 GB logical unit are used in ZDB sessions:

$1 \times 200 \text{ GB} + 1 \times 500 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 1.12 \text{ TB}$  for the "Zero Downtime Backup for 1 TB" license.

Split mirror or snapshot copies of one 200 GB logical unit, one 120 GB logical unit, and one 300 GB logical unit are kept for the purpose of instant recovery:

$1 \times 200 \text{ GB} + 1 \times 120 \text{ GB} + 1 \times 300 \text{ GB} = 0.62 \text{ TB}$  for the "Instant Recovery for 1 TB" license.

One "Zero Downtime Backup for 1 TB" licenses and one "Instant Recovery for 1 TB" license are sufficient if all three examples in "ZDB-to-disk sessions" through "ZDB-to-disk+tape sessions" are configured in a cell.

## Data Protector Functional Extensions

The functional extensions licenses are required once per instance (system, library and terabyte) for:

- On-line extension for one UNIX system and On-line extension for one Windows / Linux system
- The Manager-of-Managers functionality
- Libraries with more than 60 media slots
- Data Protector encryption extension for one client system
- Instant Recovery
- NDMP backup
- Granular recovery extension for one database server

## Capacity based license reports

In the capacity based licensing mode, Data Protector lists only the number of capacity based licenses (with a granularity of 1 TB) and licenses that are not covered by capacity based licenses, that is the Software Encryption extension. Traditional licenses which are covered by capacity based licensing are not displayed.

**Figure 49: Capacity based license report TBD**

```
#omnicc -check_license -detail
```

WARNING: Calculation of total protected data size may take some time.

```
Report generated      : 03/03/2016 1:48:27 AM
Licensing mode       : Server
License server       : host.domain.com
```

```
-----
-
```

```
License Category      : Encryption Extension for one client system
```

```
Licenses Installed          : 0
Licenses Used              : 0
Additional Licenses Required : 0
-----
-
License Category           : HPE Data Protector - capacity based per TB SW
Licenses Capacity Installed : 9 TB
Licenses Capacity In Use   : 0 TB
Add. Licenses Capacity Required : 0 TB
```

#### Summary

-----  
Licensing is covered.

```
Total Protected Data      : 4,00 TB
-----
```

```
-
Backup Type                | Total Protected Data
-----
-
MS Filesystem              | 1GB
MS SQL                    | 1GB
SAP                       | 1GB
UNIX Filesystem           | 1GB
-----
```

The Total Protected Data is defined as the aggregate amount of data being backed up from all systems. The Total Protected Data for each system is measured as the sum of the following:

- Sum of the largest full backup of each object for the file system (including synthetic backups) and virtual environment backups.
- Sum of the largest full backup of each data set for each of the application integration backups.

**Note:** The unique object for each of the file systems and virtual environments is the actual object created at the time of backup. The actual object can be either: mount point, virtual machine, or virtual machine's disk.

The unique data set for each of the application integrations is identified differently, usually this is the database instance or server name.

#### Limitations



- When backing up the same data with multiple different agents, the backup is calculated multiple times. Few such examples of double calculations are as follows:
  - File system backup of database using VSS and application integration agent backup of the same database.
  - Virtual environment integration backup of virtual host and file system agent backup run inside the virtual machine (host).

**Note:** It is recommended to backup unique objects to overcome double calculations.

- When the Oracle backup object name format is externally reconfigured, this could result in the database name not being resolved from the new object names. Such object sizes could be incorrectly handled while calculating the total protected data.

**Note:** It is essential for a reconfigured format to still include the Oracle database name defined as <DBID\_\*.dbf for correctly adding Oracle objects in the total protected data size calculation.

## Producing a license report on demand

To produce a report about licensing related information from the cell, execute:

```
omnicc -check_licenses [-detail]
```

If the `-detail` option is not specified, the command returns information on whether the Data Protector licensing is covered or not. The following information is returned: the time when the report was generated, the licensing mode, and the license server.

If the `-detail` option is specified, a detailed report is produced. The license checker returns the following information for every license in the cell: license name, licenses installed, licenses used, and additional licenses (capacity) required.

Note that for drive extension licenses-to-use, the license checker returns information about configured drives and recommended additional licenses. You need as many licenses as there are drives in use at any point in time. This is typically the total number of configured drives to allow all drives to be used simultaneously.

Note that the command does not list the expiration dates for the licenses. Depending on the environment and the number of licenses installed, the report may take some time to generate. To get the information on the licenses expiration dates, execute:

```
omnicc -password_info
```

**Important:** In a MoM environment with the CMMDB configured, when producing a license report for the items that are subject to libraries and drives, the `omnicc` command must be run on the Cell Manager with the CMMDB installed.

For more information, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

## Data Protector passwords

Once you have installed Data Protector product, you can start using it for 60 days. After this period, you must install a permanent password on the Cell Manager to enable the software. You may load the software on the Data Protector Cell Manager, but you cannot perform configuration tasks without a permanent password, because the licenses required for particular Data Protector functionality require passwords.

The Data Protector licensing requires one of the following passwords:

- Instant-On password

An Instant-On password is built in the product when first installed. You are able to use the software for 60 days after you have installed it on any system supported by Data Protector. Within this period you must request your permanent password from the *HP Password Delivery Center (PDC)* and then install it.

For an existing Data Protector installation, after the upgrade to Data Protector 8.10 your installation is running with an Instant-On password for 60 days. Within this period you must request your new permanent passwords from the HP Password Delivery Center as specified in your active support agreement. Old licenses which are not covered in the support agreement cannot be upgraded.

- Permanent passwords

The Data Protector product is shipped with an *Entitlement Certificate* license that entitles you to obtain a permanent password. The permanent password permits you to configure a Data Protector cell with regard to your backup policy, provided that you have bought all required licenses. Before you request a permanent password, you must determine the Cell Manager system and understand your cell configuration requirements.

- Emergency password

Emergency or fallback passwords are available in case the currently installed passwords do not match the current system configuration due to an emergency. They will allow operation on any system for a duration of 120 days.

Emergency passwords are issued by the support organization. They must be requested by and are issued only to HP personnel. Refer to your support contact or see the HP Licensing site at: <http://www.webware.hp.com>.

The purpose of an emergency password is to enable the backup operation while the original system configuration gets reconstructed or until you move to a new permanent installation. In case of moving the licenses, you need to fill out the License Move Form and send it to the *HP Password Delivery Center (PDC)* or go to the webpage <http://www.webware.hp.com> where passwords can be generated, moved, and so on.

For instructions on how to obtain and install a password, see "[Obtaining and installing permanent passwords](#)".

## Obtaining and installing permanent passwords

### Obtaining

The following is the procedure to obtain permanent passwords:

1. Gather the information required in the Permanent Password *Request Form*. See "[Data Protector licensing forms](#)" to find the location of the forms and get instructions on how to fill them out.
2. See "[Data Protector 8.10 product structure and licenses](#)" for more information about the product structure. The *HP Password Delivery Center* will send your permanent password using the same method that you used when you sent your request. For example, if you sent your request by e-mail then you would receive your permanent password by e-mail.
3. Do one of the following:
  - Go to the online *HP Password Delivery Center* site at <http://www.webware.hp.com>.
  - Complete the *Permanent Password Request Form* and send it to the *HP Password Delivery Center* using one of the following (see the Entitlement Certificate shipped with the product for fax numbers, telephone numbers, email addresses, and hours of operation):
    - Faxing a form to the *HP Password Delivery Center*
    - Sending an e-mail to the *HP Password Delivery Center*

You can use the electronic version of the license forms that are included in the following files on the Cell Manager and the installation media:

**On Windows Cell Manager:** `Data_Protector_home\Docs\license_forms.txt`

**On UNIX Cell Manager:** `/opt/omni/doc/C/license_forms_UNIX`

**On Windows installation DVD-ROM:** `Disk_Label:\Docs\license_forms.txt`

to “copy” and “paste” your message to the *HP Password Delivery Center (HP PDC)*.

You will receive your permanent password within 24 hours of sending your *Permanent Password Request Form*.

### Installing

This section describes the procedure to install a permanent password that the *HP Password Delivery Center (HP PDC)* has sent to you.

### Prerequisite

You must have received permanent passwords sent from the *HP Password Delivery Center* and the Data Protector user interface must be installed on the Cell Manager. The passwords are installed on the Cell Manager and are valid for the entire cell.

## Using the GUI

To install the permanent password using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Data Protector Cell** and click **Add License**.
3. Type or copy the password exactly as it appears on the *Password Certificate*.

A password consists of 4-character groups of variable length, separated by a space and followed by a string. Make sure that you do not have a line-feed or a return character within this sequence. The following is an example of a password:

```
QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR  
KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK  
ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX  
ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
```

After you have typed in the password, check the following:

- Make sure the password appears correctly on the screen.
- Make sure there are no leading or trailing spaces, or extra characters.
- Double-check "1" (number one) characters and "l" (letter l) characters.
- Double-check "O" (uppercase letter O) characters and "0" (number zero) characters.
- Make sure that you have used the correct case. The password is case-sensitive.

Click **OK**.

The password is written to the following file on the Cell Manager:

**Windows systems:** `Data_Protector_program_data\Config\server\Cell\lic.dat`

**UNIX systems:** `/etc/opt/omni/server/cell/lic.dat`

## Using the CLI

To install the permanent password using the Data Protector CLI, proceed as follows:

1. Log on to the Cell Manager.
2. Execute the following command:

```
omnicc -install_license password
```

The *password* string must be entered exactly as it appears on the *Password Certificate*. It must be formatted as a single line and must not contain any embedded carriage returns. The password must be in quotes. If the password includes also a description in quotes, the quotes in this description must be preceded with backslashes. For an example and more information, see the `omnicc` man page or the *HP Data Protector Command Line Interface Reference*.

You can also append the password to the following file on the Cell Manager:

**Windows systems:** `Data_Protector_program_data\config\server\cell\lic.dat`

**UNIX systems:** `/etc/opt/omni/server/cell/lic.dat`

If the file does not exist, create it with an editor, such as `vi` or Notepad. For an example of a password, see ["Type or copy the password exactly as it appears on the Password Certificate."](#) in the procedure for the graphical user interface.

## Verifying the password

### *Using the GUI*

To verify if the password for the license you have installed is correct, proceed as follows in the Data Protector GUI:

1. In the Help menu, click **Licenses...**
2. Click the **Licenses** tab. All installed licenses are displayed. Click the **Passwords Info** tab to see details about the installed valid passwords. Invalid passwords will either be marked as expired or suppressed.

The whole pop-up window as well as the individual columns are re-sizable.

### *Using the CLI*

To verify if the password for the license you have installed is correct, use the following command:

```
omnicc -password_info
```

This command displays all installed licenses. If the password you entered is not correct, it is listed with the remark `Password could not be decoded`.

## Finding the number of installed licenses

### *Using the GUI*

Once you have installed a permanent password, you can check how many licenses are currently installed on the Cell Manager:

1. Start the Data Protector Manager.
2. In the menu bar, click **Help**, and then **Licenses...** The About Manager window will open, displaying the installed licenses.

### *Using the CLI*

If you use the command line, proceed as follows:

1. Log on to the Cell Manager.
2. Execute the following command:

```
omnicc -query
```

A table listing the currently installed licenses will be displayed.

## Moving licenses to another Cell Manager System

You must contact the *HP Password Delivery Center* in any of the following cases:

- If you wish to move the Cell Manager to another system.
- If you plan to move a license, installed on a Cell Manager not currently in use in the cell, to another Data Protector cell.

**Note:** The UNIX product licenses apply for UNIX, Windows and Novell NetWare platforms, providing the functionality regardless of the platform, while the Windows product licenses apply for the Windows, Novell NetWare and Linux platforms only.

A Cell Manager license for HP-UX can be moved to and works for any cell manager platform. A Cell manager license for Windows or Linux cannot be moved to and does not work for an HP-UX cell manager platform.

All other licenses can be moved to any cell manager platform without restrictions. The cell manager platform type does not imply any restrictions on the license. For example, a Windows drive license can be installed on an HP-UX cell manager, however it cannot be used for a drive connected to a UNIX system.

Use the following process to move licenses from one Cell Manager to another:

1. Fill out one *License Move Form* for each new Cell Manager and send it to the *HP Password Delivery Center*. To move licenses for products, which can no longer be purchased, you should use the *License Move Forms* delivered with the previous version of the product. See "[Data Protector licensing forms](#)".

On the form, you must specify the number of licenses you want to move from the existing Cell Manager.

Alternatively, go to the web site of the password delivery center (<http://www.webware.hp.com>) and initiate the license move online.

2. Delete the following file:

**Windows systems:**

```
Data_Protector_program_data\config\server\cell\lic.dat
```

**UNIX systems:**

```
/etc/opt/omni/server/cell/lic.dat
```

3. As soon as you have filled out the *License Move Form* and sent it to the *HP Password Delivery*

*Center (PDC)*, you are legally obliged to delete all Data Protector passwords from the current Cell Manager.

4. Install the new passwords. You will receive one password for each new Cell Manager. You will also receive one new password for the current Cell Manager if licenses are left on the current Cell Manager. This new password replaces the current password entry on the current Cell Manager.

## Centralized licensing

Data Protector allows you to configure centralized licensing for a whole multicell environment, which simplifies license management. All licenses are kept on the Manager-of-Managers (MoM) Manager system. Licenses are allocated to specific cells although they remain configured on the MoM Manager.

For more information on how to configure licenses, see the *HP Data Protector Help*.

**Note:** The UNIX product licenses apply for UNIX, Windows and Novell NetWare platforms, providing the functionality regardless of the platform, while the Windows product licenses apply for the Windows, Novell NetWare and Linux platforms only.

A Cell Manager license for HP-UX can be moved to and works for any cell manager platform. A Cell manager license for Windows or Linux cannot be moved to and does not work for an HP-UX cell manager platform.

All other licenses can be moved to any cell manager platform without restrictions. The cell manager platform type does not imply any restrictions on the license. For example, a Windows drive license can be installed on an HP-UX cell manager, however it cannot be used for a drive connected to a UNIX system.

The MoM functionality allows you to move (re-assign) licenses among the MoM cells. For more information, see the *HP Data Protector Help* index: “MoM environment”.

If you are installing a new Data Protector license, ensure that you check the MoM functionality before you request any licenses. If you decide to use centralized licensing at a later date, you will then have to go through the procedure of moving licenses.

**Note:** The MoM functionality allows centralized licensing. This means you can install all licenses on the MoM Manager and then distribute them to the Cell Managers that belong to the MoM cell. You can later move (re-distribute) licenses among the MoM cells. For more information, see the *HP Data Protector Help* index: “MoM environment”.

## Data Protector 8.10 product structure and licenses

### Password considerations

Consider the following to help determine the right number of passwords.

- Instant-On passwords are built-in. They are available for every new installation and every existing Data Protector installation upgraded to version 8.10 for 60 days without any extra license password installation requirements, and they offer you the full product functionality for evaluation purposes.

After 60 days the Instant-On passwords expire and the product stops working, unless permanent license key have been installed.

**Important:** The evaluation period for the full product ends as soon as the first regular license key is installed. As soon as at least one license key is installed, only the functionality can be used, for which license keys have been installed.

- Permanent licenses can be moved to a different Cell Manager. However, you need to use the License Move Form(s) and send them to the *HP Password Delivery Center (PDC)*.
- Passwords are installed on the Cell Manager and are valid for the entire cell.
- Centralized licensing is provided within the Manager-of-Managers (MoM) functionality. You can have all the licenses installed on the MoM system if you purchase multiple licenses for several cells.
- You need one Cell Manager license for each cell.
- The license keys or passwords are regularly checked by the software when you perform a Data Protector configuration task or start a backup session.
- Instant-On passwords can be used on any system, while evaluation and permanent passwords can be used only on the Cell Manager system for which you requested the licenses.

**Note:** To change the IP address of the Cell Manager, to move the Cell Manager to another system, or to move licenses from one cell to another (where MoM functionality is not used), you should contact the *HP Password Delivery Center (PDC)* in order to update the licenses. For information about contacting the HP Password Delivery Center, see "[Obtaining and installing permanent passwords](#)".

## License migration to Data Protector 8.10

Data Protector 6.20, 7.00 and 8.00 customers on support contract will receive Data Protector 8.10 free of charge including new license keys for all licenses on the support contract.

You can go to the MyUpdates portal at the Software Support Online (SSO)  
<http://support.openview.hp.com/downloads.jsp>.

Here you get access to the software and license keys downloads which you are entitled for according to your active support contract (SAID).

You can see all software associated to the SAID, check the box in front of Data Protector 8.10 and click **Get updates**. Note that next to Data Protector 8.10, there is a message new license key is required.

Three tabs are displayed:



- **Get software:** For downloading the software.
- **Get licenses:** To get licenses for the LTUs mapped to Data Protector 8.10
- **Get documentation:** To download the product documentation.

When you click the **Get license** link, this directs you to the update order the HP Software Licensing Portal (<http://www.webware.hp.com>) where you can get license keys for the LTUs and quantities that are on your Service Agreement Identifier (SAID).

## Data Protector licensing forms

This section discusses Data Protector Licensing forms. Fill them out to order permanent passwords using one of the following methods:

- Order permanent passwords using the online *Password Delivery Center* site at <http://www.webware.hp.com>.
- Print the electronic version of the license forms that are included in the following files on the Cell Manager system and the installation media:

**HP-UX and Linux systems:** /opt/omni/doc/C/license\_forms\_UNIX

**Windows installation DVD-ROM:** *DriveLetter*:Docs\license\_forms.txt

or use the electronic files to “copy” and “paste” your message to the *Password Delivery Center (PDC)*.

**Important:** Make sure that you type information clearly and that you do not forget the required fields.

The common fields in the licensing forms that you are required to fill out are briefly described beneath:

Personal Data	This field contains customer information, including to whom the new password should be delivered.
Licensing Data	Provide licensing information about your Data Protector cell.
Current Cell Manager	Enter the required information about your current Cell Manager.
New Cell Manager	Enter the required information about your New Cell Manager.
Order Number	Enter the <i>Order Number</i> printed on the <i>Entitlement Certificate</i> . The <i>Order Number</i> is required to verify that you are entitled to request a permanent password.

IP Address	<p>This field defines for which system the <i>Password Delivery Center</i> will generate the passwords. In case you want to use centralized licensing (MoM environments only) then this system must be the MoM Manager system.</p> <p>If the Cell Manager has the several LAN cards, you can enter any of the IP addresses. HP recommends that you enter the primary one.</p> <p>If you have Data Protector in an HP Serviceguard or Microsoft Cluster environment, enter the IP address of your virtual server. For more information on clusters, see the <i>HP Data Protector Help</i>.</p>
The <i>Password Delivery Center</i> Fax Numbers	For contact information, see the <i>Entitlement Certificate</i> shipped with your product.
Product License Type	In the fields next to the <i>Product Numbers</i> , enter the quantity of licenses you want to install on this Cell Manager. The quantity can be all or a subset of the licenses purchased with the <i>Order Number</i> .

# Chapter 6: Troubleshooting installation and upgrade

This chapter contains information specific to installation related problems. For general troubleshooting information, see the *HP Data Protector Troubleshooting Guide*.

## Name resolution problems when installing the Windows Cell Manager

During the installation of the Data Protector Cell Manager on Windows, Data Protector detects and warns you if the DNS or the LMHOSTS file is not set up as required. In addition, Data Protector notifies you if the TCP/IP protocol is not installed on your system.

### *Problem*

#### **Name resolution fails when using DNS or LMHOSTS**

If the name resolution fails, the “error expanding hostname” message is displayed and the installation is aborted.

- If you encounter resolution problems when using DNS, you get a warning message about your current DNS configuration.
- If you encounter resolution problems when using LMHOSTS file, you get a warning message to check your LMHOSTS file configuration.
- If you have not configured either DNS or LMHOSTS, you get a warning message to enable the DNS or the LMHOSTS resolution in the TCP/IP properties dialog.

### *Action*

Check your DNS or LMHOSTS file configuration or activate it. See ["Verifying DNS connections within Data Protector cell"](#) .

### *Problem*

#### **The TCP/IP protocol is not installed and configured on your system**

Data Protector uses the TCP/IP protocol for network communications; it must be installed and configured on every client in the cell. Otherwise, the installation is aborted.

### *Action*

Check the TCP/IP setup. For information, see ["Changing the default Data Protector Inet port"](#) .

## Verifying DNS connections within Data Protector cell

DNS (Domain Name System) is a name service for TCP/IP hosts. The DNS is configured with a list of host names and IP addresses, enabling users to specify remote systems by host names rather than by IP addresses. DNS ensures proper communication among the members of the Data Protector cell.

If DNS is not configured properly, name resolution problems may occur in the Data Protector cell and the members will not be able communicate with each other.

Data Protector provides the `omnicheck` command to verify the DNS connections among the members of the Data Protector cell. Although all possible connections in the cell can be checked with this command, it is enough to verify the following connections, which are essential in the Data Protector cell:

- Cell Manager to any other member of the cell and the other way round
- Media Agent to any other member of the cell and the other way round

## Using the `omnicheck` command

### *Limitations*

- The command verifies connections among the cell members only; it does not verify DNS connections in general.

The synopsis of the `omnicheck` command is:

```
omnicheck -dns [-host Client | -full] [-verbose]
```

You can verify the following DNS connections in the Data Protector cell using different options:

- To check that the Cell Manager and every Media Agent in the cell resolve DNS connections to every Data Protector client in the cell properly and the other way round, execute:

```
omnicheck -dns [-verbose]
```

- To check that a particular Data Protector client resolves DNS connections to every Data Protector client in the cell properly and the other way round, execute:

```
omnicheck -dns -host client [-verbose]
```

where *client* is the name Data Protector client checked.

- To check all possible DNS connections in the cell, execute:

```
omnicheck -dns -full [-verbose]
```

When the `[-verbose]` option is specified, the command returns all the messages. If this option is not set (default), only the messages that are the result of failed checks are returned.

For more information, see the `omnicheck` man page.

"Return messages " lists return messages for the `omnicheck` command. If the return message indicates a DNS resolution problem, see the "Troubleshooting Networking and Communication" chapter of the *HP Data Protector Troubleshooting Guide*.

**Table 7: Return messages**

Return message	Meaning
<code>client_1</code> cannot connect to <code>client_2</code>	Timeout connecting to <code>client_2</code> .
<code>client_1</code> connects to <code>client_2</code> , but connected system presents itself as <code>client_3</code>	The  <code>%SystemRoot%\System32\drivers\etc\hosts</code> (UNIX systems) file on the <code>client_1</code> is not correctly configured or the hostname of the <code>client_2</code> does not match its DNS name.
<code>client_1</code> failed to connect to <code>client_2</code>	<code>client_2</code> is either unreachable (for example, disconnected) or the  <code>%SystemRoot%\System32\drivers\etc\hosts</code> (Windows systems) or <code>/etc/hosts</code> (UNIX systems) file on the <code>client_1</code> is not correctly configured.
checking connection between <code>client_1</code> and <code>client_2</code>	
all checks completed successfully.	
<code>number_of_failed_checks</code> checks failed.	
<code>client</code> is not a member of the cell.	
<code>client</code> contacted, but is apparently an older version. Hostname is not checked.	

## Troubleshooting common issues

### Problem

One of the following error messages is reported

- The Windows Installer Service could not be accessed.
- This application must be installed to run.

- This patch package could not be opened.
- The system cannot open the device or file specified.

After installation or upgrade to Data Protector 8.10, Windows may report that some applications are not installed or that a reinstall is required.

The reason is an error in the Microsoft Installer upgrade procedure. Microsoft Installer version 1.x data information is not migrated to the Microsoft Installer version 2.x that Data Protector installs on the computer.

### *Action*

On how to solve the problem, see article Q324906 in the Microsoft Knowledge Base.

### *Problem*

**Cell Manager installation on a Windows system, which is not part of any Windows domain, fails**

The following error message is reported:

Setup is unable to match the password with the given account name.

### *Actions*

Two solutions are available:

- Make the Windows system, on which you are installing the Cell Manager, part of a domain.
- Use the local administrator account for the CRS service.

### *Problem*

**The following error message is reported**

msvcr90.dll file is not found

The MSVCR90.dll library (upper case) cannot be found, because only msvcr90.dll (lower case) is available on the network share. Since MSVCR90.dll and msvcr90.dll are not treated as the same files, setup.exe fails to find the appropriate dll.

### *Action*

Rename the file from msvcr90.dll (lower case) to MSCVCR90.dll (upper case) or reconfigure the network share not to be case-sensitive.

### *Problem*

**Canceling of installation does not uninstall already installed components**

If you cancel the Data Protector installation while some components have been already installed, Data Protector does not uninstall them. The installation finishes with an error.

### *Action*

Manually uninstall already installed components after you cancelled the installation.

## Troubleshooting installation on UNIX systems

### Problem

#### Remote installation of UNIX clients fails

Remote installation or upgrade of a UNIX client fails with the following error message:

```
Installation/Upgrade session finished with errors.
```

When installing or upgrading UNIX clients remotely, the available disk space on a client system in the folder `/tmp` should be at least the size of the largest package being used for the installation. On Solaris client systems, the same amount of disk space should be available also in the `/var/tmp` folder.

### Action

Check if you have enough disk space in the above mentioned directories and restart the installation or upgrade procedure.

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

### Problem

#### Problems with the installation of an HP-UX client

When adding a new HP-UX client to a Data Protector cell, the following error message is displayed:

```
/tmp/omni_tmp/packet: you do not have the required permissions to perform this SD function.....
```

Access denied to root at to start agent on registered depot `/tmp/omni_tmp/packet`. No insert permission on host.

### Action

Stop the `swagent` daemon and restart it by either killing the process and then restarting it by running the `/opt/omni/sbin/swagentd` command, or by running the `/opt/omni/sbin/swagentd -r` command.

Ensure that you have a local host, loopback entry in the hosts file (`/etc/hosts`).

### Problem

#### Problems with the installation of a Mac OS X client

When adding a Mac OS X client to a Data Protector cell, the `com.hp.omni` process is not started.

### Action

On Mac OS X, `launchd` is used to start the `com.hp.omni` process.

To start the service, go to:

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

Execute:

```
launchctl load com.hp.omni
```

## Problem

### Inet process cannot be started after installing the UNIX Cell Manager

When starting the Cell Manager, the following error is displayed:

```
ERROR: Cannot start "omniinet" service, system error: [1053] Unknown error 1053.
```

## Action

Check if the `inetd` or `xinetd` service is running:

**HP-UX systems:** `ps -ef | grep inetd`

**Linux systems:** `ps -ef | grep xinetd`

To start the service, execute:

**HP-UX systems:** `/usr/sbin/inetd`

**Linux systems:** `rcxinetd start`

## Problem

### Installation of Data Protector 8.10 creates unusable certificate

When installing the Data Protector 8.10 Cell Manager, unusable certificate is created and the Manager reports the following error:

A server error has occurred. Reported error message:

```
Unknown SSL protocol error in connection to cellmanager1.company.com:7116
```

## Action

To create a valid certificate, perform the following:

1. Read the `/etc/opt/omni/client/components/webservice.properties` file and store the value of the `keystorePassword` for the next step.
2. Use the `omnigencert.pl` script to recreate the certificate.
3. Restart the Data Protector services after using the script.

**Note:** The argument `-cert_expire` specifies the last valid date of the certificate by counting the number of days starting from today. The default version of `omnigencert.pl` is only capable of producing end dates till the year 2038. The range of 10 years from the date of certificate creation is expressed with the value of 3650. The following arguments for the `omnigencert.pl` script must be set:

- `server_id` - Is the fully qualified domain name of the Cell Manager.
- `store_password` - Is the value of the `keystorePassword`.



- `cert_expire` - Is the validity range measured in days.
- `user_id` - Uses the fixed value `hdpd`.

## Troubleshooting installation on Red Hat 7 systems

### Problem

#### Installation of Data Protector 8.10 on Red Hat 7 systems fails

While installing the Data Protector 8.10MR Cell Manager, the installation of Cell Server packet fails with the following output:

```
Installing OB2-CS packet
Preparing... ##### [100%]
Updating / installing...
1:OB2-CS-A.08.10-1 ##### [100%]
NOTE: No Data Protector A.08.10 Internal Database found. Initializing...
Configuring and starting up Internal Database... Done!
Configuring and starting up Internal Database Connection Pool... Done!
Initializing Internal Database version A.08.10... Done!
Configuring and starting up Application Server...
ERROR: Unable to reload Application Server (Return code = 1)
For more detail please refer to /var/opt/omni/server/log/DPIDBsetup_14124.log
warning: %post(OB2-CS-A.08.10-1.x86_64) scriptlet failed, exit status 3
```

### Action

After a failed Data Protector 8.10MR Cell Manager installation, follow these steps to make the Cell Manager fully operational:

1. Stop all Data Protector services:

```
omnisv -stop
```

**Note:** Ensure that no Data Protector processes are left running by executing: `ps -ef | grep omni` command and stop any running processes, if found.

2. Replace the `omnigencert.pl` script. Perform the following:

- Create temporary folder and change the current path to the created folder:

```
mkdir /tmp/omni_tmp
```

```
cd /tmp/omni_tmp
```

- Download 8.13\_207 (or newer) Cell Server patch to /tmp/omni\_tmp.

- Extract omnigencert.pl script from the Cell Server patch:

```
rpm2cpio DPLNX_00397.rpm | cpio -id ./opt/omni/sbin/omnigencert.pl
```

- Replace existing omnigencert.pl with the extracted one:

```
cp /tmp/omni_tmp/opt/omni/sbin/omnigencert.pl /opt/omni/sbin/
```

3. Execute IDBSetup.sh:

```
/opt/omni/sbin/IDBSetup.sh
```

4. Update /etc/opt/omni/client/omni\_info with cs component:

```
/opt/omni/bin/omnicc -put_component_str cs client/omni_format client/omni_info  
A.08.10
```

5. Re-import the Cell Manager host and Installation Server(if installed) to the cell:

```
omnicc -import_host cm_hostname
```

```
omnicc -import_is cm_hostname
```

6. Continue with the normal procedure for applying the latest patches.

## Troubleshooting installation on Windows systems

### *Problem*

#### **Remote installation of Windows clients fails**

Remote installation of a Data Protector client to a Windows system fails and reports the following error message:

```
[Normal] Connecting to client computer.company.com...
```

```
[Normal] Done.
```

```
[Normal] Installing the Data Protector bootstrap service on client  
computer.company.com...
```

```
[Critical] Cannot connect to the SCM (Service Control Manager) on client  
computer.company.com: [5] Access is denied.
```

### Action

1. On the Installation Server system, execute the following command to mark a user account from the local operating system Administrators user group to be used by the Installation Server during remote installation:

```
omniinetpasswd -inst_srv_user User@Domain
```

Note that the user account must already be added to the local Inet configuration. For details, see the `omniinetpasswd` command description in the *HP Data Protector Command Line Interface Reference*.

2. Start remote installation of the Data Protector client once again.

### Problem

#### Remote installation of Windows clients fails (Windows XP)

When a Windows XP system is a member of a workgroup and the Simple File Sharing security policy setting is turned on, users attempting to access this system through the network are forced to use the Guest account. During remote installation of a Data Protector client, Data Protector repeatedly asks for a valid username and password because administrator rights are required for the remote installation.

### Action

Turn off Simple File Sharing: in Windows XP, open **Windows Explorer** or **My Computer**, click the **Tools** menu, click **Folder Options**, click the **View** tab, then clear the **Use simple file sharing (Recommended)** check box.

The Simple File Sharing policy is ignored:

- when the computer is a member of a domain
- when the Network access: Sharing and security model for local accounts security policy setting is set to Classic: Local users authenticate as themselves

### Problem

#### Digital signature verification might fail, if Windows 7 or Windows 2008 R2 systems are disconnected.

Digital signature verification fails with the following error message:

```
[Critical] <computer.company.com> [70:32] Digital Signature verification of the  
install kit failed.
```

### Action

Perform either one of the following:

- Enable internet connection and wait until the proper certificates are imported into the trusted root and intermediate certificate authorities automatically.

(Or)

- Refer to the following articles to understand how to update the trusted root certificates on disconnected systems:

<https://support.microsoft.com/en-us/kb/3004394>

<https://support.microsoft.com/en-us/kb/2813430>

### *Problem*

#### **When installing a Cell Manager, the Application Server service fails to start**

The Application Server service fails to start with the message

Timeout reached before Data Protector Application Server started.

The following error is logged to the installation summary log file:

Caused by: org.jboss.as.cli.

CommandLineException: The controller is not available at localhost:9999

The installation process cannot access various utilities because the PATH system environment variable does not contain the directory %SystemRoot%\system32.

### *Action*

Add the %SystemRoot%\system32 directory to the PATH variable.

## **Verifying Data Protector client installation**

Verifying Data Protector client installation consists of the following:

- Checking the DNS configuration on the Cell Manager and client systems, and ensuring that the results of the `omnicheck -dns` command on the Cell Manager and client system match the specified system.
- Checking the software components installed on the client.
- Comparing the list of files required for a certain software component to be installed with the files installed on the client.
- Verifying the checksum for every read-only file required for a certain software component.

### *Prerequisite*

An Installation Server must be available for the type of client system (UNIX, Windows) that you select.

### *Limitation*

To verify a Data Protector installation using the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Clients**, right-click the Cell Manager system, and then click **Check**

**Installation** to start the wizard.

3. Follow the wizard to verify the installation of the systems in the cell. The Check Installation window opens, displaying the results of the installation.

For details, see the *HP Data Protector Help*.

If your installation has not succeeded, see ["Using log files"](#) .

On how to verify the installation on UNIX systems using the Data Protector CLI, see the `ob2install` man page.

## Troubleshooting upgrade

### Problem

**Upgrading to Data Protector 8.10 fails if the previous version of the product is installed in a long path**

Data Protector 8.10 does not support installing the Cell Manager to a path longer than 80 characters. As a consequence, the upgrade fails.

### Action

1. Copy the `omnimigrate.pl` script from the Data Protector 8.10 installation DVD, from the directory `x8664\tools\Upgrade`, to a temporary directory, for example `c:\temp`.

2. Export the IDB using the `omnimigrate` command:

```
perl c:\temp\omnimigrate.pl -export -shared_dir c:\output
```

Use the Perl version that is a part of the Data Protector installation and resides in the default commands directory.

3. Remove the previous version of Data Protector, but leave the configuration and database data. Do not remove the `Data_Protector_program_data\db40` directory.

4. Install Data Protector 8.10. Make sure the path you install to is shorter than 80 characters.

5. Stop all Data Protector services:

```
omnisv -stop
```

6. Copy the files from the old `Data_Protector_program_data\db40` directory (left after the removal of the previous version of Data Protector) to the new `Data_Protector_program_data\db40` folder. Make sure that you do *not* move the DCBF directories.

7. Copy the configuration from the old `Data_Protector_program_data\Config\Server` folder to the new one:

- a. Copy the old configuration directory to the new one, but keep the old files. Do not copy the files from the directory `Data_Protector_program_data\Config\Server\install`.
  - b. If you want to keep the cell configuration (clients, Installation Server), copy and overwrite the `Data_Protector_program_data\Config\Server\cell\cell_info` and `Data_Protector_program_data\Config\Server\cell\installation_servers` files.
8. Merge the new notification and global options file:
  - a. To merge the notifications, execute the `omnnotifupg.exe` tool:  

```
omnnotifupg.exe -quiet
```
  - b. To merge the global options file, execute:  

```
mrgcfg.exe -global -except BackupDeviceIdle -rename  
DbFVerLimit=DbFnamesDatLimit,SessSuccessfulWhenNoObjectsBackedUp  
=SessSuccessfulWhenNoObjectsBackedUp
```

Alternatively, you can manually merge the global options file from the old installation.
9. Start the Data Protector services:  

```
omnisv -start
```
10. Import the IDB to the new installation. Execute:  

```
omnimigrate.pl -import -shared_dir c:\output -force
```

## Problem

### Upgrading to Data Protector 8.10 fails if the previous version of the product is installed in a path with unsupported characters

Data Protector 8.10 does not support installing the Cell Manager to a path that:

- contains non-ASCII characters
- contains the characters "@" or "#"
- contains a directory that ends with the character "!"

As a consequence, the upgrade fails.

## Action

1. Copy the `omnimigrate.pl` script from the Data Protector 8.10 installation DVD, from the directory `x8664\tools\Upgrade`, to a temporary directory, for example `c:\temp`.
2. Create two directories with ASCII names for example:

```
c:\output\cdb
```

```
c:\output\mmdb
```

3. Export the MMDB and CDB:

```
omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb
```

This process can take a while. You can stop the omnidbutil process using **Ctrl+C** when it starts exporting filenames because this data is not needed for upgrade.

4. Export the IDB using the omnimigrate command:

```
perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output
```

Use the Perl version that is a part of the Data Protector installation and resides in the default commands directory.

5. Create a ANSI charset file, c:\output\old\_cm. The file should contain the following two lines:

```
OLDCM_SHORTNAME=OLdCmName  
OLDCM_ENDIANNES=LITTLE_ENDIAN
```

Replace *OldCmName* with the short name of the Cell Manager.

6. Remove the previous version of Data Protector, but leave the configuration and database data. Do not remove the *Data\_Protector\_program\_data\db40* directory.

7. Install Data Protector 8.10. Make sure the path you install to does not contain any non-ASCII characters.

8. Stop all Data Protector services:

```
omnisv -stop
```

9. Copy the files from the old *Data\_Protector\_program\_data\db40* directory (left after the removal of the previous version of Data Protector) to the new *Data\_Protector\_program\_data\db40* folder. Make sure that you do *not* move the DCBF directories.

10. Copy the configuration from the old *Data\_Protector\_program\_data\Config\Server* folder to the new one:

a. Copy the old configuration directory to the new one, but keep the old files. Do not copy the files from the directory *Data\_Protector\_program\_data\Config\Server\install*.

b. If you want to keep the cell configuration (clients, Installation Server), copy and overwrite the *Data\_Protector\_program\_data\Config\Server\cell\cell\_info* and *Data\_Protector\_program\_data\Config\Server\cell\installation\_servers* files.

11. Merge the new notification and global options file:

- a. To merge the notifications, execute the omninotifupg.exe tool:

```
omninotifupg.exe -quiet
```

- b. To merge the global options file, execute:

```
mrgcfg.exe -global -except BackupDeviceIdle -rename  
DbFVerLimit=DbFNamesDatLimit,SessSuccessfulWhenNoObjectsBackedUp  
=SessSuccessfulWhenNoObjectsBackedUp
```

Alternatively, you can manually merge the global options file from the old installation.

12. Start the Data Protector services:

```
omnisv -start
```

13. Import the IDB to the new installation. Execute:

```
omnimigrate.pl -import -shared_dir c:\output -force
```

### *Problem*

#### **The upgrade process is aborted if the old (Raima DB based) IDB is corrupted**

During upgrade, the following corrupted fields in the IDB are detected and corrected:

- media blocks\_used is set to 0
- media blocks\_total is set to blocks\_used
- pool media\_age\_limit is set to the default value (the media\_age\_limit for the default pool with the same media class)
- pool media\_overwrite\_limit is set to the default value (the media\_overwrite\_limit for the default pool with the same media class)

However, if any other fields in the IDB are corrupted, the upgrade is aborted.

### *Action*

Revert your Data Protector installation back to the old version:

1. Remove Data Protector 8.10.
2. Reinstall the previous version of Data Protector.
3. Restore the old IDB.

Before attempting another upgrade, you need to fix the old IDB. Contact HP support for further assistance.

### *Problem*

#### **The upgrade process is aborted if the Velois IDB is corrupted**



During upgrade, the following corrupted fields in the IDB are detected and corrected:

- `media blocks_used` is set to 99
- `media blocks_total` is set to `blocks_used`
- `pool media_age_limit` is set to the default value (the `media_age_limit` for the default pool with the same media class)
- `pool media_overwrite_limit` is set to the default value (the `media_overwrite_limit` for the default pool with the same media class)

However, if any of the following fields in the IDB are corrupted, the upgrade is aborted.

Media: `LAST_SEGMENT`

Positions:

`SEQUENCE_NR`

`START_SEGMENT`

`START_OFFSET`

`LOG_LEVEL`

`DCBF_OFFSET`

`DCBF_NUMOFDIRS`

`DCBF_NUMOFITEMS`

`DCBF_SIZE`

### *Action*

Revert your Data Protector installation back to the old version:

1. Remove Data Protector 8.10.
2. Reinstall the previous version of Data Protector.
3. Restore the old IDB.

Before attempting another upgrade, you need to fix the old IDB. Contact HP support for further assistance.

### *Problem*

#### **IDB and configuration files are not available after upgrade**

After upgrading the Cell Manager from a previous release version, the IDB and all configuration files are not available. This occurs if the upgrade procedure was interrupted for any reason.

### *Action*

Restore Data Protector from the backup made before the upgrade, eliminate the reason of the interruption, and start the upgrade again.

## Problem

### Old Data Protector patches are not removed after upgrade

Old Data Protector patches are listed among installed programs if the `swlist` command is run after the Data Protector upgrade has finished. The patches were removed from your system during the upgrade, but they remained in the sw database.

To check which Data Protector patches are installed, see .

## Action

To remove the old patches from the sw database, run the following command:

```
swmodify -upatch.*patch
```

For example, to remove a patch “PHSS\_30143” from the sw database, run the following command:

```
swmodify -u PHSS_30143.* PHSS_30143
```

## Problem

### Upgrade of a Media Agent client which uses the StorageTek Library causes connectivity problems

After you upgrade the Data Protector Media Agent component on a system which uses the StorageTek Library, connectivity to the library is lost, and the Data Protector sessions which involve the library may stop responding or terminate abnormally.

## Action

Restarting the StorageTek Library supporting service or daemon may solve the problem:

**Windows systems:** Using the administrative tool Services, restart the LibAttach service.

**HP-UX and Solaris systems:** Run the commands `/opt/omni/acs/ssi.sh stop` and `/opt/omni/acs/ssi.sh start ACSLS_hostname` where `ACSLs_hostname` is the name of the system on which the Automated Cartridge System library software is installed.

**AIX systems:** Run the commands `/usr/omni/acs/ssi.sh stop` and `/usr/omni/acs/ssi.sh start ACSLS_hostname` where `ACSLs_hostname` is the name of the system on which the Automated Cartridge System library software is installed.

# Troubleshooting remote upgrade on Windows systems

## Problem

### Error starting setup process

When using Data Protector remote installation functionality to upgrade Windows clients, you get the following error:

Error starting setup process, err=[1326] Logon failure: unknown user name or bad password.

The problem is that the Data Protector Inet service on the remote computer is running under a user account that does not have access to the OmniBack share on the Installation Server computer. This is most probably a local user.

### Action

Change the user for the Data Protector Inet service to one that can access the Data Protector share.

## Manual process for local upgrade on UNIX systems

Normally, you upgrade Data Protector 6.20, 7.00, 8.00 on UNIX Cell Manager and Installation Server by executing the `omnisetup.sh` command, which performs an automated upgrade procedure. However, you can also perform the upgrade manually. See ["Upgrading on HP-UX and Linux systems using native tools"](#).

## Using log files

If you run into problems installing Data Protector, you can examine any of the following log files to determine your problem:

- setup log files (Windows)
- system log files (UNIX)
- Data Protector log files

Which log files to check in case of installation problems depends on the type of the installation (local or remote) and on the operating system.

## Local installation

In case of problems with local installation, check the following log files:

### **HP-UX Cell Manager:**

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log` (for more details)

### **Linux Cell Manager:**

`/var/opt/omni/log/debug.log`

### **Windows client** (the system where setup is running):

- `Temp\SetupLog.log`
- `Temp\OB2DBG_did__setup_HostName_DebugNo_setup.txt` (for more details)

where:

- *did* (debugging ID) is the process ID of the first process that accepts the debugging parameters. This ID is used as an ID for the debugging session. All further processes will use this ID.
- *HostName* is the name of the host where the trace file is created.
- *DebugNo* is a number generated by Data Protector.
- *Temp\CLUS\_DBG\_DebugNo.TXT* (in cluster environments)

The location of the *Temp* directory is specified by the *TEMP* environment variable. To examine the value of this variable, run the *set* command.

## Remote installation

In case of problems with remote installation, check the following log files:

### **UNIX Installation Server:**

*/var/opt/omni/log/IS\_install.log*

**Windows client** (the remote system to which components are to be installed):

- *SystemRoot\TEMP\OB2DBG\_did\_INSTALL\_SERVICE\_DebugNo\_debug.txt*
- *SystemRoot\TEMP\CLUS\_DBG\_DebugNo.TXT*

The location of the *Temp* directory is specified by the *TEMP* environment variable, and *SystemRoot* is a path specified in the *SystemRoot* environment variable.

In case the setup log files are not created, run the remote installation with the debug option. See ["Creating installation execution traces"](#).

## Data Protector log files

The Data Protector log files listed below are located in:

**Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012:** *Data\_Protector\_program\_data\log*

**Other Windows systems:** *Data\_Protector\_home\log*

**HP-UX, Solaris, and Linux systems:** */var/opt/omni/log* and */var/opt/omni/server/log*

**Other UNIX systems and Mac OS X systems:** */usr/omni/log*

The following log files are important for troubleshooting installation:

<i>debug.log</i>	Contains unexpected conditions. While some can be meaningful to you, the information is mainly used by the support organization.
<i>inet.log</i>	Contains requests made to the Data Protector <i>inet</i> service. It can be useful to check the recent activity of Data Protector on clients.

IS_ install.log	Contains a trace of remote installation and resides on the Installation Server.
omnisv.log	Contains information on when Data Protector services were stopped and started.
upgrade.log	This log is created during upgrade and contains upgrade core part (UCP) and upgrade detail part (UDP) messages.
OB2_ Upgrade.log	This log is created during upgrade and contains traces of the upgrade process.

For more log files, see the *HP Data Protector Troubleshooting Guide*.

## Creating installation execution traces

Run the installation with the debug option if this is requested by the HP Customer Support Service. For more information on debugging, including the debug options below, and preparing data to be sent to the HP Customer Support Service, see the *HP Data Protector Troubleshooting Guide*.

For debugging remote installation, run the Data Protector GUI with the debug option:

```
Manager -debug 1-200 DebugPostfix
```

Once the session is finished/aborted, collect the debug output from the following locations:

- On the Installation Server system:

```
Data_Protector_program_data\tmp\OB2DBG_did__BM_ Hostname_DebugNo_DebugPostfix
```

- On the remote system:

```
SystemRoot:\Temp\OB2DBG_did__INSTALL_SERVICE_Hostname_DebugNo_DebugPostfix
```



# Appendix A: Installing and upgrading using UNIX system native tools

This appendix describes how to install and upgrade Data Protector on UNIX systems, using the native installation tools — `swinstall` on HP-UX systems and `rpm` on Linux systems.

**Note:** The recommended method for installing or upgrading Data Protector is using the `omnisetup.sh` script. See ["Installing and upgrading using UNIX system native tools"](#) and ["Upgrading the UNIX Cell Manager and Installation Server"](#).

## Installing on HP-UX and Linux systems using native tools

**Note:** The native installation procedures on HP-UX and Linux are only documented if you intend to install an Installation Server with a limited set of remote installation packages. It is recommended to install Data Protector using `omnisetup.sh`.

## Installing a Cell Manager on HP-UX systems using `swinstall`

To install the UNIX Cell Manager on an HP-UX system:

1. Insert and mount the HP-UX installation DVD-ROM and run the `/usr/sbin/swinstall` utility.
2. In the Specify Source window, select **Network Directory/CDROM**, and then enter `Mountpoint/hpux/DP_DEPOT` in the **Source Depot Path**. Click **OK** to open the SD Install - Software Selection window.
3. In the list of available packages for the installation, the Data Protector product is displayed under the name B6960MA.
4. Right-click **DATA-PROTECTOR**, and then click **Mark for Install** to install the whole software.

In case you do not need all subproducts, double-click **DATA-PROTECTOR** and then right-click an item from the list. Click **Unmark for Install** to exclude the package or **Mark for Install** to select it for installation.

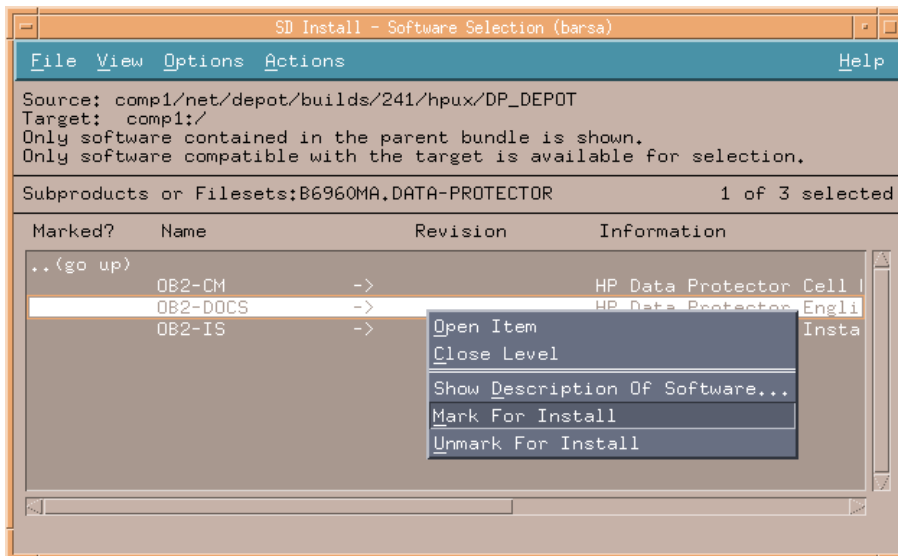
The following subproducts are included in the product:

OB2-CM	Cell Manager software
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the <i>HP Data Protector Help</i> in the WebHelp format.
OB2-IS	The Data Protector Installation Server

Make sure that the Marked? status value next to the OB2-CM package is set to Yes if you are installing the Cell Manager for UNIX on the system. See "[SD install - software selection window](#)".

**Note:** If you are using user IDs longer than 32 bits, you must remotely install the User Interface component (OMNI-CS) on the Cell Manager after you have installed the Core Cell Manager software component.

**Figure 50: SD install - software selection window**



- In the Actions list, click **Install (analysis)**, then click **OK** to proceed. If the Install (analysis) fails, displaying an error message, click **Logfile** to view the file.

**Note:** To install software from a tape device across the network, you first need to mount the source directory on your computer.

## Installing the Cell Manager on Linux systems using rpm

To install the Cell Manager on a Linux system:



1. Insert and mount the Linux installation DVD-ROM.
2. Change to the directory `linux_x86_64/DP_DEPOT`.
3. To install a component, execute:

```
rpm -i package_name-A.08.10-1.x86_64.rpm
```

where *package\_name* is the name of the respective sub-product package.

The following components must be installed:

OB2-CORE	Data Protector Core software.
OB2-TS-CORE	Data Protector Core Technology Stack Libraries
OB2-CC	Cell Console software. This contains the command-line interface.
OB2-TS-CS	Cell Manager Technology Stack Libraries.
OB2-TS-JRE	Java Runtime Environment for use with Data Protector.
OB2-TS-AS	Data Protector Application Server
OB2-WS	Data Protector Web Services
OB2-JCE-DISPATCHER	Job Control Engine Dispatcher
OB2-JCE-SERVICEREGISTRY	Job Control Engine Service Registry
OB2-CS	Cell Manager software.
OB2-DA	Disk Agent software. This is required, otherwise it is not possible to back up the IDB.
OB2-MA	The General Media Agent software. This is required to attach a backup device to the Cell Manager.
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the <i>HP Data Protector Help</i> in the WebHelp format.

**Important:** The components on Linux are dependent on each other. You should install the components in the order in which they are listed above.

4. Restart the Data Protector services:

```
omnisv stop
```

```
omnisv start
```

## Installing an Installation Server on HP-UX systems using swinstall

1. Insert and mount the HP-UX installation DVD-ROM and run the `/usr/sbin/swinstall` utility.
2. In the Specify Source window, select **Network Directory/CDROM**, and then enter `Mountpoint/hpux/DP_DEPOT` in the **Source Depot Path**. Click **OK** to open the SD Install - Software Selection window.
3. In the list of available components for the installation, the Data Protector product is displayed under the name B6960MA. Double-click it to display the DATA-PROTECTOR product for UNIX systems. Double-click it to display the contents.

The following sub-product components are included in the product:

OB2-CM	Cell Manager software
OB2-DOCS	Data Protector documentation subproduct that includes the Data Protector guides in the PDF format and the <i>HP Data Protector Help</i> in the WebHelp format.
OB2-IS	The Data Protector Installation Server

4. In the SD Install - Software Selection window, double-click **DATA-PROTECTOR** to list the software for the installation. Right-click **OB2-IS**, and then click **Mark for Install**.
5. From the Actions menu, click **Install (analysis)**. Click **OK** to proceed.

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

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

## Installing an Installation Server on Linux systems using rpm

### Local installation on Linux

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

1. Insert the Linux installation DVD-ROM.
2. Change to the directory containing the installation archive (in this case `Mount_point/linux_x86_64/DP_DEPOT`).

3. For each component, execute:

```
rpm -i package_name-A.08.10-1.x86_64.rpm
```

The following components (*package\_name*) related to Installation Server installation are included in the product:

OB2-CORE	Data Protector Core software. Note that this is already installed, if you are installing the Installation Server on the Cell Manager system.
OB2-TS-CORE	Data Protector Core Technology Stack Libraries.
OB2-CORE-IS	Installation Server Core software.
OB2-CFP	Common Installation Server Core software for all UNIX platforms.
OB2-TS-CFP	Common Installation Server Technology Stack software for all UNIX platforms
OB2-DAP	Disk Agent remote installation packages for all UNIX systems.
OB2-MAP	Media Agent remote installation packages for all UNIX systems.
OB2-NDMPP	The NDMP Media Agent component.
OB2-CCP	Cell Console remote installation packages for all UNIX systems.

Also, if you are setting up an independent Installation Server (that is, not on the Cell Manager) and want to use the user interface:

OB2-CC	Cell Console software. This contains the command-line interface.
--------	------------------------------------------------------------------

4. Once you have installed these components, use `rpm` to install the remote installation package for all the components you will want to install remotely. For instance:

OB2-INTGP	Data Protector Integrations Core software. This component is necessary to install integrations.
OB2-TS-PEGP	PEGASUS Technology Stack component.
OB2-SAPP	SAP Integration component.
OB2-SAPDBP	SAP MaxDB Integration component.
OB2-SAPHANAP	SAP HANA Integration component.
OB2-INFP	Informix Integration component.
OB2-LOTP	Lotus Notes/Domino Integration component.

OB2-SYBP	Sybase Integration component.
OB2-OR8P	Oracle Integration component.
OB2-DB2P	DB2 Integration component.
OB2-EMCP	EMC Symmetrix Integration component.
OB2-SMISAP	HP P6000 / HP 3PAR SMI-S Agent component.
OB2-SSEAP	HP P9000 XP Agent component.
OB2-VEPAP	Virtual Environment Protection Agent component.
OB2-SODAP	StoreOnce Software Deduplication component.
OB2-AUTODRP	Automatic Disaster Recovery component.
OB2- VMWAREGRE- AGENTP	VMware Granular Recovery Extension component.
OB2-DOCSP	English Documentation (Guides, Help) component.
OB2-FRAP	French Documentation (Guides, Help) component.
OB2-JPNP	Japanese Documentation (Guides, Help) component.
OB2-CHSP	Simplified Chinese Documentation (Guides, Help) component.

For a complete list of components and dependencies, see .

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

**Important:** If you do not install an Installation Server for UNIX on your network, you will have to install every UNIX client locally from the Linux installation DVD-ROM.

**Important:** install Data Protector to linked directories, for instance:

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

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

### What's next?

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

1. If you have set up an independent Installation Server (that is, not on the Cell Manager) you must manually add (import) the system to the Data Protector cell. See ["Importing an Installation Server to a cell"](#) .

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

2. Install the Installation Server for Windows in case you have any Windows systems in your Data Protector cell. See ["Installing on HP-UX and Linux systems using native tools"](#) .
3. Distribute the software to clients. See ["Installing Data Protector clients"](#) .

## Installing the clients

The clients are not installed during a Cell Manager or Installation Server installation. The clients must be installed either by using `omnisetup.sh` or by remotely installing the components from the Data Protector GUI. For detailed information on how to install the clients, see ["Installing Data Protector clients"](#) .

## Upgrading on HP-UX and Linux systems using native tools

### Upgrading Data Protector on HP-UX systems using `swinstall`

An upgrade of a Cell Manager must be performed from HP-UX installation DVD-ROM.

If you are upgrading a Cell Manager with an Installation Server installed, you must first upgrade the Cell Manager and then the Installation Server.

Client components that are installed on the Cell Manager system are *not* upgraded during a Cell Manager upgrade and must be upgraded either by using `omnisetup.sh` or by remotely installing the components from the Installation Server. For details, see ["Local installation on UNIX and Mac OS X systems"](#) or ["Remote installation"](#) .

#### *Upgrade procedure*

To upgrade to Data Protector 8.10, using `swinstall`, proceed as follows:

1. **Data Protector 6.20 or 7.00:**

Export the existing IDB:

- a. Mount the Data Protector 8.10 DVD-ROM and copy the `omnimigrate.pl` script to a temporary directory:

```
cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-
CS/opt/omni/sbin/omnimigrate.pl /tmp
```

- b. Export the IDB using the `omnimigrate.pl` command:

```
/opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
/var/opt/omni/server/exported-export
```

2. Log in as `root` and stop the Data Protector services by executing the `omnisv -stop` command.

Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no Data Protector services listed after executing the `ps -ef | grep omni` command.

3. To upgrade a Cell Manager or/and an Installation Server, follow the procedures described ["Installing a Cell Manager on HP-UX systems using swinstall"](#) or/and ["Installing an Installation Server on HP-UX systems using swinstall"](#).

The installation procedure will automatically detect the previous version and upgrade *only the selected* components. If a component that was installed in the previous version of Data Protector is not selected, it is *not* upgraded. Therefore, you must ensure that you select all components that must be upgraded.

**Note:** The `Match what target` has option is *not* supported if you are upgrading both, the Cell Manager and Installation Server on the same system.

## Upgrading Data Protector on Linux systems using rpm

To upgrade the Linux Cell Manager or Installation Server, uninstall the old version and install the new version of the product.

Client components that are installed on the Cell Manager system are *not* upgraded during a Cell Manager upgrade and must be upgraded either by using `omnisetup.sh` or by remotely installing the components from the Installation Server. For details, see ["Local installation on UNIX and Mac OS X systems"](#) or ["Remote installation"](#).

### Upgrade procedure

To upgrade to Data Protector 8.10 using `rpm`, proceed as follows:

1. **Data Protector 6.20 or 7.00:**

- a. Mount the Data Protector 8.10 DVD-ROM and copy the `omnimigrate.pl` script to a temporary directory:

```
cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omn
imigrate.pl /tmp
```

- b. Export the IDB using the `omnimigrate.pl` command:

```
/opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir  
/var/opt/omni/server/exported-export
```

2. Log in as `root` and stop the Data Protector services executing the `omnisv -stop` command.

Type `ps -ef | grep omni` to verify whether all the services have been shut down. There must be no Data Protector services listed after executing the `ps -ef | grep omni` command.

3. Uninstall Data Protector using `rpm`.

The configuration files and the database are preserved during this procedure.

4. Run the `rpm -q` command to verify that you uninstalled the old version of Data Protector. Old versions of Data Protector should not be listed.

Verify that the database and configuration files are still present. The following directories should still exist and contain binaries:

- `/opt/omni`
- `/var/opt/omni`
- `/etc/opt/omni`

5. If you are upgrading a Cell Manager, insert and mount the Linux installation DVD-ROM and use `rpm` to install the Cell Manager. For detailed steps, see ["Installing the Cell Manager on Linux systems using rpm"](#).

If you are upgrading an Installation Server, insert and mount the Linux installation DVD-ROM and install the Installation Server. For detailed steps, see ["Installing an Installation Server on Linux systems using rpm"](#).





## Appendix B: System preparation and maintenance tasks

This appendix provides some additional information about tasks that are beyond the scope of this guide but strongly influence the installation procedure. These tasks include system preparation and maintenance tasks.

### Network configuration on UNIX systems

When you install Data Protector on a UNIX system, Data Protector Inet is registered as a network service. Typically this involves the following steps:

- Modification of the `/etc/services` file for registering a port on which Data Protector Inet will listen.
- Registration of Data Protector Inet in the system's `inetd` daemon or its equivalent (`xinetd`, `launchd`).

When you modify a network configuration, the initial Data Protector Inet configuration may become incomplete or even invalid. This happens whenever you add or remove Internet Protocol version 6 (IPv6) network interfaces, due to the system-specific settings for adding IPv6 support to network services. It may happen in other circumstances as well.

In order to update the Data Protector Inet configuration, you can use the `dpsvcsetup.sh` utility. This utility, also used by the installation, which gathers the necessary information and accordingly updates the system configuration, is located in the directory `/opt/omni/sbin` (HP-UX, Solaris, and Linux systems) or `/usr/omni/bin` (other UNIX systems).

- To update the Data Protector Inet configuration, execute:

```
dpsvcsetup.sh -update.
```

- To register the Data Protector Inet as a network service, execute:

```
dpsvcsetup.sh -install.
```

- To unregister the Data Protector Inet as a network service, execute:

```
dpsvcsetup.sh -uninstall.
```

### Checking the TCP/IP setup

An important aspect of the TCP/IP configuration process is the setup of a hostname resolution mechanism. Each system in the network must be able to resolve the address of the Cell Manager as well as all clients with Media Agents and physical media devices attached. The Cell Manager must be able to resolve the names of all clients in the cell.

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig/ifconfig` commands to verify the TCP/IP configuration.

Note that on some systems the `ping` command cannot be used for IPv6 addresses, the `ping6` command should be used instead.

1. At the command line, execute:

**Windows systems:** `ipconfig /all`

**UNIX systems:** `ifconfig interface` or `ifconfig -a` or `netstat -i`, depending on the system

The precise information on your TCP/IP configuration and the addresses that have been set for your network adapter. Check if the IP address and subnet mask are set correctly.

2. Type `ping your_IP_address` to confirm the software installation and configuration. By default, you should receive four echo packets.
3. Type `ping default_gateway`.

The gateway should be on your subnet. If you fail to ping the gateway, check if the gateway IP address is correct and that the gateway is operational.

4. If the previous steps have worked successfully, you are ready to test the name resolution. Enter the name of the system while running the `ping` command to test the hosts file and/or DNS. If your machine name was `computer`, and the domain name was `company.com`, you would enter: `ping computer.company.com`.

If this does not work, verify that the domain name in the TCP/IP properties window is correct. You should also check the hosts file and the DNS. Be sure that the name resolution for the system, which is intended to be the Cell Manager, and the systems, which are intended to be the clients, is working in both ways:

- On the Cell Manager you can ping each client.
- On the clients you can ping the Cell Manager and each client with a Media Agent installed.

**Note:** When using the hosts file for the name resolution, the above test does not guarantee that name resolution works properly. In this case, you may want to use **DNS check tool** once Data Protector is installed.

**Important:** If the name resolution, as specified above, is not working, Data Protector cannot be installed properly.

Also note that the Windows computer name must be the same as the hostname. Otherwise, Data Protector setup reports a warning.

5. After Data Protector has been installed and a Data Protector cell has been created, you can use the DNS check tool to check that the Cell Manager and every client with a Media Agent installed resolve DNS connections to all other clients in the cell properly and vice versa. You do this by executing the `omnicheck -dns` command. Failed checks and the total number of failed checks are listed.

For detailed information on the `omnicheck` command, see the *HP Data Protector Command Line Interface Reference*.

## Changing the default Data Protector ports

### Changing the default Data Protector Inet port

The Data Protector `Inet` service (process), which starts other processes needed for backup and restore, should use the same port on each system within the Data Protector cell.

By default, `Inet` uses the port number 5555. To verify that this particular port is not used by another program, inspect the local `/etc/services` file (UNIX systems) or the output of the locally invoked `netstat -a` command (Windows systems). If the port is already in use by another program, you must reconfigure `Inet` to use an unused port. Such reconfiguration must be done on *each* system of the cell so that *all* systems in the cell use the same port.

Once changed on the Cell Manager which also acts as the Installation Server, or on a standalone Installation Server, the new port is automatically used by all clients which are remotely installed using this Installation Server. The `Inet` port can, therefore, be changed most easily when establishing the cell.

**Caution:** Do not change the default `Inet` listen port on systems that are prepared for disaster recovery. In the opposite case, if such systems are struck by a disaster, the disaster recovery process may fail.

#### UNIX systems

To change the `Inet` port on a UNIX system that will become your Cell Manager, Installation Server, or Data Protector client, follow the steps:

- Create the file `/tmp/omni_tmp/socket.dat` with the desired port number.

To change the `Inet` port on a UNIX system that is already your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. Edit the `/etc/services` file. By default, this file should contain the entry:

```
omni 5555/tcp # DATA-PROTECTOR
```

Replace the number 5555 with the number of an unused port.

2. If the files `/etc/opt/omni/client/customize/socket` and `/opt/omni/newconfig/etc/opt/omni/client/customize/socket` exist on the system, update their content with the desired port number.
3. Restart the `Inet` service by terminating the process concerned using the `kill -HUP inetd_pid` command. To determine the process ID (`inetd_pid`), run the `ps -ef` command.
4. If you are reconfiguring `Inet` on the Cell Manager, set a new value for the `Port` global option.
5. If you are reconfiguring `Inet` on the Cell Manager, restart the Data Protector services:

- `omnisv stop`
- `omnisv start`

## Windows systems

To change the `Inet` port on a Windows system that will become your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. From the command line, run `regedit` to open the Registry editor.
2. Under the key `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Common`, create the registry entry `InetPort`:

Name of the registry entry: `InetPort`

Type of the registry entry: `REG_SZ` (string)

Value of the registry entry: *PortNumber*

To change the `Inet` port on a Windows system that is already your Cell Manager, Installation Server, or Data Protector client, follow the steps:

1. From the command line, run `regedit` to open the Registry editor.
2. Expand **HKEY\_LOCAL\_MACHINE**, **SOFTWARE**, **Hewlett-Packard**, **OpenView**, **OmniBack**, and select **Common**.
3. Double-click **InetPort** to open the Edit String dialog box. In the Value data text box, enter the number of an unused port. The same must be done in the Parameters subfolder of the Common folder.
4. In the Windows Control Panel, open **Administrative Tools**, **Services**, then select the **Data Protector Inet** service, and restart the service by clicking the **Restart** icon on the toolbar.

## Changing the default Data Protector IDB ports and user accounts on UNIX systems

On UNIX systems the installation is performed by the `omnisetup.sh` script and is not interactive. You must change the port values in the file `/tmp/omni_tmp/DP.dat` before you start the installation.

The following port entries correspond to the IDB services:

- HP Data Protector IDB (hdpd-idb) service port: `PGPORT`
- HP Data Protector IDB Connection Pooler (hdpd-idb-cp) port: `PGCPORT`
- HP Data Protector Application Server (hdpd-as) service port: `APPSSPORT`
- HP Data Protector Application Server (hdpd-as) management port: `APPSNATIVEMGTPORT`

You can change the default user account under which the IDB is run by setting the variable `PGOSUSER`.

Example DP .dat file:

```
PGPORT=7112  
PGCPPORT=7113  
PGOSUSER=hpdp  
APPSSPORT=7116  
APPSNATIVEMGTPORT=7119
```

## Preparing a Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 for Data Protector installation

To enable cluster-aware installation of Data Protector on a server cluster with Microsoft Cluster Service (MSCS) running on the Windows Server 2008 or Windows Server 2012 operating system, you need to prepare the cluster in advance. Failing to do so may result in failed sessions for backing up the local CONFIGURATION object, which must be backed up during preparation for disaster recovery, and potentially even in a data loss. For information for which combinations of Data Protector cell roles and Windows operating system releases cluster awareness is supported, see the latest support matrices at <http://support.openview.hp.com/selfsolve/manuals>.

### Prerequisites

- Ensure that you are logged on to the system with a domain user account. The domain user account must be a member of the local Administrators group.

### Preparation procedure

To properly prepare your cluster for Data Protector installation, perform the following:

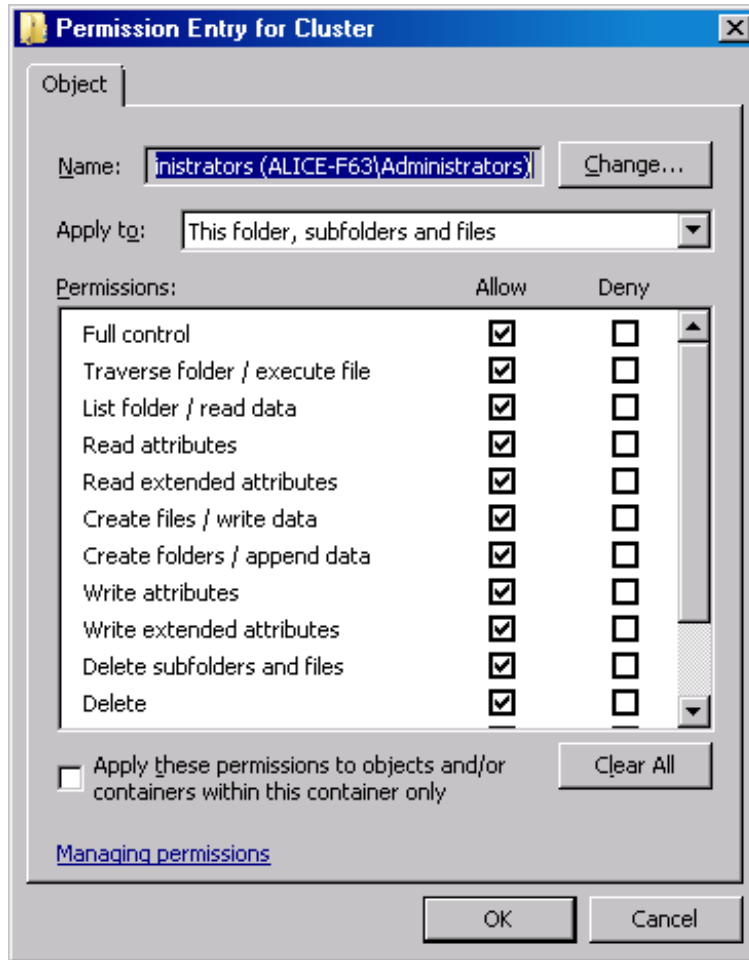
1. On both cluster nodes, start Windows Firewall and enable exceptions for the program `File and Printer Sharing`.
2. On the active cluster node, start Failover Cluster Management, and verify that the witness disk in quorum resource is online. If the resource is offline, bring it online.

Perform the steps that follow on the active cluster node only.

3. If you are preparing a cluster without a Majority Node Set (MNS) configured, start Windows Explorer and change ownership of the folder `WitnessDiskLetter:\Cluster` to the local Administrators group. While changing the ownership in the Advanced Security Settings for Cluster window, ensure that the option **Replace owner on subcontainers and objects** is selected. In the Windows Security dialog box, confirm the suggested action by clicking **Yes**, and confirm the notification that follows by clicking **Yes**.
4. If you are preparing a cluster without an MNS configured, in Windows Explorer, change permissions of the folder `WitnessDiskLetter:\Cluster` to allow full control for the SYSTEM and local

Administrators groups. Verify that the permission settings for both groups match the settings shown on " [Appropriate permissions for the Cluster folder and local users group Administrators](#) " .

**Figure 51: Appropriate permissions for the Cluster folder and local users group Administrators**



5. If you are preparing a cluster which will take the role of the Data Protector Cell Manager, in Failover Cluster Management, add a Cluster Access Point resource. Select **Add a resource** and click **1-Client Access Point** to start the New Resource wizard:
  - a. On the Client Access Point pane, enter the network name of the virtual server in the Name text box.
  - b. Enter the IP address of the virtual server in the Address text box.
6. If you are preparing a cluster which will take the role of the Data Protector Cell Manager, in Failover Cluster Management, add a shared folder to the cluster. Start the Provision a Shared Folder wizard by clicking **Add a shared folder**:
  - a. On the Shared Folder Location pane, enter a directory path in the Location text box. Ensure that the chosen directory has sufficient free space to store data created during the Data Protector installation. Click **Next**.

- b. On the NTFS Permissions, Share Protocols, and SMB Settings panes, leave the default option values unchanged. Click **Next** to move to the next pane.
- c. On the SMB Permissions pane, select the option **Administrators have Full Control; all other users and groups have only Read Access and Write Access**. Click **Next**.
- d. On the DFS Namespace Publishing, leave the default option values. Click **Next**.
- e. On the Review Settings and Create Share pane, click **Create**.

## Installing Data Protector on Microsoft Cluster Server with Veritas Volume Manager

To install Data Protector on Microsoft Cluster Server (MSCS) with Veritas Volume Manager, first follow the general procedure for installation of Data Protector on MSCS. See ["Installing Data Protector on a Microsoft Cluster Server"](#).

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. Initiate maintenance mode by execute the `omnisv -maintenance` command on the Cell Manager.
2. Define a new system environment variable `OB2CLUSTERDISKTYPES` with Volume Manager Disk Group as a value, or set the `omnirc` option on both cluster nodes as follows:

```
OB2CLUSTERDISKTYPES=Volume Manager Disk Group
```

To specify additional proprietary disk resources, such as NetRAID4 disk, simply append the resource type name to the `OB2CLUSTERDISKTYPES` environment variable value:

```
OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
```

For more information on using the `omnirc` file options, see the *HP Data Protector Troubleshooting Guide*.

3. Quit the maintenance mode by executing the `omnisv -maintenance -stop` command.

## Preparing a NIS server

This procedure enables your NIS server to recognize your Data ProtectorCell 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 is not available. See ["Changing the default Data Protector Inet port"](#) .

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
```

## Changing the Cell Manager name

When Data Protector is installed it uses the current hostname for the Cell Manager name. If you change the hostname of your Cell Manager, you need to update the Data Protector files manually.

**Important:** It is necessary to update the client information about the Cell Manager name. Before changing the hostname of your Cell Manager, export the clients from the cell. For the procedure, see ["Exporting clients from a cell"](#) . After you have changed the hostname, import the clients back to the



cell. For the procedure, see "[Importing clients to a cell](#)".

**Note:** Any devices and backup specifications that were configured using the old Cell Manager name must be modified to reflect the correct name.

## On UNIX systems

On a UNIX Cell Manager, do the following:

1. Change the computer or domain name.

**Note:** Ensure that the new hostname is resolved by DNS by all members and in both directions. Do not continue this procedure, if the name resolution does not work.

2. Execute the following command:

```
omnisv stop
```

**Note:** Ensure that no instances of the old hostname exists in the following file:  
`/etc/opt/omni/client/components`

You can execute the following command:

```
"grep -rn /etc/opt/omni/client/components -e "<OLD_HOSTNAME_FQDN>"
```

3. Change the Cell Manager hostname entries in the following files:

```
/etc/opt/omni/client/cell_server
```

```
/etc/opt/omni/server/cell/cell_info
```

```
/etc/opt/omni/server/config
```

```
/etc/opt/omni/server/cell/installation_servers
```

```
/etc/opt/omni/server/users/UserList
```

4. Regenerate the certificate by executing the following command:

```
# perl -CA /opt/omni/sbin/omnigencert.pl -server_id <NEW_HOSTNAME_FQDN> -server_
san dns:<short_hostname>,dns:< NEW_HOSTNAME_FQDN > -user_id hdpd -store_password
<STORE_PASSWORD>
```

**Note:** You can find the keystorepassword by executing the following command:

```
# grep keystorePassword /etc/opt/omni/client/components/webservice.properties
```

5. Execute the following command:

```
omnisv start
```

6. Change the Cell Manager name in the IDB by executing:

```
omnidbutil -change_cell_name
```

7. Connect to the Cell Manager using the Data Protector GUI and accept the new certificate.
8. If a tape device is connected to the Cell Manager, navigate to **Devices and Media**, and change the hostname in the properties of the tape device.
9. In case of a configured file device:

- a. To view the configured devices, use the following:

```
"omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"
```

- b. To modify the hostname in the Library, navigate to # omnidownload -library <LIBRARY\_NAME> >/tmp/file\_lib.txt and edit the file\_lib.txt file as follows:

```
# omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt
```

- c. To modify the hostname in Devices, navigate to # omnidownload -device <DRIVE\_NAME> >/tmp/writer\_0.txt and edit the writer\_0.txt file as follows:

```
# omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt
```

10. Delete the backup specification in the Data Protector IDB and recreate a new one.
11. Change the other backup specifications that are affected by the hostname change.
12. Update the UNIX or LINUX clients for the Cell Server hostname change in the following:

```
/etc/opt/omni/client/cell_server
```

13. Update the Windows clients for the Cell Server hostname change in the registry:

```
HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II ->  
Site -> CellServer
```

14. Check the following config file for the old hostname:

```
# grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"
```

**Note:** It is fine to view the old hostname in the following locations:

```
/etc/opt/omni/server/dr/p1s -> If the system recovery data has been stored in  
the past.
```

```
/etc/opt/omni/server/certificates -> old certificate  
  
/etc/opt/omni/client/certificates -> old certificate
```

15. Check the IDB content and export it to the following file:

```
/opt/omni/sbin/omnidbutil -writedb /tmp
```

<ENTER>

**Note:** The `dpidb.dat` file contains the main part of the Internal Database. Tables where the old hostname can still remain is as follows:

`dp_frontend_application`

`dp_catalog_object`

`dp_catalog_object_datastream` (in case the old device name(s) contain the old hostname)

`dp_management_session`

`dp_medmng_library` (in case the current device name(s) contain the old hostname)

`dp_medmng_media_pool` (in case the old pool name(s) contain the old hostname)

`dp_medmng_cartridge` (in case the old pool name(s) contain the old hostname)

Also, the `dpjce.dat` file contains the Job Control Engine (JCE) database. It contains few URL entries that are essential for advanced scheduler. The old hostname must not exist in this file.

If you find the old hostname in the `jce_service_description` table, proceed as follows:

- a. Login to the `hpjce` database.

**Note:** You can find the database credentials in `/etc/opt/omni/server/idb/idb.config` file.

```
# grep PGSUPERPASSWORD /etc/opt/omni/server/idb/idb.config  
  
PGSUPERPASSWORD='a2ZudGV4cjBpdTZnMg==';  
  
# export PGPASSWORD=`echo 'a2ZudGV4cjBpdTZnMg==' | base64 -d`  
  
# echo $PGPASSWORD  
  
kfntexr0iu6g2
```

b. Create a connection. Proceed as follows:

- i. In a command prompt, navigate to the bin location (/opt/omni/idb/bin/).
- ii. Execute the following command to login to the hpjce database using the hpdp user:

```
# /opt/omni/idb/bin/psql -h localhost -p 7112 -U hpdp hdpidb  
  
psql (9.1.9)  
  
Type "help" for help.
```

- iii. Check the current content by executing the following command in the hpjce database:

```
hpjce=# select url from jce_service_description;
```

**Note:** If you need to change the hostname, execute the following commands:

```
hpjce=# update jce_service_description  
  
hpjce=# set url=replace(url, 'old_hostname', 'new_hostname');  
  
hpjce=# \q
```

## On Windows systems

On a Windows Cell Manager, do the following:

1. Change the computer or domain name.

**Note:** Ensure that the new hostname is resolved by DNS by all members and in both directions. Do not continue this procedure, if the name resolution does not work.

2. Execute the following command:

```
omnisv stop
```

3. Change the Cell Manager name in the following registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site\CellServer\newname  
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Packages\newname
```

4. Navigate to the following file to ensure that no instances of the old hostname still exists:

```
Data_Protector_program_data\Config\client\components
```

**Note:** Use the Windows find in file function.

5. Change the Cell Manager hostname entries in the following files:

*Data\_Protector\_program\_data\Config\Server\users\UserList*

*Data\_Protector\_program\_data\Config\Server\config*

*Data\_Protector\_program\_data\Config\Server\cell\cell\_info*

*Data\_Protector\_program\_data\Config\Server\cell\installation\_servers*

6. Regenerate the certificate by executing the following command from C:\Program Files\OmniBack\bin folder:

```
perl omnigencert.pl -server_id <NEW_HOSTNAME> -server_san
```

```
dns:<hostname>,dns:<FQDN> -user_id hdpd -store_password <PASSWORD>
```

**Note:** You can find the keystorepassword from the following location:

*Data\_Protector\_program\_data\Config\client\components\webservice.properties*

7. Execute the following command:

```
omnisv start
```

8. Change the Cell Manager name in the IDB by executing:

```
omnidbutil -change_cell_name
```

9. Connect to the Cell Manager using the Data Protector GUI and accept the new certificate.
10. If a tape device is connected to the Cell Manager, navigate to **Devices and Media**, and change the hostname in the properties of the tape device.
11. In case of a configured file device:

- a. To view the configured devices, use the following:

```
"omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"
```

- b. To modify the hostname in the Library, navigate to "omnidownload -library <LIBRARY\_NAME>  
> c:\temp\file\_lib.txt" and edit the file\_lib.txt file as follows:

```
omniupload -modify_library <LIBRARY_NAME> -file c:\temp\file_lib.txt
```

- c. To modify the hostname in Devices, navigate to "omnidownload -device <Device Name> >

c:\temp\device.txt" and edit the device.txt file as follows:

```
omniupload -modify_device <Device Name> -file c:\temp\device.txt
```

12. Delete the backup specification in the Data Protector IDB and recreate a new one.
13. Change the other backup specifications that are affected by the hostname change.
14. Update the UNIX or LINUX clients for the Cell Server hostname change in the following:

```
/etc/opt/omni/client/cell_server
```

15. Update the Windows clients for the Cell Server hostname change in the registry:

```
HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II ->  
Site -> CellServer
```

16. Check the following config file using the Windows "find in file" function to search the old hostname:

```
Data_Protector_program_data\Config
```

**Note:** It is fine to view the old hostname in the following locations:

```
Data_Protector_program_data\Config\Server\dr -> If system recovery has been stored in  
the past.
```

```
Data_Protector_program_data\Config\Server\certificates -> old certificate
```

```
Data_Protector_program_data\Config\client\certificates -> old certificate
```

17. Check the IDB content and export it to the following file:

```
omnidbutil -writedb e:\idb_export
```

<ENTER>

**Note:** The dpidb.dat file contains the main part of the Internal Database. Tables where the old hostname can still remain is as follows:

```
dp_frontend_application
```

```
dp_catalog_object
```

```
dp_catalog_object_datastream (in case the old device name(s) contain the old  
hostname)
```

```
dp_management_session
```

```
dp_medmng_library (in case the current device name(s) contain the old
hostname)

dp_medmng_media_pool (in case the old pool name(s) contain the old hostname)

dp_medmng_cartridge (in case the old pool name(s) contain the old hostname)
```

Also, the `dpjce.dat` file contains the Job Control Engine (JCE) database. It contains few URL entries that are essential for advanced scheduler. The old hostname must not exist in this file.

If you find the old hostname in the `jce_service_description` table, proceed as follows:

- a. Login to the hpjce database.

**Note:** You can find the database credentials in `Data_Protector_program_data\Config\Server\idb\idb.config` file. You can use the following link to decode the PGSUPERPASSWORD:

<https://www.base64decode.org>

- b. Create a connection. Proceed as follows:

- i. In a command prompt, navigate to the bin location (`C:\Program Files\OmniBack\idb\bin`).
- ii. Execute the following command to login to the hpjce database using the hpdp user:  

```
.\psql -h localhost -p 7112 -d hpjce -U hpdp <Enter the decoded password>
```
- iii. Check the current content by executing the following command in the hpjce database:  

```
hpjce=# select url from jce_service_description;
```

**Note:** If you need to change the hostname, execute the following commands:

```
hpjce=# update jce_service_description
hpjce=# set url=replace(url, 'old_hostname', 'new_hostname');
hpjce=# \q
```

## Changing the hostname in Job Control Engine (JCE) database

### On UNIX systems

To change the hostname in JCE database with PGADMIN3, proceed as follows:

1. Navigate to `/var/opt/omni/server/db80/pg/pg_hba.conf` file.
2. Change `host all all 127..0.0.1/32 md5` to `host all all 10.17.0.0/16 md5`.

(OR)

Change `host all all 127..0.0.1/32 md5` to connect to a specific host (`host all all 10.17.16.121/32 md5`) only.

3. Reload the `pg config` file and execute the following commands:

```
su hpdp
```

```
/opt/omni/idb/bin/pg_ctl reload -D /var/opt/omni/server/db80/pg
```

4. Connect to pgAdmin3.

### *On Windows systems*

To change the hostname in JCE database using the command line with PGADMIN3, proceed as follows:

1. Execute the following command:

```
omnidbutil -set_passwd hpdp
```

2. Set the password.
3. Navigate to the `C:\Program Files\OmniBack\idb\bin` folder and run **pgadmin3.exe**.

The pgAdmin3 program gets started.

4. Add the server by clicking on the  plug-in.

The New Server Registration window is displayed.

5. In the New Server Registration window, perform the following:

- a. In the Name field, enter local or as per your requirement.

For example, enter `jce_service_description`.

- b. In the Host field, enter `localhost`.
- c. In the Port field, enter `7112`.
- d. In the Service field, leave it empty.
- e. In the Maintenance DB field, select `hdpidb`.
- f. In the Username field, enter `hpdp`.



- g. In the Password field, enter the password that you set with the `omnidbutil -set_passwd hdpd` command in [Step 1](#).
6. Click **OK**.
7. In the Object browser area, expand the server that you added by expanding Databases > hpjce > Schemas > hpjce\_app > Tables.

For example: You can see the `jce_service_description` table name. Click `jce_service_description`.

8. Select the SQL button in the tool bar.

You get to view the SQL Editor with the following command:

```
UPDATE jce_service_description  
  
SET url=replace (url, 'old_hostname', 'new_hostname');
```

For example, you can use `testHostname.1` as the `old_hostname` and `testHostname` as the `new_hostname`. Then execute this command with the Play button.

In the Data Output tab, you get to view the message stating the number of rows that were changed.

### Using CLI

To change hostname in the JCE database without PGADMIN3, proceed as follows:

1. Execute the following:

On Windows system:

```
C:\Program Files\OmniBack\idb\psql --port=7112 -U hdpd -d hpjce -h localhost
```

On UNIX system:

```
/opt/omni/idb/bin/psql --port=7112 -U hdpd -d hpjce -h localhost
```

2. Execute the following commands:

```
hpjce=# select url from jce_service_description;  
  
hpjce=# update jce_service_description  
  
hpjce=# set url=replace(url, 'old_hostname', 'new_hostname');  
  
hpjce=# \q
```



## Appendix C: Device and media related tasks

This Appendix provides some additional Data Protector specific information about tasks that are beyond the scope of this guide. These tasks include device driver configuration, managing SCSI robotics, maintaining the SCSI environment, and similar.

### Using tape and robotics drivers on Windows systems

Data Protector supports the native tape drivers that are loaded by default for an enabled tape drive attached to a Windows system. The Windows native drivers loaded for Medium changers (robotics) devices are not supported by Data Protector.

In the examples below, an HP 4mm DDS tape device is attached to the Windows system. The native driver loaded for medium changer devices needs to be disabled if the HP 4mm DDS tape device is connected to the Windows system and will be configured for use with Data Protector. This section describes the related procedures.

#### *Tape drivers*

A driver is usually delivered with Windows, if the device is listed in the Hardware Compatibility List (HCL). HCL is a list of the devices supported by Windows and can be found at the following site:

<http://www.microsoft.com/whdc/hcl/default.mspix>

The device drivers then load automatically for all enabled devices once the computer has been started. You do not need to load the native tape driver separately, but you can update it. To update or replace the native tape driver on a Windows system, proceed as follows:

1. In the Windows Control Panel, double-click **Administrative Tools**.
2. In the **Administrative Tools** window, double-click the **Computer Management**. Click **Device Manager**.
3. Expand Tape Drives. To check which driver is currently loaded for the device, right-click the tape drive and then click **Properties**.
4. Select the **Driver** tab and click **Update Driver**. Then, follow the wizard, where you can specify if you want to update the currently installed native tape driver or replace it with a different one.
5. Restart the system to apply the changes.

**Important:** If a device has already been configured for Data Protector without using the native tape driver, you have to rename the device files for all configured Data Protector backup devices that reference the particular tape drive (for example, from `scsi1:0:4:0` to `tape3:0:4:0`).

For details, see "[Creating device files \(SCSI Addresses\) on Windows systems](#)".

#### *Robotics drivers*

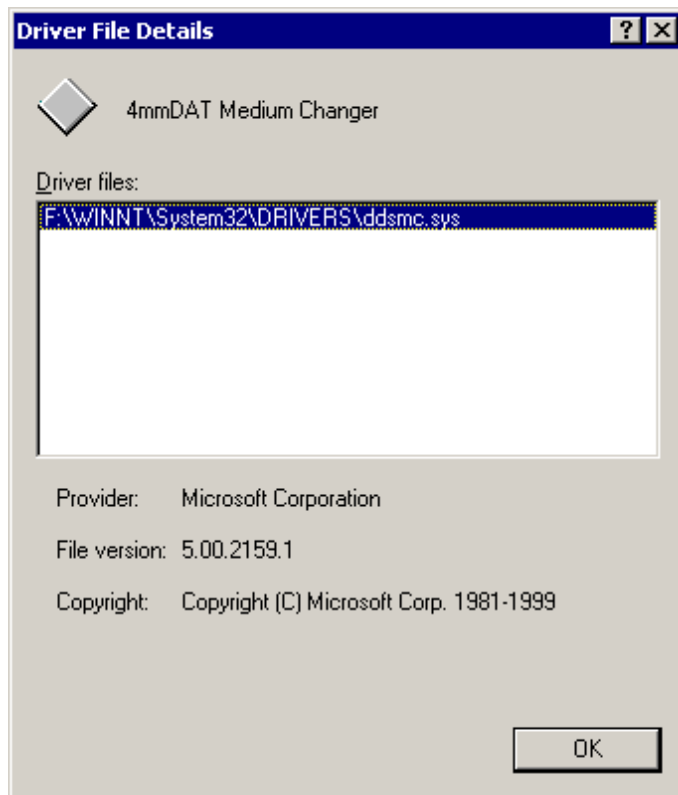
On Windows, the robotics drivers are automatically loaded for enabled tape libraries. In order to use the library robotics with Data Protector, you have to disable the respective driver.

An HP 1557A tape library using the 4mm DDS tapes is used in the example below. Proceed as follows to disable the automatically loaded robotics driver(`ddsmc.sys`) on a Windows system:

1. In the Windows Control Panel, double-click **Administrative Tools**.
2. In the Administrative Tools window, double-click the **Computer Management**. Click **Device Manager**.
3. In the Results Area of the Device Manager window, expand Medium Changers.
4. To check which driver is currently loaded, right-click the **4mm DDS Medium Changer** and then **Properties**.

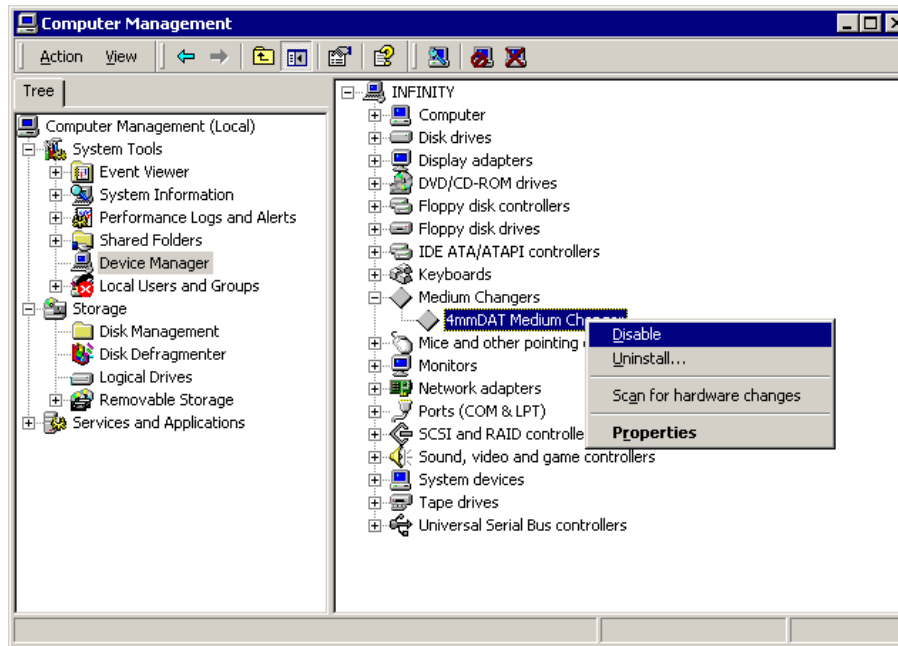
Select the **Driver** tab and click **Driver details**. In this case, the following window will display:

**Figure 52: Medium changer properties**



To disable the native robotics driver, right-click the **4mm DDS Medium Changer** and then select **Disable**.

**Figure 53: Disabling robotics drivers**



5. Restart the system to apply the changes. The robotics can now be configured with Data Protector.

## Creating device files (SCSI Addresses) on Windows systems

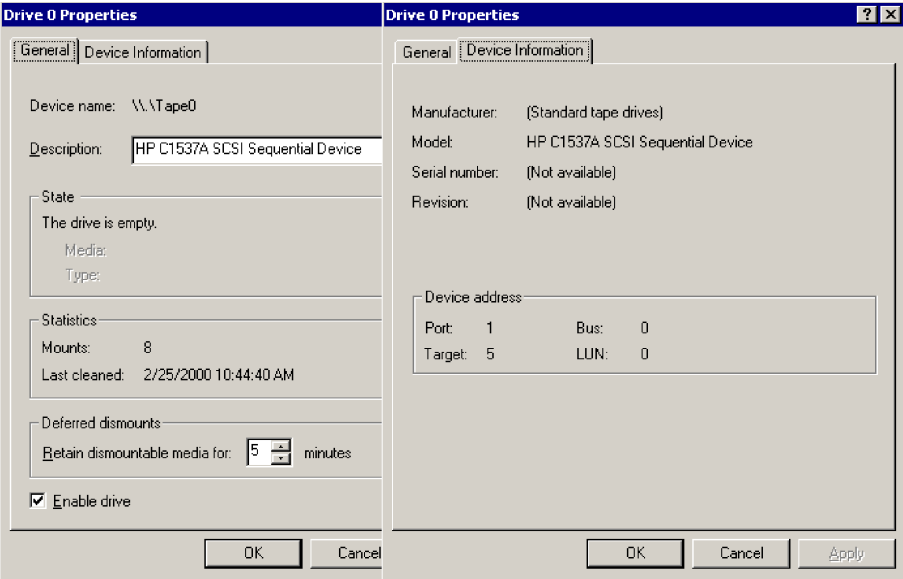
The tape device filename syntax depends on whether the native tape driver was loaded (tapeN:B:T:L) or unloaded (scsiP:B:T:L) for a tape drive.

### *Windows using the native tape driver*

To create a device file for a tape drive connected to a Windows system that uses the native tape driver, proceed as follows:

1. In the Windows Control Panel, double-click **Administrative Tools**.
2. In the Administrative Tools window, double-click the **Computer Management**. Expand Removable Storage, then Physical Locations. Right-click the tape drive and select **Properties**.
3. If the native tape driver is loaded, the device file name is displayed in the General property page. Otherwise, you can find the relevant information in the Device Information property page. See "[Tape drive properties](#)".

Figure 54: Tape drive properties



The file name for the tape drive in "Tape drive properties " is created as follows:

Native Tape Driver Used	Tape0 or Tape0:0:5:0
Native Tape Driver NOT Used	scsii1:0:5:0

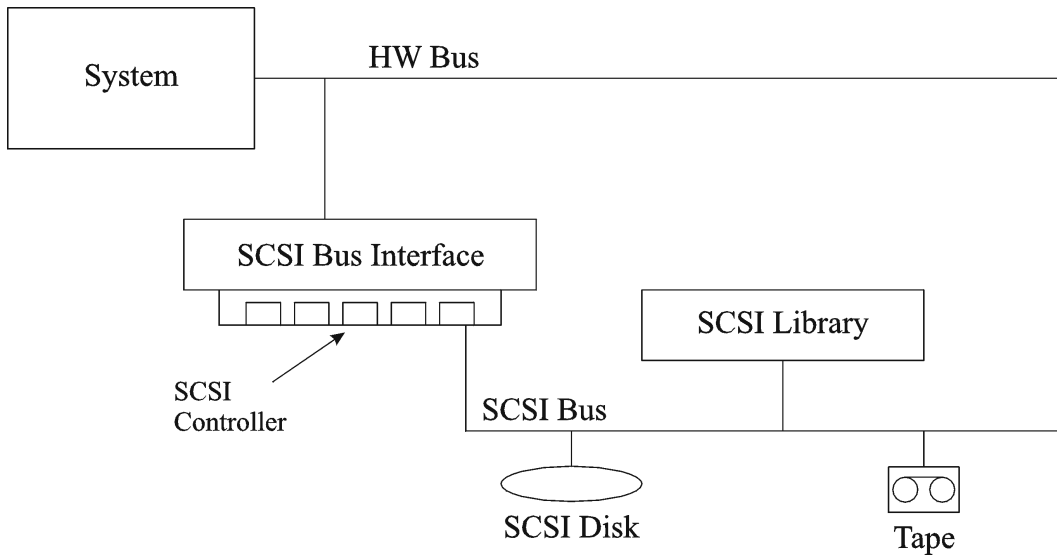
*Magneto-optical devices*

If you connect a magneto-optical device to a Windows system, a drive letter is assigned to the device after you restart the system. This drive letter is then used when you create the device file. For example, E : is the device file created for a magneto-optical drive which has been assigned a drive letter E.

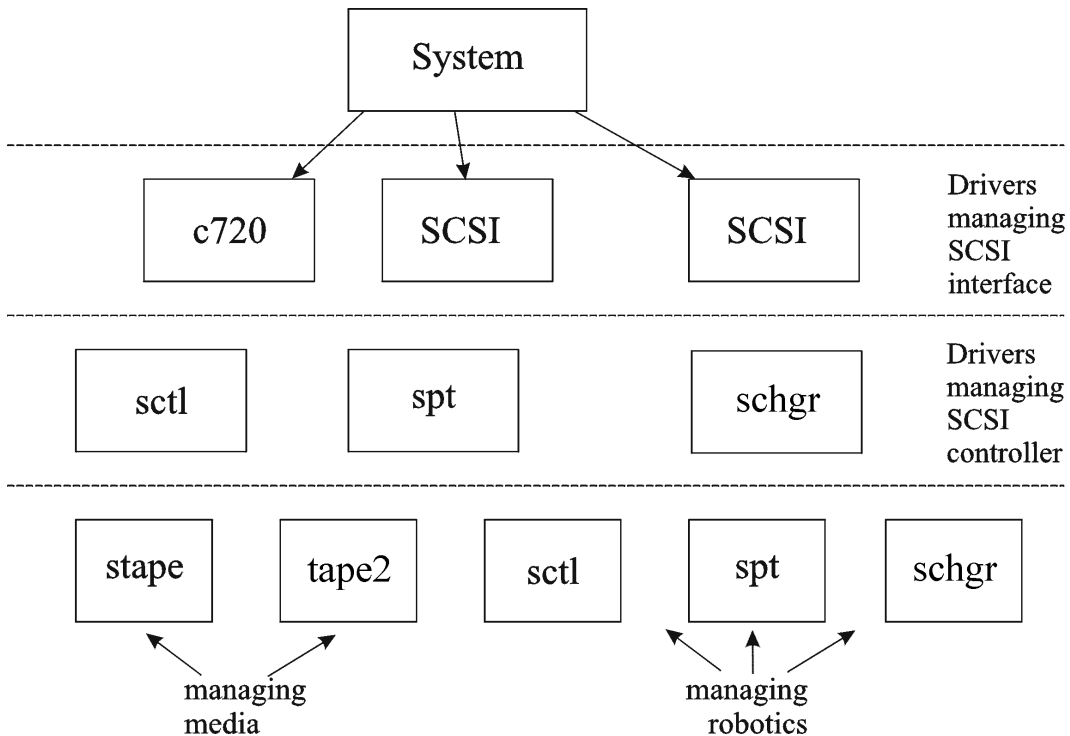
**SCSI robotics configuration on HP-UX systems**

On HP-UX systems, a SCSI Pass-Through Driver is used to manage the SCSI controller *and* control device (also referred to as robotics or picker) of the Tape Library devices (like HP 12000e). The control device in a library is responsible for loading/unloading media to/from the drives and importing/exporting media to/from such a device.

**Figure 55: SCSI controlled devices**



**Figure 56: 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"](#).

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 57: Status of the SCSI pass-through driver (sctl)**

```
root@superhik$ ioscan -f
```

Class	I	H/W Path	Driver	S/W State	H/W Type	Description
=====						
bc	0		root	CLAIMED	BUS_NEXUS	
bc	1	8	ccio	CLAIMED	BUS_NEXUS	I/O Adapter
unknown	-1	8/0		CLAIMED	DEVICE	GSC-to-PCI Bus Bridge
ext_bus	0	8/12	c720	CLAIMED	INTERFACE	GSC Fast/Wide SCSI Interfac
e						
target	0	8/12.0	tgt	CLAIMED	DEVICE	
disk	0	8/12.0.0	sdisk	CLAIMED	DEVICE	SEAGATE ST19171W
target	1	8/12.1	tgt	CLAIMED	DEVICE	
tape	5	8/12.1.0	stape	CLAIMED	DEVICE	QUANTUM DLT7000
target	2	8/12.2	tgt	CLAIMED	DEVICE	
ctl	0	8/12.2.0	sctl	CLAIMED	DEVICE	EXABYTE EXB-210
target	3	8/12.7	tgt	CLAIMED	DEVICE	
ctl	0	8/12.7.0	sctl	CLAIMED	DEVICE	Initiator
ba	0	8/16	bus_adapter	CLAIMED	BUS_NEXUS	Core I/O Adapter
ext_bus	2	8/16/0	CentIf	CLAIMED	INTERFACE	Built-in Parallel Interface
audio	0	8/16/1	audio	CLAIMED	INTERFACE	Built-in Audio
tty	0	8/16/4	asio0	CLAIMED	INTERFACE	Built-in RS-232C
ext_bus	1	8/16/5	c720	CLAIMED	INTERFACE	Built-in SCSI
target	4	8/16/5.2	tgt	CLAIMED	DEVICE	
disk	2	8/16/5.2.0	sdisk	CLAIMED	DEVICE	TOSHIBA CD-ROM XM-5401TA
target	7	8/16/5.3	tgt	NO_HW	DEVICE	
tape	3	8/16/5.3.0	stape	NO_HW	DEVICE	SONY SDX-300C
target	6	8/16/5.5	tgt	NO_HW	DEVICE	
tape	0	8/16/5.5.0	stape	NO_HW	DEVICE	SONY SDX-300C
target	5	8/16/5.7	tgt	CLAIMED	DEVICE	

In ["Status of the SCSI pass-through driver \(sctl\)"](#), 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 58: 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	
lan tty	0	56.2	lan tty0	CLAIMED	INTERFACE	
processor	0	62	processor	CLAIMED	PROCESSOR	Processor
memory	0	63	memory	CLAIMED	MEMORY	Memory
#						

In " [Status of the SCSI pass-through driver \(spt\)](#) ", you can see an example of a connected tape device with robotics controlled by the spt SCSI Pass-Through Driver. The particular device is an HP 12000e tape library device that uses the SCSI address 4 and is connected to the SCSI bus with the H/W Path 52. The matching hardware path is 52.4.1. The robotics is correctly assigned to the spt SCSI Pass-Through Driver.

If the sctl, spt, or schgr driver is not assigned to the robotics, you have to add the H/W Path of the robotics to the driver statement in the system file and rebuild the kernel. Follow the procedure below.

The following procedure explains how to *manually* add a SCSI Robotic Driver to the kernel, assign it to the robotics, and then manually rebuild a new kernel:

1. Login as a *root* user and switch to the build directory:

```
cd /stand/build
```

2. Create a new system file from your existing kernel:

```
/usr/sbin/sysadm/system_prep -s system
```

3. Check which SCSI Robotic Driver is already built in your current kernel. From the /stand directory, execute the following command:

```
grep SCSIRoboticDriver system
```

where the *SCSIRoboticDriver* can be either spt, sctl, or schgr. The system will display the corresponding line if the driver is already built in the current kernel.

4. Use an editor to append a driver statement:

```
driver H/W Path spt
```

to the /stand/build/system file, where *H/W Path* is the complete hardware path of the device.

For the HP 12000e Tape library from the previous example you would enter:

```
driver 52.4.1 spt
```

For several libraries connected to the same system, you have to add a driver line for each library robotics with the appropriate hardware path.

When configuring the `schgr` driver, append the following line to a driver statement:

```
schgr
```

5. Enter the `mk_kernel -s ./system` command to build a new kernel.
6. Save the original old system file using a different name and move the new system file to the original name so that it becomes the current one:

```
mv /stand/system /stand/system.prev
```

```
mv /stand/build/system /stand/system
```

7. Save the old kernel with a different name and move the new kernel to the original name so that it becomes the current one:

```
mv /stand/vmunix /stand/vmunix.prev
```

```
mv /stand/vmunix_test /stand/vmunix
```

8. Restart the system from the new kernel by entering the following command:

```
shutdown -r 0
```

9. Once you have restarted the system, verify the changes you have made using the `/usr/sbin/ioscan -f` command.

## Creating device files on HP-UX systems

### *Prerequisites*

Before you create a device file, you should have the backup device already connected to the system. Use the `/usr/sbin/ioscan -f` command to check whether the device is properly connected. Use the `/usr/sbin/infs -e` command to create device files for some backup devices automatically.

If the device files that correspond to a particular backup device have not been created during the system initialization (boot process) or after running the `infs -e` command, you have to create them manually. This is the case with the device files required to manage the library control device (library robotics).

We will use an example of creating a device file for the robotics of the HP 12000e library device connected to an HP-UX system. The device file for the tape drive has already been created automatically after the restart of the system, while the device file for the control device must be created manually.

In "[Status of the SCSI pass-through driver \(spt\)](#)", you can see the output of the `ioscan -f` command on the selected HP-UX system.

**Figure 59: List of connected devices**

```
# 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	scsi1	CLAIMED	INTERFACE	HP 28655A - SCSI Interface
target	4	52.1	target	CLAIMED	DEVICE	
disk	4	52.1.0	disc3	CLAIMED	DEVICE	SEAGATE ST15150N
target	1	52.2	target	CLAIMED	DEVICE	
disk	0	52.2.0	disc3	CLAIMED	DEVICE	TOSHIBA CD-ROM XM-4101TA
target	3	52.4	target	CLAIMED	DEVICE	
tape	0	52.4.0	tape2	CLAIMED	DEVICE	HP C1533A
spt	1	52.4.1	spt	CLAIMED	DEVICE	HP C1553A
target	6	52.5	target	CLAIMED	DEVICE	
disk	5	52.5.0	disc3	CLAIMED	DEVICE	SEAGATE ST15150N
target	2	52.6	target	CLAIMED	DEVICE	
disk	1	52.6.0	disc3	CLAIMED	DEVICE	SEAGATE ST15150N
lanmux	0	56	lanmux0	CLAIMED	INTERFACE	LAN/Console
tty	0	56.0	mux4	CLAIMED	INTERFACE	
lan	0	56.1	lan3	CLAIMED	INTERFACE	
lantty	0	56.2	lantty0	CLAIMED	INTERFACE	
processor	0	62	processor	CLAIMED	PROCESSOR	Processor
memory	0	63	memory	CLAIMED	MEMORY	Memory

```
# █
```

The SCSI bus interface is controlled by the `scsi1` system driver. This is a SCSI NIO interface. To access the library robotics on the SCSI NIO bus we must use the `spt` SCSI Pass-Through driver that is already installed and assigned to the robotics of the HP 12000e Tape device that uses the hardware path 52.4.1.

**Note:** If you do not use a SCSI NIO based bus interface, the `spt` driver is not required but the `sctl` driver is used instead.

To create the device file, you need to know the *Major number* character of the SCSI Pass-Through driver and the *Minor Number* character, which does not depend on the SCSI Pass-Through driver you use.

To obtain the character *Major number* belonging to `spt`, run the system command:

```
lsdev -d spt
```

In the example (see " [List of connected devices](#) ") the command reported the *Major number* character 75.

To obtain the character *Major number* belonging to `sctl`, run the system command:

```
lsdev -d sctl
```

In our case, the command reported the *Major number* character 203.

The *Minor Number* character, regardless of which SCSI Pass-Through driver is in use, has the following format:

```
0xIITL00
```

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 might require additional configuration on some SCSI controllers.

On Windows systems, 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.

$\text{MaximumSGList} = (\text{OBBlockSize in kB} / 4) + 1$

For example, to enable block sizes up to 260 kB, MaximumSGList has to be at least  $(260 / 4) + 1 = 66$ .

3. Restart the system.

**Note:** This registry value sets the upper limit of the block size. The actual block size for a device must be configured using the Data Protector GUI for device configuration.

## Finding the unused SCSI addresses on HP-UX systems

A backup device connected to an HP-UX system is accessed and controlled through a device file that must exist for each physical device. Before you can create the device file, you have to find out which SCSI addresses (ports) are still unused and available for a new device.

On HP-UX systems, the `/usr/sbin/ioscan -f` system command is used to display the list of the SCSI addresses that are already occupied. Thus, the addresses not listed in the output of the `/usr/sbin/ioscan -f` command are still unused.

In " [Output of the ioscan -f command on an HP-UX system](#) ", there is the output of the /usr/sbin/ioscan -f command on an HP-UX 11.x system.

**Figure 60: Output of the ioscan -f command on an HP-UX system**

```
# ioscan -f
Class      I  H/W Path  Driver      S/W State H/W Type  Description
=====
bc          0                root        CLAIMED    BUS_NEXUS
ext_bus     0  52        scsi1       CLAIMED    INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target      CLAIMED    DEVICE
disk        4  52.1.0    disc3       CLAIMED    DEVICE      SEAGATE ST15150N
target      1  52.2      target      CLAIMED    DEVICE
disk        0  52.2.0    disc3       CLAIMED    DEVICE      TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target      CLAIMED    DEVICE
tape        0  52.4.0    tape2       CLAIMED    DEVICE      HP C1533A
spt         1  52.4.1    spt         CLAIMED    DEVICE      HP C1553A
target      6  52.5      target      CLAIMED    DEVICE
disk        5  52.5.0    disc3       CLAIMED    DEVICE      SEAGATE ST15150N
target      2  52.6      target      CLAIMED    DEVICE
disk        1  52.6.0    disc3       CLAIMED    DEVICE      SEAGATE ST15150N
lanmux      0  56        lanmux0     CLAIMED    INTERFACE  LAN/Console
tty         0  56.0      mux4        CLAIMED    INTERFACE
lan         0  56.1      lan3        CLAIMED    INTERFACE
lantty      0  56.2      lantty0     CLAIMED    INTERFACE
processor   0  62        processor   CLAIMED    PROCESSOR  Processor
memory      0  63        memory      CLAIMED    MEMORY     Memory
# █
```

Only the third (H/W Path) and the fifth (S/W State) columns are relevant for the purpose of determining the available SCSI addresses. A dismembered (H/W Path) format would look like this:

*SCSI\_bus\_H/W\_Path. SCSI\_address. LUN\_number*

In this particular case, there is just one SCSI bus, using the H/W Path 52. On this bus, you can use the SCSI addresses 0 and 3 because they do not appear in the list.

You can see in " [Output of the ioscan -f command on an HP-UX system](#) " which SCSI addresses on the selected SCSI bus are already occupied:

- SCSI address 1 by a SCSI disk
- SCSI address 2 by a CD-ROM
- SCSI address 4, LUN 0, by a tape drive
- SCSI address 4, LUN 1, by the tape library robotics
- SCSI address 5 by a SCSI disk
- SCSI address 6 by a SCSI disk
- SCSI address 7 by a SCSI controller

**Note:** The SCSI address number 7 is *not* listed although it is, by default, occupied by the SCSI controller.

All devices have the S/W State value set to CLAIMED and the H/W Type value set to H/W DEVICE, meaning that the devices are currently connected. If there was an UNCLAIMED value in the S/W State or NO-HW in the H/W Type column it would mean that the system cannot access the device.

The SCSI address 4 is claimed by the tape library that has the tape drive with LUN 0 and the robotics with LUN 1. The drive is controlled by the `tape2` driver and the robotics is controlled by the `spt` SCSI Pass-Through driver. Looking at the description, you can see that the device is an HP 12000e library; it is easily recognized among the SCSI libraries because it uses the same SCSI address for the tape drive and robotics but uses different LUNs.

The whole SCSI bus is controlled by the `scsi1` interface module.

## Finding the unused SCSI target IDs on Solaris systems

A backup device connected to a Solaris system is accessed and controlled through a device file. This device file is created automatically by the Solaris operating system, in the directory `/dev/rmt`, when the backup device is connected and the client system and backup device are powered up.

Before the backup device is connected, however, the available SCSI addresses must be checked and the address of the backup device set to an address not already allocated.

To list the available SCSI addresses on a Solaris system:

1. Stop the system by pressing **Stop** and **A**.
2. Run the `probe-scsi-all` command at the ok prompt:

```
probe-scsi-all
```

You may be asked by the system to start the `reset-all` command before executing the `probe-scsi-all` command.

3. To return to normal operation, enter `go` at the ok prompt:

```
go
```

After listing the available addresses and choosing one to use for your backup device, you must update the relevant configuration files before connecting and starting up the device. See the next section for instructions on updating the configuration files.

## Updating the device and driver configuration on Solaris systems

### Updating configuration files

The following configuration files are used for device and driver configuration. They must be checked, and if necessary, edited before attached devices can be used:

- `st.conf`
- `sst.conf`

### *st.conf: all devices*

This file is required on each Data Protector Solaris client with a tape device connected. It must contain device information and one or more SCSI addresses for each backup device connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

1. Check the unused SCSI addresses on the client, as described in the previous section, and choose an address for the device you want to attach.
2. Set the chosen SCSI address(es) on the backup device.
3. Power down the client system.
4. Attach the backup device.
5. First power up the device and then the client system.
6. Stop the system by pressing `Stop` and `A`.
7. Enter the `probe-scsi-all` command at the `ok` prompt:

```
probe-scsi-all
```

This will provide information on the attached SCSI devices, including the correct device ID string for the newly attached backup device.

8. Return to normal running:

```
go
```

9. Edit the `/kernel/drv/st.conf` file. This file is used by the Solaris `st` (SCSI tape) driver. It contains a list of devices officially supported by Solaris and a set of configuration entries for third party devices. If you are using a supported device, it should be possible to connect the device and use it without any further configuration. Otherwise, you should add the following types of entries to `st.conf`:

- A tape configuration list entry (plus a tape data variable definition). Example entries are supplied in the file, commented out. You can use one of these, if applicable, or modify one to suit your needs.

The entry must come before the first `name=` entry in the file and the required format is as follows:

```
tape-config-list= "Tape unit", "Tape reference name", "Tape data";
```

where:

<i>Tape unit</i>	The vendor and product ID string for the tape device. This must be correctly specified as described in the device manufacturer's documentation.
<i>Tape reference name</i>	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.
<i>Tape data</i>	A variable that references a series of additional tape device configuration items. The variable definition must also be supplied and be correctly specified, as described in the device manufacturer's documentation.

For example:

```
tape-config-list="Quantum DLT4000","Quantum DLT4000","DLT-data";
```

```
DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

The second parameter, 0x38, designates the DLTtape tape type as "other SCSI drive". The value specified here should be defined in `/usr/include/sys/mtio.h`.

**Note:** Ensure that the last entry in the tape-config-list is terminated with a semi-colon (;).

- For multidrive devices, target entries as follows:

```
name="st" class="scsi"
```

```
target=X lun=Y;
```

where:

<i>X</i>	is the SCSI port assigned to the data drive (or robotic mechanism).
<i>Y</i>	is the logical unit value.

For example:

```
name="st" class="scsi"
```

```
target=1 lun=0;
```

```
name="st" class="scsi"
```

```
target=2 lun=0
```

Normally target entries are required in `st.conf` only for the drives, not for the robotics mechanism, which is on a different target. Entries for these are usually provided in the `sst.conf` file (see below). However, there are some devices, for example the HP 24x6, that treat the robotics



mechanism similar to another drive. In this case two entries with the same target are required (one for the drive and one for the robotics), but with different LUNs.

For example:

```
name="st" class="scsi"

target=1 lun=0;

name="st" class="scsi"

target=1 lun=1
```

### *sst.conf: library devices*

This file is required on each Data Protector Solaris client to which a multi-drive library device is connected. Generally speaking, it requires an entry for the SCSI address of the robotic mechanism of each library device connected to the client (there are some exceptions, such as the HP 24x6 mentioned in the previous section).

1. Copy the sst driver (module) and configuration file `sst.conf` to the required directory:

- For 32-bit operating systems:

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

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

- For 64-bit operating systems:

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

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

2. Edit the `sst.conf` file and add the following entry:

```
name="sst" class="scsi" target=X lun=Y;
```

where:

X	is the SCSI address of the robotic mechanism.
Y	is the logical unit.

For example:

```
name="sst" class="scsi" target=6 lun=0;
```

3. Add the driver to the Solaris kernel:

```
add_drv sst
```

## Creating and checking device files

After setting up the configuration files and installing the drivers, you can create new device files as follows:

1. Remove all existing device files from the `/dev/rmt` directory:

```
cd /dev/rmt rm *
```

2. Enter the following to shut down the system:

```
shutdown -i0 -g0
```

3. Restart the system:

```
boot -rv
```

The `r` switch in the `boot` command enables a kernel compile and includes the creation of device special files used for communication with the tape device. The `v` switch enables verbose mode display of system startup. With verbose mode, the system should indicate that the device is attached by displaying the *Tape reference name* string you selected during the `/devices` directory configuration phase of boot.

4. Enter the following command to verify the installation:

```
mt -t /dev/rmt/0 status
```

The output of this command depends on the configured drive. It will be similar to the following:

```
Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention residual= 0 retries= 0  
file no= 0 block no= 0
```

5. When the system restart has completed, you can check the device files that have been created using the command `ls -all`. For a library device, the output of this command might be:

<code>/dev/rmt/0hb</code>	for a first tape drive
<code>/dev/rmt/1hb</code>	for a second tape drive
<code>/dev/rsst6</code>	for a robotic drive

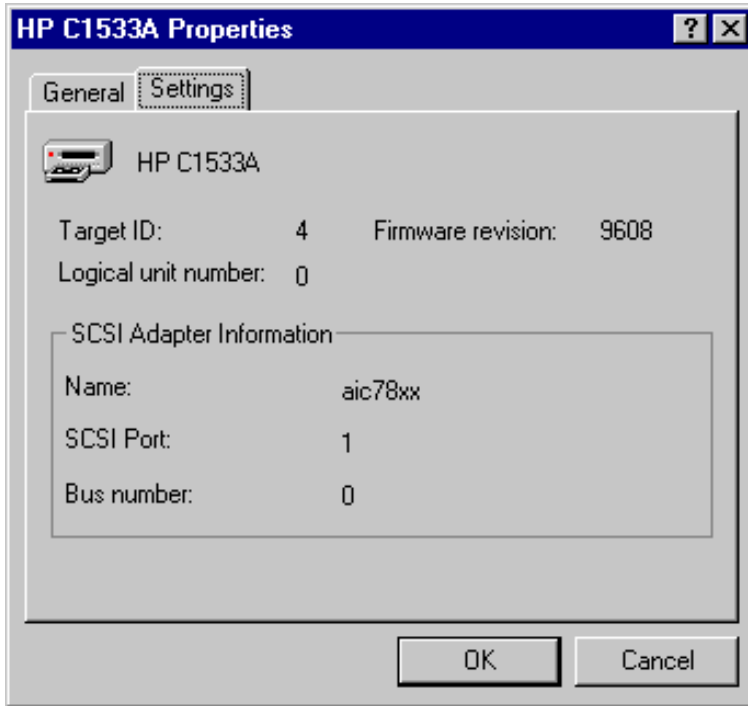
## Finding unused SCSI target IDs on Windows systems

Follow the steps below to determine the unused SCSI Target IDs (SCSI Addresses) on a Windows system:

1. In the Windows Control Panel, click **SCSI Adapters**.
2. For each device connected to a SCSI Adapter in the list, check its properties. Double-click the name of a device, and then click **Settings** to open the property page. See "[Device settings](#)".

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 61: Device settings**



## Setting SCSI IDs on an HP 330fx library

Once you have chosen the unused SCSI IDs for the robotics and drives, you can check and configure them using the Control Panel of the library device.

EXAMPLE: If you have a library model HP 330fx, you can find the configured SCSI IDs as follows:

1. From the READY state, press **NEXT**, and then ADMIN\* will appear.
2. Press **ENTER**, and then you will be asked for the password. Enter the password.
3. TEST\* will appear, press **NEXT** until SCSI IDs \* appears.
4. Press **ENTER**. VIEW IDs\* appears.
5. Press **ENTER**. JKBX ID 6 LUN 0 appears.
6. Press **NEXT**. DRV 1 ID 5 LUN 0 appears.
7. Press **NEXT**. DRV 2 ID 4 LUN 0 appears, and so on.

You can return to the READY state by pressing CANCEL several times.

## Connecting backup devices

The following procedure describes the general steps to follow in order to connect a backup device to an HP-UX, Solaris, Linux, or Windows system.

1. Select the client to which you will connect the backup device.
2. Install a Media Agent on the selected system. See ["Remote installation"](#) .
3. Determine the unused SCSI address that can be used by the device. For HP-UX systems, see ["Finding the unused SCSI addresses on HP-UX systems"](#) . For Solaris systems, see ["Finding the unused SCSI target IDs on Solaris systems"](#) . For a Windows system, see ["Finding unused SCSI target IDs on Windows systems"](#) .

- 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"](#) .

If you need to configure a SCSI Pass-Through Driver, see ["SCSI robotics configuration on HP-UX systems"](#) .

- If connecting to a Solaris system, check that the required drivers are installed and the configuration files are updated for the device to be installed. See ["Updating the device and driver configuration on Solaris systems"](#) . This also tells you how to update the `sst.conf` file if you need to configure a SCSI Pass-Through Driver.
- If connecting to a Windows client, the native tape driver can be loaded or disabled, depending on the Windows system version. See ["Using tape and robotics drivers on Windows systems"](#) .

If you load the native tape driver for a device which has been already configured in Data Protector and did not use the native tape driver, make sure that you rename the device filenames for all configured Data Protector logical devices that reference this specific device (for example, from `scsi1:0:4:0` to `tape3:0:4:0`) .

For more information on an appropriate device filename, see ["Creating device files \(SCSI Addresses\) on Windows systems"](#) .

4. Set the SCSI addresses (IDs) on the device. Depending on the device type, this can be usually done using the switches on the device. For details, see the documentation that comes with the device.

For an example, see ["Setting SCSI IDs on an HP 330fx library"](#) .

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

**Note:** On a Windows systems with the Adaptec SCSI adapter installed and a SCSI device connected, the Host Adapter BIOS option must be enabled so that the system does not have problems issuing SCSI commands.

To set the Host Adapter BIOS option, press **Ctrl+A** during the boot of the system to enter the SCSI Adapter menu, then select **Configure/View Host Adapter Settings > Advanced Configuration Options** and enable Host Adapter BIOS.

5. First, switch on the device, and then the computer, and then wait until the boot process completes. Verify that the system correctly recognizes your new backup device.

**Windows systems:** You can verify that the system correctly recognizes your new backup device if you use the devbra utility. In the default Data Protector commands directory, execute the devbra - dev command.

In the output of the devbra command you will find the following lines for each connected and properly recognized device:

*backup device specification*

*hardware\_path*

*media\_type*

.....

For example, the following output:

HP:C1533A

tape3:0:4:0

DDS

...

...

means that an HP DDS tape device (with the native tape driver loaded) has the Drive instance number 3, and is connected to the SCSI bus 0, the SCSI Target ID 4 and LUN number 0.

Or, the following output:

HP:C1533A

scsi1:0:4:0

DDS

...

...

means that an HP DDS tape device (with the native tape driver unloaded) is connected to the SCSI port 1, SCSI bus 0, and the tape drive has the SCSI Target ID 4, and LUN number 0.

**HP-UX systems:** Run the command `/usr/sbin/ioscan -fn` to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

If the device file has not been created automatically during the system startup process, you should create it manually. See ["Creating device files on HP-UX systems"](#).

**Solaris systems:** Run the `ls -all` command on the `/dev/rmt` directory to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

**Linux systems:** Run the `ls -all` command on the `/dev/rmt` directory to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected device with the correct SCSI addresses.

**AIX systems:** Run the command `lsdev -C` to display the list of connected devices with the corresponding device files.

## Hardware compression

Most modern backup devices provide built-in hardware compression that can be enabled when you create a device file or SCSI address in the device configuration procedure. For detailed steps, see the *HP Data Protector Help*.

Hardware compression is done by a device that receives the original data from a Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

When software compression is used and hardware compression is disabled, the data is compressed by the Disk Agent and sent compressed to a Media Agent. The compression algorithm can take a substantial amount of resources from the Disk Agent system if software compression is used, but this reduces the network load.

To enable hardware compression on Windows systems, 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 systems, 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 systems, select a proper device file. Consult the device and operating system documentation for details.

## What's next?

At this stage, you should have the backup devices connected that enable you to configure backup devices and media pools. For more information about further configuration tasks, see the *HP Data Protector Help* index: "configuring, backup devices".

You must have a Media Agent installed on your system. See ["Remote installation"](#).

The following sections describe how to connect an HP Standalone 24 Tape Device, HP 12000e Library, and HP DLT Library 28/48-Slot to an HP-UX and a Windows system.

## Connecting an HP 24 standalone device

The 24 DDS backup device is a standalone tape drive based on DDS3 technology.

### *Connecting to an HP-UX system*

Follow the steps below to connect the HP 24 Standalone device to an HP-UX system:

1. Check that the required drivers (`stape` or `tape2`) are *installed* and *built* into the current kernel. See ["Checking the kernel configuration on HP-UX"](#).
2. Determine an unused SCSI address that can be used by the tape drive. See ["Finding the unused SCSI addresses on HP-UX systems"](#).
3. Set the SCSI addresses (IDs) on the device. Use the switches at the back of the device.

For details, see the documentation that comes with the device.

4. First, switch on the device, and then the computer, and wait until the boot process completes.
5. Verify that the system correctly recognizes the newly connected tape drive. Use the `ioscan` utility:

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

to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected tape drive, which has the correct SCSI address. The device file for the drive has been created during the boot process.

### *What's next?*

After properly connecting the device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

### *Connecting to a Windows system*

Follow the steps below to connect the HP 24 Standalone device to a Windows system:

1. Determine an unused SCSI address (Target ID) that can be used by the tape drive. See ["Finding unused SCSI target IDs on Windows systems"](#).
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. In the Data Protector commands directory, execute the `devbra -dev` command.

In the output of the `devbra` command, you should find the newly connected tape drive of the HP 24 Standalone device.

## What's next?

After properly connecting the device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

## Connecting an HP DAT Autoloader

Both the HP 12000e and the DAT24x6 libraries have a repository for six cartridges, one drive, and one robotic arm used for moving cartridges to and from the drive. The two libraries also have built-in dirty tape detection.

### Connecting to an HP-UX system

Follow the steps below to connect the HP 12000e library device to an HP-UX system:

1. On the rear side of the autoloader, set the mode switch to 6.
2. Check that the required drivers (`stape` or `tape2`) are *installed* and *built* into the current kernel. See ["Checking the kernel configuration on HP-UX"](#).
3. Check that the required SCSI Pass-Through drivers (`sctl` or `spt`) are *installed* and *built* into the current kernel. See ["SCSI robotics configuration on HP-UX systems"](#).
4. Determine an unused SCSI address that can be used by the tape drive and the robotics. See ["Finding the unused SCSI addresses on HP-UX systems"](#).

**Note:** The HP 12000e Library uses the same SCSI address for the tape drive and for the robotics, but uses different LUN numbers.

5. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.
6. First, switch on the device, and then the computer, and then wait until the boot process completes.
7. Verify that the system correctly recognizes the newly connected tape drive. Use the `ioscan` utility

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

to display a list of connected devices with the corresponding hardware paths and device files, where you should find your newly connected tape drive, having the correct SCSI address.

8. The device file for the drive has been created during the boot process, while the device file for the robotics must be created manually. See ["Creating device files on HP-UX systems"](#).
9. Verify that the system correctly recognizes the newly created device file for the library robotics. Run the `ioscan` utility:

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

You should see your newly created device file in the output of the command.



### What's next?

After properly connecting the library device, see the *HP Data Protector Help* index: “configuring, backup devices” for instructions about configuring a Data Protector backup device for your newly connected device.

### Connecting to a Windows system

Follow the steps below to connect the HP 12000e library device to a Windows system:

1. On the rear side of the autoloader, set the mode switch to 6.
2. Determine an unused SCSI address that can be used by the tape drive and for the robotics. See ["Finding unused SCSI target IDs on Windows systems"](#).
3. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.

**Note:** The HP 12000e Library uses the same SCSI address for the tape drive and for the robotics, but uses different LUN numbers.

4. First, switch on the device, and then the computer, and wait until the boot process completes.
5. Verify that the system correctly recognizes the newly connected tape drive and the robotics. In the default Data Protector commands directory, execute the `devbra -dev` command.

In the output of the `devbra` command, you should find the newly connected tape drive and the robotics of the HP 12000e Library device.

### What's next?

After properly connecting the library device, see the *HP Data Protector Help* index: “configuring, backup devices” for instructions about configuring a Data Protector backup device for your newly connected device.

## Connecting an HP DLT Library 28/48-Slot

The HP DLT Library 28/48-Slot is a multi-drive library for enterprise environments with 80-600 GB to back up. It has four DLT 4000 or DLT 7000 drives with multiple data channels, a mail slot, and a barcode reader.

### Connecting to an HP-UX system

Follow the steps below to connect the HP DLT Library 28/48-Slot library device to an HP-UX system:

1. Check that the required drivers (`stape` or `tape2`) drivers are *installed* and *built* into the current kernel. See ["Checking the kernel configuration on HP-UX"](#).
2. Check that the required SCSI Pass-Through drivers (`sct1` or `spt`) are *installed* and *built* into the current kernel. See ["SCSI robotics configuration on HP-UX systems"](#).

3. Determine an unused SCSI address that can be used by the tape drive and the robotics. See ["Finding the unused SCSI addresses on HP-UX systems"](#).

**Note:** The HP DLT Library 28/48-Slot has four tape drives and the robotics, so you need five unused SCSI addresses in case you will be using all tape drives. The tape drives and the robotics must use different SCSI addresses.

4. Set the SCSI addresses (IDs) on the device. For details, see the documentation that comes with the device.

5. Switch on the device, and then the computer, and wait until the boot process completes.

6. Verify that the system correctly recognizes the newly connected tape drives. Use the `ioscan` utility

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

to display a list of connected devices with the corresponding hardware paths and device files, where you must find your newly connected tape drives, having the correct SCSI addresses.

7. The device files for the drives have been created during the boot process, while the device file for the robotics must be created manually. See ["Creating device files on HP-UX systems"](#).

8. Verify that the system correctly recognizes the newly created device file for the library robotics. Use the `ioscan` utility:

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

You should see your newly created device file in the output of the command.

### *What's next?*

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

### *Connecting to a Solaris system*

To configure the HP C5173-7000 library device on a Solaris system, follow the steps below. For this example, it is assumed that two drives are to be allocated to Data Protector:

1. Copy the `sst` driver (module) and configuration file `sst.conf` to the required directory:

- For 32-bit operating systems:

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

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

- For 64-bit operating systems:

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

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

2. Add the driver to the Solaris kernel:

```
add_drv sst
```

3. Remove all existing device files from the /dev/rmt directory:

```
cd /dev/rmt rm *
```

4. Stop the system by pressing **Stop** and **A**.

5. Run the probe-scsi-all command at the "ok" prompt to check which SCSI addresses are available for use.

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

The system may ask you to start the reset-all command before executing the probe-scsi-all command.

In our case, we will use port 6 for the SCSI control device, port 2 for the first drive, and port 1 for the second drive; lun is 0)

6. Return to normal running:

```
ok go
```

7. Copy the st.conf configuration file into the required directory:

```
$cp /opt/omni/spt/st.conf /kernel/drv/st.conf
```

The st.conf file is present on each Solaris Data Protector client and contains SCSI addresses for each backup device connected to the client.

8. Edit the /kernel/drv/st.conf file and add the following lines:

```
tape-config-list= "QUANTUM DLT7000", "Digital DLT7000", "DLT-data3";
```

```
DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;
```

```
name="st" class="scsi"
```

```
target=1 lun=0;
```

```
name="st" class="scsi"
```

```
target=2 lun=0;
```

```
name="st" class="scsi"
```

```
target=6 lun=0;
```

These entries provide the SCSI addresses for drive 1, drive 2, and the robotic drive, respectively.

9. Edit the `sst.conf` file (that you copied across in ["Copy the sst driver \(module\) and configuration file sst.conf to the required directory:"](#) and add the following line:

```
name="sst" class="scsi" target=6 lun=0;
```

**Note:** This entry must match that for the robotic drive in the `st.conf` file. See ["Edit the /kernel/drv/st.conf file and add the following lines:"](#) 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:

<code>/dev/rmt/0hb</code>	for a first tape drive
<code>/dev/rmt/1hb</code>	for a second tape drive
<code>/dev/rsst6</code>	for a robotic drive

### What's next?

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

### Connecting to a Windows system

Follow the steps below to connect the HP DLT 28/48-Slot library device to a Windows system:

1. Determine the unused SCSI addresses (Target IDs) that can be used by the tape drive and by the robotics. See ["Finding unused SCSI target IDs on Windows systems"](#).
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.

**Note:** The HP DLT Library 28/48-Slot has four tape drives and the robotics, so you need five unused SCSI addresses in case you will be using all tape drives. The tape drives and the robotics must use different SCSI Target IDs.

3. First, switch on the device, then the computer, and then wait until the boot process completes.
4. Verify that the system correctly recognizes the newly connected tape drives and the robotics. In the default Data Protector commands directory, execute the `devbra -dev` command.

In the output of the `devbra` command, you should find the newly connected tape drives and the robotics of the HP DLT Library 28/48-Slot library device.

### *What's next?*

After properly connecting the HP DLT Library 28/48-Slot library device, see the *HP Data Protector Help* index: “configuring, backup devices” for instructions about configuring a Data Protector backup device for your newly connected library device.

## Connecting a Seagate Viper 200 LTO Ultrium Tape Drive

The Seagate Viper 200 LTO Ultrium Tape Drive is a standalone device for enterprise environments with 100-200 GB to back up.

### *Connecting to a Solaris system*

To configure the Seagate Viper 200 LTO Ultrium Tape Drive on a Solaris system, follow the steps below:

1. Determine the unused SCSI addresses that can be used by the tape drive. Run the `modinfo` or `dmesg` command to find the SCSI controllers in use and the SCSI target devices installed:

```
dmesg | egrep "target" | sort | uniq
```

The following output should be received:

```
sd32 at ithps0: target 2 lun 0
sd34 at ithps0: target 4 lun 0
st21 at ithps1: target 0 lun 0
st22 at ithps1: target 1 lun 0
```

**Note:** It is recommended that you use either a `glm` or `isp` SCSI controller when connecting the Viper 200 LTO device to a Solaris system. It is also recommended that you use either Ultra2 SCSI or Ultra3 SCSI controllers.

2. Edit the `/kernel/drv/st.conf` file and add the following lines:

```
tape-config-list=
"SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , \
"SEAGATE_LTO";
SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
0x00, 1;
```

3. Power down the client system and attach the device.
4. Power up the device first and then the client system.

The system will now boot and automatically create device files for the tape drive. These can be listed using the command `ls -all`.

### *What's next?*

After properly connecting the Seagate Viper 200 LTO Ultrium Tape Drive, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

### *Connecting to a Windows system*

Follow the steps below to connect the Seagate Viper 200 LTO Ultrium Tape Drive to a Windows system:

1. Determine the unused SCSI addresses (Target IDs) that can be used by the tape drive. See ["Finding unused SCSI target IDs on Windows systems"](#).
2. Set the SCSI addresses (Target IDs) on the device. For details, see the documentation that comes with the device.
1. First, switch on the device, then the computer, and then wait until the boot process completes.
2. Verify that the system correctly recognizes the newly connected tape drives and the robotics. In the default Data Protector commands directory, execute the `devbra -dev` command.

In the output of the `devbra` command, you should find the newly connected tape drive of the Seagate Viper 200 LTO Ultrium Tape Drive.

### *What's next?*

After properly connecting the Seagate Viper 200 LTO Ultrium Tape Drive, see the *HP Data Protector Help* index: "configuring, backup devices" for instructions about configuring a Data Protector backup device for your newly connected device.

**Note:** When configuring the Seagate Viper 200 LTO Ultrium Tape Drive with Data Protector, make sure that the compression mode is set. This is done by specifying the `C` parameter after the SCSI address of the drive, for example:

```
scsi2:0:0:0C
```

## Appendix D: Command line changes after upgrading to Data Protector 8.10

The commands listed in this chapter have been changed or provide extended functionality in terms of new options in Data Protector 8.10. Commands and options marked with an asterisk (\*) are only introduced, changed, or made obsolete in the most recent set of patches for this Data Protector release version. Check and modify the scripts that use the old commands. For usage synopses, see the *HP Data Protector Command Line Interface Reference* or the corresponding man pages.

Depending on the version from which you upgraded your Cell Manager, see the corresponding table:

- After upgrading from Data Protector 6.20, see "[Upgrade from Data Protector 6.20](#)".
- After upgrading from Data Protector 7.00, see "[Upgrade from Data Protector 7.00](#)".
- After upgrading from Data Protector 8.00, see "[Upgrade from Data Protector 8.00](#)".

**Table 8: Upgrade from Data Protector 6.20**

Command	Affected options or arguments, notes	Status
NNMpost.ovpl		OBSOLETE COMMAND
NNMpre.ovpl		OBSOLETE COMMAND
NNMScript.exe		OBSOLETE COMMAND
ob2install	saphana	NEW SOFTWARE COMPONENT
	javagui ov	OBSOLETE SOFTWARE COMPONENTS

Command	Affected options or arguments, notes	Status
omnib	-storedrim -idb_list -priority	NEW OPTIONS
	-copy	UPDATED OPTION  This option can be specified also for backup using the Microsoft SQL Server integration.
	-barmode	UPDATED OPTION  The value <code>incr</code> can be specified also for backup of Microsoft Hyper-V virtual machines using the Virtual Environment integration.
	-netware -omnidb	OBSOLETE OPTIONS
omnib2dinfo	This command is available on systems with the Media Agent component installed.	NEW COMMAND
omnicc	-import_vcd	NEW OPTION
omnidb	-idb -saphana	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS



Command	Affected options or arguments, notes	Status
omnidbcheck	-connection -database_consistency -media_consistency -schema_consistency -verify_db_files	NEW OPTIONS
	-dc -extended -quick	UPDATED OPTIONS
	-core -filenames	OBSOLETE OPTIONS
omnidbrestore		OBSOLETE COMMAND
omnidbupgrade		OBSOLETE COMMAND

Command	Affected options or arguments, notes	Status
omnidbutil	-all -autovacuum -cp -disabled -enabled -freeze_max_age -on_n_rows -on_percentage -param -set -set_passwd -sync_srv -table -to_default	NEW OPTIONS
	-info -readdb -show_db_files -writedb	UPDATED OPTIONS

Command	Affected options or arguments, notes	Status
	<ul style="list-style-type: none"> <li>-cdb</li> <li>-check_overs</li> <li>-chktblspace</li> <li>-extendfnames</li> <li>-extendinfo</li> <li>-extendtblspace</li> <li>-filenames</li> <li>-force</li> <li>-list_large_directories</li> <li>-list_mpos_without_overs</li> <li>-maxsize</li> <li>-mmdb</li> <li>-modifytblspace</li> <li>-no_detail</li> <li>-purge_stop</li> <li>-top</li> <li>-upgrade_info</li> </ul>	OBSOLETE OPTIONS
omnidbxb	<ul style="list-style-type: none"> <li>-user -add -username -password</li> <li>-user -check -host</li> <li>-user -update -username -password</li> <li>-user -list</li> <li>-user -remove</li> </ul>	NEW OPTIONS AND OPTION COMBINATIONS
omnidbzdb	This command is available on Windows, HP-UX (Itanium), and Linux systems with the Data Protector User Interface component installed.	NEW COMMAND

Command	Affected options or arguments, notes	Status
omnidownload	-dev_info -list_devices -list_libraries -detail	UPDATED OPTIONS AND OPTION COMBINATIONS  Updated options and option combinations for Backup to Disk devices.
omnidr	-omit_deleted_files	NEW OPTION
omniinstlic		OBSOLETE COMMAND
omniiso	-out -net -use_raw_object -host -remotehost -move_to -unique_name -exec_script -password -anyobj	NEW OPTIONS
	-session	CHANGED OPTION
	-iso	OBSOLETE OPTION  Replaced by -out. Can be used for backward compatibility.

Command	Affected options or arguments, notes	Status
omnimm	-delete_unprotected_media	NEW OPTION  New option for Backup to Disk devices.
	-all -recycle -remove_slots	UPDATED OPTIONS  Updated options for Backup to Disk devices.
omniobjconsolidate	-priority	NEW OPTION
omniobjcopy	-replication -replist -idb -saphana -priority	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS
omniobjverify	-idb -saphana -priority	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS

Command	Affected options or arguments, notes	Status
omniofflr	The command was moved from the User Interface component to the Core installation component, thus becoming available on systems with any Data Protector component installed.	RELOCATED COMMAND
	-rawdisk -section -idb -autorecover -changedevhost -read -force -session -save -skiprestore -logview -opview	NEW OPTIONS
	-omnidb	OBSOLETE OPTION

Command	Affected options or arguments, notes	Status
omnir	-idb -priority	NEW OPTIONS
	-tail_log	NEW OPTION  New option for Microsoft SQL Server restore.
	-host/cluster -resourcePool -specificHost -fromSession -untilSession	NEW OPTIONS  New options for VMware vSphere using the Virtual Environment integration.
	-neworganization -virtual_datacenter_path -virtual_datacenter_uuid -vapp_path -vapp_uuid -vcenter_path -vcenter_uuid -network_name -network_uuid	NEW OPTIONS  New options for VMware vCloud Director using the Virtual Environment integration.

Command	Affected options or arguments, notes	Status
	-restoredb -restoreconf -restoredcbf -pre -post -targetdir -port -nodbrecover -nouseasnewidb -keeprecent -nooverwrite	<b>NEW OPTIONS</b>  New options for Data Protector Internal Database restore.
	-targetstoragepath	<b>NEW OPTION</b>  New option for Microsoft Hyper-V using the Virtual Environment integration.
	-deleteafter -keep_for_forensics -new_name	<b>NEW OPTIONS</b>  New options for VMware vSphere using the Virtual Environment integration.
	-deletebefore -skip	<b>UPDATED OPTIONS</b>  These options can be specified also for Microsoft Hyper-V restore using the Virtual Environment integration.



Command	Affected options or arguments, notes	Status
omnirpt	-copyback -check_config -no_check_config -force_prp_replica	UPDATED OPTIONS  Added support for instant recovery on HP 3PAR StoreServ Storage.
	-virtual-environment -method	UPDATED OPTIONS  These options can be specified also for VMware vCloud Director using the Virtual Environment integration.
	-network_name	UPDATED OPTION  This option can be specified also for VMware vSphere using the Virtual Environment integration.
	-omnidb -netware -trustee -vsr_only	OBSOLETE OPTIONS
	-db_purge -db_purge_preview -db_system	OBSOLETE OPTIONS

Command	Affected options or arguments, notes	Status
omnisetup.sh	saphana	NEW SOFTWARE COMPONENT
	javagui ov	OBSOLETE SOFTWARE COMPONENT
	-bundleadd -bundlerem	NEW OPTIONS
omnisrdupdate	-use_raw_object	NEW OPTION
	-session	CHANGED OPTION
	-anyobj	NEW OPTION
omni	-anyobj	NEW OPTION
omnisv	-maintenance -mom -mom_stop	NEW OPTIONS

Command	Affected options or arguments, notes	Status
vepa_util.exe	--list-organizations	NEW OPTION  New option for VMware vCloud Director using the Virtual Environment integration.
	--check-config --config --configvm --virtual-environment	UPDATED OPTIONS  These options can be specified also for VMware vCloud Director using the Virtual Environment integration.
	--show-incremental-flag --enable-incremental --disable-incremental --list-vms	NEW OPTIONS  New options for Microsoft Hyper-V using the Virtual Environment integration.
winomnimigrate.pl		OBSOLETE COMMAND

**Table 9: Upgrade from Data Protector 7.00**

Command	Affected options or arguments, notes	Status
NNMpost.ovpl		OBSOLETE COMMAND
NNMpre.ovpl		OBSOLETE COMMAND
NNMScript.exe		OBSOLETE COMMAND
ob2install	saphana	NEW SOFTWARE COMPONENT
	javagui ov	OBSOLETE SOFTWARE COMPONENT

Command	Affected options or arguments, notes	Status
omnib	-storedrim -idb_list -priority	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS
omnidb	-idb -saphana	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS
omnidbcheck	-connection -database_consistency -media_consistency -schema_consistency -verify_db_files	NEW OPTIONS
	-dc -extended -quick	UPDATED OPTIONS
	-core -filenames	OBSOLETE OPTIONS
omnidbrestore		OBSOLETE COMMAND
omnidbupgrade		OBSOLETE COMMAND

Command	Affected options or arguments, notes	Status
omnidbutil	-all -autovacuum -cp -disabled -enabled -freeze_max_age -on_n_rows -on_percentage -param -set -set_passwd -sync_srv -table -to_default	NEW OPTIONS
	-info -readdb -show_db_files -writedb	UPDATED OPTIONS

Command	Affected options or arguments, notes	Status
	<ul style="list-style-type: none"><li>-cdb</li><li>-check_overs</li><li>-chktblspace</li><li>-extendfnames</li><li>-extendinfo</li><li>-extendtblspace</li><li>-filenames</li><li>-force</li><li>-list_large_directories</li><li>-list_mpos_without_overs</li><li>-maxsize</li><li>-mmdb</li><li>-modifytblspace</li><li>-no_detail</li><li>-purge_stop</li><li>-top</li><li>-upgrade_info</li></ul>	OBSOLETE OPTIONS

Command	Affected options or arguments, notes	Status
omnidbzdb	--list --session --ir --excluded --original --datalist --show --purge --force --host --delete --reference --preview --force --sync_check	NEW OPTIONS
	--diskarray	CHANGED OPTION This option also accepts the new keyword 3PAR, related to the Data Protector HP P6000 / HP 3PAR SMI-S Agent.
omnidr	-omit_deleted_files	NEW OPTION
omniiso	--host --remotehost --move_to --unique_name --exec_script --password --anyobj	NEW OPTIONS
	--session	CHANGED OPTION

Command	Affected options or arguments, notes	Status
omniobjconsolidate	-priority	NEW OPTION
omniobjcopy	-idb -saphana -priority	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTIONS
omniobjverify	-idb -saphana -priority	NEW OPTIONS
	-netware -omnidb	OBSOLETE OPTION
omniofflr	The command was moved from the User Interface component to the Core installation component, thus becoming available on systems with any Data Protector component installed.	RELOCATED COMMAND
	-idb -autorecover -changedevhost -read -force -session -save -skiprestore -logview -opview	NEW OPTIONS
	-omnidb	OBSOLETE OPTION



Command	Affected options or arguments, notes	Status
omnir	-idb -priority	NEW OPTIONS
	-restoredb -restoreconf -restoredcbf -pre -post -targetdir -port -nodbrecover -nouseasnewidb -keeprecent -nooverwrite	NEW OPTIONS  New options for Data Protector Internal Database restore.
	-omnidb -netware -trustee -vsr_only	OBSOLETE OPTIONS
	-copyback -check_config -no_check_config -force_prp_replica	UPDATED OPTIONS  Added support for instant recovery on 3PAR StoreServ Storage.
omnirpt	-db_purge -db_purge_preview -db_system	OBSOLETE OPTIONS
omnisetup.sh	saphana	NEW SOFTWARE COMPONENT
	javagui ov	OBSOLETE SOFTWARE COMPONENT

Command	Affected options or arguments, notes	Status
omnisrdupdate	-session	CHANGED OPTION
	-anyobj	NEW OPTION
omnisv	-maintenance -mom -mom_stop	NEW OPTIONS
winomnimigrate.pl		OBSOLETE COMMAND

**Table 10: Upgrade from Data Protector 8.00**

Command	Affected options or arguments, notes	Status
omnidbzdb	--list -session --ir --excluded --original --datalist -show --purge --force --host --delete --reference --preview --force --sync_check	NEW OPTIONS
omnidr	-omit_deleted_files	NEW OPTION
omniiso	-anyobj	NEW OPTION

Command	Affected options or arguments, notes	Status
omnir	-copyback -check_config -no_check_config -force_prp_replica	UPDATED OPTIONS  Added support for instant recovery on HP3PAR StoreServ Storage.
omnisrdupdate	-anyobj	NEW OPTION



# Glossary

## A

### **access rights**

See user rights.

### **ACSLS (StorageTek specific term)**

The Automated Cartridge System Library Server (ACSLS) software that manages the Automated Cartridge System (ACS).

### **Active Directory (Windows specific term)**

The directory service in a Windows network. It contains information about resources on the network and makes them accessible to users and applications. The directory services provide a consistent way to name, describe, locate, access, and manage resources regardless of the physical system they reside on.

### **AES 256-bit encryption**

The Data Protector software encryption, based on the AES-CTR (Advanced Encryption Standard in Counter Mode) encryption algorithm that uses random keys of 256-bit length. The same key is used for both encryption and decryption. With AES 256-bit encryption, data is encrypted before it is transferred over a network and before it is written to media.

### **AML (ADIC/GRAU specific term)**

Automated Mixed-Media library.

### **AMU (ADIC/GRAU specific term)**

Archive Management Unit.

### **application agent**

A component needed on a client system to back up or restore online database integrations. See also Disk Agent.

### **application system (ZDB specific term)**

A system the application or database runs on. The application or database data is located on source volumes. See also backup system and source volume.

### **archive logging (Lotus Domino Server specific term)**

Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.

### **archived log files (Data Protector specific term)**

Files that keep track of changes made to the Data Protector Internal Database (IDB). They are used for online or offline IDB restore and recovery where the IDB needs to be recreated either in its latest possible state, beyond the time of the most recent IDB backup session, or in a state between the times of two consecutive IDB backup sessions.

### **archived redo log (Oracle specific term)**

Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to an archived log destination. This copy is the archived redo log. The presence or absence of an archived redo log is determined by the mode the database is using: ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A "hot" backup can be performed only when the database is running in this mode. NOARCHIVELOG - The filled online redo log files are not archived. See also online redo log.

### **ASR set**

A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of

the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory <Data\_Protector\_program\_data>\Config\Server\dr\asr (Windows systems) or /etc/opt/omni/server/dr/asr (UNIX systems), as well as on the backup medium. After a disaster occurs, the ASR archive file is extracted to diskettes which you need to perform ASR.

### **audit logs**

Data files to which auditing information is stored.

### **audit report**

User-readable output of auditing information created from data stored in audit log files.

### **auditing information**

Data about every backup session that was performed over an extended, user-defined period for the whole Data Protector cell.

### **autochanger**

See library.

### **autoloader**

See library.

### **Automatic Storage Management (ASM) (Oracle specific term)**

A filesystem and volume manager integrated into Oracle which manages Oracle database files. It eliminates complexity associated with data and disk management and optimizes performance by providing striping and mirroring capabilities.

### **auxiliary disk**

A bootable disk that has a minimal operating system with networking and

Data Protector Disk Agent installed. It can be carried around and used to boot the target system in Phase 1 of Disk Delivery Disaster Recovery of UNIX clients.

## **B**

### **BACKINT (SAP R/3 specific term)**

A Data Protector interface program that lets the SAP R/3 backup programs communicate with the Data Protector software via calls to an open interface. For backup and restore, SAP R/3 programs issue commands through the Data Protector backint interface.

### **backup API (Oracle specific term)**

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 reading and writing of data to media and also to allow creation, searching, and removing of backup files.

### **backup chain**

See restore chain.

### **backup device**

A device configured for use with Data Protector that can write data to and read data from storage media. This can be, for example, a standalone DDS/DAT drive or a library.

### **backup generation**

One backup generation includes one full backup and all incremental backups until the next full backup.

### **backup ID**

An identifier of an integration object that equals the session ID of the backup of this object. The backup ID is preserved when an object is copied, exported, or imported.

### **backup object**

A backup unit that contains all items backed up from one disk volume (logical disk or mount point). The backed up items can be any number of files, directories, or the entire disk or mount point. Additionally, a backup object can be a database/application entity or a disk image (rawdisk). A backup object is defined by: client name (hostname of the Data Protector client where the backup object resides), mount point (for filesystem objects - the access point in a directory structure on the client where the backup object is located (drive on Windows systems and mount point on UNIX systems), for integration objects - backup stream identification, indicating the backed up database/application items), description (for filesystem objects - uniquely defines objects with identical client name and mount point, for integration objects - displays the integration type), and type (for filesystem objects - filesystem type, for integration objects - "Bar").

### **backup owner**

Each backup object in the IDB has an owner. The default owner of a backup is the user who starts the backup session.

### **backup session**

A process that creates a copy of data on storage media. The activities are specified in a backup specification or an interactive session. The result of a backup session is a set of media, which was written to, also called the backup or media set. See also backup specification, incremental backup, and full backup.

### **backup set**

A complete set of integration objects associated with a backup.

### **backup set (Oracle specific term)**

A logical grouping of backed up files that are created using the RMAN backup command. A backup set is a complete set of files associated with a backup. The files can be multiplexed to increase performance. A backup set contains either datafiles or archived logs, but not both together.

### **backup specification**

A list of objects to be backed up, together with a set of devices or drives to be used; backup options for all objects in the specification; and days and time that you want backups to be performed. The objects are entire disks/volumes or parts of them such as files, directories, or even the Windows Registry (for example). File selection lists, such as include-lists and exclude-lists, can be specified. All clients configured in one backup specification are backed up at the same time in one backup session using the same backup type (full or incremental).

### **backup system (ZDB specific term)**

A system connected to target volumes of one or multiple application systems. The backup system is typically connected to a backup device to perform the backup of the data in a replica. See also application system, target volume, and replica.

### **backup types**

See incremental backup, differential backup, transaction backup, full backup, and delta backup.

### **backup view**

Data Protector provides different views of your 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 Continuances are processes that allow customers to access and manage instant copies of EMC Symmetrix standard devices.

**BC Process (EMC Symmetrix specific term)**

A protected storage environment solution, which uses specially configured EMC Symmetrix devices as mirrors or Business Continuation Volumes to protect data on EMC Symmetrix standard devices. See also BCV.

**BCV (EMC Symmetrix specific term)**

Business Continuation Volumes, or BCV devices, are dedicated SLDs that are pre-configured in the ICDA on which the business continuation operation runs. BCV devices are assigned separate SCSI addresses, differing from the addresses used by the SLDs they mirror. The BCV devices are used as splittable mirrors of the primary EMC Symmetrix SLDs that need to be protected. See also BC and BC Process.

**Boolean operators**

The Boolean operators for the full text search functionality of the Data Protector Help system are AND, OR, NOT, and NEAR. Used when searching, they enable you to define your query precisely by creating a relationship between search terms. If no operator is specified in a multi-word search, AND is used by default. For example, the query manual disaster recovery is equivalent to manual AND disaster AND recovery.

**boot volume/disk/partition**

A volume/disk/partition containing files required for the initial step of the boot process. Microsoft terminology defines the boot volume/disk/partition as a volume/disk/partition containing the operating system files.

**BRARCHIVE (SAP R/3 specific term)**

An SAP R/3 backup tool that allows you to archive redo log files. BRARCHIVE also saves all the logs and profiles of the archiving process. See also BRBACKUP and BRRESTORE.

**BRBACKUP (SAP R/3 specific term)**

An SAP R/3 backup tool that allows an online or offline backup of the control file, of individual data files, or of all tablespaces and, if necessary, of the online redo log files. See also BRARCHIVE and BRRESTORE.

**BRRESTORE (SAP R/3 specific term)**

An SAP R/3 tool that can be used to restore files of the following type: Database data files, control files, and online redo log files saved with BRBACKUP; Redo log files archived with BRARCHIVE; Non-database files saved with BRBACKUP. You can specify files, tablespaces, complete backups, log sequence numbers of redo log files, or the session ID of the backup. See also BRARCHIVE and BRBACKUP.

**BSM**

The Data Protector Backup Session Manager, which controls the backup session. This process always runs on the Cell Manager system.



**C****CAP (StorageTek specific term)**

The Cartridge Access Port built into the door panel of a library. The purpose is to enter or eject media.

**Catalog Database (CDB)**

A part of the Data Protector Internal Database (IDB) that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. This part of the IDB is always local to the cell. It is stored in the embedded database. See also MMDB.

**catalog protection**

Defines how long information about backed up data (such as filenames and file attributes) is kept in the IDB. See also data protection.

**CDB**

See Catalog Database (CDB).

**CDF file (UNIX systems 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 allocate licenses to specific cells to suit your needs. See also MoM.

**Centralized Media Management Database (CMMDB)**

See CMMDB.

**Certificate Server**

A Windows certificate server can be installed and configured to provide certificates for clients. It provides customizable services for issuing and managing certificates for the enterprise. These services issue, revoke, and manage certificates employed in public key-based cryptography technologies.

**Change Journal (Windows specific term)**

A Windows filesystem feature that logs a record of each change as it occurs to the files and directories on a local NTFS volume.

**Change Log Provider**

A module that can be queried to determine which objects on a filesystem have been created, modified, or deleted.

**channel (Oracle specific term)**

An Oracle Recovery Manager resource allocation. Every allocated channel starts a new Oracle process, which performs backup, restore, and recovery actions. The type of channel allocated determines the type of media used: type 'disk' or type 'sbt\_tape'. If the specified channel is of type 'sbt\_tape' and Oracle is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

**circular logging (Microsoft Exchange Server and Lotus Domino Server specific term)**

Circular logging is a Microsoft Exchange Server database and Lotus Domino Server database mode, in which the transaction log file contents are periodically overwritten after the corresponding data is committed to the database. Circular logging reduces disk storage space requirements.

**client backup**

A backup of all volumes (filesystems) mounted on a Data Protector client. What is actually backed up depends on how you select objects in a backup specification. If you select the check box next to the client system name, a single backup object of the Client System type is created. As a result, at the time of the backup, Data Protector first detects all volumes that are mounted on the selected client and then backs them up. On Windows clients, CONFIGURATION is also backed up. If you individually select all volumes that are mounted on the client system, a separate backup object of the Filesystem type is created for each volume. As a result, at the time of the backup, only the selected volumes are backed up. Volumes that have been potentially mounted on the client after the

backup specification was created are not backed up.

**client or client system**

Any system configured with any Data Protector functionality and configured in a cell.

**cluster continuous replication (Microsoft Exchange Server specific term)**

Cluster continuous replication (CCR) is a high availability solution that uses cluster management and failover options to create and maintain an exact copy (CCR copy) of a storage group. A storage group is replicated to a separate server. CCR removes any single point of failure in your Exchange back-end servers. You can perform backups using VSS on your passive Exchange Server node where a CCR copy is located and thus reducing the load on the active node. A CCR copy is used for disaster recovery since you can switch to the CCR copy in a few seconds. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) like an ordinary storage group. See also Exchange Replication Service and local continuous replication.

**cluster-aware application**

It is an application that supports the cluster Application Programming Interface. Each cluster-aware application declares its own critical resources (disk volumes (on Microsoft Cluster Server), volume groups (on HP Serviceguard), application services, IP names and addresses ...).

**CMD script for Informix Server (Informix Server specific term)**

A Windows CMD script that is created in INFORMIXDIR when an Informix Server database is configured. The CMD script

is a set of system commands that export environment variables for Informix Server.

### **CMMDB**

The Data Protector Centralized Media Management Database (CMMDB) is the result of merging MMDBs from several cells in the MoM environment. It allows you to share high-end devices and media across multiple cells in a MoM environment. One cell can control the robotics, serving the devices that are connected to systems in other cells. The CMMDB must reside on the Manager-of-Managers. A reliable network connection between the MoM cell and the other Data Protector cells is highly recommended. See also MoM.

### **COM+ Class Registration Database (Windows specific term)**

The COM+ Class Registration Database and the Windows Registry store COM+ application attributes, class attributes, and computer-level attributes. This guaranties consistency among these attributes and provides common operation on top of these attributes.

### **command device (HP P9000 XP Disk Array Family specific term)**

A dedicated volume in the disk array which acts as the interface between a management application and the disk array's storage system. It cannot be used for data storage and only accepts requests for operations that are then executed by the disk array.

### **command-line interface (CLI)**

A set commands that you can use in shell scripts to perform Data Protector configuration, backup, restore, and management tasks.

### **concurrency**

See Disk Agent concurrency.

### **container (HP P6000 EVA Disk Array Family specific term)**

Space on a disk array, which is pre-allocated for later use as a standard snapshot, vsnap, or snapclone.

### **control file (Oracle and SAP R/3 specific term)**

A data file that contains entries specifying the physical structure of the database. It provides database consistency information used for recovery.

### **copy set (HP P6000 EVA Disk Array Family specific term)**

A pair that consists of the source volumes on a local P6000 EVA and their replica on a remote P6000 EVA. See also source volume, replica, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

### **CRS**

The Data Protector Cell Request Server process (service), which runs on the Cell Manager, starts and controls the backup and restore sessions. The service is started as soon as Data Protector is installed on the Cell Manager. The CRS runs under the account root on UNIX systems. On Windows systems it runs under the account of the user, specified at installation time.

### **CSM**

The Data Protector Copy and Consolidation Session Manager process controls the object copy and object consolidation sessions and runs on the Cell Manager system.

**D****data file (Oracle and SAP R/3 specific term)**

A physical file created by Oracle that contains data structures such as tables and indexes. A data file can only belong to one Oracle database.

**data protection**

Defines how long the backed up data on media remains protected, that is, Data Protector will not overwrite it. When the protection expires, Data Protector will be able to reuse the media in one of the next backup sessions. See also catalog protection.

**Data 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 replication (DR) group (HP P6000 EVA Disk Array Family specific term)**

A logical grouping of HP P6000 EVA Disk Array Family virtual disks. It can contain up to eight copy sets provided they have common characteristics and share a common HP CA P6000 EVA log. See also copy set.

**data stream**

Sequence of data transferred over the communication channel.

**Data\_Protector\_home**

A reference to the directory containing Data Protector program files (on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2012) or the directory containing Data Protector program files and data files (on other Windows operating systems). Its default path is %ProgramFiles%\OmniBack, but the path can be changed in the Data Protector Setup Wizard at installation time. See also Data\_Protector\_program\_data.

**Data\_Protector\_program\_data**

A reference to the directory containing Data Protector data files on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2012. Its default path is %ProgramData%\OmniBack, but the path can be changed in the Data Protector Setup Wizard at installation time. See also Data\_Protector\_home.

**database library**

A Data Protector set of routines that enables data transfer between Data Protector and a server of an online database integration, for example, Oracle Server.

**database parallelism**

More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.

**database server**

A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.

**Dbobject (Informix Server specific term)**

An Informix Server physical database object. It can be a blob space, db space, or logical log file.

### **DC directory**

A directory that contains DC binary files, one for each configured Data Protector backup medium. DC directories constitute the Detail Catalog Binary Files part of the Data Protector Internal Database. See also Detail Catalog Binary Files (DCBF) and Internal Database (IDB).

### **DCBF**

See Detail Catalog Binary Files (DCBF).

### **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.

### **Detail Catalog Binary Files (DCBF)**

A part of the Data Protector Internal Database that stores names, versions, and metadata of the backed up items. It consists of DC directories with DC binary files. See also DC directory and Internal Database (IDB).

### **device**

See backup device.

### **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. -Get configuration, status, and performance statistics by device group. -Issue control operations that apply to all devices in the device group.

### **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 writing to the tape, and so on. If data is written to the tape slower than it is delivered to the device then the device is streaming. Streaming significantly improves the use of space and the performance of the device.

### **DHCP server**

A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic IP address assignment and network configuration for DHCP clients.

### **differential backup**

An incremental backup that backs up changes made since the last full backup. To perform this type of backup, specify the Incr1 backup type. See also incremental backup.

### **differential backup (Microsoft SQL Server specific term)**

A database backup that records only the data changes made to the database after the last full database backup. See also backup types.

### **differential database backup**

A differential database backup records only those data changes made to the database after the last full database backup.

**directory junction (Windows specific term)**

Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.

**disaster recovery**

A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.

**disaster recovery operating system**

See DR OS.

**Disk Agent**

A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.

**Disk Agent concurrency**

The number of Disk Agents that are allowed to send data to one Media Agent concurrently.

**disk group (Veritas Volume Manager specific term)**

The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.

**disk image (rawdisk) backup**

A high-speed backup where Data Protector backs up files as bitmap images. A disk image (rawdisk) backup does not track the files and directory

structure stored on the disk, but stores a disk image structure on byte level. You can perform a disk image backup of either specific disk sections or a complete disk.

**disk quota**

A concept to manage disk space consumption for all or a subset of users on a computer system. This concept is used by several operating system platforms.

**disk staging**

The process of backing up data in several phases to improve the performance of backups and restores, reduce costs of storing the backed up data, and increase the data availability and accessibility for restore. The backup stages consist of backing up data to one media type first (for example disk) and later copying it to a different media type (for example tape).

**distributed file media format**

A media format, available with the file library, which supports a space efficient type of synthetic backup called virtual full backup. Using this format is a prerequisite for virtual full backup. See also virtual full backup.

**Distributed File System (DFS)**

A service that connects file shares into a single namespace. The file shares can reside on the same or on different computers. DFS provides client access to the resources in a location-transparent manner.

**DMZ**

The Demilitarized Zone (DMZ) is a network inserted as a "neutral zone" between a company's private network (intranet) and the outside public network (Internet). It prevents outside users from getting direct access to company servers in the intranet.

### **DNS server**

In the DNS client-server model, this is the server containing information about a portion of the DNS database that makes computer names available to client resolvers querying for name resolution across the Internet.

### **DR image**

Data required for temporary disaster recovery operating system (DR OS) installation and configuration.

### **DR OS**

An operating system environment in which disaster recovery runs. It provides Data Protector with a basic runtime environment (disk, network, tape, and filesystem access). It has to be installed on disk or loaded into memory and configured before the Data Protector disaster recovery can be performed. DR OS can be either temporary or active. A temporary DR OS is used exclusively as a host environment for some other operating system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. An active DR OS not only hosts the Data Protector disaster recovery process but can also be a part of the restored system because it replaces its own configuration data with the original configuration data.

### **drive**

A physical unit that receives data from a computer system and can write it onto a magnetic medium. It can also read the data from the medium and send it to the computer system.

### **drive index**

A number that identifies the mechanical position of a drive inside a library device.

This number is used by the robotic control to access a drive.

### **drive-based encryption**

The Data Protector drive-based encryption uses the encryption functionality of the drive. While performing the backup, the drive encrypts both the data and the metadata that is written to the medium.

## **E**

### **EMC Symmetrix Agent**

A Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

### **emergency boot file (Informix Server specific term)**

The Informix Server configuration file `ixbar.<server_id>` that resides in the directory `<INFORMIXDIR>/etc` (on Windows systems) or `<INFORMIXDIR>/etc` (on UNIX systems). `<INFORMIXDIR>` is the Informix Server home directory and `<server_id>` is the value of the `SERVERNUM` configuration parameter. Each line of the emergency boot file corresponds to one backup object.

### **encrypted control communication**

Data Protector secure communication between the clients in the Data Protector cell is based on a Secure Socket Layer (SSL) that uses export grade SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.

### **encryption key**

A 256-bit randomly generated number used by the Data Protector encryption algorithm to encode information during backups for which AES 256-bit software encryption or drive-based encryption has been specified. The same key is used for subsequent decryption of the information. Encryption keys for a Data Protector cell are stored in a central keystore on the Cell Manager.

### **encryption KeyID-StoreID**

Combined identifier used by the Data Protector Key Management Server to identify and administer encryption keys used by Data Protector. KeyID identifies the key within the keystore. StoreID identifies the keystore on the Cell Manager. If Data Protector has been upgraded from an earlier version with encryption functionality, there may be several StoreIDs used on the same Cell Manager.

### **enhanced incremental backup**

Conventional incremental backup backs up files that have changed since a previous backup, but has certain limitations in detection of changes. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up also renamed and moved files, as well as files with changes in attributes.

### **enterprise backup environment**

Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes all clients located in several Data Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept. See also MoM.

### **Event Log (Data Protector Event Log)**

A central repository of all Data Protector related notifications. By default, all notifications are sent to the Event Log. The Event Log is accessible only to Data Protector users in the Admin group and to Data Protector users who are granted the Reporting and notifications user rights. You can view or delete all events in the Event Log.

### **Event Logs (Windows specific term)**

Files in which Windows logs all events, such as the starting or stopping of services and the logging on and off of users. Data Protector can back up Windows Event Logs as part of the Windows configuration backup.

### **Exchange Replication Service (Microsoft Exchange Server specific term)**

The Microsoft Exchange Server service that represents storage groups that were replicated using either local continuous replication (LCR) or cluster continuous replication (CCR) technology. See also cluster continuous replication and local continuous replication.

### **exchanger**

See library.

### **exporting media**

A process that removes all data about backup sessions, such as systems, objects, and filenames, which reside on the media from the IDB. Information about the media and their relation to a pool is also removed from the IDB. The data on the media remains unchanged. See also importing media.



**Extensible Storage Engine (ESE)  
(Microsoft Exchange Server specific term)**

A database technology used as a storage system for information exchange in Microsoft Exchange Server.

**F****failover**

Transferring of the most important cluster data, called group (on Windows systems) or package (on UNIX systems) from one cluster node to another. A failover can occur mostly because of software or hardware failures or maintenance on the primary node.

**failover (HP P6000 EVA Disk Array Family specific term)**

An operation that reverses the roles of source and destination in HP Continuous Access + Business Copy (CA+BC) P6000 EVA configurations. See also HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

**FC bridge**

See Fibre Channel bridge.

**Fibre Channel**

An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

**Fibre Channel bridge**

A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries

to a Fibre Channel environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.

**file depot**

A file containing the data from a backup to a file library device.

**file jukebox device**

A device residing on disk consisting of multiple slots used to store file media.

**file library device**

A device which resides on a disk emulating a library with several media, hence containing multiple files, referred to as file depots.

**File Replication Service (FRS)**

A Windows service that replicates the domain controller store logon scripts and group policies. FRS also enables replication of Distributed File System (DFS) shares between systems and allows any server to perform replication activity.

**file tree walk**

The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

**file version**

The same file can be backed up multiple times in case of full backups and incremental backups (if the file changed). If the log level ALL is selected for backup, Data Protector retains one entry in the IDB for the filename itself and one for each version (date/time) of the file.

### **filesystem**

The organization of files on a hard disk. A filesystem is backed up so that the file attributes and the file contents are stored on the backup media.

### **first-level mirror (HP P9000 XP Disk Array Family specific term)**

A mirror of an internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which can be further mirrored itself, producing second-level mirrors. For Data Protector zero downtime backup and instant recovery purposes, only first-level mirrors can be used. See also primary volume and mirror unit (MU) number.

### **flash recovery area (Oracle specific term)**

A directory, filesystem, or Automatic Storage Management (ASM) disk group managed by Oracle that serves as a centralized storage area for files related to backup, restore, and database recovery (recovery files). See also recovery files.

### **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). Use the Force operation option to reformat Data Protector media with non-protected data. Data Protector media with protected data are not formatted until the protection expires or the media are unprotected/recycled.

### **free pool**

An auxiliary source of media for use by media pools when they run out of media. The media pools must be configured to use free pools.

### **full backup**

A backup in which all selected objects are backed up, whether or not they have been recently modified. See also backup types.

### **full database backup**

A backup of all data in a database, not only the data that has been changed after the last (full or incremental) backup of the database. A full database backup does not depend on any other backup.

### **full mailbox backup**

A full mailbox backup is a backup of the entire mailbox content.

### **full ZDB**

A ZDB-to-tape or ZDB-to-disk+tape session in which all selected objects are streamed to tape, even if there are no changes from the previous backup. See also incremental ZDB.

## **G**

### **global options**

A set of options that define behavior of the entire Data Protector cell. The options are stored in a plain text file on the Cell Manager.

### **group (Microsoft Cluster Server specific term)**

A collection of resources (for example disk volumes, application services, IP names and addresses) that are needed to run a specific cluster-aware applications.

### **GUI**

A graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. It is available for Microsoft Windows operating systems.

**H****hard recovery (Microsoft Exchange Server specific term)**

A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.

**heartbeat**

A cluster data set with a time stamp carrying information about the operational status of a particular cluster node. This data set or packet is distributed among all cluster nodes.

**Hierarchical Storage Management (HSM)**

A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to less expensive optical platters. When needed, the data is migrated back to hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.

**Holidays file**

A file that contains information about holidays. You can set different holidays by editing the Holidays file that resides on the Cell Manager at the following location: <Data\_Protector\_program\_data>\Config\Server\holidays (Windows systems) and /etc/opt/omni/server/Holidays (UNIX systems).

**hosting system**

A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.

**HP Business Copy (BC) P6000 EVA (HP P6000 EVA Disk Array Family specific term)**

A local replication software solution that enables creation of point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the P6000 EVA firmware. See also replica, source volume, snapshot, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

**HP Business Copy (BC) P9000 XP (HP P9000 XP Disk Array Family specific term)**

An HP P4000 SAN Solutions configuration that enables creation and maintenance of internal copies of LDEVs for various purposes, such as data duplication and backup. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system. For Data Protector zero downtime backup purposes, P-VOLs should be available to the application system, and one of the S-VOL sets should be available to the backup system. See also LDEV, HP Continuous Access (CA) P9000 XP, Main Control Unit (MCU), application system, and backup system.

**HP Command View (CV) EVA (HP P6000 EVA Disk Array Family specific term)**

The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, or mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed

by a Web browser. See also HP P6000 / HP 3PAR SMI-S Agent and HP SMI-S P6000 EVA Array provider.

**HP Continuous Access (CA) P9000 XP (HP P9000 XP Disk Array Family specific term)**

An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of remote copies of LDEVs for purposes such as data duplication, backup, and disaster recovery. HP CA P9000 XP operations involve main (primary) disk array units and remote (secondary) disk array units. The main disk array units are connected to the application system and contain primary volumes (P-VOLs), which store original data. The remote disk array units are connected to the backup system and contain secondary volumes (S-VOLs). See also HP BC P9000 XP (HP P9000 XP Disk Array Family specific term), Main Control Unit (MCU), and LDEV.

**HP Continuous Access + Business Copy (CA+BC) P6000 EVA (HP P6000 EVA Disk Array Family specific term)**

An HP P6000 EVA Disk Array Family configuration that enables creation and maintenance of copies (replicas) of the source volumes on a remote P6000 EVA, and later use of these copies as the source for local replication on this remote array. See also HP BC P6000 EVA, replica, and source volume.

**HP P6000 / HP 3PAR SMI-S Agent**

A Data Protector software module that executes all tasks required for the HP P6000 EVA Disk Array Family integration. With the P6000 / 3PAR SMI-S Agent, the control over the array is established through an appropriate SMI-S provider, which directs communication between incoming requests and the storage system's native interface. See

also HP Command View (CV) EVA and HP SMI-S P6000 EVA Array provider.

**HP P9000 XP Agent**

A Data Protector software component that executes all tasks needed by the Data Protector HP P9000 XP Disk Array Family integration. It communicates with the P9000 XP Array storage system via the RAID Manager Library.

**HP SMI-S P6000 EVA Array provider**

An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the HP P6000 / HP 3PAR SMI-S Agent, communicates with HP Command View EVA for information or method invocation, and returns standardized responses. See also HP P6000 / HP 3PAR SMI-S Agent and HP Command View (CV) EVA.

**ICDA (EMC Symmetrix specific term)**

EMC's Symmetrix Integrated Cached Disk Arrays (ICDA) is a disk array device that combines a set of physical disks, a number of FWD SCSI channels, an internal cache memory, and control and diagnostic software commonly referred to as the microcode.

**IDB**

See Internal Database (IDB).

**IDB recovery file**

A file that maintains information about completed IDB backup sessions and the

backup media and backup devices used in them. If available, it significantly simplifies and speeds up offline recovery of the Internal Database in case of a Cell Manager disaster. Its filename is obdrindex.dat.

### **importing media**

A process that re-reads all data about backup sessions which are on the medium back into the IDB. This then allows for fast and convenient access to the data on the media. See also exporting media.

### **incremental (re-)establish (EMC Symmetrix specific term)**

A BCV or SRDF control operation. In BCV control operations, an incremental establish causes the BCV device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired. In SRDF control operations, an incremental establish causes the target (R2) device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.

### **incremental backup**

A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, which enables detailed control of restore chain length. See also backup types.

### **incremental backup (Microsoft Exchange Server specific term)**

A backup of the Microsoft Exchange Server data that has changed since the last full or incremental backup. With the incremental backup, only the transaction log files are backed up. See also backup types.

### **incremental mailbox backup**

An incremental mailbox backup backs up all the changes made to the mailbox after the last backup of any type.

### **incremental restore (EMC Symmetrix specific term)**

A BCV or SRDF control operation. In BCV control operations, an incremental restore reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are updated with only the data that was written to the BCV device during the time of the original pair split, and the data that was written to the standard device during the split is overwritten with data from the BCV mirror. In SRDF control operations, an incremental restore reassigns a target (R2) device as the next available mirror of the source (R1) device in the pair. However, the source (R1) devices are updated with only the data that was written to the target (R2) device during the time of the original pair split, and the data that was written to the source (R1) device during the split is overwritten with data from the target (R2) mirror.

### **incremental ZDB**

A filesystem ZDB-to-tape or ZDB-to-disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape. See also full ZDB.

### **Incremental1 Mailbox Backup**

An incremental1 mailbox backup backs up all the changes made to the mailbox after the last full backup.

### **Inet**

A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication

between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

**Information Store (Microsoft Exchange Server specific term)**

The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users. See also Key Management Service and Site Replication Service.

**Informix Server (Informix Server specific term)**

Refers to Informix Dynamic Server.

**initializing**

See formatting.

**Installation Server**

A computer system that holds a repository of the Data Protector installation packages for a specific architecture. The Installation Server is used for remote installation of Data Protector clients. In mixed environments at least two Installation Servers are needed: one for UNIX systems and one for Windows systems.

**instant recovery (ZDB specific term)**

A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape sessions, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore

from tape. Depending on the application/database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery. See also replica, zero downtime backup (ZDB), ZDB to disk, and ZDB to disk+tape.

**integration object**

A backup object of a Data Protector integration, such as Oracle or SAP MaxDB.

**Internal Database (IDB)**

An entity in Data Protector that keeps information regarding which data was backed up, to which media it was backed up, how and when backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on. It is implemented with an embedded database and a collection of proprietary data files which reside on the Cell Manager. See also DC directory and Detail Catalog Binary Files (DCBF).

**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).

**ISQL (Sybase specific term)**

A Sybase utility used to perform system administration tasks on Sybase SQL Server.

**J****jukebox**

See library.

### **jukebox device**

A device consisting of multiple slots used to store either optical or file media. When being used to store file media, the jukebox device is known as the 'file jukebox device'.

## **K**

### **Key Management Service (Microsoft Exchange Server specific term)**

The Microsoft Exchange Server service that provides encryption functionality for enhanced security. See also Information Store and Site Replication Service.

### **keychain**

A tool that eliminates the supply of a passphrase manually when decrypting the private key. It needs to be installed and configured on the Installation Server if you perform remote installation using secure shell.

### **keystore**

All encryption keys are centrally stored in the keystore on the Cell Manager and administered by the Key Management Server (KMS).

## **KMS**

Key Management Server (KMS) is a centralized service that runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started as soon as Data Protector is installed on the Cell Manager.

## **L**

### **LBO (Symmetric specific term)**

A Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as

one entity and can only be restored as a whole.

### **LDEV (HP P9000 XP Disk Array Family specific term)**

A logical partition of a physical disk of a disk array of the HP P9000 XP Disk Array Family. An LDEV is the entity that can be replicated using the split-mirror or snapshot functionality of such disk array. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and replica.

### **library**

Also called autochanger, jukebox, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to media. The library can contain multiple drives.

### **lights-out operation or unattended operation**

A backup or restore operation that takes place outside of normal business hours without an operator. This implies that no operator personnel is present to work with the backup application or service mount requests, for example.

### **LISTENER.ORA (Oracle specific term)**

An Oracle configuration file that describes one or more Transparent Network Substrate (TNS) listeners on a server.

### **load balancing**

By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during

backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used for each object in the backup specification. Data Protector will access the devices in the specified order.

#### **local and remote recovery**

Remote recovery is performed if all Media Agent hosts specified in the SRD file are accessible. If any of them fails, the disaster recovery process fails over to the local mode. This means that the target system is searched for locally attached devices. If only one device is found, it is automatically used. Otherwise, Data Protector prompts you to select the device, which will be used for restore.

#### **local continuous replication (Microsoft Exchange Server specific term)**

Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying. An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and

can be backed up (using VSS) as a normal storage group. See also cluster continuous replication and Exchange Replication Service.

#### **lock name**

You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

#### **log\_full shell script (Informix Server UNIX systems specific term)**

A script provided by ON-Bar that you can use to start backing up logical log files when Informix Server issues a logfull event alarm. The Informix Server ALARMPROGRAM configuration parameter defaults to the `<INFORMIXDIR>/etc/log_full.sh`, where `<INFORMIXDIR>` is the Informix Server home directory. If you do not want logical logs to be backed up continuously, set the ALARMPROGRAM configuration parameter to `<INFORMIXDIR>/etc/no_log.sh`.

#### **logging level**

An option that determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings mainly influence the IDB growth and the convenience of browsing data for restore.



**logical-log files**

This applies to online database backup. Logical-log files are files in which modified data is first stored before being flushed to disk. In the event of a failure, these logical-log files are used to roll forward all transactions that have been committed as well as roll back any transactions that have not been committed.

**login ID (Microsoft SQL Server specific term)**

The name a user needs to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

**login information to the Oracle Target Database (Oracle and SAP R/3 specific term)**

The format of the login information is <user\_name>/<password>@<service>, where: <user\_name> is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights. <password> must be the same as the password specified in the Oracle password file (orapwd), which is used for authentication of users performing database administration. <service> is the name used to identify an SQL\*Net server process for the target database.

**login information to the Recovery Catalog Database (Oracle specific term)**

The format of the login information to the Recovery (Oracle) Catalog Database is <user\_name>/<password>@<service>, where the description of the user name, password, and service name is the same as in the Oracle SQL\*Net V2 login information to the Oracle target database.

In this case, <service> is the name of the service to the Recovery Catalog Database, not the Oracle target database. Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

**Lotus C API (Lotus Domino Server specific term)**

An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

**LVM**

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

**M****Magic Packet**

See Wake ONLAN.

**mailbox (Microsoft Exchange Server specific term)**

The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

**mailbox store (Microsoft Exchange Server specific term)**

A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

**Main Control Unit (MCU) (HP P9000 XP Disk Array Family specific term)**

An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP Array or HP CA+BC P9000 XP Array configuration and acts as a master device. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

**maintenance mode**

An operating mode you can initiate on the Cell Manager to prevent changes in the Internal Database. It enables you to perform various maintenance tasks, such as upgrading and patching the installation.

**make\_net\_recovery**

make\_net\_recovery is an Ignite-UX command, which allows you to create a recovery archive over the network onto the Ignite-UX server or any other specified system. The target system can be recovered across subnets after booting either from a bootable tape created by the Ignite-UX make\_boot\_tape command or the system boots directly from the Ignite-UX server. Booting directly from the Ignite-UX server can be automated with the Ignite-UX bootsys command or interactively specified on the boot console.

**make\_tape\_recovery**

make\_tape\_recovery is a command on Ignite-UX which creates a bootable recovery (installation) tape, customized for your system and enables you unattended disaster recovery by connecting the backup device directly to the target system and booting the target system from the bootable recovery tape. The backup device has to be locally connected to the client during the creation of the archive and recovery of the client.

**Manager-of-Managers**

See MoM.

**MAPI (Microsoft Exchange specific term)**

The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

**MCU**

See Main Control Unit (MCU).

**Media Agent**

A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore or object verification session, a Media Agent locates data on the backup medium and sends it to the Disk Agent for processing. For a restore session, the Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

**media allocation policy**

Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.

**media condition**

The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of

read and write errors with tape media. Media need to be replaced when they are marked as POOR.

**media condition factors**

The user-assigned age threshold and overwrite threshold used to assert the condition of a medium.

**media label**

A user-defined identifier used to describe a medium.

**media location**

A user-defined physical location of a medium, such as "building 4" or "off-site storage".

**media management session**

A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.

**media pool**

A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

**media set**

The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.

**media type**

The physical type of media, such as DDS or DLT.

**media usage policy**

The media usage policy controls how new backups are added to the already used media. It can be Appendable, Non-Appendable, or Appendable for incrementals only.

**medium ID**

A unique identifier assigned to a medium by Data Protector.

**merging**

This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored. See also overwrite.

**Microsoft Exchange Server**

A "client-server" messaging and a workgroup system that offers a transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

**Microsoft Management Console (MMC) (Windows specific term)**

An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.

**Microsoft SQL Server**

A database management system designed to meet the requirements of distributed "client-server" computing.

**Microsoft Volume Shadow Copy Service (VSS)**

A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow

copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets. See also shadow copy, shadow copy provider, replica, and writer.

**mirror (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)**

See target volume.

**mirror rotation (HP P9000 XP Disk Array Family specific term)**

See replica set rotation.

**mirror unit (MU) number (HP P9000 XP Disk Array Family specific term)**

A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family. See also first-level mirror.

**mirrorclone (HP P6000 EVA Disk Array Family specific term)**

A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.

**MMD**

The Media Management Daemon process (service) (MMD) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.

**MMDB**

The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots

configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells. See also CMMDB and Catalog Database (CDB).

**MoM**

Several cells can be grouped together and managed from a central cell. The management system of the central cell is the Manager-of-Managers (MoM). The cells are called MoM clients. The MoM enables you to configure and manage multiple cells from a central point.

**mount point**

The access point in a directory structure for a disk or logical volume, for example /opt or d:. On UNIX systems, the mount points are displayed using the bdf or df command.

**mount request**

A screen prompt that tells you to insert a specific medium into a device. Once you respond to the mount request by providing the required medium and confirm the mount request, the session continues.

**MSM**

The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.

**multisnapping (HP P6000 EVA Disk Array Family specific term)**

Simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot. See also snapshot.

## O

### **OBDR capable device**

A device that can emulate a CD-ROM drive loaded with a bootable disk and can thus be used as a backup or boot device for disaster recovery purposes.

### **obdrindex.dat**

See IDB recovery file.

### **object**

See backup object.

### **object consolidation**

The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.

### **object consolidation session**

A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.

### **object copy**

A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

### **object copy session**

A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.

### **object copying**

The process of copying selected object versions to a specific media set. You can

select object versions from one or several backup sessions to be copied.

### **object ID (Windows specific term)**

The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

### **object mirror**

A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

### **object mirroring**

The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

### **object verification**

The process of verifying the data integrity of backup objects, from the Data Protector point of view, and the ability of Data Protector to deliver them to the required destination. The process can be used to provide a level of confidence in the ability to restore object versions created by backup, object copy, or object consolidation sessions.

### **object verification session**

A process that verifies the data integrity of specified backup objects or object versions and the ability of selected Data Protector network components to deliver them to a specified host. Object verification sessions can be run interactively, or as specified in automated post-backup, or scheduled specifications.

### **offline backup**

A backup during which an application database cannot be used by the

application. For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to the tape is finished. For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process. See also zero downtime backup (ZDB) and online backup.

### **offline recovery**

Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Cell Manager can only be recovered offline.

### **offline redo log**

See archived redo log.

### **ON-Bar (Informix Server specific term)**

A backup and restore system for Informix Server. ON-Bar enables you to create a copy of your Informix Server data and later restore the data. The ON-Bar backup and restore system involves the following components: the onbar command, Data Protector as the backup solution, the XBSA interface, and ON-Bar catalog tables, which are used to back up dbobjects and track instances of dbobjects through multiple backups.

### **ONCONFIG (Informix Server specific term)**

An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, Informix Server uses the configuration values from the onconfig file located in

the directory <INFORMIXDIR>\etc (on Windows systems) or <INFORMIXDIR>/etc/ (on UNIX systems).

### **online backup**

A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period that the backup application requires access to the original data objects. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. For simple backup methods (non ZDB), backup mode is required for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to tape is finished. For ZDB methods, backup mode is required for the short period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process. In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored. See also zero downtime backup (ZDB) and offline backup.

### **online recovery**

A type of the Internal Database recovery that you can use when the Cell Manager is accessible. In this case, the Cell Manager runs sessions, the sessions are logged into the IDB, and you can monitor the session progress using the GUI.

### **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.

## **OpenSSH**

A set of network connectivity tools used to access remote machines securely, by using a variety of authentication and encryption methods. It needs to be installed and configured on the Installation Server and the client if you perform remote installation using secure shell.

## **Oracle Data Guard (Oracle specific term)**

Oracle Data Guard is Oracle's primary disaster recovery solution. Oracle Data Guard is able to maintain up to nine standby databases, each of which is a real-time copy of the production (primary) database, to protect against corruptions, data failures, human errors, and disasters. If a failure occurs on the production (primary) database, then a failover to one of the standby databases which becomes the new primary database is possible. In addition, planned downtime for maintenance can be reduced because the production processing can be moved from the current primary database to a standby database and back quickly.

## **Oracle instance (Oracle specific term)**

Each installation of an Oracle database on one or more systems. One computer system can have several instances of a database running.

## **ORACLE\_SID (Oracle specific term)**

A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired <ORACLE\_SID>. The <ORACLE\_SID> is included in the CONNECT DATA parts of the connect descriptor in a TNSNAMES.ORA file and in the definition of the TNS listener in the LISTENER.ORA file.

## **original system**

The system configuration backed up by Data Protector before a computer disaster hits the system.

## **overwrite**

An option that defines one mode to resolve file conflicts during restore. All files are restored from a backup even if they are older than existing files. See also merging.

## **ownership**

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. When copying or consolidating backup objects, the owner of the resulting objects is the user who started the original backup session.

## **P**

## **P1S file**

P1S file contains information on how to format and partition all disks installed in the system during Enhanced Automated Disaster Recovery (EADR). It is created during full backup and is saved on backup medium and on Cell Manager into the

directory <Data\_Protector\_program\_data>\Config\Server\dr\p1s (Windows systems) or /etc/opt/omni/dr/p1s (UNIX systems) with the filename recovery.p1s.

**package (HP ServiceGuard and Veritas Cluster Specific Term)**

A collection of resources (for example volume groups, application services, IP names, and addresses) that are needed to run a specific cluster-aware application.

**pair status (HP P9000 XP Disk Array Family specific term)**

The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP P9000 XP Agent:

PAIR - The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty.

SUSPENDED - The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time.

COPY - The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.

**parallel restore**

Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents, that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical

volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

**parallelism**

The concept of reading multiple data streams from an online database.

**phase 0 of disaster recovery**

Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.

**phase 1 of disaster recovery**

Installation and configuration of DR OS, establishing previous storage structure.

**phase 2 of disaster recovery**

Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.

**phase 3 of disaster recovery**

Restoration of user and application data.

**physical device**

A physical unit that contains either a drive or a more complex unit such as a library.

**post-exec**

A backup option that executes a command or script after the backup of an object or after the entire session completes. Post-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows systems and as shell scripts on UNIX systems. 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 systems and as shell scripts on UNIX systems.

### **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 systems and as shell scripts on UNIX systems. See also post-exec.

### **primary volume (P-VOL) (HP P9000 XP Disk Array Family specific term)**

An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU). See also secondary volume (S-VOL) and Main Control Unit (MCU).

### **protection**

See data protection and catalog protection.

### **public folder store (Microsoft Exchange Server specific term)**

The part of the Information Store that maintains information in public folders. A

public folder store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

### **public/private backed up data**

When configuring a backup, you can select whether the backed up data will be: public, that is visible (and accessible for restore) to all Data Protector users private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

## **R**

### **RAID**

Redundant Array of Independent Disks.

### **RAID Manager Library (HP P9000 XP Disk Array Family specific term)**

A software library that is used for accessing the configuration, status, and performance measurement data of a P9000 XP Array storage system, and for invoking operations on the disk array. It translates function calls into sequences of low-level SCSI commands. See also HP P9000 XP Agent.

### **RAID Manager P9000 XP (HP P9000 XP Disk Array Family specific term)**

A software application that provides a command-line interface to disk arrays of the HP P9000 XP Disk Array Family. It offers an extensive set of commands for reporting and controlling the status of a P9000 XP Array storage system, and for performing various operations on the disk array.

### **rawdisk backup**

See disk image backup.

### **RCU**

See Remote Control Unit (RCU).

**RDBMS**

Relational Database Management System.

**RDF1/RDF2 (EMC Symmetrix specific term)**

A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices.

**Recovery Catalog (Oracle specific term)**

A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about the physical schema of the Oracle target database, data file and archived log backup sets, data file copies, archived redo logs, and stored scripts.

**Recovery Catalog Database (Oracle specific term)**

An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

**recovery files (Oracle specific term)**

Recovery files are Oracle specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces. See also flash recovery area.

**Recovery Manager (RMAN) (Oracle specific term)**

An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the

recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

**RecoveryInfo**

When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume, and network configuration). This information is needed for disaster recovery.

**recycle or unprotect**

A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.

**redo log (Oracle specific term)**

Every Oracle database has a set of two or more redo log files. The set of redo log files for the database is known as the database's redo log. Oracle uses the redo log to record all changes made to data.

**Remote Control Unit (RCU) (HP P9000 XP Disk Array Family specific term)**

An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.

**Removable Storage Management Database (Windows specific term)**

A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications

to access and share the same media resources.

**reparse point (Windows specific term)**

A system-controlled attribute that can be associated with any directory or file. The value of a reparse attribute can have user-controlled data. The format of the data is understood by the application that stored the data and a filesystem filter that was installed to interpret the data and process such files. Whenever the filesystem encounters a file with a reparse point, it attempts to find the filesystem filter associated with the data format.

**replica (ZDB specific term)**

An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware or software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror), or a virtual copy (for example, a snapshot). From perspective of a basic operating system, the complete physical disk containing a backup object is replicated. However, if a volume manager is used on a UNIX system, the whole volume/disk group containing a backup object is replicated. If partitions are used on a Windows system, the whole physical volume containing the selected partition is replicated. See also snapshot, snapshot creation, split mirror, and split mirror creation.

**replica set (ZDB specific term)**

A group of replicas, all created using the same backup specification. See also replica and replica set rotation.

**replica set rotation (ZDB specific term)**

The use of a replica set for regular backup production: Each time the same backup

specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set. See also replica and replica set.

**restore chain**

Backup images that are needed to restore a backed up object to the state it was in at the selected point in time. In general, a restore chain of an object consists of its full backup image and one or more related incremental backup images.

**restore session**

A process that copies data from backup media to a client.

**resync mode (HP P9000 XP Disk Array Family VSS provider specific term)**

One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL. See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), MU number, and replica set rotation.

**RMAN (Oracle specific term)**

See Recovery Manager.

**RSM**

The Data Protector Restore Session Manager controls restore and object

verification sessions. This process always runs on the Cell Manager system.

### **RSM (Windows specific term)**

Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.

## **S**

### **scanning**

A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device if someone has manually manipulated media without using Data Protector to eject or enter, for example.

### **Scheduler**

A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.

### **secondary volume (S-VOL) (HP P9000 XP Disk Array Family specific term)**

An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration. See also primary volume (P-VOL) and Main Control Unit (MCU).

### **session**

See backup session, media management session, and restore session.

### **session ID**

An identifier of a backup, restore, object copy, object consolidation, object verification, or media management session, consisting of the date when the session ran and a unique number.

### **session key**

This environment variable for the pre- 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 (Microsoft VSS specific term)**

A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant. See also Microsoft Volume Shadow Copy Service and replica.

### **shadow copy provider (Microsoft VSS specific term)**

An entity that performs the work on creating and representing the volume shadow copies. Providers own the shadow copy data and expose the shadow copies. Providers can be software (for example, system providers) or hardware (local disks, disk arrays). See also shadow copy.

**shadow copy set (Microsoft VSS specific term)**

A collection of shadow copies created at the same point in time. See also shadow copy and replica set.

**shared disks**

A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

**Site Replication Service (Microsoft Exchange Server specific term)**

The Microsoft Exchange Server service that permits compatibility with Microsoft Exchange Server 5.5 by emulating the Exchange Server 5.5 directory service. See also Information Store and Key Management Service.

**slot**

A mechanical position in a library. Each slot can hold a medium, such as a DLT tape. Data Protector references each slot with a number. To read a medium, a robotic mechanism moves the medium from a slot into the drive.

**SMB**

See split mirror backup.

**SMBF**

The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, restore, object copy, object consolidation, object verification, and media management sessions. One binary file is created per session. The files are grouped by year and month.

**SMI-S Agent (SMISA)**

See HP P6000 / HP 3PAR SMI-S Agent.

**snapshot (HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)**

A type of target volumes created using a specific replication technology.

Depending on the disk array model and the chosen replication technique, a range of snapshot types with different characteristics is available. Basically, each snapshot may be either a virtual copy, still reliant upon the contents of the source volume, or an independent duplicate (clone) of the source volume. See also replica and snapshot creation.

**snapshot backup**

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

**snapshot creation (HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)**

A replica creation process in which copies of the selected source volumes are created using storage virtualization technology. Such a replica is considered to be created at a particular point in time, and is immediately available for use. However, with certain snapshot types, a background data copying process continues to run on the disk array after the moment of the replica creation. See also snapshot.

**source (R1) device (EMC Symmetrix specific term)**

An EMC Symmetrix device that participates in SRDF operations with a target (R2) device. All writes to this device are mirrored to a target (R2) device in a remote EMC Symmetrix unit. An R1 device must be assigned to an RDF1 group type. See also target (R2) device.

**source volume (ZDB specific term)**

A storage volume containing data to be replicated.

**sparse file**

A file that contains data with portions of empty blocks. Examples are: -A matrix in which some or much of the data contains zeros -files from image applications -high-speed databases If sparse file processing is not enabled during restore, it might be impossible to restore this file.

**split mirror (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)**

A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes. See also replica and split mirror creation.

**split mirror backup (EMC Symmetrix specific term)**

See ZDB to tape.

**split mirror backup (HP P9000 XP Disk Array Family specific term)**

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

**split mirror creation (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)**

A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes. See also split mirror.

**split mirror restore (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)**

A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards.

Individual backup objects or complete sessions can be restored using this method. See also ZDB to tape, ZDB to disk+tape, and replica.

**sqlhosts file or registry (Informix Server specific term)**

An Informix Server connectivity information file (on UNIX systems) or registry (on Windows systems) 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**

A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows system and stored on the Cell Manager. It contains system information required for installing and configuring the operating system on the target system in the case of a disaster. See also target system.

**SRDF (EMC Symmetrix specific term)**

The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.

**SSE Agent (SSEA)**

See HP P9000 XP Agent.

### **sst.conf file**

The file /usr/kernel/drv/sst.conf is required on each Data Protector Solaris client to which a multi-drive library device is connected. It must contain an entry for the SCSI address of the robotic mechanism of each library device connected to the client.

### **st.conf file**

The file /kernel/drv/st.conf is required on each Data Protector Solaris client with a backup device connected. It must contain device information and a SCSI address for each backup drive connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

### **stackers**

Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

### **standalone file device**

A file device is a file in a specified directory to which you back up data.

### **Storage Group (Microsoft Exchange Server specific term)**

A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.

### **storage volume (ZDB specific term)**

A storage volume represents an object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, file systems, or other objects may exist.

Typically, these can be created or exist within a storage system such as a disk array.

### **StorageTek ACS library (StorageTek specific term)**

Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.

### **switchover**

See failover.

### **Sybase Backup Server API (Sybase specific term)**

An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

### **Sybase SQL Server (Sybase specific term)**

The server in the Sybase "client-server" architecture. The Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

### **SYMA**

See EMC Symmetrix Agent.

### **synthetic backup**

A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

**synthetic full backup**

The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

**System Backup to Tape (SBT) (Oracle specific term)**

An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

**system databases (Sybase specific term)**

The four system databases on a newly installed Sybase SQL Server are the: - master database (master) -temporary database (tempdb) -system procedure database (sybsystemprocs) -model database (model).

**System Recovery Data file**

See SRD file.

**System State (Windows specific term)**

The System State data comprises the Registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory services and the SysVol directory are also contained in the System State data. If the server is running the Cluster service, the System State data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

**system volume/disk/partition**

A volume/disk/partition containing operating system files. Microsoft

terminology defines the system volume/disk/partition as the volume/disk/partition containing files required for the initial step of the boot process.

**SysVol (Windows specific term)**

A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

**T****tablespace**

A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

**tapeless backup (ZDB specific term)**

See ZDB to disk.

**target (R2) device (EMC Symmetrix specific term)**

An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type. See also source (R1) device.

**target database (Oracle specific term)**

In RMAN, the target database is the database that you are backing up or restoring.



**target system (disaster recovery specific term)**

A system after a computer disaster has occurred. The target system is typically in a non-bootable state and the goal of disaster recovery is to restore this system to the original system configuration. The difference between a faulty system and a target system is that a target system has all faulty hardware replaced.

**target volume (ZDB specific term)**

A storage volume to which data is replicated.

**Terminal Services (Windows specific term)**

Windows Terminal Services provide a multi-session environment that allows clients to access a virtual Windows desktop session and Windows-based programs running on the server.

**thread (Microsoft SQL Server specific term)**

An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

**TimeFinder (EMC Symmetrix specific term)**

A business continuation process that creates an instant copy of single or multiple EMC 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**

See Tape Library Unit.

**TNSNAMES.ORA (Oracle and SAP R/3 specific term)**

A network configuration file that contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

**transaction**

A mechanism for ensuring that a set of actions is treated as a single unit of work. Databases use transactions to keep track of database changes

**transaction backup**

Transaction backups generally use fewer resources than database backups, so they can be created more frequently than database backups. By applying transaction backups, you can recover the database to a specific point in time prior to when a problem occurred.

**transaction backup (Sybase and SQL specific term)**

A backup of the transaction log providing a record of changes made since the last full or transaction backup.

**transaction log backup**

Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.

**transaction log files**

Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.

**transaction log table (Sybase specific term)**

A system table in which all changes to the database are automatically recorded.

**transportable snapshot (Microsoft VSS specific term)**

A shadow copy that is created on the application system and can be presented to the backup system which performs the backup. See also Microsoft Volume Shadow Copy Service (VSS).

**U****unattended operation**

See lights-out operation.

**user account (Data Protector user account)**

You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

**User Account Control (UAC)**

A security component in Windows Vista and Windows Server 2008 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

**user disk quotas**

NTFS quota-management support enables an enhanced tracking mechanism and control over disk space usage on shared storage volumes. Data Protector backs up user disk quotas on the whole system and for all configured users at a time.

**user group**

Each Data Protector user is member of a User Group. Each User Group has a set

of user rights that are given to every user in that User Group. The number of User Groups with their associated user rights can be defined as desired. Data Protector provides three default user groups: admin, operator, and user.

**user profile (Windows specific term)**

Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.

**user rights**

User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

**user\_restrictions file**

A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than admin and operator.

**V****vaulting media**

The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

**verify**

A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.

**Virtual Controller Software (VCS) (HP P6000 EVA Disk Array Family specific term)**

The firmware that manages all aspects of storage system operation, including communication with HP Command View EVA through the HSV controllers. See also HP Command View (CV) EVA.

**Virtual Device Interface (Microsoft SQL Server specific term)**

This is a Microsoft SQL Server programming interface that allows fast backup and restore of large databases.

**virtual disk (HP P6000 EVA Disk Array Family specific term)**

A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array. See also source volume and target volume.

**virtual full backup**

An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

**Virtual Library System (VLS)**

A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

**virtual server**

A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

**virtual tape**

An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs. See also Virtual Library System (VLS) and virtual tape library (VTL).

**virtual tape library (VTL)**

Data storage virtualization software that is able to emulate tape devices and libraries thus providing the functionality of traditional tape-based storage. See also Virtual Library System (VLS).

**volser**

A VOLUME SERIAL number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

**volume group**

A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

**volume mountpoint (Windows specific term)**

An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to

the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

### **Volume Shadow Copy Service**

See Microsoft Volume Shadow Copy Service (VSS).

### **VSS**

See Microsoft Volume Shadow Copy Service (VSS).

### **VSS compliant mode (HP P9000 XP Disk Array Family VSS provider specific term)**

One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching of the disks. See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

### **VxFS**

Veritas Journal Filesystem.

### **VxVM (Veritas Volume Manager)**

A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.

## **W**

### **Wake ONLAN**

Remote power-up support for systems running in power-save mode from some other system on the same LAN.

### **Web reporting**

The Data Protector functionality that allows you to view reports on backup, object copy, and object consolidation status and Data Protector configuration using the Web interface.

### **wildcard character**

A keyboard character that can be used to represent one or many characters. The asterisk (\*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

### **Windows configuration backup**

Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.

### **Windows Registry**

A centralized database used by Windows to store configuration information for the operating system and the installed applications.

### **WINS server**

A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.

**writer (Microsoft VSS specific term)**

A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.

**X****XBSA Interface (Informix Server specific term)**

ON-Bar and Data Protector communicate with each other through the X/Open Backup Services Application Programmer's Interface (XBSA).

**Z****ZDB**

See zero downtime backup.

**ZDB database (ZDB specific term)**

A part of the IDB, storing ZDB related information such as source volumes, replicas and security information. The ZDB database is used for ZDB, instant recovery, and split mirror restore. See also zero downtime backup (ZDB).

**ZDB to disk (ZDB specific term)**

A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time. Multiple replicas, produced using the same backup specification at different times, can be kept in a replica set. A replica from ZDB to disk can be restored using the instant recovery process. See also zero downtime backup (ZDB), ZDB to tape, ZDB to disk+tape, instant recovery, and replica set rotation.

**ZDB to disk+tape (ZDB specific term)**

A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored using the instant recovery process, the standard Data Protector restore from tape, or with specific disk array families, split mirror restore. See also zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.

**ZDB to tape (ZDB specific term)**

A form of zero downtime backup where data in the replica produced is streamed to a backup medium, typically tape. Instant recovery is not possible from such a backup, so the replica need not be retained on the disk array after backup completion. The backed up data can be restored using standard Data Protector restore from tape. With specific disk array families, split mirror restore can also be used. See also zero downtime backup (ZDB), ZDB to disk, ZDB to disk+tape, instant recovery, and replica.

**zero downtime backup (ZDB)**

A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation. See also ZDB to disk, ZDB to tape, ZDB to disk+tape, and instant recovery.

# Index

## A

- access rights
  - adding to root account, on Linux 67
- ACS Client 89
- adding
  - access rights, on Linux 67
  - SCSI robotics driver to kernel, on HP-UX 345
- Adding clients to the cell
  - GUI 81
- adding software components
  - overview 223
  - to HP-UX systems 224
  - to Linux systems 224
  - to Windows systems 223
- ADIC library 88
- ADIC/GRAU library
  - connecting drives 89
  - installing Media Agent to clients 90
  - Media Agent installation 88
  - preparing clients 89
- AIX client
  - connecting backup devices 71
  - installing 70
- allow\_hosts file 161-163
- authorized systems list, security 159
- automatically configured files, on UNIX 29
- AutoPass utility
  - uninstalling 217

## B

- backup devices
  - setting SCSI IDs, for HP 330fx Library 355
- backup devices, connecting
  - ADIC/GRAU library drives 89
  - AIX clients 71
  - HP-UX clients 57
  - HP 12000e Autoloader 360
  - HP DAT 24 Tape Drive 359
  - HP DLT Library 24/48-Slot 361
  - Linux clients 68
  - overview 356
  - Seagate Viper 200 LTO Tape Drive 365
  - Solaris clients 64
  - Windows clients 54
- backup environment concepts 15

## C

- cell
  - concepts 15
  - enabling security 161
  - exporting clients 154
  - exporting Microsoft Cluster Server client 155
  - importing clients 149
  - importing clusters 151
  - importing Installation Server 151
  - licenses 269, 271
  - securing clients 159
  - upgrading, overview 229
  - verifying DNS connections 292

## Cell Manager

- choosing the system 19-20
- concepts 15
- directory structure, on UNIX 28
- functions 19
- installation prerequisites, on UNIX 24
- installation prerequisites, on Windows 31
- installation sequence 23
- installing, on HP-UX 27
- installing, on HP-UX, using native tools 311
- installing, on Linux 27
- installing, on Linux, using native tools 312
- installing, on Windows 31
- uninstalling, from HP-UX 216
- uninstalling, from HP Serviceguard 217
- uninstalling, from Linux 220
- uninstalling, from Windows 215
- upgrading from 6.20, 7.00, and 8.00 on UNIX 231
- upgrading SSE 247
- Cell Request Server (CRS) service 29, 36
- cell\_info file 226
- certificate generation utility
  - directory structure 203
  - examples 191
  - introduction 188
  - syntax 188
- changing
  - default port 323
  - hostname 335
  - name 328
  - software components 223
- changing software components 223
- changing the hostname 335
- changing the name 328
- checking
  - installation on clients 300
  - licenses 271
  - log files, installation 307
  - patches 212
  - TCP/IP setup, on Windows 321
- checking configuration
  - LDAP 187
- checking configuration changes 237
- CLI 15
- client 321
  - adding root access rights, on Linux 67
  - changing software components 223
  - cluster-aware integration installation, overview 97
  - cluster-aware, importing to a cell 151
  - concepts 15
  - configuring after installation, on Solaris 59
  - configuring for backup devices usage, on Solaris 350
  - configuring for Veritas Volume Manager, on Microsoft Cluster Server 327
  - creating device files, on HP-UX 346
  - creating device files, on Solaris 354
  - denying access from hosts 163
  - enabling access verification 159

- exporting from a cell 154
- importing to a cell 149
- installation, overview 43
- integration installation, overview 95
- local installation, on OpenVMS 71
- Microsoft Cluster Server, exporting from a cell 155
- preparing for ADIC/GRAU library 89
- preparing for StorageTek ACS library 92
- remote installation, overview 77
- removing access verification 162
- securing 159
- security concepts 156
- troubleshooting 293, 295, 298, 307, 309
- uninstalling remotely 214
- upgrading from 6.20, 7.00, and 8.00 241
- upgrading from 6.20, 7.00, and 8.00 on HP Serviceguard 242
- upgrading, on Microsoft Cluster Server 267
- verifying installation 300
- client, connecting backup devices
  - ADIC/GRAU library drives 89
  - AIX clients 71
  - HP-UX clients 57
  - Linux clients 68
  - Solaris clients 64
  - Windows clients 54
- client, installing
  - DB2 integration 105
  - HP 3PAR StoreServ Storage integration 125
  - HP P4000 SAN Solutions integration 113
  - HP P6000 EVA Disk Array Family integration 113
  - Informix integration 103
  - Lotus integration 106
  - Media Agent for ADIC/GRAU library 90
  - Media Agent for StorageTek ACS library 94
  - Microsoft Exchange Server 2007 integration 98
  - Microsoft Exchange Server 2010 integration 98
  - Microsoft SharePoint Server 2007 integration 101
  - Microsoft SQL integration 100
  - Microsoft Volume Shadow Copy Service integration 102
  - NDMP integration 110
  - on OpenVMS systems 71
  - on AIX systems 70
  - on ESX Server systems 69
  - on HP-UX systems 55
  - on HP Serviceguard systems 133
  - on IBM HACMP cluster systems 144
  - on Linux systems 65
  - on Mac OS X systems 69
  - on Microsoft Cluster Server systems 141
  - on Solaris systems 58
  - on UNIX systems 85
  - on Veritas Cluster systems 144
  - on Windows systems 50
  - Oracle integration 105
  - SAP MaxDB integration 104-105



- SAP R/3 integration 104
- Single Server Edition 130
- Sybase integration 103
- Virtual Environment integration 106
- VMware Granular Recovery Extension 107
- client,installing
  - HP P9000 XP Disk Array Family integration 119
- cluster
  - changing software components 224
  - importing to a cell 151
  - installing 133
  - installing clients 141, 144
  - installing integrations 97
  - Microsoft Cluster Server, exporting from a cell 155
  - uninstalling 215
- command 231, 323
- command-line interface (CLI) 15, 21
- commands
  - CLI changes, after upgrade 367
  - infs 346
  - ioscan 344, 346, 348
  - netstat 323
  - omnicc 281
  - omnicheck 213, 292
  - omnisetup.sh 231-232
- concepts
  - backup environment 15
  - cell 15
  - Cell Manager 15
  - client 15
  - Disk Agent 15
  - exporting 154
  - graphical user interface (GUI) 21
  - importing 149
  - Installation Server 15
  - Media Agent 15
  - NDMP Media Agent 15
  - remote installation 17
  - User Interface 15
- configuration files
  - automatically configured files, on UNIX 29
  - cell\_info 226
  - checking changes after upgrade from 6.20, 7.00, and 8.00 237
  - global 237
  - inet.conf 328
  - installation\_servers 40
  - modifying, Solaris client installation 59
  - nsswitch.conf 328
  - omni\_info 225
  - omnirc 238
  - sst.conf 353
  - st.conf 351
  - st.conf file 59
  - upgrade problems 305
- configuring
  - clients with Veritas Volume Manager, on Microsoft Cluster Server 327
  - Disk Agent, on OpenVMS 75
  - LDAP login module 183

- Media Agent, on OpenVMS 76
- SCSI robotics, on HP-UX 342
- Solaris clients, after installation 59
- Solaris clients, before using backup devices 350
- sst.conf file 353
- st.conf file 59, 351
- with Veritas Volume Manager, on MSCS 327
- configuring for Veritas Volume Manager, on Microsoft Cluster Server 327
- connecting backup devices
  - ADIC/GRAU library drives 89
  - AIX clients 71
  - HP-UX clients 57
  - HP 12000e Autoloader 360
  - HP DAT 24 Tape Drive 359
  - HP DLT Library 24/48-Slot 361
  - Linux clients 68
  - overview 356
  - Seagate Viper 200 LTO Tape Drive 365
  - Solaris clients 64
  - Windows clients 54
- creating
  - device files, on HP-UX 346
  - device files, on Solaris 354
  - device files, on Windows 341
  - execution trace files, installation 309
- CRS 29
- D**
- DAS Client 89
- database growth 20
- DB2 integration, installing 105
- debug option
  - overview 309
- default port, changing 323
- deny\_hosts file 163
- denying access from hosts 163
- determining
  - installed licenses 285
  - required licensing passwords 287
  - unused SCSI addresses, on HP-UX 348
  - unused SCSI addresses, on Solaris 350
  - unused SCSI addresses, on Windows 354
- device file
  - creating, on HP-UX 346
  - creating, on Solaris 354
  - creating, on Windows 341
- disabling SCSI robotics drivers, on Windows 339
- Disk Agent
  - concepts 15
  - configuring, on OpenVMS 75
- DNS
  - omnicheck command 292
  - verifying connections in a cell 292
- DNS check tool 322
- domain name system 292
- DVD-ROM
  - list of installation DVD-ROMs 18
- E**
- enabling access verification
  - on a cell 161

- on a client 159
- environment variables, setting on UNIX 30
- ESX Server client
  - installing 69
- excessive logging 163
- execution trace files
  - debug option 309
- exporting
  - clients 154
  - Microsoft Cluster Server client 155
- F**
- files
  - allow\_hosts 161-163
  - deny\_hosts 163
  - services 323
- G**
- global file 237
- granting permissions
  - LDAP users or groups 186
- graphical user interface (GUI)
  - concepts 21
  - views 21
- GRAU library 88
- GUI 21
- H**
- HP-UX
  - automatically configured files 29
  - setting environment variables 30
  - troubleshooting 301, 307
- HP-UX Cell Manager
  - directory structure 28
  - installation prerequisites 24
  - installing 27
  - installing, using native tools 311
  - migrating from PA-RISC to Itanium 248
- HP-UX client
  - connecting backup devices 57
  - installing 55
  - troubleshooting 295
- HP-UX Installation Server
  - installing, using native tools 314
- HP-UX systems
  - uninstalling 216
- HP 12000e Autoloader, connecting 360
- HP 330fx Library, setting SCSI IDs 355
- HP 3PAR StoreServ Storage integration
  - installing 125
- HP DAT 24 Tape Drive, connecting 359
- HP DLT Library 24/48-Slot, connecting 361
- HP P4000 SAN Solutions integration
  - installing 113
- HP P6000 EVA Disk Array Family integration
  - installing 113
- HP P9000 XP Disk Array Family integration
  - installing 119
- HP Serviceguard
  - excessive logging to inet.log file 163
  - importing 153
  - installing 132
  - installing clients 133
  - uninstalling Cell Manager 217

- uninstalling Installation Server 217
  - upgrading 260
  - upgrading clients from 6.20, 7.00, and 8.00 242
- I**
- IBM HACMP cluster
    - installing clients 144
  - IDB
    - growth 20
    - troubleshooting upgrade 305
  - importing
    - clients 149
    - clusters 151
    - Installation Server 151
    - multiple LAN card clients 150
    - NDMP clients 150
    - OpenVMS clients 150
    - VLS device 150
  - Inet service 37
  - inet.conf
    - file 328
  - inet.log file 161-163, 263
  - Informix integration, installing 103
  - infs command 346
  - initializing
    - LDAP login module 182
  - installation
    - client installation, overview 43
    - cluster-aware integrations 97
    - components 15
    - general steps 16
    - integrations, overview 95
    - log files 307
    - omnisetup.sh 220-221
    - overview 15
    - preparing Microsoft server cluster with Windows Server 2008 or Windows Server 2012 for 325
    - remote installation, overview 77
    - remote, concepts 17
    - software component codes 86
    - software components 46
    - troubleshooting clients, on UNIX 295
    - troubleshooting, on Windows 293, 298
    - verifying clients 300
  - installation components 15
    - Disk Agent 15
    - General Media Agent 15
    - Media Agent 15
    - NDMP Media Agent 15
    - User Interface 15
  - installation overview 38
  - Installation Server
    - concepts 15
    - importing to a cell 151
    - installation prerequisites, on UNIX 38
    - installation prerequisites, on Windows 40
    - installing, on HP-UX, using native tools 314
    - installing, on Linux, using native tools 314
    - installing, on UNIX 38
    - installing, on Windows 40

- uninstalling, from HP-UX 216
- uninstalling, from HP Serviceguard 217
- uninstalling, from Linux 221
- uninstalling, from Windows 215
- upgrading from 6.20, 7.00, and 8.00 on UNIX 230-231
- upgrading from 6.20, 7.00, and 8.00, on UNIX 232
- Installation Server 6.20, 7.00, and 8.00, on Windows
  - upgrading from Data Protector 234
- installation\_servers file 40
- installing
  - clients locally 50, 71, 85
  - cluster-aware 132-133
  - cluster-aware clients 133, 141, 144
  - DB2 integration 105
  - HP 3PAR StoreServ Storage integration 125
  - HP P4000 SAN Solutions integration 113
  - HP P6000 EVA Disk Array Family integration 113
  - HP P9000 XP Disk Array Family integration 119
  - Informix integration 103
  - integrations 95
  - Lotus integration 106
  - Media Agent for ADIC/GRAU library 88, 90
  - Media Agent for StorageTek ACS library 88, 94
  - Microsoft Exchange Server 2007 integration 98
  - Microsoft Exchange Server 2010 integration 98
  - Microsoft SharePoint Server 2007 integration 101
  - Microsoft SQL integration 100
  - Microsoft Volume Shadow Copy Service integration 102
  - NDMP integration 110
    - on HP Serviceguard systems 132
    - on Microsoft Cluster Server systems 133
  - Oracle integration 105
  - overview 38
  - permanent licensing passwords 285
  - SAP MaxDB integration 104-105
  - SAP R/3 integration 104
  - Single Server Edition 130
  - Sybase integration 103
  - Virtual Environment integration 106
  - VMware Granular Recovery Extension 107
  - Web Reporting 131
- installing Cell Manager
  - on HP-UX systems 27
  - on HP-UX systems using native tools 311
  - on Linux systems 27
  - on Linux systems using native tools 312
  - on Windows systems 31
  - prerequisites, on UNIX 24
  - prerequisites, on Windows 31
- installing clients
  - on OpenVMS system 71
  - on AIX systems 70
  - on ESX Server systems 69

- on HP-UX systems 55
- on HP Serviceguard systems 133
- on IBM HACMP cluster systems 144
- on Linux systems 65
- on Mac OS X systems 69
- on Microsoft Cluster Server systems 141
- on Solaris systems 58
- on UNIX systems 85
- on Veritas Cluster systems 144
- on Windows systems 50
- installing Installation Server
  - on HP-UX systems, using native tools 314
  - on Linux systems, using native tools 314
  - on UNIX systems 38
  - on Windows systems 40
  - prerequisites, on UNIX 38
  - prerequisites, on Windows 40
- installing, on HP Serviceguard 132
- installing, on Microsoft Cluster Server 133
- integration
  - upgrading to > 245
- integration client 95
- integrations 245
  - cluster-aware installation 97
  - local installation 97
  - Oracle, on UNIX 243
  - overview 95
  - remote installation 97
  - SAP R/3, on UNIX systems 244
  - upgrading 245
  - upgrading Oracle, on Windows 243
  - upgrading SAP R/3, on Windows systems 244
  - upgrading VSS 245
- integrations, installing
  - DB2 integration 105
  - HP 3PAR StoreServ Storage integration 125
  - HP P4000 SAN Solutions integration 113
  - HP P6000 EVA Disk Array Family integration 113
  - HP P9000 XP Disk Array Family integration 119
  - Informix integration 103
  - Lotus integration 106
  - Microsoft Exchange 2007 integration 98
  - Microsoft Exchange Server 2010 integration 98
  - Microsoft SharePoint Server 2007 integration 101
  - Microsoft SQL integration 100
  - Microsoft Volume Shadow Copy Service integration 102
  - NDMP integration 110
  - Oracle integration 105
  - SAP HANA MaxDB integration 105
  - SAP MaxDB integration 104
  - SAP R/3 integration 104
  - Sybase integration 103
  - Virtual Environment Integration 106
  - VMware Integration 107
- introduction
  - user authentication and LDAP 181
- ioscan command 344, 346, 348

## K

### kernel

- adding SCSI robotics driver, on HP-UX 345
- rebuilding, on HP-UX 345

Key Management Server (KMS) 30, 37

Key Management Server (KMS) service 37

KMS 30

## L

LDAP 181

- checking the configuration 187
- configuring login module 183
- granting permissions to LDAP users or groups 186
- initializing login module 182

license-to-use. 287

licenses 287

### licensing

- capacity based licensing, examples 276, 279
- Cell Manager 272
- centralized licensing, configuring 287
- checking and reporting licenses 271
- determining installed licenses 285
- determining required passwords 287
- emergency passwords 282
- Instant-On passwords 282
- license migration 288
- licensing forms 289
- moving licenses 286
- obtaining and installing permanent passwords 285

overview 287

password types 282

permanent passwords 282

permanent passwords, obtaining and installing 285

producing license reports 281

product structure 269, 287

upgrade from 6.20, 7.00, and 8.00 230

upgrade from SSE 247

using licenses, after upgrade 230, 247

verifying passwords 285

licensing forms 289

### limitations

- on Windows systems 41, 50
- Single Server Edition 130
- upgrade 228
- upgrade of Manager-of-Managers 230

### Linux

- automatically configured files 29
- setting environment variables 30

### Linux Cell Manager

- directory structure 28
- installation prerequisites 24
- installing 27
- installing, using native tools 312
- uninstalling 220

### Linux client

- connecting backup devices 68
- installing 65
- troubleshooting remote installation 67

- Linux Installation Server
  - installing, using native tools 314
- local installation, clients 50, 71, 85
- log files
  - checking, installation 307
  - description 308
  - inet.log 161-163, 263
  - location 308
- Lotus integration, installing 106
- LTU 287
- M**
- Mac OS X client
  - installing 69
- maintenance mode 147
- Manager-of-Managers
  - upgrade overview 230
  - upgrading 246
- Media Agent
  - concepts 15
  - configuring, on OpenVMS 76
  - installing for ADIC/GRAU library 90
  - installing for StorageTek ACS library 94
  - types 15
- Media Management Daemon (MMD) 37
- Media Management Daemon (MMD)
  - service 30, 37
- Microsoft Cluster Server
  - configuring with Veritas Volume Manager 327
  - configuring clients with Veritas Volume Manager 327
  - exporting 155
  - importing 152
  - installing 133
  - installing clients 141
  - upgrading 264
  - upgrading clients 267
- Microsoft Exchange integration
  - installing on systems with HP P6000 EVA Disk Array Family 118
  - installing on systems with HP P9000 XP Disk Array Family 124
- Microsoft Exchange Server 2007 integration
  - installing 98
- Microsoft Exchange Server 2010 integration
  - installing 98
- Microsoft Installer 50, 294
- Microsoft server cluster
  - preparing Windows Server 2008 or Windows Server 2012 systems for installation 325
- Microsoft SharePoint Server 2007 integration
  - installing 101
- Microsoft SQL integration
  - installing 100
  - installing on systems with EMC Symmetrix disk array 129
  - installing on systems with HP P6000 EVA Disk Array Family 119
  - installing on systems with HP P9000 XP Disk Array Family 125
- Microsoft Terminal Services Client 32
- Microsoft Volume Shadow Copy Service
  - integration, installing 102



migrating

Cell Manager on HP-UX, PA-RISC to  
Itanium 248

licenses 288

Migrating

Cell Manager on Windows, 32-bit to 64-  
bit 248

MMD 30

moving licenses 286

multiple LAN card client, importing 150

**N**

NDMP client, importing 150

NDMP integration, installing 110

NDMP Media Agent, concepts 15

netstat 323

NIS server, preparing 327

nsswitch.conf

file 328

nsswitch.conf file 328

**O**

obtaining permanent licensing  
passwords 285

omni\_info file 225

omnicc command 281

omnicheck command 213, 292

omniinet process 37

omnirc file 238

omnisetup.sh 220-221

omnisetup.sh command

upgrade 231-232

OpenVMS client

configuring Disk Agent 75

configuring Media Agent 76

importing 150

uninstalling 215

Oracle integration 110

installing 105

installing on systems with EMC  
Symmetrix disk array 126

installing on systems with HP P6000  
EVA Disk Array Family 114

installing on systems with HP P9000 XP  
Disk Array Family 120

uninstallation specifics 224

upgrading from 6.20, 7.00, or 8.00 243

overview

changing software components 223

connecting backup devices 356

debug option 309

execution trace files 309

importing application cluster  
packages 151

importing cluster-aware client 151

installing 38

installing clients 43

installing cluster-aware integrations 97

installing integrations 95

integrations 95

licensing 287

product structure 269

remotely installing clients 77

software components 46

uninstallation 213

upgrade 227

- upgrading from 6.20, 7.00, and 8.00 230
- overwriting certificates
  - creating new store files 208
  - existing store files 206
- overwriting existing certificates 206
- P**
- patches
  - omnicheck command 213
  - verifying 212
- preparing for installation
  - Microsoft server cluster running on Windows Server 2008 or Windows Server 2012 325
- preparing NIS server 327
- prerequisites
  - Cell Manager installation, on UNIX 24
  - Cell Manager installation, on Windows 31
  - Installation Server installation, on UNIX 38
  - Installation Server installation, on Windows 40
  - upgrade from 6.20, 7.00, and 8.00 230
- processes
  - Cell Request Server (CRS) service 29, 36
  - Inet service 37
  - Key Management Server (KMS) 30, 37
  - Media Management Daemon (MMD) 37
  - Media Management Daemon (MMD) service 30
- R**
- rebuilding kernel, on HP-UX 345
- Red Hat 7 systems
  - troubleshooting 297
- related licenses 272
- remote installation
  - clients 77
  - integrations 97
  - troubleshooting, on Linux 67
- removing
  - access verification on a client 162
  - software components, from UNIX 224-225
  - software components, from Windows 223
  - software components, overview 223
  - software manually, from UNIX 222
- reporting licenses 271
- robotics. 339, 342
- rpm utility 220-221
- S**
- SAP MaxDB integration, installing 104-105
- SAP R/3 integration 111
  - installing 104
  - installing on systems with EMC Symmetrix disk array 127
  - installing on systems with HP P6000 EVA Disk Array Family 116
  - installing on systems with HP P9000 XP Disk Array Family 121
  - upgrading 244
- SCSI addresses. 350
- SCSI controller. 348

## SCSI interface

- adding robotics driver to kernel, on HP-UX 345

- configuring robotics, on HP-UX 342

- determining unused addresses, on HP-UX 348

- determining unused addresses, on Solaris 350

- determining unused addresses, on Windows 354

- disabling robotics drivers, on Windows 339

- setting controller parameters, on Windows 348

- setting IDs, for HP 330fx Library 355

- using tape drivers, on Windows 339

SCSI robotics. 342

SCSI tape drivers. 339

Seagate Viper 200 LTO Tape Drive,  
connecting 365

## securing

- cell 161

- client 159

## security

- allow\_hosts file 161-163

- deny\_hosts file 163

- denying access from hosts 163

- enabling security for a cell 161

- enabling security for a client 159

- excessive logging to inet.log file 163

- list of authorized systems 159

- potential problems 158

- removing access verification on a client 162

security concepts 156

## services

- hpd-idb 30, 37

- hpd-idb-as 30, 37

- hpd-idb-cp 30, 37

services file 323

## setting

- environment variables, on UNIX 30

- SCSI controller parameters, on Windows 348

- SCSI IDs, for HP 330fx Library 355

setting environment variables, on UNIX 30

## Single Server Edition

- installing 130

- limitations 130

- upgrading from multiple installations 248

- upgrading to Data Protector 8.10 247

## software components

- adding, to HP-UX 224

- adding, to Linux 224

- adding, to Windows 223

- changing, on cluster clients 224

- changing, overview 223

- component codes 86

- dependencies, on Solaris 225

- overview 46

- removing, from UNIX 224-225

- removing, from Windows 223

## Solaris

- setting environment variables 30

- troubleshooting 301, 307

## Solaris Cell Manager

- directory structure 28

- installation prerequisites 24

## Solaris client

- configuring, after installation 59

- connecting backup devices 64

- installing 58

- troubleshooting 295

SSE 247

SSE. 246

sst.conf file 353

st.conf file 59, 351

STK ACS 88

## StorageTek ACS library

- connecting drives 89

- installing Media Agent to clients 94

- Media Agent installation 88

- preparing clients 92

StorageTek library 88

swagent daemon 295

swremove utility 216

Sybase integration, installing 103

syntax 188

## T

tape drivers. 339

## TCP/IP

- checking setup, on Windows 321

Terminal Services Client 32

trace files. 309

troubleshooting 293, 301, 307, 309

## troubleshooting installation

- Cell Manager, on Windows 37

- clients, on -UX 295

- debug option 309

- execution trace files 309

- installation, on Red Hat 7 systems 297

- log files 307

- Mac OS X client 295

- Microsoft Installer problems 293

- omnicheck command 292

- remote installation, on Linux 67

- remote installation, on UNIX 295

- remote installation, on Windows 298

- software, on Windows 293

- swagent daemon 295

## troubleshooting upgrade

- configuration files not available 305

- IDB not available 305

- Microsoft Installer problems 293

- patches 306

- software, on Windows 293

## U

### uninstallation

- Oracle integration specifics 224

- overview 213

- prerequisites 214

- rpm utility 220-221

- swremove utility 216

### uninstalling

- AutoPass utility 217

- Cell Manager, from HP-UX 216

- Cell Manager, from HP Serviceguard 217
- Cell Manager, from Linux 220
- Cell Manager, from Windows 215
- clients, from OpenVMS 215
- clients, remotely 214
- cluster clients 215
- Installation Server, from HP-UX 216
- Installation Server, from HP Serviceguard 217
- Installation Server, from Linux 221
- Installation Server, from Windows 215
- UNIX Cell Manager
  - upgrading from 6.20, 7.00, and 8.00 231
- UNIX Installation Server
  - upgrading from 6.20, 7.00, and 8.00 232
- unused SCSI addresses. 354
- upgrade
  - before upgrading 227
  - CLI changes 367
  - global file 237
  - limitations 228
  - omnirc file 238
  - omnisetup.sh 231
  - omnisetup.sh command 232
  - overview 227
  - sequence 229
  - troubleshooting IDB 305
  - troubleshooting, on UNIX 301
  - troubleshooting, on Windows 293, 301
- upgrading
  - Manager-of-Managers 246
  - manually, on UNIX 307
  - SAP R/3 integration 244
  - SSE to Data Protector 8.10 247
  - VSS integration 245
- upgrading from , , and
  - , in HP Serviceguard 260
  - , on Microsoft Cluster Server 264
  - clients, on Microsoft Cluster Server 267
- upgrading from 6.20, 7.00, and 8.00
  - Cell Manager, on UNIX 231
  - checking configuration changes 237
  - clients 241
  - clients, on HP Serviceguard 242
  - Installation Server on Windows 234
  - Installation Server, on UNIX 230-232
  - overview 230
  - prerequisites 230
- upgrading from 6.20, 7.00, or 8.00
  - Oracle integration 243
- upgrading manually, on UNIX 307
- upgrading to >
  - integration 245
- upgrading, in HP Serviceguard 260
- upgrading, on Microsoft Cluster Server 264
- user interface 15
- User Interface
  - choosing the system 21
  - concepts 15
- using
  - licenses 230
  - log files 307

SCSI tape drivers, on Windows 339

## V

### verifying

client installation 300

DNS connections in a cell 292

licensing passwords 285

patches 212

### Veritas Cluster

importing 153

installing clients 144

limitations, failover 144

### Veritas Volume Manager

configuring , on Microsoft Cluster  
Server 327

configuring clients, on Microsoft Cluster  
Server 327

views, graphical user interface 21

### Virtual Environment integration

installing 106

virtual server, importing to a cell 151

VLS device, importing 150

### VMware Granular Recovery Extension

installing 107

### VSS integration

upgrading 245

## W

Web Reporting, installing 131

### Windows

troubleshooting 293, 301

### Windows Cell Manager

installation prerequisites 31

installing 31

migrating from 32-bit to 64-bit 248

troubleshooting installation 37

### Windows client

connecting backup devices 54

installing 50

troubleshooting 293, 298, 307

uninstalling 214

### Windows Server 2008 and Windows Server 2012

preparing Microsoft server cluster for  
installation 325

### Windows systems

uninstalling 215

## Z

ZDB integration client 95

## We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

### **Feedback on Installation Guide (Data Protector 8.10)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [AutonomyTPFeedback@hpe.com](mailto:AutonomyTPFeedback@hpe.com).

