HP Data Protector 8.00 Troubleshooting Guide

HP Part Number: N/A
Published: June 2013
Edition: Second

© Copyright 2013 Hewlett-Packard Development Company, L.P.
Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Java is a registered trademark of Oracle and/or its affiliates.

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

UNIX® is a registered trademark of The Open Group.

LiveVault® is a registered trademark of Autonomy Corporation plc.

Contents

Publication history

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

Table 1 Edition history

Part number	Guide edition	Product
N/A	June 2013	Data Protector release 8.00
N/A	June 2013 (second edition)	Data Protector release 8.00

About this guide

This guide describes how to troubleshoot problems you may encounter when using Data Protector. It contains general problems and proposed actions to solve them.

NOTE: This guide does not contain troubleshooting information that is specific to the Data Protector installation, integrations, zero downtime backup functionality, and disaster recovery. The related information is covered in the respective guides.

Intended audience

This guide is intended for backup administrators responsible for maintaining and backing up systems on the network.

Documentation set

The Help and other guides provide related information.

NOTE: The documentation set available at the HP support website at http://support.openview.hp.com/selfsolve/manuals contains the latest updates and corrections.

Help

Data Protector provides Help topics and context-sensitive (F1) Help for Windows and UNIX platforms. Install the Help during the Data Protector setup procedure by selecting the installation component `English Documentation (Guides, Help)` (Windows systems) or `OB2-DOCS` (on UNIX systems). Once installed, the Help resides in the following directory:

Windows systems: *`Data_Protector_home`*`\help\enu`

UNIX systems: `/opt/omni/help/C/help_topics`

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

Windows systems: Open `DP_help.chm`.

UNIX systems: Unpack the zipped tar file `DP_help.tar.gz` and open `DP_help.htm`.

Guides

Data Protector guides are available in the electronic PDF format. Install the PDF files during the Data Protector setup procedure by selecting the installation component `English Documentation (Guides, Help)` (on Windows systems) or `OB2-DOCS` (on UNIX systems). Once installed, the guides reside in the following directory:

Windows systems: *`Data_Protector_home`*`\docs`

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

You can also access the guides:

- From the **Help** menu of the Data Protector graphical user interface
- From the HP support website at http://support.openview.hp.com/selfsolve/manuals (where the most up-to-date guide versions are available)

Data Protector guides are:

- *HP Data Protector Getting Started Guide*

  This guide contains information to get you started with using Data Protector. It lists installation prerequisites, provides instructions on installing and configuring a basic backup environment and procedures for performing backup and restore. It also lists resources for further information.

- *HP Data Protector Concepts Guide*

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

- *HP Data Protector Installation and Licensing Guide*

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

- *HP Data Protector Troubleshooting Guide*

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

- *HP Data Protector Disaster Recovery Guide*

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

- *HP Data Protector Command Line Interface Reference*

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

  Windows systems: `Data_Protector_home\docs\MAN`

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

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

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

  This guide gives a description of new features of HP Data Protector 8.00. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.

- *HP Data Protector Integration Guides*

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

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

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

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

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

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

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

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

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

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

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

- *HP Data Protector Integration Guide for Virtualization Environments*

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

- *HP Data Protector Zero Downtime Backup Concepts Guide*

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

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

  This guide describes how to configure and use the integration of Data Protector with HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, HP 3PAR StoreServ Storage, and EMC Symmetrix Remote Data Facility and TimeFinder. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

- *HP Data Protector Zero Downtime Backup Integration Guide*

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

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

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

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

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

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

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

- *HP Data Protector Deduplication*

  This technical white paper describes basic data deduplication concepts, principles of Data Protector integration with Backup to Disk devices and its use of deduplication. It also provides instructions how to configure and use deduplication in Data Protector backup environments.

- *HP Data Protector Integration with Autonomy IDOL Server*

  This technical white paper describes all aspects of integrating Data Protector with Autonomy IDOL Server: integration concepts, installation and configuration, Data Protector backup image indexing, full content search-based restore, and troubleshooting.

- *HP Data Protector Integration with Autonomy LiveVault*

  This technical white paper all aspects of integrating Data Protector with Autonomy LiveVault: integration concepts, installation and configuration, backup policy management, cloud backup, cloud restore, and troubleshooting.

Documentation map

Abbreviations

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

Abbreviation	Documentation item
CLI	Command Line Interface Reference
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
GRE Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	Help
Install	Installation and Licensing Guide
IG IBM	Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
IG MS	Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server
IG VSS	Integration Guide for Microsoft Volume Shadow Copy Service
IG O/S	Integration Guide for Oracle and SAP
IG Var	Integration Guide for Sybase and Network Data Management Protocol Server
IG VirtEnv	Integration Guide for Virtualization Environments
IG IDOL	Integration with Autonomy IDOL Server
IG LV	Integration with Autonomy LiveVault

Abbreviation	Documentation item
PA	Product Announcements, Software Notes, and References
Trouble	Troubleshooting Guide
ZDB Admin	ZDB Administrator's Guide
ZDB Concepts	ZDB Concepts Guide
ZDB IG	ZDB Integration Guide

Map

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

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

Integrations

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

Software application	Guides
Autonomy IDOL Server	IG IDOL
Autonomy LiveVault	IG LV
IBM DB2 UDB	IG IBM
Informix Server	IG IBM
Lotus Notes/Domino Server	IG IBM
Microsoft Exchange Server	IG MS, ZDB IG, GRE Exchange

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

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

Disk array family	Guides
EMC Symmetrix	all ZDB
HP P4000 SAN Solutions	ZDB Concepts, ZDB Admin, IG VSS
HP P6000 EVA Disk Array Family	all ZDB, IG VSS
HP P9000 XP Disk Array Family	all ZDB, IG VSS
HP 3PAR StoreServ Storage	ZDB Concepts, ZDB Admin, IG VSS

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 12)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

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

IMPORTANT: Provides clarifying information or specific instructions.

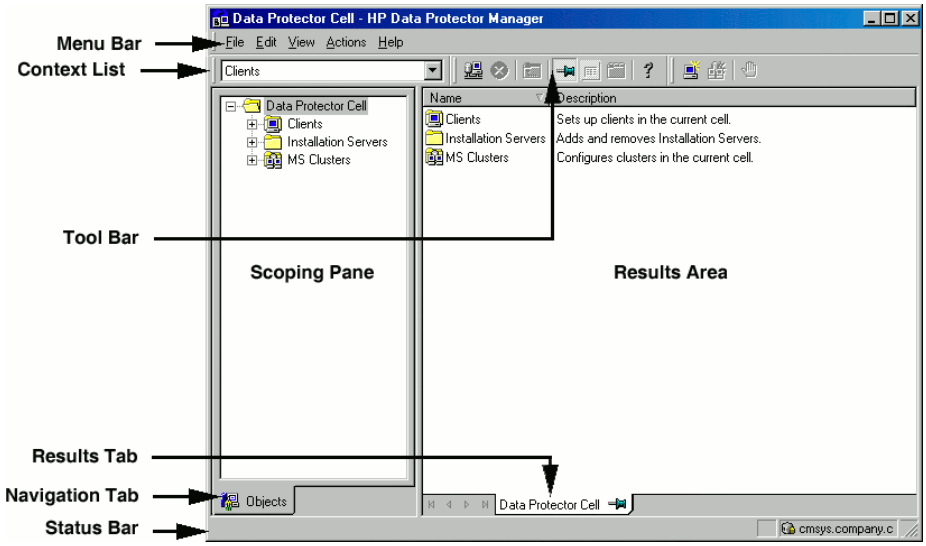
NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Data Protector graphical user interface

Data Protector provides a graphical user interface for Microsoft Windows operating systems. For information about it, see the *HP Data Protector Help*.

Figure 1 Data Protector graphical user interface



General information

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

HP technical support

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

HP websites

For additional information, see the following HP websites:

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

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message with the subject line `Feedback on Data Protector documentation` to **AutonomyTPFeedback@hp.com**. All submissions become the property of HP.

1 About troubleshooting Data Protector

Introduction

If you encounter problems when using Data Protector, you can often solve them yourself. This guide is intended to help you.

How to use this guide

To solve problems quickly and efficiently:

1. Make yourself familiar with the general troubleshooting information in this chapter.
2. Check if your problem is described in this guide, or troubleshooting sections in other guides:
   - To troubleshoot installation and upgrade, see the *HP Data Protector Installation and Licensing Guide*.
   - To troubleshoot application integration sessions, see the *HP Data Protector Integration Guide*.
   - To troubleshoot zero downtime backup and instant recovery, see the *HP Data Protector Zero Downtime Backup Administrator's Guide* and *HP Data Protector Zero Downtime Backup Integration Guide*.
   - To troubleshoot disaster recovery, see the *HP Data Protector Disaster Recovery Guide*.
3. If you cannot find a solution to your problem, report the problem to the HP Customer Support Service. On how to prepare the required data for the support organization, see "Before calling support" (page 57).

TIP: For an overview and hints on performance aspects of Data Protector, see the *HP Data Protector Help* index: "performance".

General checks

Before proceeding, ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Data Protector limitations and recommendations, as well as known Data Protector and non-Data Protector problems, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- Your problem is not related to third-party hardware or software. In this case, contact the respective vendor for support.
- You have the latest Data Protector patches installed. Patches can be obtained from: http://www.itrc.hp.com.

  On how to check which Data Protector patches are installed on your system, see the *HP Data Protector Help* index: "patches".
- You have appropriate operating system patches installed.

  The required operating system patches are listed in the *HP Data Protector Product Announcements, Software Notes, and References*.
- For application backups, the backup is not failing because the application is down.
- The debug logs or redo logs filesystem has not overflown.
- The application data filesystem has not overflown.
- The system is not running low on memory.

Data Protector log files

If you encounter a problem using Data Protector, the information in the log files can help you determine the problem.

Location of log files

Most Data Protector log files 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

Format of log files

Most Data Protector log file entries are of the following format:

time_stamp process.PID.Thread_ID source_file_info Data Protector_version log_entry_message

Example

```
03/16/2013 8:47:00 PM  INET.3048.3036 ["inetnt/allow_deny.c
/main/dp61/6":467] A.08.00
A request 0 (BDF) came from host computer.company.com
(10.17.xx.xxx) which is not in AllowList: not proceeding with this request!
```

Contents of log files

The table below describes the Data Protector log files:

Table 3 Data Protector log files

debug.log	Contains unexpected conditions. While some can help you, the information is mainly used by the support organization.
inet.log	Contains local security related events for the client, such as denied requests. On UNIX systems, it contains also all requests made to the Data Protector Inet service.
enhincr.log	Contains information on enhanced incremental backup activities, for example detailed error information for problems with the enhanced incremental backup repository.
Ob2EventLog.txt	Contains Data Protector events and notifications. The Event Log represents a centralized Data Protector event depository.
media.log	Each time a medium is used for backup, initialized, or imported, a new entry is created in this log file. The file can be used when recovering the IDB to find the medium with the IDB backup and to find out which media have been used after the last backup of the IDB.
omnisv.log	Contains information on when Data Protector services were stopped and started.
security.log	Contains security related events on the Cell Manager. Some events may be a result of normal operation and simply mean that an operation was attempted that is not allowed by a particular user. On the other hand, events can indicate that deliberate break-in attempts may be in progress.
purge.log	Contains traces of the background purge of the IDB.
PostgreSQL logs	Contain the IDB logs. The log files reside on the Cell Manager in: ***Windows systems:*** Data_Protector_program_data\server\db80\pg\pg_log ***UNIX systems:*** /var/opt/omni/server/db80/pg/pg_log

Table 3 Data Protector log files *(continued)*

`pgbouncer.log`	Contains the pgBouncer logs.
`Application Server logs`	Contain the application server logs. The log files reside in: ***Windows systems:*** `Data_Protector_program_data\log\AppServer` ***UNIX systems:*** `/var/opt/omni/log/AppServer`
`sanconf.log`	Contains session reports generated by the `sanconf` command.
`sm.log`	Contains details on internal errors that occurred during backup and restore sessions, such as errors in parsing backup specifications.
`upgrade.log`	This log is created during upgrade and contains upgrade core part (UCP) and upgrade detail part (UDP) messages.
`OB2_Upgrade.log` (UNIX systems specific)	This log is created during upgrade and contains traces of the upgrade process.
`IS_install.log`	Contains a trace of remote installation and resides on the Installation Server.
`sap.log`, `oracle8.log`, `informix.log`, `sybase.log`, `db2.log`	Application specific logs contain traces of integration calls between the application and Data Protector. The files reside on the application systems.

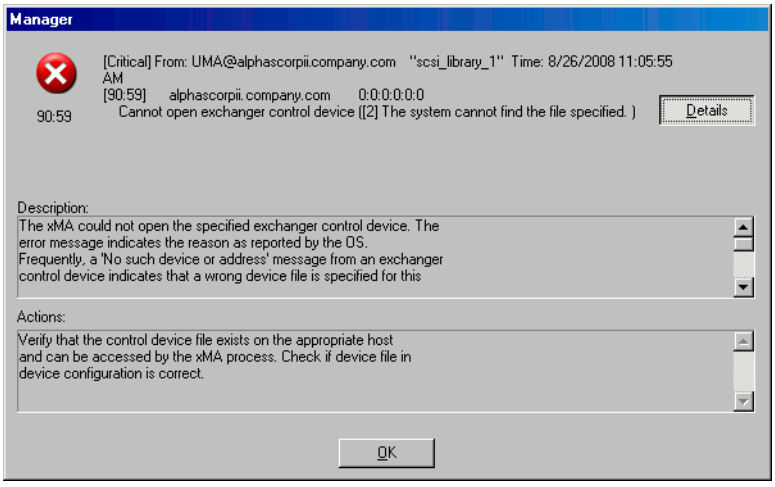
Data Protector error messages

Many Data Protector error messages have troubleshooting information associated with them, providing detailed explanations of errors and suggestions for correcting problems. Such messages contain an error number that can be used to access this information.

Error messages in the Data Protector GUI

Some error messages in the session output provide the error number, presented as a clickable link. If you click the link, the error message dialog displays more information about the error. Click **Details** for a detailed description of the error and suggested actions.

Figure 2 Sample error message dialog



Error messages in the Data Protector CLI

If you receive an error message containing the error number in the Data Protector CLI, you can look up the error details in the troubleshooting file. This is a text file containing all Data Protector error messages, each of them with a description and possible actions.

The troubleshooting file is located on the Cell Manager:

Windows systems: *Data_Protector_home*\help\enu\Trouble.txt

UNIX systems: /opt/omni/gui/help/C/Trouble.txt

Example

```
MESSAGE:
[12:1051] Client security violation. Access denied.
DESCRIPTION:
The target host is secured and has been accessed by a
host that is not on its list of cell authorities.
ACTION:
* Check and update the client's list of cell
authorities.
* In case your client has been locked out, edit the allow_hosts file manually.
```

Data Protector customization

Sometimes you can solve Data Protector issues by customizing its global or omnirc options.

Global options

Global options are a set of parameters, such as timeouts and limits, that define behavior of the entire Data Protector cell. They can be set on the Cell Manager.

NOTE: Most users should be able to operate the Data Protector without changing the global options.

Global options can be set in two ways:

- By using the Data Protector graphical user interface
- By editing the global options file in a text editor

Global options setting in GUI

To set global options using the Cell Manager GUI:

1. In the Context List, click **Internal Database**.
2. In the Scoping Pane, under **Internal Database**, click **Global Options**.

   In Results area, the Global Options table is displayed, consisting of six columns:

   - Group — represents the contextual section the option belongs to.
   - In use— indicates the status of an option. Selected options are active, while the empty check box indicates the inactive options that are commented out in the global options file.
   - Name
   - Origin — indicates the file which the option is loaded from. If the column is hidden, display it using filters in the table headings.
   - Value — represents the value to which the option is currently set.
   - Description — informs you how to use the option.

   To change the table appearance, use the filters in the table headings.
3. To modify an option, click on its value. Changing an inactive option automatically selects the option as In use.

   To add an option, click **Add new option**, enter its parameters in the dialog box, and click **Add**.

   The changed rows get highlighted in red, while a red triangle implies the modified cell.

4. Click **Save** to confirm the changes.

In case anything goes wrong during the saving process, a copy of the original global options file named `global.old` is made in the global options folder.

Global options file editing

> **CAUTION:** HP recommends using the GUI to set the global options, as it ensures validation of changes upon saving and reduces the chance of issues arising from the out-of-range or invalid settings, accidental deletions, typographical or spelling errors.

To set the global options, you can edit the `global` file in a text editor. The file is located on Cell Manager at:

Windows systems: *`Data_Protector_program_data`*`\Config\Server\Options\global`

UNIX systems: `/etc/opt/omni/server/options/global`

To activate an option, remove the "#" mark in front of its name and set it to the desired value.

After editing the file on Windows systems, make sure you save it in the Unicode format.

Most often used global options

The following list describes the most often used global options. For a complete description, see the global options table in GUI.

- `MaxSessions`: Specifies the maximum number of Data Protector sessions (of any type) that can concurrently run in the cell. Default: `1000`.
- `MaxBSessions`: Specifies the maximum number of Data Protector backup sessions that can concurrently run in the cell. Default: `100`.
- `MaxMAperSM`: Specifies the maximum number of Data Protector backup devices that can be concurrently used in one backup, object copy, object consolidation, or restore session. Default: `100`.
- `MaxDAperMA`: Specifies the maximum Disk Agent concurrency (device concurrency) for Data Protector backup, object copy, and object consolidations sessions. Default: `32`.
- `DCDirAllocation`: Determines the algorithm used for selecting the DC (Detail Catalog) directory for a new DC binary file: `Fill in sequence`, `Balance size` (default), `Balance number`. For more information on the DC directory selection algorithms, see the *HP Data Protector Help* index: "maintenance of DCBF".
- `MediaView`: Changes the fields and their order in the Media Management context.
- `InitOnLoosePolicy`: Enables Data Protector to automatically initialize blank or unknown media if the `loose` media policy is used.
- `DailyMaintenanceTime`: Determines the time after which the daily maintenance tasks can begin. Default: `12:00` (noon). For a list of daily maintenance tasks, see the *HP Data Protector Help* index: "checks performed by Data Protector".
- `DailyCheckTime`: Determines the time after which the daily check can begin. Default: `12:30 P.M.`. You can also disable the daily check. For a list of daily check tasks, see the *HP Data Protector Help* index: "checks performed by Data Protector".
- `SessionStatusWhenNoObjectToCopy` and `SessionStatusWhenNoObjectToConsolidate`: Enable you to control the session status

of object copy and object consolidation sessions if there are no objects to copy or to consolidate.

If the value is set to:

- `0` (default), then the session will be marked as failed and a critical error will be displayed.
- `1`, then the session will be marked as successful and a warning will be displayed.
- `2`, then the session will be marked as successful and a normal message will be displayed.

Omnirc options

The `omnirc` options are useful for troubleshooting or overriding other settings affecting the behavior of the Data Protector client only. However, use them only if your operating environment demands it. The Disk Agents and Media Agents use the values of these options.

The omnirc options can be set on each client in the file:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: *`Data_Protector_program_data`*`\omnirc`

Other Windows systems: *`Data_Protector_home`*`\omnirc`

HP-UX, Solaris, and Linux systems: `/opt/omni/.omnirc`

Other UNIX systems and Mac OS X systems: `/usr/omni/.omnirc`

How to use omnirc options?

To set omnirc options:

1. Depending on the platform, copy the template `omnirc.tmpl` or `.omnirc.TMPL` to `omnirc` or `.omnirc`, respectively.
2. Edit the file `omnirc` or `.omnirc`. Uncomment the line of the desired option by removing the "#" mark, and set the desired value.
3. After setting the options:
   - When creating the `omnirc` file (either by copying or by using an editor), verify its permissions. On UNIX systems, permissions will be set according to your umask settings and may be such that some processes may be unable to read the file. Set the permissions to 644 manually.
   - When changing the `omnirc` file, restart the Data Protector services/daemons on the Data Protector client where you modified the `omnirc` file. This is mandatory for the `crs` daemon on UNIX systems and recommended for Data Protector CRS and `Inet` services on Windows systems. Specifically on Windows systems, restarting is not required when adding or changing entries, only when removing entries (or renaming the file).

NOTE: When using special characters in option names in the `omnirc` file, take into account operating system specific limitations regarding supported characters for setting environment variables. For example, on UNIX systems, variables cannot contain any of the following characters: `Space Tab / : * " < > |`.

On how to set omnirc options during disaster recovery, see the *HP Data Protector Disaster Recovery Guide*.

Most often used omnirc options

The following list includes the most often used omnirc options. See the `omnirc` file for a complete description.

- `OB2_SSH_ENABLED`: To enable secure remote installation using secure shell (SSH), set this option to `1 on the Installation Server`. The default value is `0` (not set).
- `OB2_ENCRYPT_PVT_KEY`: To use encrypted private keys for secure remote installation, set this option to `1` on the Installation Server. The default value is `0` (not set).
- `OB2_ENCRYPT_MEDIUM_STRICT`: Enables you to control whether to strictly use drive-based encryption in backup, object consolidation, object copy, and automated media copy sessions. The option is only considered when the GUI option Drive-based encryption is selected for the current session.

  If the value is set to `1`, then:

  - if the selected tape drive does not support encryption, the session will be aborted by default.
  - if the selected tape drive supports encryption, but the medium in it does not support encryption, a mount request will be issued (in case of a standalone tape drive) or the next available medium will be checked for encryption support first and eventually a mount request will be issued if no media with encryption support are found (in case of a tape library).
  - if the selected tape drive and the medium in it both support encryption, the data writing operation will be performed in an encrypted mode.

  If the value is set to `0`, then:

  - if the selected tape drive does not support encryption, the data writing operation will be performed in an unencrypted mode.
  - if the selected tape drive supports encryption, but the medium in it does not support encryption, the data writing operation will be performed in an unencrypted mode.
  - if the selected tape drive and the medium in it both support encryption, the data writing operation will be performed in an encrypted mode.
- `OB2_ENCRYPT_FORCE_FORMAT`: Enables you to control the formatting behavior when using Data Protector drive-based encryption.

  If the value is set to:

  - `0` (default), a formatting operation aborts.
  - `1`, a formatting operation is forced.
- `OB2BLKPADDING_n`: Specifies the number of empty blocks written to media at the initialization time. When copying media, this helps to prevent the target media from running out of space before all data is copied.
- `OB2DEVSLEEP`: Changes the sleep time between each retry while loading a device.
- `OB2ENCODE`: Enables you to always use data encoding, regardless of how the backup options are set in the backup specification.
- `OB2OEXECOFF`: Enables you to restrict or disable any object `pre-` and `post-exec` scripts defined in backup specifications for a specific client.
- `OB2REXECOFF`: Enables you to disable any remote session `pre-` and `post-exec` scripts for a specific client.

- `OB2CHECKCHANGETIME` (UNIX systems specific): Defines when to use the "last inode change" time for incremental backups.
- `OB2INCRDIFFTIME` (UNIX systems specific): Specifies an "incremental latency" period that is enforced when checking the "last inode change" time with incremental backups. This option takes effect only when the `OB2CHECKCHANGETIME` option is set to 2.
- `OB2RECONNECT_ACK`: Defines how long Data Protector should wait for a message of acknowledgment (default: 1200 seconds). If the agent does not get an acknowledgment in this time, it assumes that the socket connection is no longer valid.
- `OB2RECONNECT_RETRY`: Defines how long a Data Protector Disk Agent or Media Agent should try to reconnect after a connection failure. Default: 600 seconds.
- `OB2SHMEM_IPCGLOBAL`: This option should be set to 1 on HP-UX clients that have both the Disk Agent and a Media Agent installed in case the following error occurs during backup:

  ```
  Cannot allocate/attach shared memory (IPC Cannot Allocate
  Shared Memory Segment)
  System error: [13] Permission denied) => aborting
  ```

- `OB2VXDIRECT`: Enables direct reading (without cache) for Advanced VxFS filesystems, which improves performance.
- `OB2_CLP_MAX_ENTRIES` (Windows systems specific): Sets the number of entries the Windows NTFS Change Log Provider can hold in memory. The amount of memory that the Change Log Provider uses depends on the filename length of all entries. Minimum: 15 000 entries (this represents approximately 25 MB of RAM). Default: 100 000 entries (approximately 120 MB of RAM). If the number is changed to a smaller value so that not all entries can be kept in memory, the backup time may increase.
- `OB2_CLP_CREATE_EI_REPOSITORY` (Windows systems specific): Specifies whether the Windows NTFS Change Log Provider creates the Enhanced Incremental Repository the first time it runs. Set this option to 1 to create the Enhanced Incremental Repository. Default: `0` (not created). With this option set, the backup time increases, since the Enhanced Incremental Repository is always updated. However, this enables a fallback to a conventional enhanced incremental backup.
- `OB2_ENHINC_SQLITE_MAX_ROWS`: Specifies the maximum number of rows in the enhanced incremental backup database (SQLite on Windows, HP-UX, and Linux systems) that can be stored in the internal memory cache. If the backup consists of a large number (millions) of directories, this option is used to improve the Disk Agent performance by increasing the maximum number of rows stored in the cache.
- `OB2SANCONFSCSITIMEOUT=s` (Windows systems specific): Sets the timeout for `sanconf` related operations. It must be set on all clients affected by `sanconf` before running the command. Default: 20 seconds.
- `OB2PORTRANGE`: Limits the range of port numbers that Data Protector uses when allocating listen ports dynamically. This option is typically set to enable the administration of a cell through a firewall. Note that the firewall needs to be configured separately and that the specified range does not affect the `Inet` listen port.
- `OB2PORTRANGESPEC`: Limits the range of port numbers that specific Data Protector processes use. Note that the firewall needs to be configured separately and that the specified range does not affect the `Inet` listen port.

  For examples of port range configuration, see the *HP Data Protector Help* index: “firewall support”.

2 Troubleshooting networking and communication

Hostname resolution problems

An important aspect of the TCP/IP configuration process is the setup of a hostname resolution mechanism.

For successful communication, host A needs to resolve host B by its fully qualified domain name (FQDN). Resolving a host means that host A can interpret the FQDN of host B and determine its IP address.

Hostname resolution must be provided at least for the following:

- Each client must be able to resolve the address of the Cell Manager and the clients with Media Agents.
- The Cell Manager must be able to resolve the names of all clients in the cell.
- The MoM Server, if used, must additionally be able to resolve the names of all Cell Managers in the MoM environment.

Checking the TCP/IP setup

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig` (Windows) or `ifconfig` (UNIX) utilities 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.

Testing DNS resolution

Test DNS resolution among hosts by executing:

```
omnicheck -dns
```

This will check all DNS connections needed for normal Data Protector operation.

For more information on the command, see the *HP Data Protector Help* index: "checking DNS configuration" and the `omnicheck` man page.

Problem

Connected system presents itself as client X

The response to the `omnicheck` command is:

`client_1` `connects to` *`client_2`*`, but connected system presents itself as` *`client_3`*

The `hosts` file on *`client_1`* is not correctly configured or the hostname of *`client_2`* does not match its DNS name.

Action

Consult your network administrator. Depending on how your environment is configured to perform name resolution, the problem needs to be resolved either in your DNS configuration or the `hosts` file on the affected clients, located in:

Windows systems: *`%SystemRoot%`*`\System32\drivers\etc`

UNIX systems: `/etc`

Problem

Client A failed to connect to client B

The response to the `omnicheck` command is:

`client_1` `failed to connect to` *`client_2`*

The `hosts` file on *`client_1`* is not correctly configured or *`client_2`* is unreachable (for example disconnected).

Action

Configure the `hosts` file correctly or connect the disconnected system.

Problem

Cannot connect to client X

The response to the `omnicheck` command is:

`client_1` `cannot connect to` *`client_2`*

This means that the packet has been sent, but not received because of a timeout.

Action

Check for network problems on the remote host and resolve them.

Checking time settings in the cell

Data Protector uses timestamps extensively for communication between various cell components (Cell Manager, clients). If the system clocks on the Cell Manager and clients differ significantly, such as weeks or even months (for example, if you changed settings for testing purposes, the system clock was not updated after a restore of a virtual machine and so on), unexpected results may occur, including communication errors, failures to search or restore backups, and similar.

Check the system time settings and make sure that the system clocks do not differ significantly.

Recovering from power outages

Problem

The IDB is not reachable after a system recovery

The database is capable to recover into a consistent state after such unexpected events as power outages, severe operating system or hardware failures, and so on. However, the first access to the database (after the system recovery) might fail with an internal error. This is a temporary problem which occurs only once.

Action

Reaccess the database.

Problem

Data Protector sessions are actually not running but remain marked as In Progress

In the Internal Database context of the Data Protector GUI, the session status of one or more Data Protector sessions that are actually not running remains marked as `In Progress`.

Action

1. Close the Data Protector GUI.
2. Execute the `omnidbutil -clear` command to set the status of all sessions that are actually not running but are marked as `In Progress` to `Failed`.
3. Restart the Data Protector GUI.

Problem

The hpdp-idb-cp service fails to start

The hpdp-idb-cp service does not start.

Action

1. Stop the Data Protector services.
2. Delete the following file:

   Windows systems: *Data_Protector_program_data*\log\hpdp-idb-cp.pid

   UNIX systems: /var/opt/omni/log/pgbouncer.pid
3. Restart the Data Protector services.

Novell Open Enterprise Server (OES) problems

Problem

TSA login denied

The following message is displayed:

```
From: VRDA@computer.company.com
"/media/nss/NSS_VOLUME_5"
TSA: Cannot connect to Target Service (login denied).
```

Action

Run the HPLOGIN utility /usr/omni/bin/hplogin with the correct user credentials.

Other problems

Problem

Client fails with "Connection reset by peer"

On Windows systems, default configuration parameters of the TCP/IP protocol may cause problems with connectivity. This may happen due to a high network or computer use, unreliable network, or especially when connecting to a different operating system. The following error is reported:

```
[10054] Connection reset by peer.
```

Action

You can configure the TCP/IP protocol to use 8 instead of the default 5 retransmissions. It is better not to use higher values because each increment doubles the timeout. The setting applies to all network connections, not only to connections used by Data Protector.

On Windows systems, apply the change on the Cell Manager system first.

If the Cell Manager is running on a Windows system, apply the change on the Cell Manager system first. If the problem persists or if the Cell Manager is running on a UNIX system, apply the change to the problematic Windows clients.

1. Add the DWORD parameter TcpMaxDataRetransmissions and set its value to 0x00000008(8) under the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
2. Restart the system.

△ **CAUTION:** Making a mistake when editing the registry may cause your system to become unstable or even unusable.

Problem

Client fails with "The client is not a member of any cell"

When performing a Data Protector operation on a client and the Cell Manager information is not found on the client, the operation fails with the following error:

```
The Client is not a member of any cell.
```

Action

- If the client is listed in the Clients context of the Data Protector GUI:
  1. In the Clients context, expand **Clients**, right-click the client, and click **Delete**.
  2. A dialog asks you if you also want to uninstall Data Protector from the client. Click **No**.
  3. Right-click **Clients** and click **Import Client**.
  4. Specify the client and click **Finish**.
- If the client is not listed in the Clients context:
  1. In the Clients context, right-click **Clients** and click **Import Client**.
  2. Specify the client and click **Finish**.

Problem

Excessive logging to the `inet.log` file

If clients are not secured and the Cell Manager is configured in the MC/ServiceGuard environment or has multiple names or IP addresses, the `inet.log` file may contain many entries of the following type:

```
A request 3 (vbda.exe) came from host computer.company.com which is not
a cell manager of this client.
```

This happens because a client that is not secured recognizes only the primary hostname of the Cell Manager. Requests from any other client are allowed, but are logged to the `inet.log` file.

Action

Secure the client. For instructions, see the *HP Data Protector Help* index: "securing client systems". Requests from the clients listed in the `allow_hosts` file will not be logged to `inet.log`. Requests from other clients will be denied.

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 resolve the excessive logging issue.

IMPORTANT: All possible hostnames for the Cell Manager nodes should be listed in the `allow_hosts` file on each client that is being secured. This enables access to the client also in case of a failover. If you accidentally lock out a client, you can manually edit the `allow_hosts` file on that client. For more information, see the *HP Data Protector Help* index: "client security".

3 Troubleshooting Data Protector services and daemons

Introduction

The Data Protector services (Windows) and daemons (UNIX) run on the Cell Manager. Run the `omnisv -status` command to check whether services/daemons are running.

If the Data Protector services/daemons seem to be stopped or have not been installed on the target Data Protector client, make sure that you do not have a name resolution problem. For more information, see "Troubleshooting networking and communication" (page 23).

Data Protector processes

"Data Protector processes running during different operations" (page 27) shows which processes run while Data Protector is idle or performing some basic operations, such as a backup, a restore, or a media management session.

Table 4 Data Protector processes running during different operations

		Always	Backup	Restore	Media management

Cell Manager	Windows	`omniinet.exe`
		`mmd.exe`
		`crs.exe`
		`kms.exe`
		`hpdp-idb`
		`hpdp-idb-cp`
		`hpdp-as`
			`bsm.exe`	`rsm.exe`	`msm.exe`

	UNIX	`mmd`
		`crs`
		`kms`
		`hpdp-idb (postgres)`
		`hpdp-idb-cp (pgbouncer)`
		`hpdp-as (standalone.sh)`
			`bsm`	`rsm`	`msm`

Disk Agent client	Windows	`omniinet.exe`	`vbda.exe`	`vrda.exe`	
	UNIX		`vbda`	`vrda`	
Media Agent client	Windows	`omniinet.exe`	`bma.exe`	`rma.exe`	`mma.exe`
	UNIX		`bma`	`rma`	`mma`

Problems starting Data Protector services on Windows

Problem

You do not have permission to start the services

The following error displays:

`Could not start the` *`ServiceName`* `on` *`SystemName`*`.`

`Access is denied.`

Action

The system administrator should grant you the permission to start, stop, and modify services on the system that you administer.

rProblem

Changed service account properties

If the service account does not have the permission to start the service or if the service account properties (for example, the password) have been changed, the following error displays:

```
The Data Protector Inet service failed to start due to the following
error:
The service did not start due to a logon failure.
```

Action

1. In the `Windows Control Panel > Administrative Tools > Services`, modify the service parameters.
2. If the problem persists, contact your system administrator to set up the account with appropriate permissions. The account should be a member of the `Admin` group and should have the `Log on as a service` user right.

Problem

A specific service has not been found

The location of the service is registered in the `ImagePath` registry key. If the executable does not exist in the location specified under this key, the following error displays:

`Could not start the` *`ServiceName`* `on` *`SystemName`*`. The system can not find the file specified!`

Action

Reinstall Data Protector on the Cell Manager, preserving the IDB.

Problem

MMD fails upon starting the CRS service

If the Data Protector CRS service fails to start and `mmd.exe` invokes a *Dr.Watson* diagnosis, the database log files are probably corrupted.

Action

1. Delete the `mmd.ctx` file from the *`Data_Protector_program_data`*`\server\db80` directory.
2. Restart the services using the `omnisv –stop` and `omnisv –start` commands.

Problems starting Data Protector daemons on UNIX

The following daemons run on the UNIX Cell Manager:

- In the directory `/opt/omni/lbin`:
  - Data Protector CRS daemon: `crs`
  - Data Protector IDB daemon: `hpdp-idb` (`postgres`)
    , `hpdp-idb-cp (pgbouncer)`, `hpdp-as (standalone.sh)`
  - Data Protector Media Management daemon: `mmd`

Normally, these daemons are started automatically during the system startup.

The Data Protector `Inet` process (`/opt/omni/lbin/inet`) is started by the system inet daemon when an application tries to connect to the Data Protector port (by default 5555).

To manually stop, start, or check the status of the Data Protector daemons, log on to the Cell Manager as `root` and from the `/opt/omni/sbin` directory, run:

- `omnisv -stop`
- `omnisv -start`
- `omnisv -status`

Problem

Data Protector Cell Manager daemon could not be started

The output of the `omnisv -start` command is:

```
Could not start the Cell Manager daemon.
```

Action

See `/var/opt/omni/tmp/omni_start.log` for details.

Ensure that the following configuration files exist:

- `/etc/opt/omni/server/options/global`
- `/etc/opt/omni/server/options/users/UserList`
- `/etc/opt/omni/server/options/ClassSpec`

Problem

The hpdp-idb service fails to start, reporting shared memory deficiency

On HP-UX systems, the hpdp-idb service fails to start and the following error is logged to the PostgreSQL log file (`/var/opt/omni/server/db80/pg/pg_log`):

```
FATAL: could not create shared memory segment: Not enough space
DETAIL: Failed system call was shmget(key=7112001, size=2473459712,
03600).
```

The issue appears because the hpdp-idb service cannot obtain the requested amount of shared memory due to memory fragmentation on the system.

Action

Restart the system to defragment the memory.

Problem

MMD fails upon starting the CRS service

The Data Protector CRS service fails to start and the following error is displayed:

```
[Critical] From: CRS@computer.company.com "" Time: 03/04/13 11:47:24
Unable to start MMD: Unknown internal error..
```

The database log files are probably corrupted.

Action

1. Delete the `mmd.ctx` file from the `/var/opt/omni/server/db80` directory.
2. Restart the services using the `omnisv -stop` and `omnisv -start` commands.

Other problems with Data Protector processes

Problem

Data Protector performance on Red Hat Enterprise Linux is lower than on other operating systems

Data Protector performance on Red Hat Enterprise Linux (RHEL) is negatively affected if the Name Server Caching (`nscd`) daemon is disabled.

Action

Enable Name Server Caching on RHEL, or switch to a local DNS, and then start the services using the `omnisv -start` command.

Problem

When performing a backup, the backup session stops after a certain period of time and the BSM stops responding

This issue may be caused by firewall closing an inactive connection.

Action

Ensure that the connection remains active so that the firewall does not close it. Set the following `omnirc` options:

```
OB2IPCKEEPALIVE=1
OB2IPCKEEPALIVETIME=number_of_seconds
OB2IPCKEEPALIVEINTERVAL=number_of_seconds
```

`OB2IPCKEEPALIVETIME` specifies how long the connection may remain inactive before the first keep-alive packet is sent and `OB2IPCKEEPALIVEINTERVAL` specifies the interval for sending successive keep-alive packets if no acknowledgement is received.

The options must be set on the Cell Manager system.

4 Troubleshooting the user interface

Graphical user interface problems

Data Protector graphical user interface problems are usually a result of services not running or not installed, or problems with network communication.

Connectivity and accessibility problems

Problem

No permission to access the Cell Manager

The following message displays:

```
Your Data Protector administrator set your user rights so that you do
not have access to any Data Protector functionality.
Contact your Data Protector administrator for details.
```

Action

Contact the Data Protector administrator to add you as a user and give you appropriate user rights in the cell. On how to configure user groups, see the *HP Data Protector Help* index: "user groups".

Problem

Connection to a remote system refused

On Windows systems, the response of the `telnet hostname 5555` command is `Connection refused`.

Action

- If the Data Protector `Inet` service is not running on the remote system, run the `omnisv -start` command to start it.
- If Data Protector is not installed on the remote system, install it.

Problem

Inet is not responding on the Cell Manager

The following message displays:

```
Cannot access the system (inet is not responding). The Cell Manager
host is not reachable, is not up and running, or has no Data Protector
software installed and configured on it.
```

Action

If the problem is not communication between the systems, check the installation using `telnet`.

Some components may not have been installed (properly). Check the installation steps in the *HP Data Protector Installation and Licensing Guide*.

If the installation is correct, run the `omnisv -status` command to check whether the services on the Cell Manager are running properly.

Command-line interface problems

Problem

Data Protector commands cannot be invoked

After you attempt to invoke a Data Protector command in the Command Prompt or Terminal window, the command-line interpreter reports that the command cannot be found.

Action

Extend the value of the `PATH` environment variable in your operating system configuration with the paths to the command locations. This action enables you to invoke the Data Protector commands from any directory. If the value has not been extended, the commands can only be invoked from their locations, listed in the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* and the `omniintro` man page.

5 Troubleshooting devices and media

General device and media problems

Backup devices are subject to specific Data Protector licenses. See the *HP Data Protector Product Announcements, Software Notes, and References* for details.

Problems involving device SCSI addresses are explained in detail in Appendix B of the *HP Data Protector Installation and Licensing Guide*.

Problem

Cannot access exchanger control device on Windows

Data Protector uses the SCSI mini-port driver to control backup drives and libraries. Data Protector may fail to manage devices if other device drivers are loaded on the same system. When device operations such as media formatting or scanning are started, the following error displays:

```
Cannot access exchanger control device
```

Action

On the system where the devices are located, list all physical devices configured on the system:

```
Data_Protector_home\bin\devbra -dev
```

If any of the SCSI addresses have the status value CLAIMED, they are used by another device driver.

Disable the Windows robotics driver. For instructions, see the *HP Data Protector Help* index: "robotics drivers".

Problem

SCSI device remains locked and session fails

SCSI drive or robotic control remains locked due to an incomplete SCSI reserve or release operation. The following message is displayed:

```
Cannot open device.
```

If there is a Media Agent failure, the reserved device cannot be released again. Data Protector may fail to unlock the SCSI drive or robotic control and the subsequent session cannot use it.

Action

Ensure that no other application is using this device. To unlock the SCSI drive or SCSI robotic control, the device needs to be power cycled.

Problem

Device open problem

When trying to use a DDS device, the following error displays:

```
Cannot open device (not owner)
```

Action

Check whether you are using a medium that is incompatible with the Media Recognition System. Media used with DDS drives must comply with the Media Recognition System.

Problem

Using unsupported SCSI HBAs/FC HBAs on Windows

The system fails due to the usage of unsupported SCSI HBAs/FC HBAs with backup devices.

Typically, the problem occurs when the SCSI device was accessed by more than one Media Agent at the same time or when the length of the transferred data defined by the device's block size was larger than the length supported by the SCSI HBA/FC HBA.

Action

You can change the block size of the device. For instructions, see the *HP Data Protector Help* index: "setting advanced options for devices and media".

For information on supported SCSI HBAs/FC HBAs, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Problem

Library reconfiguration failure

Configuration errors are reported during modification of an existing library configuration using the `sanconf` command after the device list file has been altered. The library configuration remains only partially created.

Action

You can recover the previous library configuration if you reuse the file with a list of hosts in your SAN environment and scan the hosts with `sanconf` again.

1. Scan the hosts in the cell:

   ```
   sanconf -list_devices mySAN.txt -hostsfile hosts.txt
   ```

2. Configure your library using the saved configuration file:

   ```
   sanconf -configure mySAN.txt -library LibrarySerialNumber LibraryName
   [RoboticControlHostName] [DeviceTypeNumber] -hostsfile hosts.txt
   ```

   The previous successful library configuration is automatically recovered.

If you add, remove, or modify the library later and configuration with the `sanconf` command fails, you can repeat the above procedure to restore the successful configuration.

Problem

An encrypted medium is marked as poor after a read or write operation

During a read or write operation on a medium that was written to using drive-based encryption, the session fails and the medium is automatically marked as poor. The following error displays:

```
Cannot read from device ([5] I/O error)
```

This happens if a read or write operation was performed on a platform that does not support drive-based encryption. The medium quality is not affected. For an up-to-date list of supported platforms, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Action

To correct the media condition status, reset the media condition by using the `omnimm -reset_poor_medium` option. For details, see the `omnimm` man page or the *HP Data Protector Command Line Interface Reference*.

Problem

Various media problems

Action

Use the **Medium Quality Statistics** functionality to detect problems with media while they are still in their early stages.

Before each medium is ejected from a drive, Data Protector uses the `SCSI log sense` command to query medium read and write statistical information. The information is written to the `media.log` file.

The medium quality statistics feature is disabled by default. To enable it, set the global option `Ob2TapeStatistics` to `1`. For instructions, see "Global options" (page 18).

If you receive media related errors during read or write operations, or if the medium is marked as poor, you can check the `media.log` file for media errors statistics.

`Media.log` contains the following error statistics, where *n* is the number of errors:

Table 5 Media error statistics

Error statistics	Description
`errsubdel=`*n*	errors corrected with substantial delays
`errposdel=`*n*	errors corrected with possible delays
`total=`*n*	total number of re-writes
`toterrcorr=`*n*	total number of errors corrected and recovered while writing
`totcorralgproc=`*n*	total number of times correction algorithm processed
`totb=`*n*	total bytes processed (write)
`totuncorrerr=`*n*	total number of uncorrected errors (write)

If a parameter has the value `-1`, the device does not support this statistics parameter. If all parameters have the value `-1`, either an error occurred during the tape quality statistics processing or the device does not support medium quality statistics.

For `total bytes processed`, statistical results are reported in bytes for most devices. However, LTO and DDS devices report data sets and groups, respectively, and not bytes.

Examples

Here are a few examples from the `media.log` file:

- Log sense write report for DLT/SDLT devices - total bytes processed.

  ```
  Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium Label= DLT10;
  Logical drive= dlt1; Errors corrected no delay= 0; Errors corrected
  delay= 0; Total= 13639; Total errors corrected= 13639; Total correction
  algorithm processed= 0; Total bytes processed= 46774780560; Total
  uncorrected errors= 0
  ```

  46774780560 bytes of native data after compression were processed (a full DLT8000 tape).

- Log sense write report for LTO devices - total data sets processed.

  ```
  Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium Label= ULT2;
  Logical drive=ultrium1; Errors corrected no delay= 0; Errors corrected
  delay= 0; Total= 0;Total errors corrected= 0; Total correction algorithm
  processed= 0; Total bytes processed= 47246; Total uncorrected errors= 0
  ```

  One data set is 404352 bytes. To calculate the amount of total bytes processed, use the following formula:

  ```
  47246 data sets * 404352 bytes = 19104014592 bytes after compression
  (a full tape)
  ```

- Log sense write report for DDS devices - total groups processed.

  ```
  Media ID from tape= 0fa0049f:3df881e9:41f3:0001;
  Medium Label= Default DDS_5; Logical drive= DDS;
  Errors corrected no delay= -1; Errors corrected delay= -1;
  Total= -1; Total errors corrected= 0; Total correction algorithm
  processed= 154;
  Total bytes processed= 2244; Total uncorrected errors= 0
  ```

DDS1/2: One group is 126632 bytes.

DDS3/4: One group is 384296 bytes.

To calculate the amount of total bytes processed, use the following formula:

```
2244 groups * 126632 bytes = 284162208 bytes after compression
(a 359 MB backup on DDS2)
```

359 MB of data was backed up, resulting in 271 MB of native data on tape.

Problem

Medium header sanity check errors

By default, Data Protector performs a medium header sanity check before a medium is ejected from a drive.

In case the medium header sanity check detects any header consistency errors on the medium, an error message is displayed and all objects on the medium are marked as failed.

If the medium header is corrupt, all objects on the affected medium are marked as failed and the medium is marked as poor.

Action

Export the medium from the IDB and restart the failed session using a different medium.

Problem

Problems with device serial number

When performing any operation involving the problematic backup device (such as backup, restore, format, scan, and so on) or robotics, the following error displays:

`Device` *`DeviceName`* `could not be opened (Serial number has changed).`

The error is reported when the device path points to a device with a different serial number than the number stored in the IDB. This can happen in the following cases:

- You misconfigured the device (for example, using the `omniupload` command, or if you configured an incorrect device file).
- You replaced the physical device without updating the corresponding logical device (reloading the new serial number).
- You physically replaced a SCSI tape drive located in a SCSI library. Either the option **Automatically discover changed SCSI address** is not enabled or the omnirc option `OB2MADETECTDRIVESWAP` is set to `0`.
- A path in a multipath device is misconfigured.

Action

1. In the Data Protector GUI, switch to the **Devices & Media** context.
2. In the Scoping Pane, expand **Devices**, right click the problematic device, and click **Properties**.
3. Click the **Control** tab and enable the **Automatically discover changed SCSI address** option.
4. Click **Reload** to update the device serial number in the IDB.

   In case of a physically replaced SCSI tape drive located in a SCSI library, make sure that the omnirc option `OB2MADETECTDRIVESWAP` is set to `1` (default). You do not need to reload the device serial number.

Problem

Cannot restore or copy corrupt data

By default, CRC values are always checked when available on a tape and data found corrupt by CRC mismatch is never restored or copied. However, in certain situations, you may still want to restore or copy such data.

Action

Temporarily set the omnirc option `OB2CRCCHECK` on the Media Agent host to 0. After the recovery of corrupt objects (data) revert the setting to the default value (`1`).

Problem

Common hardware-related problems

Action

Check the SCSI communication between the system and the device, such as adapters or SCSI cables and their length. Try running an OS-provided command, such as `tar`, to verify that the system and the device are communicating.

ADIC/GRAU DAS and STK ACS libraries problems

Problem

ADIC/GRAU DAS library installation failed

Action

1. Install a Media Agent on the client controlling the GRAU robotics (PC/robot).
2. Install a Media Agent on the clients where a drive is connected (PC/drive).
3. Copy `aci.dll + winrpc.dll + ezrpcw32.dll` to `winnt\system32` and *`Data_Protector_home`*`\bin` directory.
4. Create the `aci` directory on PC/robot.
5. Copy `dasadmin.exe`, `portmapper`, and `portinst` to the `aci` directory.
6. Start `portinst` to install `portmapper` (only on PC/robot).
7. Install the `mmd` patch on the Cell Manager.
8. Restart the system.
9. In `Windows Control Panel > Administrative Tools > Services`, check if `portmapper` and both `rpc` services are running.
10. On the OS/2 system within the GRAU library, edit the file `/das/etc/config`. Add a client called OMNIBACK containing the IP address of the PC/robot.

Problem

You cannot see any drives

Action

Run the following commands from PC/robot:

1. `dasadmin listd`
2. `dasadmin all DLT7000 UP` *`AMUCLIENT`*
3. `dasadmin mount` *`VOLSER`* (then press the `UNLOAD` button on the drive)
4. `dasadmin dismount` *`VOLSER`* or `dasadmin dismount -d` *`DRIVENAME`*)

Where:

- *`AMUCLIENT`* = `OMNIBACK`
- *`VOLSER`* is for example `001565`

- *DRIVENAME* is for example DLT7001
- all stands for allocate

If you are not successful with these commands (communication to DAS Server (OS/2)), try running these commands on the OS/2 system from the /das/bin/ directory.

When running these commands from the OS/2 system, use *AMUCLIENT* = AMUCLIENT.

1. Log in to the AMU client. Common logins are:

   user: Administrator pwd: administrator

   user: Supervisor pwd: supervisor
2. It may be necessary to set the media type:set ACI_MEDIA_TYPE set ACI_MEDIA_TYPE=DECDLT
3. Restart the library:
   a. Shut down OS/2 and then switch off the robotics.
   b. Restart OS/2 and when OS/2 is ready, the AMU log will display that the robotics is not ready. Switch on the robotics.

Problem

GRAU CAPs are not configured properly

Action

You can only move media from the CAP to a slot and then to a drive using the device's robotics. Use the import and export commands, for example:

```
import CAP: I01
import CAP range: I01-I03
export CAP: E01
export CAP range: E01-E03
```

Problem

The library operations fail

Action

Use the following syntax when you using the Data Protector uma utility to manage the GRAU and STK library drives:

uma -pol *POLNUMBER* -ioctl *LIBRARYNAME* -type *MEDIATYPE*

where *POLNUMBER* is 8 for GRAU and 9 for STK.

For example: uma -pol 8 -ioctl grauamu

The default media type is DLT.

6 Troubleshooting backup and restore sessions

Full backups are performed instead of incrementals

You specified an incremental backup, but a full backup is performed. There are several possible reasons for this behavior:

Reason

No previous full backup

Before performing an incremental backup of an object, Data Protector requires a full backup as a base for comparison to determine which files have changed and consequently need to be included in the incremental backup. If a protected full backup is not available, a full backup is performed.

Action

Ensure that a protected full backup of the object exists.

Reason

The description has changed

A backup object is defined by the client, mount point, and description. If any of these three values changes, Data Protector considers it as a new backup object and performs a full backup instead of an incremental.

Action

Use the same description for full and incremental backups.

Reason

Trees have changed

A protected full backup already exists but with different trees than the incremental backup. There are two possible reasons for this:

- You have changed the trees in the backup specification of the protected full backup.
- You have created multiple backup specifications with the same backup object but different trees specified for the backup object.

Action

If you have multiple backup specifications with the same backup object, change the (automatically generated) universal description of the backup object. Data Protector will consider them as new objects and a full backup will be run. After a full backup is performed, incremental backups will be possible.

Reason

The backup owner is different

If your backups are configured to run as private, the user starting the backup is the owner of the data. For example, if user A performs a full backup and user B tries to start an incremental backup, the incremental backup will be performed as a full backup. This is because the data for user A is private and cannot be used as a base for user B's incremental backup.

Action

Configure backup ownership in the advanced backup specification options. The backup owner should be in the `Admin` user group. This will make this user the owner of all backups based on

this backup specification, regardless of who actually starts the backup session. For instructions, see the *HP Data Protector Help* index: "setting backup options".

Reason

Enhanced incremental is not performed after the upgrade

This problem may occur on Windows, HP-UX, and Linux systems. If you upgraded Data Protector from version A.06.11, the old enhanced incremental backup repository cannot be used with the new product version anymore. Therefore, a full backup is performed. During a full backup, a new enhanced incremental backup repository is created at the following location:

Windows systems: `Data_Protector_home\enhincrdb`

UNIX systems: `/var/opt/omni/enhincrdb`

Action

Run the full backup. The new enhanced incremental backup repository will be created and you will be able to perform enhanced incremental backups.

Data Protector fails to start a session

Problem

Interactive session fails to start

Every time a backup is started, the permission to start a backup session is required and checked for the user who is currently running Data Protector. If the user does not have this permission, the session cannot be started.

Action

Make sure the user is in a user group with appropriate user rights. On how to configure user groups, see the *HP Data Protector Help* index: "user groups".

Problem

Scheduled sessions no longer run

Scheduled sessions no longer run since the Data Protector system account, which is supposed to start scheduled sessions, is not in the `Admin` user group on the Cell Manager.

This account is added to the Data Protector `Admin` group on the Cell Manager at installation time. If this is modified and the permission for this account is removed, or if the service account changes, scheduled sessions no longer run.

Action

Add the Data Protector account to the `Admin` user group on the Cell Manager.

Problem

Session fails with status No licenses available

A backup session is started only after Data Protector has checked the available licenses. If no licenses are available, the session fails and Data Protector issues the session status `No licenses available`.

Action

Obtain information on available licenses by running:

```
omnicc -check_licenses -detail
```

Request new licenses and apply them. For licensing details, see the *HP Data Protector Installation and Licensing Guide*.

Problem

Scheduled backups do not start (UNIX specific)

Action

Run the `crontab -l` command to check whether the `omnitrig` program is included in the `crontab` file. If the following line does not display, the `omnitrig` entry was automatically added by Data Protector:

```
0,15,30,45 * * * * /opt/omni/sbin/omnitrig
```

Restart the Data Protector daemons by running `omnisv -stop` and `omnisv -start`.

Mount request is issued

Mount request although media are in the device

During a backup session, Data Protector issues a mount request, although media are available in the backup device. There are several possible reasons for this:

Reason

The media in the device are in a media pool that has the Non Appendable policy

Although there is still available space on the media, the media will not be used because of the `Non Appendable` policy of the pool.

Action

Modify the media pool policy to `Appendable` to enable the appending of backups until the media are full.

Reason

The media in the device are not formatted

By default, media are not formatted automatically. If no formatted media are available, a mount request is issued.

Action

Format the media. For instructions, see the *HP Data Protector Help* index: "formatting media".

Reason

The media in the device are different from those in the preallocation list

The media in the device are formatted but are different from those in the preallocation list of the backup specification, and the media pool specified has the `Strict` policy.

If you use a preallocation list of media in combination with the `Strict` media policy, the exact media specified in the preallocation list need to be available in the device when a backup is started.

Action

- To use media available in the device in combination with the preallocation list, modify the media pool policy to `Loose`.
- To use any available media in the device, remove the preallocation list from the backup specification. Do this by changing backup device options in the backup specification.

Mount request for a file library

Problem

File library device disk full

When using a file library device, you may receive a mount request with the following message:

```
There is no disk space available for file library "File Library Device".
Please add some new disk space to this library.
```

Action

Create more space on the disk where the file library is located:

- Free some space on the disk where the files are being backed up.
- Add more disks to the system where the file library device resides.

File name problems

Problem

File names or session messages are not displayed correctly in the Data Protector GUI

Some file names or session messages containing non-ASCII characters are displayed incorrectly. This happens when an inappropriate character encoding is used to display file names and session messages in the Data Protector GUI.

Action

Specify the appropriate encoding. From the **View** menu, select **Encoding** and select the appropriate coded character set.

Problem

Problems with non-ASCII characters in file names

In mixed platform environments, there are some limitations regarding handling of file names containing non-ASCII characters in the Data Protector GUI, if the IDB has not yet been converted to a new internal character encoding. For information, see the *HP Data Protector Installation and Licensing Guide*.

Action

Convert the IDB to the new internal character encoding and then upgrade Disk Agents on your clients.

If you do not perform the conversion of the IDB, a workaround for trees that cannot be selected for backup or restore is to select a tree above the desired tree, assuming that the parent tree can be successfully specified (for example, its name consists of ASCII characters only).

For backups, this means that more data will be backed up. Usually, this is not an issue since typically entire disks or at least major trees are backed up (for example, `/home` or `\My Documents`). For restores, you can choose to restore the parent tree to a new location, using the `Restore as` or `Restore to new location` option, to prevent any damage by restoring more than just the desired file or directory.

For restores, when in doubt, restore one tree or file per restore session. A message `"Nothing restored"` indicates that the tree was not restored. If the default file conflict handling is used (`Keep most recent`), this message may also indicate that the files are already on the disk and were not overwritten.

The `Restore Into` option, on the other hand, would restore the files into the specified path. When only a few files are restored, you can also use the `List restored data` option.

For internationalization limitations, see the *HP Data Protector Help* index: “internationalization”.

Cluster problems

Problem

IDB services are not synchronized

On UNIX systems, when performing a restore of the IDB to a different location in a MC/ServiceGuard environment and one or more cluster nodes are offline, the IDB services are not synchronized for all nodes after the session completes.

Action

To synchronize the location of the IDB data files for all nodes in a cluster environment, execute the `omnidbutil -sync_srv` command on the active cluster node.

Problem

An incremental filesystem backup of a cluster shared volume using the Windows NTFS Change Log Provider falls back to a full backup after a cluster failover

When performing an incremental filesystem backup of a cluster shared volume that has the option **Use native Filesystem Change Log Provider if available** selected in a backup specification, a full backup is performed instead and the following error message is displayed:

`[Major] From: VBDA@`*`Host Name`* `"F:" Time:` *`Date Time`*

```
The Change Log Provider could not use the Directory Database. This
session will use the normal file system traversal.
```

Action

To make sure that incremental backups are correctly performed, create a symbolic link of the Change Log Provider database to a separate cluster shared volume as follows:

1. Select a shared disk to which you can direct the Change Log Provider database for shared volumes. In case of the Data Protector cluster Cell Manager, you can choose the Data Protector shared disk.
2. Create a directory on the shared disk, for example: `E:\Omniback\clp`.
3. Go to the directory *`Data_Protector_home`*`\clp` and create a symbolic link to the created directory.

   For example, to back up a shared disk `J`, execute `mklink /D J E:\Omniback\clp\J`, where `E:\Omniback\clp\J` is a symbolic link created for a shared disk `J`, and `E` is a cluster shared volume accessible from the other cluster nodes.

Create the Change Log Provider database link for the shared volume on all cluster nodes on which incremental backups are performed after a cluster failover.

Problem

Restore problems if the Cell Manager is configured in a cluster

A backup with a cluster-aware Data Protector Cell Manager was performed with the `Restart backup of all objects` backup option enabled. A failover occurred during the backup and the backup session was restarted on another cluster node and successfully finished. When trying to restore from the last backup, the following error is reported although the session finished successfully:

```
You have selected a version that was not successfully completed. If you
restore from such a backup, some or all the files may not be restored
correctly.
```

If the system times on the Cell Manager cluster nodes are not synchronized, it is possible that the failed backup has a newer timestamp than the restarted backup. When selecting data for restore, the last backup version is selected by default, resulting in a restore from the failed backup.

Action

To restore from the last successful backup, select the correct backup version for restore.

To prevent such errors, it is recommended to configure a time server on your network. This will ensure automatic synchronization of the system times on your Cell Manager cluster nodes.

Problem

Backup of CONFIGURATION object of a Microsoft Cluster Server node fails

On a Windows Server 2008 system, backup of the CONFIGURATION object on a cluster node fails with the following error:

```
[Minor] From: VBDA@computer.company.com "CONFIGURATION:" Time: Date
Time[81:141] \Registry\0.Cluster Cannot export configuration object:
(Details unknown.) => backup incomplete
```

Action

Restart the Data Protector Inet service under the user account that is used to run Cluster Service, and restart the backup.

Other problems

Problem

Backup protection expiration

When scheduling backups, you have set the same protection period for full and incremental backups, which means that incremental backups are protected for the same duration as the relevant full backup. Consequently, your data will actually only be protected until the full backup expires. You cannot restore incremental backups that are based on expired full backups.

Action

Configure the protection for your full backups so that they are protected for longer than your incremental backups.

The time difference between the protection for the full backup and the incremental backup should be the amount of time between the full backup and the last incremental backup before the next full backup.

For example, if you run incremental backups Monday through Friday and full backups on Saturday, you should set the protection of the full backup to at least 6 days more than for the incremental backups. This will keep your full backup protected and available until your last incremental backup expires.

Problem

Intermittent “Connection refused” error

The backup session aborts with a critical error:

```
Cannot connect to Media Agent on system computer.company.com, port 40005
(IPC Cannot Connect System error: [10061] Connection refused)
```

This problem may occur if a Media Agent is running on a non-server edition of Windows and the Disk Agent concurrency is set to more than `5`. Due to the TCP/IP implementation on non-server editions of Windows, the operating system can accept only 5 incoming connections simultaneously.

Action

Set the Disk Agent concurrency to `5` or less.

It is recommended to use server editions of Windows for systems involved in intensive backup operations, such as the Cell Manager, Media Agent clients, application agent clients, file servers, and so forth.

Problem

Enhanced incremental backup fails because of a large number of files

On HP-UX systems, enhanced incremental backup fails when a large number of files is being backed up.

Action

To enable that a Disk Agent accesses more memory for enhanced incremental backup on HP-UX, set the tunable kernel parameter `maxdsiz` as follows:

HP-UX 11.11 systems:

```
kmtune set maxdsiz=2147483648

kmtune set maxdsiz_64bit=2147483648
```

HP-UX 11.23/11.31 systems:

```
kctune set maxdsiz=2147483648

kctune set maxdsiz_64bit=2147483648
```

Problem

Unexpected mounted filesystems detected when restoring a disk image

When restoring a disk image, you get a message that the disk image being restored is a mounted filesystem and will not be restored:

```
Object is a mounted filesystem => not restored.
```

This happens when an application on the disk image leaves some patterns on the disk image. The patterns confuse the system call that verifies whether the filesystem on the disk image is mounted or not, so the system call reports that there is a mounted filesystem on the disk image.

Action

Before you start a restore, erase the disk image on the Data Protector client with the disk image being restored:

```
prealloc null_file 65536
dd if=null_file of=device_file
```

where *`device_file`* is a device file for the disk image being restored.

Problem

Problems with application database restores

When trying to restore a database, it fails with one of the following messages:

- `Cannot connect to target database`
- `Cannot create restore set`

A poorly configured DNS environment could cause problems with database applications. The problem is as follows:

When backing up a database, the agent that starts on the client where the database is located logs the client name to the database as *`computer.company.com`*.

At restore time, the Restore Session Manager tries to restore to *`computer.company.com`*, but it cannot because it knows this client only as *`computer`*. The client name cannot be expanded to the full name because the DNS is improperly configured.

This situation can also be the other way around, where DNS is configured on the Cell Manager and not on the Application Client.

Action

Set up the TCP/IP protocol and configure DNS properly. For information, see Appendix B in the *HP Data Protector Installation and Licensing Guide*.

Problem

Asynchronous reading does not improve backup performance

With the **Asynchronous reading** (Windows specific) option selected in the backup specification, there is no backup performance improvement, or there may even be performance degradation.

Action

1. Check if the omnirc option `OB2DAASYNC` is set to 0. Either set the option to 1 to always use asynchronous reading, or comment out the option and use the **Asynchronous reading** option in the backup specification.
2. Consider if asynchronous reading is suitable for your backup environment. In general, asynchronous reading is suitable for files larger than 1 MB. Additionally, you can try to fine-tune the omnirc option `OB2DAASYNC_SECTORS`. As a rule, the size of your files (in bytes) should be 2-3 times larger than the value of the option.

Problem

Backup of the IIS configuration object fails on Windows Vista, Windows 7, and Windows Server 2008 systems

On a Windows Vista, Windows 7, and Windows Server 2008 system, while backing up the IIS configuration object, the following error is reported:

```
[Minor] From: VBDA@computer.company.com "CONFIGURATION:" Time: Date &
Time [81:141] \IISDatabase Cannot export configuration object: (Details
unknown.) => backup incomplete.
```

Action

Install the **IIS Metabase and IIS 6 configuration compatibility** component under **IIS 6 Management Compatibility** and restart the backup.

Problem

Restore of a subtree from a volume with hard links present fails

Restore of a subtree from a volume with hard links present fails with the following error message:

```
Lost connection to Filesystem restore DA named ""
```

Action

Set the global option `RepositionWithinRestoredObject` to `0` if you are restoring trees with hard links.

Although setting this option to `0` may make the restores slightly slower, it is needed whenever restoring hard links.

By default, this option is set to `1`.

Problem

On Mac OS X, backup sessions fail due to insufficient amount of shared memory

On Mac OS X, if you increase the device block size, the backup session may fail with the following error message:

```
[80:1003] Cannot allocate/attach shared memory (IPC Cannot Create Shared
Memory Segment System error: [12] Cannot allocate memory ) => aborting.
```

Action

Increase the kernel parameter `kern.sysv.shmmax` (maximum size of a shared memory segment) to a larger value. HP recommends to set the parameter to 32 MB.

7 Troubleshooting object operations sessions

Object copy problems

Problem

Fewer objects are copied than expected

With post-backup or scheduled object copy, the number of objects that match the selected filters is higher than the number of objects that are actually copied.

The following message is displayed:

```
Too many objects match specified filters.
```

Action

- Tighten the criteria for object version selection.
- Increase the maximum number of objects copied in a session by setting the global option `CopyAutomatedMaxObjects`. For instructions, see "Global options" (page 18).

Problem

Not all objects in the selected library are copied

With post-backup or scheduled object copy, some objects that reside on media in the selected library are not copied. This happens if an object does not have a complete media set in the selected library.

Action

Insert the missing media into the selected library, or select the library that has a complete media set for these objects.

Problem

Mount request for additional media is issued

In an interactive object copy session from the Media starting point, you selected a specific medium. A mount request for additional media is issued. This happens if an object residing on the medium spans to another medium.

Action

Insert the required medium into the device and confirm the mount request.

Problem

When creating an object copy, the protection end time is prolonged

When creating an object copy, the protection end time is not inherited from the original object. The protection length is copied, but the start time is set at the object copy creation time and not at the object creation time. This results in a longer protection then for the original. The more time passes between the original backup and the object copy session, the bigger the difference between the protection end times.

For example, if the object was created on September 5, with the protection set to 14 days, the protection will expire on September 19. If the object copy session was started on September 10, the object copy protection will expire on September 24.

In some cases, such behavior is not desirable and the protection end time must be preserved.

Action

Set the global option `CopyDataProtectionEndtimeEqualToBackup` to `1` to ensure that the object copy protection end time is equal to backup object protection end time. By default, the option is set to 0.

Problem

Replicating session with multiple objects stops responding

When replicating a session onto another device, the session stops responding. The session output provides the following information:

```
[Normal] From: BMA@company.com "d2d1_1_gw1 [GW
26177:1:15198446278003495809]" Time: 3/21/2013 9:13:06 AM
COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"
```

The problem is known to occur in a dual IP stack network configurations with HP-UX Media Agent.

Action

When configuring a dual IP stack network, add a separate entry for IPv6 localhost addresses to the `/etc/hosts` file on the Media Agent client.

For example, you have the following entry in your `hosts` file:

```
::1 localhost loopback
```

To resolve the issue, add the following line for IPv6 addresses:

```
::1 ipv6-localhost ipv6-loopback
```

Object consolidation problems

Problem

Object consolidation of many points in time opens too many files

If you start an object consolidation operation with many points in time, Data Protector reads all media necessary to complete the operation. This opens all files at the same time. When Data Protector opens more files than the number allowed by your operating system, a message similar to the following one is displayed:

```
|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128"
Time: time /omni/temp/Cons_Media/AFL1/0a1109ab54417fab351d15500c6.fd
Cannot open device ([24] Too many open files)
```

Action

Increase the maximum number of allowed files.

HP-UX systems:

1. Set the maximum number of open files using the System Administration Manager (SAM):

   Select **Kernel Configuration** > **Configurable parameters**. And then, **Actions** > **Modify Configurable Parameter**. Enter the new **maxfiles_lim** and **maxfiles** values in the **formula/value** field.
2. Restart your computer after applying the new values.

Solaris systems:

1. Set the maximum number of open files by editing the `/etc/system` file. Add the following lines:

   ```
   set rlim_fd_cur=value
   set rlim_fd_max=value
   ```
2. Restart your computer after applying the new values.

8 Troubleshooting the Data Protector Internal Database (IDB)

Problems due to missing directories

You can find a list of IDB directories that should exist on the Cell Manager in the directory *Data_Protector_program_data*\server\db80 (Windows systems) or /var/opt/omni/server/db80 (UNIX systems).

Problem

Cannot open database/file or Database network communication error

If one or several IDB data files or directories are missing, the following errors are displayed when Data Protector tries to access the IDB:

- `Cannot open database/file`
- `Database network communication error`

Action

Reinstall the IDB data files and directories:

1. Reinstall Data Protector.
2. Restart the Cell Manager.

Problem

Cannot access the Data Protector

When the Data Protector GUI tries to connect to the Cell Manager, the following error message is displayed if the Data Protector temporary directory is missing:

```
Cannot access the Cell Manager system. (inet is not responding) The
Cell Manager host is not reachable or is not up and running or has no
Data Protector software installed and configured on it.
```

Action

1. On the Cell Manager, close the Data Protector GUI.
2. Initiate the maintenance mode:

   ```
   omnisv -maintenance
   ```
3. Manually create the directory `tmp` in:

   Windows systems: *Data_Protector_program_data*

   UNIX systems: /var/opt/omni
4. Quit the maintenance mode:

   ```
   omnisv -maintenance –stop
   ```
5. Restart the Data Protector GUI.

Problems during backup or import

Problem

File names are not logged to the IDB during backup

When performing backups using Data Protector, file names are not logged to the IDB if:

- You have selected the `No log` option for backup.
- The DCBF part of the IDB is running out of space, or the disk where the IDB is located is running low on disk space. An error in the session output informs you about this.

Action

- Check if you have selected the `No log` option for backup.
- Check the session messages of the backup session for warnings and errors.

Problem

The BSM or RSM is terminated during the IDB backup or import

If the BSM or RSM get terminated during the IDB backup or import session, the following error is displayed:

```
IPC Read Error System Error: [10054] Connection reset by peer
```

In the Internal Database context of the Data Protector GUI, the session status is still marked as `In Progress` but the session is actually not running.

Action

1. Close the Data Protector GUI.
2. Execute the `omnidbutil -clear` command to set the status of all sessions that are actually not running but are marked as `In Progress` to `Failed`.
3. Execute the `omnidbutil -show_locked_devs` command to see if any devices and media are locked by Data Protector.
4. If there are, execute the `omnidbutil -free_locked_devs` to unlock them.
5. Restart the Data Protector GUI.

Problem

The MMD is terminated during the IDB backup or import

If the media management daemon (MMD) is terminated during the IDB backup or import session, the following errors are displayed:

- `Lost connection to MMD`
- `IPC Read Error System Error: [10054] Connection reset by peer`

If the MMD services/processes are not running:

- The output of the `omnisv -status` command indicated that the MMD service/process is down.
- You notice the following:

  Windows systems: In the Windows Task Manager, the Data Protector MMD process (`mmd.exe`) is not displayed.

  UNIX systems: When listing the Data Protector processes using the ps `-ef | grep omni` command, the Data Protector MMD process (`/opt/omni/lbin/mmd`) is not displayed.

Action

1. Close the Data Protector GUI.
2. Execute the `omnisv -stop` command to stop the Data Protector services/processes.
3. Execute the `omnisv -start` command to start the Data Protector services/processes.
4. Execute the `omnisv -status` command to check if all the services/processes are running.

Problem

The DC binary files are corrupted or missing

When browsing backed up objects in the `Restore` context of the Data Protector GUI, the following error displays:

```
Open of Detail Catalog Binary File failed
```

- The `omnidbcheck -bf` command reports that one or several DC binary files are missing or are of incorrect size, or the `omnidbcheck -dc` command reports that one or several DC binary files are corrupted.
- The `debug.log` file on the Cell Manager contains one or several entries on Data Protector not being able to open a DC binary file.

Action

Recreate DC binary files by importing catalog from media. For instructions, see the *HP Data Protector Help* index: "minor IDB corruptions in DCBF".

Problem

The Internal Database backup fails

The session for backing up the Data Protector Internal Database fails with the following error:

```
[Critical] From: OB2BAR_POSTGRES_BAR@computer.company.com "DPIDB"  Time: 4/2/2013 4:05:20 PM
                 Error while running the PSQL script
[Normal] From: BSM@computer.company.com "idb"  Time: 4/2/2013 4:05:20 PM
                 OB2BAR application on "computer.company.com" disconnected.
[Critical] From: BSM@computer.company.com "idb"  Time: 4/2/2013 4:05:20 PM
                 None of the Disk Agents completed successfully. Session has failed.
```

If the Data Protector Inet service is running under a domain user account, the problem is most probably caused by insufficient Security Policy privileges for that account.

Action

Grant the Windows domain user account that is used for the Data Protector Inet service the following Windows operating system Security Policy privileges, and restart the session afterwards:

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

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

Performance problems

Problem

Browsing for restore is slow

When browsing object versions and single files for restore in the Data Protector GUI, it takes a long time before the information is read from the IDB and displayed. This happens because the number of object versions of the selected object in the IDB is too large.

Action

Set the time interval for browsing object versions for restore:

- For a specific restore, set the `Search interval` option in the Source page.
- Globally, for all subsequent restores:
  1. In the **File** menu, click **Preferences**.
  2. Click the **Restore** tab.
  3. Set the **Search interval** option and click **OK**.

Other problems

Problem

Interprocess communication problem because Database Session Manager is not running

While the Data Protector GUI is accessing the IDB, if the Database Session Manager process on the Cell Manager dies or is terminated, the following error displays:

```
Interprocess communication problem
```

On the Cell Manager, you notice the following:

Windows systems: In the Windows Task Manager, the Data Protector process `dbsm.exe` is not displayed.

UNIX systems: When listing the Data Protector processes using the ps `-ef | grep omni` command, `/opt/omni/lbin/dbsm` is not displayed.

Action

Restart the Data Protector GUI.

Problem

The IDB is running out of space

A part of the IDB is running out of space. The `IDB Space Low` notification is issued.

Action

Extend the IDB size. For information, see the *HP Data Protector Help* index: "extending IDB size".

Problem

MMDB and CDB are not synchronized

The MMDB and CDB may not be synchronized when:

- The MMDB and CDB contain information from different periods in time. This may be the result of importing the CDB and the MMDB (the `omnidbutil -readdb` command) from files generated in separate export sessions (the `omnidbutil -writedb` command).
- In a MoM environment, when the local CDB and CMMDB are not synchronized. This may be a result of a CMMDB restore.

Data Protector reports when an object in the IDB has no medium assigned or when data protection for a medium is not correctly set.

Action

Synchronize the MMDB and CDB by executing the following command on Cell Manager:

`omnidbutil -cdbsync` *`Cell_Manager_Hostname`*

In a MoM environment, execute the command on the MoM Manager (with the CMMDB installed) for every Cell Manager, specifying its hostname as the argument.

Problem

IDB is corrupted

Any of the following messages can be displayed:

- `Database is corrupted.`
- `Interprocess communication problem.`
- `Cannot open Database/File.`
- `Error - Details Unknown.`

Action

Recover the IDB. For information, see the *HP Data Protector Help* index: "IDB recovery".

Problem

Enhanced incremental backup database is corrupted

After the upgrade on the Windows, HP-UX, and Linux systems, the new enhanced incremental database is corrupted or the enhanced incremental repository cannot be used for an enhanced incremental backup.

Action

Delete the enhanced incremental backup repository from the following location:

Windows systems: *Data_Protector_home*\enhincrdb

UNIX systems: /var/opt/omni/enhincrdb

A new enhanced incremental backup repository will be created when the full backup is run.

Problem

Merging of a MMDB into the CMMDB fails

After executing the `omnidbuitl -mergemmdb` command, merging of a client cell's MMDB into the CMMDB fails with the following error: `Could not establish connection`.

Action

Before using the `omnidbutil -mergemmdb`, a remote database connection needs to be enabled. To enable establishing a connection, modify the configuration file and restart the services:

1. On MoM client, navigate to:

   Windows systems: *Data_Protector_program_data*\server\db80\pg

   UNIX systems: /var/opt/omni/server/db80/pg
2. Open `pg_hba.conf` file in text editor and add the following line:

   ```
   host hpdpidb hpdpidb_app CMMDB_Server_IP_Address/32 trust
   ```
3. Restart services on MoM client.

   ```
   omnisv -stop
   omnisv -start
   ```

9 Troubleshooting reporting and notifications

Reporting and notification problems

Problem

Data Protector GUI stops responding when the send method is e-mail on Windows

If you use Microsoft Outlook XP with the latest security patch installed, the following problem appears: when you add a report to a report group specifying e-mail as a send method, and then try to start the report group, the GUI stops responding. The same happens if you configure a notification and select the e-mail send method.

The cause of the problem is that Outlook requires user interaction before sending an e-mail notification. This feature cannot be disabled since it is a part of the Outlook security policy.

Action

- If an SMTP server is available on your network, specify `E-mail (SMTP)` as the send method. This method is the recommended e-mail send method. See the *HP Data Protector Help* index: "send methods".
- Use the Data Protector CLI to start reports:

  ```
  omnirpt -report licensing -email EmailAddress
  ```

  When a warning asking whether you allow sending e-mail on your behalf appears, click `Yes` to receive the report.

  For more information on how to customize security settings, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Problem

SNMP send method fails

When sending a report as an SNMP trap, the report does not reach the destination.

Action

Use the SNMP trap send method only for reports that do not exceed the maximum size of the configured SNMP trap.

10 Troubleshooting HP Data Protector Help

Introduction

The Data Protector Help consists of two parts:

- Help topics provide conceptual information, step-by-step procedures, and examples.
- Context-sensitive Help is the dynamic, context-sensitive part of the Help, explaining screens and options in the Data Protector GUI. It is displayed by the Data Protector GUI component called Help Navigator.

The Help is available in two formats: Microsoft HTML Help and WebHelp. Current preferences for the Help viewer in the Data Protector GUI determine which format is used.

Troubleshooting Help

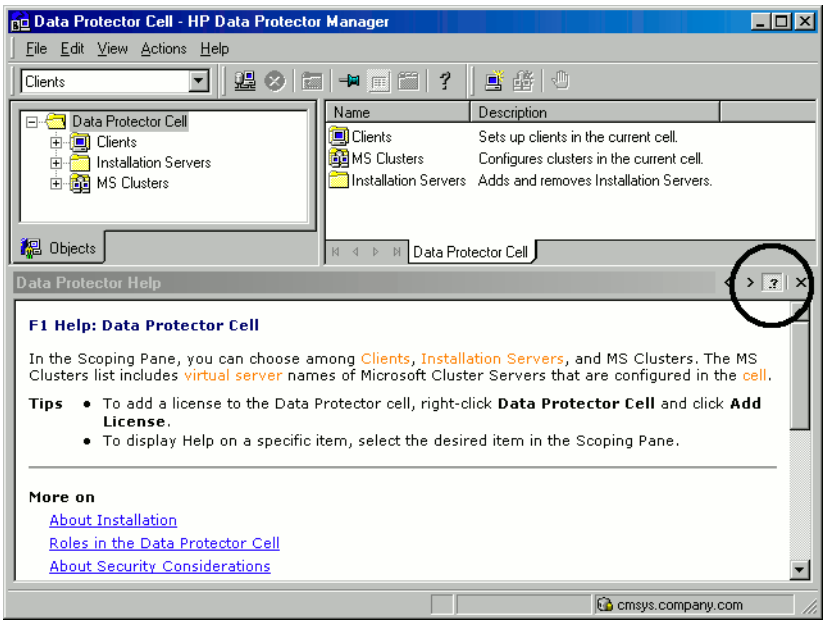
Problem

The Help Navigator contents do not change in parallel with the Data Protector windows

Action

- If you use the Microsoft HTML Help viewer for viewing the *HP Data Protector Help* in the HTML Help format (default selection), ensure that the button shown in the figure below is selected.

Figure 3 Enabled tracking button



- If you use the system default web browser for viewing the *HP Data Protector Help* in the WebHelp format, go to **File** menu, click **Preferences** and select the **Enable context-sensitive Help Navigator** option. Then restart the Help Navigator.

11 Before calling support

Before calling your support representative

If you cannot solve your problem, report it. Before contacting the HP Customer Support Service, ensure that:

- You have performed the general checks. See "General checks" (page 15).
- You have checked if your problem is described in this guide, or other applicable guides.
- You have collected the relevant data about the problem you will send to the HP Customer Support Service: a description of your problem, including the session output (or equivalent output, depending on the type of problem), and a description of your environment.

The HP Customer Support Service will then provide you with further instructions. You might be asked to:

1. Run Data Protector in the debug mode.
2. Prepare the generated data for sending to the HP Customer Support Service.

These procedures are described in the following sections. Note that you only need to perform them when the HP Customer Support Service requests this.

Debugging

Collect debugs only when the support organization requires them to resolve a technical issue. When Data Protector runs in the debug mode, it creates debug information that consumes a large amount of disk space. Consult the support organization about the required detail level and environmental conditions for debugging.

Enabling debugging

You can start Data Protector in the debug mode in different ways. For debugging options, see "Debug syntax" (page 58).

IMPORTANT: When Data Protector runs in the debug mode, debug information is generated for every action. For example, if you start a backup specification in the debug mode, Disk Agents deliver output on each client backed up in this backup specification.

NOTE: On Windows Vista, Windows 7, and Windows Server 2008 systems, to enable debugging of network share backup and restore sessions, write permissions for the operating system account running such sessions must be assigned to the folder *Data_Protector_program_data*\tmp.

Using the Data Protector GUI

In the **File** menu, click **Preferences**, and then click the **Debug** tab. Specify the debug options and restart the GUI. The GUI will restart in the debug mode.

Using the trace configuration file

Edit the trace configuration file, located in:

Windows systems: *Data_Protector_program_data*\Config\server\Options\trace

UNIX systems: /etc/opt/omni/server/options/trace

Using the OB2OPTS environment variable

Debugging parameters for Data Protector integrations can be set using the OB2OPTS environment variable. You will be instructed how to set this variable by your Support Representative.

Using the scheduler

To debug scheduled sessions, edit the schedule file, located at:

Windows systems: *Data_Protector_program_data*\Config\server\Schedules or *Data_Protector_program_data*\Config\server\Barschedules

UNIX systems: /etc/opt/omni/server/schedules or /etc/opt/omni/server/barschedules

Add debugging parameters in the first line of the file.

NOTE: Before you edit the file, make a copy of it, as the changes have to be reverted when debugging is no longer desired.

Example

```
-debug 1-200 sch.txt
-full
-only 2010
      -day 14 -month Dec
      -at 22:00
```

Debug syntax

Almost all Data Protector commands can be started with an additional `-debug` parameter that has the following syntax:

`-debug 1-200[,C:`*n*`][,T:`*s*`][,U] `*XYZ*` [`*Host*`]`

where:

- `1-200` is the debug range. Specify the range 1-200 unless instructed otherwise. Specify optional parameters as a part of the range parameter, separated by commas:
  - `C:`*n* limits the size of debug files to *n* kilobytes. The minimum value is 4 (4 kB) and the default value is 1024 (1 MB).

    For more information, see "Limiting the maximum size of debugs" (page 58).
  - `T:`*s* is the timestamp resolution, where the default value is 1, 1000 means the resolution is one millisecond and 0 means timestamps are turned off.

    On some platforms, millisecond resolution might not available.
  - `U` is the Unicode flag. If it is specified, the debug files on Windows are written in the Unicode format.
- *XYZ* is the debug postfix, for example `DBG_01.txt`.
- *Host* is a list of clients where debugging is turned on.

  Use this option to run the debugging only on the clients specified. Delimit multiple clients by spaces. Enclose the list in quotes, for example: `"computer1.company.com computer2.company.com"`.

Limiting the maximum size of debugs

Data Protector can run in a special debug mode called **circular debugging**. In this mode, debug messages are added until the size of the debug file reaches a preset size (*n*). The counter is then reset and the oldest debug messages are overwritten. This limits the debug file size, but does not affect the latest records.

Using this mode is recommended only if the problem occurs near the end of the session or if Data Protector aborts or finishes soon after the problem has occurred.

With circular debugging turned on, an estimate of the maximum required disk space is as follows:

Table 6 Disk space required for circular debugging

System	Maximum disk space required
Media Agent client	`2*n [kB]` for each running Media Agent in a backup or restore session
Disk Agent client	`2*n [kB]` for each mount point in a backup or restore session
Cell Manager	`2*n [kB]`
Integration client	`2*n [kB] * Parallelism`

For Inet and CRS debugging, the upper limit cannot be reliably determined because separate debug files are produced for various actions.

Names and locations of debug files

The debug postfix option is used for creating debug files in the following directory:

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012: `Data_Protector_program_data\tmp`

Other Windows systems: `Data_Protector_home\tmp`

UNIX systems: `/tmp`

The files are named

`OB2DBG_DID__Program_Host_PID_XYZ`

where:

- `DID` (debugging ID) is the process ID of the first process that accepts the debugging parameters. This is the ID of the debugging session and is used by all further processes.
- `Program` is the code name of the Data Protector program writing the debug file.
- `Host` is the client where the debug file is created.
- `PID` is the process ID.
- `XYZ` is the postfix as specified in the `-debug` parameter.

Once the backup or restore session ID `SID` is determined, it is added to the file name:

`OB2DBG_DID_SID_Program_Host_PID_XYZ`

Processes that add the `SID` are BMA/RMA, xBDA/xRDA, and other processes started by the session, but not by the BSM/RSM itself.

NOTE: The session ID helps you identify sets of debug files. Other debug files may belong to the same session and you may need to provide them as well.

A `ctrace.log` file is generated on the Cell Manager, containing information where (on which clients) debug files are generated and which debug prefixes are used. Note that this file does not contain a complete list of all generated files.

To change the default location of debug files on a per system basis, use the `omnirc` option `OB2DBGDIR`. For instructions, see "Omnirc options" (page 20).

Debugging Inet

NOTE: If you enable `Inet` debugs, all integrations will generate debug files.

Windows systems:

Launch the Windows Service Control Manager and restart the `Data Protector Inet` service with the following startup parameters:

`-debug 1-200 POSTFIX`

UNIX systems:

Edit the `/etc/inetd.conf` file:

1. Change the line:

   ```
   omni stream tcp nowait root /opt/omni/lbin/inet inet -log
   /var/opt/omni/log/inet.log
   ```

   to

   ```
   omni stream tcp nowait root /opt/omni/lbin/inet inet -log
   /var/opt/omni/log/inet.log -debug 1-200 DBG_01.txt
   ```

2. Save the file and execute the `/etc/inetd -c` command to apply the changes.

Debugging the CRS

NOTE: Use the `-debug` option carefully because debug files can become quite large. CRS is a multithreaded process, and each created CRS thread produces its own debug file.

Windows systems:

Launch the Windows Service Control Manager and restart the `Data Protector CRS` service with the following startup parameters:

`-debug 1-200` *`POSTFIX Cell_Manager_name`*

UNIX systems:

1. Stop the CRS by executing:

   ```
   /opt/omni/lbin/crs -shutdown
   ```

2. Restart the CRS with the debug option by executing:

   ```
   /opt/omni/lbin/crs -debug 1-200 POSTFIX
   ```

Microsoft server clusters:

In the Data Protector shared directory, edit the file:

`Data_Protector_program_data``\Config\server\options\Trace`

Add the following lines:

```
ranges=1-500
postfix=DBG
select=obpkg.rc.aus.hp.com
```

Using the Cluster Administrator utility, take the CRS service resource (OBVS_MCRS) offline.

△ **CAUTION:** Do not stop the CRS from Windows Service Control Manager, as this will cause the Data Protector cluster group to failover.

MC/ServiceGuard clusters:

1. In the file `/etc/opt/omni/server/options/trace`, uncomment and set the required debugging options. Save and close the file.
2. Start the debugging:

   ```
   /opt/omni/lbin/crs -redebug
   ```

To stop the debugging, set all debugging options in the `trace` file to an empty string, save the file, and then executing the `/opt/omni/lbin/crs -redebug` command.

Preparing the generated data to be sent to the HP Customer Support Service

The HP Customer Support Service might ask you to gather and send them data they need to resolve a technical issue.

Since Data Protector operates in large network environments, the data might sometimes be difficult to gather. The Data Protector `omnidlc` command is a tool for collecting and packing log, debug, and getinfo files. Use this command if this is requested by the HP Customer Support Service.

The `omnidlc` command can be executed from the Data Protector CLI or from the Data Protector GUI. Both methods are described in this section.

NOTE: The `omnidlc` command cannot be used to collect the Data Protector installation execution traces. On how to create and collect these, see the *HP Data Protector Installation and Licensing Guide*.

About the omnidlc command

After Data Protector debug data has been generated, the `omnidlc` command can be used to collect Data Protector debug, log, and getinfo files from the Data Protector cell (by default, from every client). The command transfers the data from selected clients to the Cell Manager where it is then packed.

The command can also selectively collect the data, for example, only log files from a certain client, or only debug files that were created during a particular Data Protector session.

NOTE: When object consolidation is scheduled as part of a post-backup session, backup and consolidation sessions get different session IDs. However, the debug ID is the same for both backup and consolidation. In this case, if you execute the `omnidlc` command and specify the consolidation session ID using the `-session` parameter, debugs will be collected for both backup and consolidation.

Limitations

- The command can only be run on Cell Managers.
- In a MoM environment, you can only collect data for each Data Protector cell separately by executing the command from the respective Cell Manager.
- When a debug and log file collector is used on HP OpenVMS, the following applies:
  - The OpenVMS ODS-2 disk structure file name can contain the maximum of 39 characters.
  - As OpenVMS systems do not have the `get_info` utility, the `get_info.out` file is blank and is not collected.
  - The `omnidlc` command executed with the `-session` option does not collect the debug files produced during specified session, because session names are not part of the OpenVMS debug filename. Instead, all available logs are collected.

Using the omnidlc command from the CLI to process debug logs

The omnidlc command syntax

```
omnidlc {-session SessionID | -did DebugID | -postfix String |
-no_filter} [-hosts List] [-pack Filename | -depot [Directory] | -space
| -delete_dbg] [-no_logs] [-no_getinfo] [-no_compress] [-no_config]
[-no_debugs | -debug_loc Directory1 [Directory2]...] [-verbose]
[-add_info [-any | Host] Path]
```

```
omnidlc -localpack [Filename]
```

```
omnidlc -unpack [Filename]
```

```
omnidlc -uncompress Filename
```

```
omnidlc [-hosts List] -del_ctracelog
```

The options are explained in the following sections.

Limiting the scope of collected data

To limit the scope of collected data, use the following `omnidlc` command options:

`{-session SessionID | -did DebugID | -postfix String | -no_filter} [-hosts List] [-no_logs] [-no_getinfo] [-no_config] [-no_debugs | -debug_loc Directory1 [Directory2]...]`

You can combine the following features:

- To collect data only from the selected clients, use the `-hosts List` option. Specify the names of the clients, separated by spaces.

  In a cluster environment, use the `-hosts` option, specifying the cluster nodes. If this option is not used, the data is collected from the active node only.
- To exclude the getinfo, the configuration information, log, or debug log files from the collected data, use the `-no_getinfo`, `-no_config`, `-no_logs`, or `-no_debugs` option, respectively. Note that `-no_getinfo` is not applicable for HP OpenVMS systems.
- To collect the debug files only from a specific session, use the `-session SessionID` option. Note that on OpenVMS, all available logs are collected.
- To collect the debug files matching a specific debug ID, use the `-did DebugID` option.
- To collect the debug files matching a specific postfix, use the `-postfix String` option.
- To collect all debug files, use the `-no_filter` option.
- To collect debug files not only from the default debug files directory but also from other directories, use the `-debug_loc Directory1 [Directory2]...` option. Note that the subdirectories are excluded from the search. If a specified directory does not exist on a particular client, the directory is ignored.

Segmentation of data

If a file to be sent to the Cell Manager is larger than 2 GB, the file is split into 2 GB-sized chunks. An extension ranging from `s001` to `s999` is appended to each chunk. A second extension (`.gz`) is added if the files are compressed.

On the Cell Manager side, if the size of all collected compressed or uncompressed files exceeds 2 GB, the collected files are packed in 2 GB-sized packages with an extension ranging from `s001` to `s999`.

Disabling compression of the collected data

By default, the collected data is compressed before it is sent to the Cell Manager. To disable the compression, use the `-no_compress` option.

Saving packed data

By default, the data is sent over the network to the Cell Manager, where it is packed and saved in the current directory as the file `dlc.pck`.

The packed file includes a generated directory structure that includes the hostnames, paths, and the collected files of the clients involved.

Limitation

- The size of the resulting packed file cannot exceed 2 GB. In such a case, do not pack the data.

Use the `-pack Filename` option to pack and save the data:

- With a different file name. Specify the *`Filename`* as a file name.
- In a different directory and with a different file name. Specify the *`Filename`* as a full pathname.

Saving unpacked data

To leave the data unpacked and save it, use the `-depot [Directory]` option. If the *`Directory`* is not specified, the files are saved on the Cell Manager in the directory:

Windows systems: *`Data_Protector_home`*`\tmp\dlc`

UNIX systems: `/tmp/dlc`

If the *`Directory`* is specified, the collected files are saved to the `dlc` directory of the specified directory.

The directories for the packed or unpacked files are generated as follows:

```
./dlc/client_1/tmp/debug_files
./dlc/client_1/log/log_files
./dlc/client_1/getinfo/get_info.txt
./dlc/client_2/tmp/debug_files
./dlc/client_2/log/log_files
./dlc/client_2/getinfo/get_info.txt
...
```

Estimating the required space

To display the amount of disk space required on the Cell Manager to gather the data, use the `-space` option.

Deleting debug files on clients

To delete the collected data on the clients, use the `-delete_dbg` option. Note that only debug files are deleted; getinfo and log files are not deleted. On HP OpenVMS, if executed together with the `-session` option, the `omnidlc` command does not delete any debugs from the debug files directory.

Deleting information about debug files

To delete `ctrace.log` files containing the information where (on which clients) debug logs are generated and which debug prefixes are used, use the `-del_ctracelog` option. Note that if used together with the `-hosts` *`List`* option, the command deletes `ctrace.log` files on specified clients only. Otherwise, `ctrace.log` files on all clients in a cell are deleted.

NOTE: Use this option for `ctrace.log` files cleanup. Note that if this file is deleted, the debug log collector will only get debugs from the default directories (`/tmp/dlc` on UNIX systems and *`Data_Protector_home`*`\tmp\dlc` on Windows systems) and not from other debug directories you specified.

Additional operations

- To pack unpacked data, compressed or uncompressed, that was sent to the Cell Manager (using the `-depot` option), use the `-localpack [`*`Filename`*`]` option.

  This option packs the directory structure of the current directory (must be the directory containing the `dlc` directory generated by the `-depot` option). If the *`Filename`* argument is not specified, the file `dlc.pck` is created in the current directory.

  This option is equivalent to the -pack option, but should be used only if the data was collected using the `-depot` option.

- To get the additional information (for example, screenshots, pictures and the like) from a specified directory on client, use the `[-add_info [-any | `*`Host`*`] `*`Path`*`]` option.

  The `-any` option is used when the directory path is the same for all clients.

- To unpack data, use the `-unpack [Filename]` option.

  If the *filename* argument is not specified, the `dlc.pck` file from the current directory is unpacked. The data is always unpacked to the `dlc` directory in the current directory.

  Use this option when the collected data was packed on the Cell Manager either using the `-pack` or `-localpack` option.
- To uncompress a compressed single file, use the `-uncompress Filename` option. Packed data must be unpacked first.
- To enable verbose output, use the `-verbose` option.

Problems and workarounds

Problem

Debug log collection fails

During the debug log collection operation, omnidlc is unable to connect to a client. The following error is displayed:

```
Collection from client1.company.com started.
Error: Data retrieval from client1.company.com failed.
Warning: Collection from client1.company.com incomplete.
```

The problem occurs when a Cell Manager name specified in the configuration file on a client does not match the name of the Cell Manager that requested the debug log collection.

Action

Add the Cell Manager hostname to the `omnidlc_hosts` file located in `/etc/opt/omni/client` (UNIX clients) or *Data_Protector_program_data*`\config\client` (Windows clients).

Examples of using the omnidlc command

1. To collect and compress all debug, log, and getinfo files from the cell and pack them in the `dlc.pck` file in the current directory on the Cell Manager, using verbose output, execute:

   ```
   omnidlc -no_filter -verbose
   ```
2. To collect only log and debug files from the clients `client1.company.com` and `client2.company.com` to the directory `c:\depot` on the Cell Manager, without compressing and packing the files, execute:

   ```
   omnidlc -no_filter -hosts client1.company.com client2.company.com
   -depot c:\depot -no_getinfo -no_compress
   ```
3. To collect log, debug, and getinfo files from the client `client1.company.com`, compress and pack them to the file `c:\pack\pack.pck` on the Cell Manager, execute:

   ```
   omnidlc -hosts client1.company.com -pack c:\pack\pack.pck
   ```
4. To collect log, debug, and getinfo files from the default location and debug files from the additional directories, `C:\tmp` and `/temp/debugs`, from the clients `client1.company.com` and `client2.company.com`, and to compress and pack the files on the Cell Manager, execute:

   ```
   omnidlc -hosts client1.company.com client2.company.com -debug_loc
   C:\tmp /tmp/debugs
   ```
5. To delete all debug files for the session with the ID `2006/05/27-9`, execute:

   ```
   omnidlc -session 2006/05/27-9 -delete_dbg
   ```

6. To display disk space needed on the Cell Manager for the uncompressed debug files with the debug ID `2351` from the client `client.company.com`, execute:

   ```
   omnidlc -did 2351 -hosts client.company.com -space -no_getinfo
   -no_logs -no_compress
   ```

7. To pack the additional file located in the `C:\debug` directory on the client `client1.company.com` together with debug log files for the session with the ID `2007/11/17-24`, execute:

   ```
   omnidlc -session 2007/11/17-24 -add_info -host client1.company.com
   C:\debug
   ```

8. To pack the directory structure in the current directory (must be the directory containing the `dlc` directory generated by the `-depot` option) to the `dlc.pck` file in the same directory, execute:

   ```
   omnidlc -localpack
   ```

9. To unpack the `dlc.pck` file to the `dlc` directory of the current directory, execute:

   ```
   omnidlc -unpack
   ```

Using the Data Protector GUI to process debug files

The following debug file operations are available in the Data Protector GUI:

- Debug files collection. Debug files are collected from client systems and stored on the Cell Manager
- Calculate debug files space. The space required on the Cell Manager for the collected files is calculated
- Delete debug files. Debug files are deleted from the client systems

They can be invoked from the Internal Database context or the Clients context.

The GUI operations use various options of the `omnidlc` CLI command. Additional operations can be performed on collected files by using the `omnidlc` command directly in the command line interface. Further information can be found in the *HP Data Protector Command Line Interface Reference*.

When performing any of the operations in the following sections, the `omnidlc` syntax used can be seen in a Results window.

Invoking debug file operations

To access debug file operations from the Clients context:

1. In the Scoping Pane, expand the Clients folder and select the client for which debug file operations are required
2. Select the operation to perform:
   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space** or **Delete Debug Files**.

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space** or **Delete**.

To access debug file operations from the Internal Database context:

1. In the Scoping Pane, expand the Sessions folder and select the session for which debug file operations are required.
2. Select the operation to perform:
   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space** or **Delete Debug Files**.

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space** or **Delete**.

In each case, selecting an operation starts a wizard that guides you through the required steps.

Collecting debug files

To collect debug files:

1. Start the Debug File Collector wizard as described in Invoking debug log operations

   If you started from the Internal Database context by selecting a session, the session will be pre-selected in the Filter section of the wizard Clients page and the clients involved in the session will be selected.

   If you started from the Client context, the clients that you selected there will be pre-selected in the wizard Clients page.
2. In the Clients page, to limit the clients from which logs are collected:
   a. Select only the client(s) from which to collect logs. If clients were pre-selected, you can de-select any of them.
   b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier. If **No filter** is selected, all debug logs on the selected client(s) will be collected. If a session ID was pre-selected for you, you cannot change this.
   c. Click **Next**.
3. In the Directories page:
   a. Enter any other directories that should be checked for debug logs in addition to the default debug files directory and click **Add**.
   b. In the directory tree, select any other directories whose contents you want collected (the contents of sub-directories will not be selected).
   c. Click **Next**.
4. In the Options and Operation page:
   a. De-select any debug collection options you don't want to use. For information on the `omnidlc` options, see the *HP Data Protector Command Line Interface Reference*.
   b. Select the operation to be used for storing the debug logs on the Cell Manager:
      - **Create Depot** stores the files (not packed) in a `dlc` directory in the following location:

        `Data_Protector_program_data``\tmp\` (Windows systems) or `/tmp/dlc` (UNIX systems).

        To specify an alternative location, enter an existing directory in **Target Path**. If you want to use the default location, make sure that the text box is clear.

        Using this option allows you to review the collected files and remove any of them before sending the information to support. You can subsequently create a pack file using the CLI command `omnidlc -localpack [`*`filename`*`]` (for more information on this, see the *HP Data Protector Command Line Interface Reference*).

      - **Create Pack File** (default) creates a pack file in the current directory. To specify an alternative directory and/or filename, enter the full path in **Target Path**.
   c. Click **Finish**.

Calculating debug files space

You can calculate the total space required on the Cell Manager for a debug file collection before actually performing the collection by entering all the required collection information in the Debug Files Space Calculation Wizard. After the calculation has been performed, you have the option to start the collection using the specified criteria.

To calculate the total space required on the Cell Manager for a debug files collection:

1. Start the Debug Files Space Calculation wizard as described in Invoking debug file operations.
2. In the Clients page, to limit the clients involved:
   a. Select only the client(s) from which you want to collect files. If clients were pre-selected, you can de-select any of them.
   b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier. If **No filter** is selected, all debug files on the selected client(s) will be collected. If a session ID was pre-selected for you, you cannot change this.
   c. Click **Next**.
3. In the Directories page:
   a. Enter any other directories that should be checked for debug files in addition to the default debug files directory and click **Add**.
   b. In the directory tree, select any other directories whose contents you want considered.
   c. Click **Next**.
4. In the Options page:
   a. De-select any debug collection options you don't want to use. For information on the `omnidlc` options, see the *HP Data Protector Command Line Interface Reference*.
   b. Click **Next**.

   The results of the check are displayed in the **Results** tab.

After the calculation, a dialog box appears asking if you want to start the debug files collection.

To start debug files collection using the options selected for the space calculation:

- Click **Yes**.

  The default operation behavior (Create Pack file) will be used on the Cell Manager. See Collecting debug files.

Deleting debug files

To delete debug files from clients:

1. Start the Delete Debug files wizard as described in Invoking debug file operations.
2. In the Clients page, to limit the clients from which debug files are deleted:
   a. Select only the client(s) from which to delete files.
   b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier. If **No filter** is selected, all debug files on the selected client(s) will be deleted.
   c. Click **Next**.
3. In the Directories page:
   a. Enter any other directories from which debug files should be deleted, in addition to the default debug files directory and click **Add**.
   b. Click **Finish**.

Example of collecting data to be sent to the HP Customer Support Service

To collect debug, log, and getinfo files for problems occurring during backup sessions involving one client and the Cell Manager:

1. Reduce the error environment as much as possible:
   - Create a backup specification that contains just one or a few files or directories.
   - Include only one failing client in the debug run.
2. Create an `info` text file that contains the following:
   - Hardware identification of the Cell Manager, Media Agent, and Disk Agent clients. For example, `HP-9000 T-600 Series; Vectra XA`.
   - The SCSI controller's name, for example, `onboard_type/Adaptec xxx/...` for Windows Media Agent clients.
   - Topology information obtained from the `omnicellinfo -cell` command output.
   - The output of the `devbra -dev` command if you have issues with backup devices.
3. Discuss the technical issue with the support organization and request the following information:
   - Debug level (For example, 1-200. This is a command option needed later.).
   - Debug scope (For example, client only, Cell Manager only, every system.).
4. Exit all user interfaces and stop all other backup activities in the cell.
5. To collect Inet or CRS debugs as well, restart the Inet or CRS service on the Cell Manager in the debug mode, as described in "Debugging Inet" (page 59) and "Debugging the CRS" (page 60), respectively.
6. On the Cell Manager, start the GUI in the debug mode:

   ```
   manager -debug 1-200 error_run.txt
   ```

   You can define the postfix of the debug file names created by substituting the `error_run` text with your preference.
7. Reproduce the problem using Data Protector.
8. Exit all user interfaces to quit the debug mode.

   If you collected Inet and CRS debugs as well, restart the Data Protector services on the Cell Manager without the debug option.
9. On the Cell Manager, execute:

   ```
   omnidlc -postfix error_run.txt
   ```

   The command compresses the log, getinfo, and debug files with the `error_run.txt` postfix on the client and sends them over the network to the Cell Manager, where they are packed and saved in the `dlc.pck` file in the current directory. For more information, see "Preparing the generated data to be sent to the HP Customer Support Service" (page 60).
10. E-mail the packed files (`dlc.pck`) to the support organization.
11. Delete the created debug files (with the `error_run.txt` postfix) on the client by executing the following command on the Cell Manager:

    ```
    omnidlc -postfix error_run.txt -delete_dbg
    ```

Glossary

A

access rights — *See* user rights.

ACSLS — *(StorageTek specific term)* The Automated Cartridge System Library Server (ACSLS) software that manages the Automated Cartridge System (ACS).

Active Directory — *(Windows specific term)* The directory service in a Windows network. It contains information about resources on the network and makes them accessible to users and applications. The directory services provide a consistent way to name, describe, locate, access and manage resources regardless of the physical system they reside on.

AES 256-bit encryption — Data Protector software encryption, based on the AES-CTR (Advanced Encryption Standard in Counter Mode) encryption algorithm that uses random keys of 256-bit length. The same key is used for both encryption and decryption. With AES 256-bit encryption, data is encrypted before it is transferred over a network and before it is written to media.

AML — *(ADIC/GRAU specific term)* Automated Mixed-Media library.

AMU — *(ADIC/GRAU specific term)* Archive Management Unit.

application agent — A component needed on a client to back up or restore online database integrations.
See also Disk Agent.

application system — *(ZDB specific term)* A system the application or database runs on. The application or database data is located on source volumes.
See also backup system and source volume.

archive logging — *(Lotus Domino Server specific term)* Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.

archived 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 and 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)* SAP R/3 backup programs can call the Data Protector backint interface program via an open interface, which enables them to communicate with Data Protector software. For backup and restore, SAP R/3 programs issue orders for the Data Protector backint interface.

backup API The Oracle interface between the Oracle backup/restore utility and the backup/restore media management layer. The interface defines a set of routines to allow the reading and writing of data to the backup media, the creation, searching and removing the backup files.

backup chain *See* restore chain.

backup device A device configured for use with Data Protector, which can write data to and read data from storage media. This can be, for example, a standalone DDS/DAT drive or a library.

backup generation One backup generation includes one full backup and all incremental backups until the next full backup.

backup ID An identifier of an integration object that equals the session ID of the backup of this object. The backup ID is preserved when an object is copied, exported, or imported.

backup object A backup unit that contains all items backed up from one disk volume (logical disk or mount point). The backed up items can be any number of files, directories, or the entire disk or mount point. Additionally, a backup object can be a database/application entity or a disk image.

A backup object is defined by:

- Client name: Hostname of the Data Protector client where the backup object resides.
- Mount point: For filesystem objects — the access point in a directory structure on the client where the backup object is located (drive on Windows 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 (for example, SAP or Lotus).
- Type: Backup object type. For filesystem objects — filesystem type (for example, WinFS). For integration objects — "Bar".

backup owner Each backup object in the IDB has an owner. The default owner of a backup is the user who starts the backup session.

backup session A process that creates a copy of data on storage media. The activities are specified in a backup specification or an interactive session. All clients configured in one backup specification are backed up together in one backup session using the same backup type. The result of a backup session is a set of media, which was written to, also called the backup or media set.
See also backup specification, full backup, and incremental backup.

backup set A complete set of integration objects associated with a backup.

backup set *(Oracle specific term)* A logical grouping of backed up files that are created using the RMAN backup command. A backup set is a complete set of files associated with a backup. The files can be multiplexed to increase performance. A backup set contains either datafiles or archived logs, but not both together.

backup specification A list of objects to be backed up, together with a set of devices or drives to be used, backup options for all objects in the specification, and days and time that you want backups to be performed. The objects are entire disks/volumes or parts of them such as files, directories, or even the Windows Registry for example. File selection lists such as include-lists and exclude-lists can be specified.

backup system *(ZDB specific term)* A system connected to a disk array together with one or multiple application systems. The backup system is typically connected to a disk array to create target volumes (a replica) and is used for mounting the target volumes (the replica).
See also application system, target volume, and replica.

backup types *See* incremental backup, differential backup, transaction backup, full backup, and delta backup.

backup view Data Protector provides different views for backup specifications:

By Type - according to the type of data available for backups/templates. Default view.

By Group - according to the group to which backup specifications/templates belong.

By Name - according to the name of backup specifications/templates.

By Manager - if you are running MoM, you can also set the Backup view according to the Cell Manager to which backup specifications/templates belong.

BC *(EMC Symmetrix specific term)* Business Continuance are processes that allow customers to access and manage instant copies of EMC Symmetrix standard devices.
See also BCV.

BC Process *(EMC Symmetrix specific term)* A protected storage environment solution that has defined specially configured EMC Symmetrix devices as mirrors or Business Continuance Volumes to protect data on EMC Symmetrix standard devices.
See also BCV.

BCV *(EMC Symmetrix specific term)* Business Continuance Volumes, or BCV devices, are dedicated SLDs that are pre-configured in the ICDA on which the business continuation operation runs. BCV devices are assigned separate SCSI addresses, differing from the addresses used by the SLDs they mirror. The BCV devices are used as splitable mirrors of the primary EMC Symmetrix SLDs that need to be protected.
See also BC and BC Process.

Boolean operators The Boolean operators for the full text search functionality of the Data Protector Help system are AND, OR, NOT, and NEAR. Used when searching, they enable you to define your query precisely by creating a relationship between search terms. If no operator is specified in a multi-word search, AND is used by default. For example, the query manual disaster recovery is equivalent to manual AND disaster AND recovery.

boot volume/disk/partition A volume/disk/partition with files required for the initial step of the boot process. Microsoft terminology defines the boot volume/disk/partition as a volume/disk/partition containing the operating system files.

BRARCHIVE *(SAP R/3 specific term)* An SAP R/3 backup tool that allows you to archive redo log files. BRARCHIVE also saves all the logs and profiles of the archiving process.
See also BRBACKUP and BRRESTORE.

BRBACKUP *(SAP R/3 specific term)* An SAP R/3 backup tool that allows an online or offline backup of the control file, of individual data files, or of all tablespaces and, if necessary, of the online redo log files.
See also BRARCHIVE and BRRESTORE.

BRRESTORE *(SAP R/3 specific term)* An SAP R/3 tool that can be used to restore files of the following type:

- Database data files, control files, and online redo log files saved with BRBACKUP
- Redo log files archived with BRARCHIVE
- Non-database files saved with BRBACKUP

You can specify files, tablespaces, complete backups, log sequence numbers of redo log files, or the session ID of the backup.
See also BRBACKUP and BRARCHIVE.

BSM The Data Protector Backup Session Manager controls the backup session. This process always runs on the Cell Manager system.

C

CAP *(StorageTek specific term)* Cartridge Access Port is a port built into the door panel of a library. The purpose is to enter or eject media.

Catalog 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 or SAN. Central control is available to administer the backup and restore policies and tasks.

Cell Manager The main system in the cell where the essential Data Protector software is installed and from which all backup and restore activities are managed. The GUI used for management tasks can be located on a different system. Each cell has one Cell Manager system.

centralized licensing Data Protector allows you to configure centralized licensing for the whole enterprise environment consisting of several cells. All Data Protector licenses are installed and kept on the Enterprise Cell Manager system. You can then allocate licenses to specific cells to suit your needs.
See also MoM.

Centralized Media Management Database (CMMDB) *See* CMMDB.

Certificate Server A Windows Certificate Server can be installed and configured to provide certificates for clients. It provides customizable services for issuing and managing certificates for the enterprise. These services issue, revoke, and manage certificates employed in public key-based cryptography technologies.

Change Journal *(Windows specific term)* A Windows filesystem feature that logs a record of each change as it occurs to the files and directories on a local NTFS volume.

Change Log Provider *(Windows specific term)* A module that can be queried to determine which objects on a filesystem have been created, modified, or deleted.

channel *(Oracle specific term)* An Oracle Recovery Manager resource allocation. Every allocated channel starts a new Oracle process, which performs backup, restore, and recovery actions. The type of channel allocated determines the type of media used:

- type 'disk'
- type 'sbt_tape'

If the specified channel is of type 'sbt_tape' and Oracle is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

circular logging *(Microsoft Exchange Server and Lotus Domino Server specific term)* Circular logging is a Microsoft Exchange Server database and Lotus Domino Server database mode, in which the transaction log file contents are periodically overwritten after the corresponding data is committed to the database. Circular logging reduces disk storage space requirements.

client backup A backup of all volumes (filesystems) mounted on a Data Protector client. What is actually backed up depends on how you select objects in a backup specification:

- If you select the check box next to the client system name, a single backup object of the `Client System` type is created. As a result, at the time of the backup, Data Protector first detects all volumes that are mounted on the selected client and then backs them up. On Windows clients, `CONFIGURATION` is also backed up.
- If you individually select all volumes that are mounted on the client system, a separate backup object of the `Filesystem` type is created for each volume. As a result, at the time of the

backup, only the selected volumes are backed up. Volumes that have been potentially mounted on the client after the backup specification was created are not backed up.

client or client system Any system configured with any Data Protector functionality and configured in a cell.

cluster continuous replication *(Microsoft Exchange Server specific term)* Cluster continuous replication (CCR) is a high availability solution that uses cluster management and failover options to create and maintain an exact copy (CCR copy) of a storage group. A storage group is replicated to a separate server. CCR removes any single point of failure in your Exchange back-end servers. You can perform backups using VSS on your passive Exchange Server node where a CCR copy is located and thus reducing the load on the active node.

A CCR copy is used for disaster recovery since you can switch to the CCR copy in a few seconds. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) like an ordinary storage group.

See also Exchange Replication Service and local continuous replication.

cluster-aware application It is an application that supports the cluster Application Programming Interface. Each cluster-aware application declares its own critical resources (disk volumes (on Microsoft Cluster Server), volume groups (on MC/ServiceGuard), application services, IP names and addresses, and so on).

CMD script for Informix Server *(Informix Server specific term)* A Windows CMD script that is created in INFORMIXDIR when an Informix Server database is configured. The CMD script is a set of system commands that export environment variables for Informix Server.

CMMDB The Data Protector Centralized Media Management Database (CMMDB) is the result of merging MMDBs from several cells in the MoM environment. It allows you to share high-end devices and media across multiple cells in a MoM environment. One cell can control the robotics, serving the devices that are connected to systems in other cells. The CMMDB must reside on the Manager-of-Managers. A reliable network connection between the MoM cell and the other Data Protector cells is highly recommended
See also MoM.

COM+ Class Registration Database *(Windows specific term)* The COM+ Class Registration Database and the Windows Registry store application attributes, class attributes, and computer-level attributes. This guarantees consistency among these attributes and provides common operation on top of these attributes.

command device *(HP P9000 XP Disk Array Family specific term)* A dedicated volume in the disk array which acts as the interface between a management application and the disk array's storage system. It cannot be used for data storage and only accepts requests for operations that are then executed by the disk array.

command-line interface (CLI) A set of commands that you can use in shell scripts to perform Data Protector configuration, backup, restore, and management tasks.

concurrency *See* Disk Agent concurrency.

container *(HP P6000 EVA Disk Array Family specific term)* Space on a disk array, which is pre-allocated for later use as a standard snapshot, vsnap, or snapclone.

control file *(Oracle and SAP R/3 specific term)* An Oracle data file that contains entries specifying the physical structure of the database. It provides database consistency information used for recovery.

copy set *(HP P6000 EVA Disk Array Family specific term)* A pair that consists of the source volumes on a local P6000 EVA and their replica on a remote P6000 EVA.
See also source volume, replica, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

CRS The Cell Request Server process (service), which runs on the Data Protector Cell Manager, and starts and controls the backup and restore sessions. The service is started as soon as Data Protector is installed on the Cell Manager. On Windows systems, the CRS runs under the account of the user specified at installation time. On UNIX systems, it runs under the account `root`.

CSM The Data Protector Copy and Consolidation Session Manager process controls the object copy and object consolidation sessions and runs on the Cell Manager system.

D

data file *(Oracle and SAP R/3 specific term)* A physical file created by Oracle that contains data structures such as tables and indexes. A data file can only belong to one Oracle database.

data protection Defines how long the backed up data on media remains protected, that is, Data Protector will not overwrite it. When the protection expires, Data Protector will be able to reuse the media in one of the next backup sessions.
See also catalog protection.

data replication (DR) group *(HP P6000 EVA Disk Array Family specific term)* A logical grouping of HP P6000 EVA Disk Array Family virtual disks. It can contain up to eight copy sets provided they have common characteristics and share a common HP CA P6000 EVA log.
See also copy set.

data stream Sequence of data transferred over the communication channel.

Data_Protector_home A reference to the directory containing Data Protector program files (on Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012) or the directory containing Data Protector program files and data files (on other Windows operating systems). Its default path is `%ProgramFiles%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_program_data.

Data_Protector_program_data A reference to the directory containing Data Protector data files on Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012. Its default path is `%ProgramData%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_home.

database library A Data Protector set of routines that enables data transfer between Data Protector and a server of an online database integration, for example, Oracle Server.

database parallelism More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.

database server A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.

Dbobject *(Informix Server specific term)* An Informix Server physical database object. It can be a blobspace, dbspace, or logical log file.

DC directory 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 (DBCF) 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 A physical unit which contains either just a drive or a more complex unit such as a library.

device chain A device chain consists of several standalone devices configured for sequential use. When a medium in one device gets full, the backup automatically continues on a medium in the next device in the device chain.

device group *(EMC Symmetrix specific term)* A logical unit representing several EMC Symmetrix devices. A device cannot belong to more than a single device group. All devices in a device group must be on the same EMC Symmetrix unit. You can use a device group to identify and work with a subset of the available EMC Symmetrix devices.

device streaming A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes to write to the tape, and so on. In other words, if the data rate written

to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.

DHCP server A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic IP address assignment and network configuration for DHCP clients.

differential backup An incremental backup that backs up changes made since the last full backup. To perform this type of backup, specify the Incr1 backup type.
See also incremental backup.

differential backup *(Microsoft SQL Server specific term)* A database backup that records only the data changes made to the database after the last full database backup.
See also backup types.

differential database backup A differential database backup records only those data changes made to the database after the last full database backup.

directory junction *(Windows specific term)* Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.

disaster recovery A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.

disaster recovery operating system *See* DR OS.

Disk Agent A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.

Disk Agent concurrency The number of Disk Agents that are allowed to send data to one Media Agent concurrently.

disk group *(Veritas Volume Manager specific term)* The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.

disk image backup A high-speed backup where Data Protector backs up files as bitmap images. A disk image backup does not track the files and directory structure stored on the disk, but stores a disk image structure on byte level. You can perform a disk image backup of either specific disk sections or a complete disk.

disk quota A concept to manage disk space consumption for all or a subset of users on a computer system. This concept is used by several operating system platforms.

disk staging The process of backing up data in several phases to improve the performance of backups and restores, reduce costs of storing the backed up data, and increase the data availability and accessibility for restore. The backup stages consist of backing up data to one media type first (for example disk) and later copying it to a different media type (for example tape).

distributed file media format A media format, available with the file library, which supports a space efficient type of synthetic backup called virtual full backup. Using this format is a prerequisite for virtual full backup.
See also virtual full backup.

Distributed File System (DFS) A service that connects file shares into a single namespace. The file shares can reside on the same or on different computers. DFS provides client access to the resources in a location-transparent manner.

DMZ The Demilitarized Zone (DMZ) is a network inserted as a "neutral zone" between a company's private network (intranet) and the outside public network (Internet). It prevents outside users from getting direct access to company servers in the intranet.

DNS server In the DNS client-server model, this is the server containing information about a portion of the DNS database that makes computer names available to client resolvers querying for name resolution across the Internet.

domain controller A server in a network that is responsible for user security and verifying passwords within a group of other servers.

DR image Data required for temporary disaster recovery operating system (DR OS) installation and configuration.

DR OS An operating system environment in which disaster recovery runs. It provides Data Protector with a basic runtime environment (disk, network, tape, and filesystem access). It has to be installed on disk or loaded into memory and configured before the Data Protector disaster recovery can be performed. DR OS can be either temporary or active. A temporary DR OS is used exclusively as a host environment for some other operating system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. An active DR OS not only hosts the Data Protector disaster recovery process but can also be a part of the restored system because it replaces its own configuration data with the original configuration data.

drive A physical unit that receives data from a computer system and can write it onto a magnetic medium (typically a tape drive). It can also read the data from the medium and send it to the computer system.

drive index A number that identifies the mechanical position of a drive inside a library device. This number is used by the robotic control to access a drive.

drive-based encryption Data Protector drive-based encryption uses the encryption functionality of the drive. While performing the backup, the drive encrypts both the data and the metadata that is written to the medium.

E

EMC Symmetrix Agent A Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

emergency boot file *(Informix Server specific term)* The Informix Server configuration file `ixbar.`*`server_id`* that resides in the directory *`INFORMIXDIR`*`/etc` (on Windows 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 Secure Socket Layer (SSL) that uses SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.

encryption key A 256-bit randomly generated number used by the Data Protector encryption algorithm to encode information during backups for which AES 256-bit software encryption or drive-based encryption has been specified. The same key is used for subsequent decryption of the information. Encryption keys for a Data Protector cell are stored in a central keystore on the Cell Manager.

encryption KeyID-StoreID Combined identifier used by the Data Protector Key Management Server to identify and administer encryption keys used by Data Protector. `KeyID` identifies the key within the keystore. `StoreID` identifies the keystore on the Cell Manager. If Data Protector has been upgraded from an earlier version with encryption functionality, there may several `StoreID`s used on the same Cell Manager.

enhanced incremental backup Conventional incremental backup backs up files that have changed since a previous backup, but has certain limitations in detection of changes. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up also renamed and moved files, as well as files with changes in attributes.

enterprise backup environment Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes all clients located in several Data Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept.
See also MoM.

Event Log (Data Protector Event Log) A central repository of all Data Protector-related notifications. By default, all notifications are sent to the Event Log. The events are logged on the Cell Manager into the file *`Data_Protector_program_data`*`\log\server\Ob2EventLog.txt` (Windows systems),

or `/var/opt/omni/server/log/Ob2EventLog.txt` (UNIX systems). The Event Log is accessible only to users of the Data Protector `Admin` user group and to users who are granted the Data Protector `Reporting and notifications` user rights. You can view or delete all events in the Event Log.

Event Logs *(Windows specific term)* Files in which Windows logs all events, such as the starting or stopping of services and the logging on and off of users. Data Protector can back up Windows Event Logs as part of the Windows configuration backup.

Exchange Replication Service *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that represents storage groups that were replicated using either local continuous replication (LCR) or cluster continuous replication (CCR) technology.
See also cluster continuous replication and local continuous replication.

exchanger Also referred to as SCSI Exchanger.
See also library.

exporting media A process that removes all data about backup sessions, such as systems, objects, and 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 *(Windows specific term)* The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

file version The same file can be backed up multiple times in case of full backups and incremental backups (if the file changed). If the log level ALL is selected for backup, Data Protector retains one entry in the IDB for the filename itself and one for each version (date/time) of the file.

filesystem The organization of files on a hard disk. A filesystem is backed up so that the file attributes and the file contents are stored on the backup media.

first-level mirror *(HP P9000 XP Disk Array Family specific term)* A mirror of an internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which can be further mirrored itself, producing second-level

mirrors. For Data Protector zero downtime backup and instant recovery purposes, only first-level mirrors can be used.
See also primary volume and mirror unit (MU) number.

flash recovery area *(Oracle specific term)* A directory, filesystem, or Automatic Storage Management (ASM) disk group managed by Oracle that serves as a centralized storage area for files related to backup, restore, and database recovery (recovery files).
See also recovery files.

formatting A process that erases any data contained on a medium and prepares it for use with Data Protector. Information about media (medium ID, description, and location) is saved in the IDB as well as on the respective media (media header). Data Protector media with protected data are not formatted until the protection expires or the media are unprotected/recycled.

free pool An auxiliary source of media for use by media pools when they run out of media. The media pools must be configured to use free pools.

full backup A backup in which all selected objects are backed up, whether or not they have been recently modified.
See also backup types.

full database backup A backup of all data in a database, not only the data that has been changed after the last (full or incremental) backup of the database. A full database backup does not depend on any other backup.

full mailbox backup A full mailbox backup is a backup of the entire mailbox content.

full ZDB A ZDB-to-tape or ZDB-to-disk+tape session in which all selected objects are streamed to tape, even if there are no changes from the previous backup.
See also incremental ZDB.

G

global options 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 on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\holidays` (Windows systems), or `/etc/opt/omni/server/Holidays` (UNIX systems).

hosting system A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.

HP Business Copy (BC) P6000 EVA *(HP P6000 EVA Disk Array Family specific term)* A local replication software solution that enables creation of point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the P6000 EVA firmware.

See also replica, source volume, snapshot, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

HP Business Copy (BC) P9000 XP

(HP P9000 XP Disk Array Family specific term) An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of internal copies of LDEVs for various purposes, such as data duplication and backup. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system. For Data Protector zero downtime backup purposes, P-VOLs should be available to the application system, and one of the S-VOL sets should be available to the backup system.
See also LDEV, HP Continuous Access (CA) P9000 XP, Main Control Unit, application system, and backup system.

HP Command View (CV) EVA

(HP P6000 EVA Disk Array Family specific term) The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, and mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed by a Web browser.
See also HP P6000 / 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 Business Copy (BC) P9000 XP, Main Control Unit, and LDEV.

HP Continuous Access + Business Copy (CA+BC) P6000 EVA

(HP P6000 EVA Disk Array Family specific term) An HP P6000 EVA Disk Array Family configuration that enables creation and maintenance of copies (replicas) of the source volumes on a remote P6000 EVA, and later use of these copies as the source for local replication on this remote array.
See also HP Business Copy (BC) P6000 EVA, replica, and source volume.

HP P6000 / 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 HP P6000 / HP 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 component that executes all tasks needed by the Data Protector HP P9000 XP Disk Array Family integration. It uses RAID Manager Library for communication with a P9000 XP Array storage system.
See also RAID Manager Library.

HP SMI-S P6000 EVA Array provider

An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the 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.

I

ICDA

(EMC Symmetrix specific term) EMC's Symmetrix Integrated Cached Disk Arrays (ICDA) is a disk array device that combines a set of physical disks, a number of FWD SCSI channels, an internal cache memory, and control and diagnostic software commonly referred to as the microcode.

IDB

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 session, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore from tape. Depending on the application or database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery.
See also replica, zero downtime backup (ZDB), ZDB to disk, and ZDB to disk+tape.

integration object A backup object of a Data Protector integration, such as Oracle or SAP DB.

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 stores its data in 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 (DBCF).

Internet Information Services (IIS) *(Windows specific term)* Microsoft Internet Information Services is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

ISQL *(Sybase specific term)* A Sybase utility used to perform system administration tasks on Sybase SQL Server.

J

jukebox *See* library.

jukebox device A device consisting of multiple slots used to store either optical or file media. When being used to store file media, the jukebox device is known as the "file jukebox device".

K

Key Management Service *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that provides encryption functionality for enhanced security.
See also Information Store and Site Replication Service.

keychain A tool that eliminates the supply of a passphrase manually when decrypting the private key. It needs to be installed and configured on the Installation Server if you perform remote installation using secure shell.

keystore All encryption keys are centrally stored in the keystore on the Cell Manager and administered by the Key Management Server (KMS).

KMS Key Management Server (KMS) is a centralized service that runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started as soon as Data Protector is installed on the Cell Manager.

L

LBO *(EMC Symmetrix specific term)* A Logical Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as one entity and can only be restored as a whole.

LDEV *(HP P9000 XP Disk Array Family specific term)* A logical partition of a physical disk of a disk array of the HP P9000 XP Disk Array Family. An LDEV is the entity that can be replicated using the split-mirror or snapshot functionality of such disk array.
See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and replica.

library Also called autochanger, jukebox, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to media. The library can contain multiple drives.

lights-out operation or unattended operation A backup or restore operation that takes place outside of normal business hours without an operator. This implies that no operator personnel is present to work with the backup application or service mount requests, for example.

LISTENER.ORA *(Oracle specific term)* An Oracle configuration file that describes one or more Transparent Network Substrate (TNS) listeners on a server.

load balancing By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used

for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery

Remote recovery is performed if all Media Agent hosts specified in the SRD file are accessible. If any of them fails, the disaster recovery process fails over to the local mode. This means that the target system is searched for locally attached devices. If only one device is found, it is automatically used. Otherwise, Data Protector prompts you to select the device, which will be used for restore.

local continuous replication

(Microsoft Exchange Server specific term) Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying.

An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal.

A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) as a normal storage group.

See also cluster continuous replication and Exchange Replication Service.

lock name

You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script

(Informix Server UNIX 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 uses to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

login information to the Oracle Target Database

(Oracle and SAP R/3 specific term) The format of the login information is *`user_name`*`/`*`password`*`@`*`service`*, where:

- *`user_name`* is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights.
- *`password`* must be the same as the password specified in the Oracle password file (`orapwd`), which is used for authentication of users performing database administration.
- *`service`* is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database

(Oracle specific term) The format of the login information to the Recovery (Oracle) Catalog Database is *`user_name`*`/`*`password`*`@`*`service`*, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the

Oracle target database. In this case, *service* is the name of the service to the Recovery Catalog Database, not the Oracle target database.

Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API *(Lotus Domino Server specific term)* An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

M

Magic Packet *See* Wake ONLAN.

mailbox *(Microsoft Exchange Server specific term)* The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

mailbox store *(Microsoft Exchange Server specific term)* A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text `.edb` file and a streaming native internet content `.stm` file.

Main Control Unit (MCU) *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP or HP CA+BC P9000 XP configuration and acts as a master device.
See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

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 Data Protector 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 (MoM) *See* MoM.

MAPI *(Microsoft Exchange Server specific term)* The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

MCU *See* Main Control Unit (MCU).

Media Agent A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore or object verification session, a Media Agent locates data on the backup medium and sends it to the Disk Agent for processing. For a restore session, the Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

media allocation policy Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.

media condition The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of read and write errors with tape media. Media need to be replaced when they are marked as POOR.

media condition factors The user-assigned age threshold and overwrite threshold used to determine the state of a medium.

media label A user-defined identifier used to describe a medium.

media location A user-defined physical location of a medium, such as "building 4" or "off-site storage".

media management session A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.

media pool A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

media set The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.

media type The physical type of media, such as DDS or DLT.

media usage policy The media usage policy controls how new backups are added to the already used media. It can be `Appendable`, `Non-Appendable`, or `Appendable for incrementals only`.

medium ID A unique identifier assigned to a medium by Data Protector.

merging This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored.
See also overwrite.

Microsoft Exchange Server A "client-server" messaging and a workgroup system that offers a transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

Microsoft Management Console (MMC) *(Windows specific term)* An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.

Microsoft SQL Server A database management system designed to meet the requirements of distributed "client-server" computing.

Microsoft Volume Shadow Copy Service (VSS) A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets.
See also shadow copy, shadow copy provider, replica, and writer.

mirror *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* *See* target volume.

mirror rotation *(HP P9000 XP Disk Array Family specific term)* *See* replica set rotation.

mirror unit (MU) number *(HP P9000 XP Disk Array Family specific term)* A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family.
See also first-level mirror.

mirrorclone *(HP P6000 EVA Disk Array Family specific term)* A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.

MMD The Media Management Daemon process (service) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.

MMDB The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells.
See also CMMDB and 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. In an offline backup session, the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the time period of the data replication process. For instance, for backup to tape, until streaming of data to the tape is finished. Normal database operation is resumed before potential post-backup operations are started.
See also zero downtime backup (ZDB) and online backup.

offline recovery Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. 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
- ON-Bar catalog tables, which are used to back up dbobjects and track instances of dbobjects through multiple backups.

ONCONFIG *(Informix Server specific term)* An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, Informix Server uses the configuration values from the `onconfig` file in the directory *`INFORMIXDIR`*`\etc` (on Windows 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 of the data replication process. For instance, for backup to tape, until streaming of data to tape is finished. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. Normal database operation is resumed before potential post-backup operations are started.

In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored.

See also zero downtime backup (ZDB) and offline backup.

online recovery 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.

Oracle Data Guard *(Oracle specific term)* Oracle Data Guard is Oracle's primary disaster recovery solution. Oracle Data Guard is able to maintain up to nine standby databases, each of which is a real-time copy of the production (primary) database, to protect against corruptions, data failures, human errors, and disasters. If a failure occurs on the production (primary) database, then a failover to one of the standby databases which becomes the new primary database is possible. In addition, planned downtime for maintenance can be reduced because the production processing can be moved from the current primary database to a standby database and back quickly.

Oracle instance *(Oracle specific term)* Each installation of an Oracle database on one or more systems. One computer system can have several instances of a database running.

ORACLE_SID *(Oracle specific term)* A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired *`ORACLE_SID`*. The *`ORACLE_SID`* is included in the CONNECT DATA

parts of the connect descriptor in a `TNSNAMES.ORA` file and in the definition of the TNS listener in the `LISTENER.ORA` file.

original system The system configuration backed up by Data Protector before a computer disaster hits the system.

overwrite An option that defines one mode to resolve file conflicts during restore. All files are restored from a backup even if they are older than existing files.
See also merging.

ownership Backup ownership affects the ability of users to see and restore data. Each backup session and all the data backed up within it is assigned an owner. The owner can be the user that starts an interactive backup, the account under which the CRS process is running, or the user specified as the owner in the backup specification options.

If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.

If a modified backup specification is started by a user, the user is the owner unless the following is true:

- The user has the Switch Session Ownership user right.
- The backup session owner is explicitly defined in the backup specification, where the username, group or domain name, and the system name are specified.

If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.

If a backup is scheduled on a Windows Cell Manager, the session owner is the user specified during the installation, unless the above conditions are true.

When copying or consolidating 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/server/dr/p1s` (UNIX systems) with the filename `recovery.p1s`.

package *(MC/ServiceGuard and Veritas Cluster specific term)* A collection of resources (for example volume groups, application services, IP names, and addresses) that are needed to run a specific cluster-aware application.

pair status *(HP P9000 XP Disk Array Family specific term)* The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP P9000 XP Agent:

- PAIR – The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty.
- SUSPENDED – The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time.
- COPY – The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.

parallel restore Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism The concept of reading multiple data streams from an online database.

phase 0 of disaster recovery Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.

phase 1 of disaster recovery Installation and configuration of DR OS, establishing previous storage structure.

phase 2 of disaster recovery Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.

phase 3 of disaster recovery Restoration of user and application data.

physical device A physical unit that contains either a drive or a more complex unit such as a library.

post-exec A backup option that executes a command or script after the backup of an object or after the entire session completes. Post-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows 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.

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.

prealloc list A subset of media in a media pool that specifies the order in which media are used for backup.

primary volume (P-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU).
See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection *See* data protection and also catalog protection.

public folder store *(Microsoft Exchange Server specific term)* The part of the Information Store that maintains information in public folders. A public folder store consists of a binary rich-text `.edb` file and a streaming native internet content `.stm` file.

public/private backed up data When configuring a backup, you can select whether the backed up data will be:

- public, that is visible (and accessible for restore) to all Data Protector users
- private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

R

RAID Redundant Array of Independent Disks.

RAID Manager Library *(HP P9000 XP Disk Array Family specific term)* A software library that is used for accessing the configuration, status, and performance measurement data of a P9000 XP Array storage system, and for invoking operations on the disk array. It translates function calls into sequences of low-level SCSI commands.
See also HP P9000 XP Agent.

RAID Manager P9000 XP *(HP P9000 XP Disk Array Family specific term)* A software application that provides a command-line interface to disk arrays of the HP P9000 XP Disk Array Family. It offers an extensive set of commands for reporting and controlling the status of a P9000 XP Array storage system, and for performing various operations on the disk array.

rawdisk backup *See* disk image backup.

RCU *See* Remote Control Unit (RCU).

RDBMS Relational Database Management System.

RDF1/RDF2
(EMC Symmetrix specific term) A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices.

Recovery Catalog
(Oracle specific term) A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about:

- The physical schema of the Oracle target database
- Data file and archived log backup sets
- Data file copies
- Archived redo Logs
- Stored scripts

Recovery Catalog Database
(Oracle specific term) An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

recovery files
(Oracle specific term) Recovery files are Oracle specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces.
See also flash recovery area.

Recovery Manager (RMAN)
(Oracle specific term) An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

RecoveryInfo
When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume, and network configuration). This information is needed for disaster recovery.

recycle or unprotect
A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.

redo log
(Oracle specific term) Every Oracle database has a set of two or more redo log files. The set of redo log files for the database is known as the database's redo log. Oracle uses the redo log to record all changes made to data.

Remote Control Unit (RCU)
(HP P9000 XP Disk Array Family specific term) An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.

Removable Storage Management Database
(Windows specific term) A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications to access and share the same media resources.

reparse point
(Windows specific term) A system-controlled attribute that can be associated with any directory or file. The value of a reparse attribute can have user-controlled data. The format of the data is understood by the application that stored the data and a filesystem filter that was installed to interpret the data and process such files. Whenever the filesystem encounters a file with a reparse point, it attempts to find the filesystem filter associated with the data format.

replica
(ZDB specific term) An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware or software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror or snapclone), or a virtual copy (for example, a snapshot). From perspective of a basic operating system, the complete physical disk containing backup objects is replicated. However, if a volume manager is used on a UNIX system, the whole volume or disk group containing a backup object (logical volume) 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), mirror unit (MU) number, and replica set rotation.

RMAN *(Oracle specific term)* *See* Recovery Manager.

RSM The Data Protector Restore Session Manager controls restore and object verification sessions. This process always runs on the Cell Manager system.

RSM *(Windows specific term)* Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.

S

SAPDBA *(SAP R/3 specific term)* An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.

scanning A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device if someone has manually manipulated media without using Data Protector to eject or enter, for example.

Scheduler A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.

secondary volume (S-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration.
See also primary volume (P-VOL) and Main Control Unit (MCU).

session *See* backup session, media management session, and restore session.

session ID An identifier of a backup, restore, object copy, object consolidation, object verification, or media management session, consisting of the date when the session ran and a unique number.

session key This environment variable for the pre-exec and post-exec script is a Data Protector unique identification of any session, including preview sessions. The session key is not recorded in the database, and it is used for specifying options for the `omnimnt`, `omnistat`, and `omniabort` commands.

shadow copy *(Microsoft VSS specific term)* A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original

volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant.
See also Microsoft Volume Shadow Copy Service and replica.

shadow copy provider *(Microsoft VSS specific term)* An entity that performs the work on creating and representing the volume shadow copies. Providers own the shadow copy data and expose the shadow copies. Providers can be software (for example, system providers) or hardware (local disks, disk arrays).
See also shadow copy.

shadow copy set *(Microsoft VSS specific term)* A collection of shadow copies created at the same point in time.
See also shadow copy and replica set.

shared disks A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

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, and high-speed databases. If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror *(EMC Symmetrix Disk Array and HP P9000 XP Disk Array Family specific term)* A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes.
See also replica and split mirror creation.

split mirror backup *(EMC Symmetrix specific term)* *See* ZDB to tape.

split mirror backup *(HP P9000 XP Disk Array Family specific term)* *See* ZDB to tape, ZDB to disk, and ZDB to disk+tape.

split mirror creation *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes.
See also split mirror.

split mirror restore *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards. Individual backup objects or complete sessions can be restored using this method.
See also ZDB to tape, ZDB to disk+tape, and replica.

sqlhosts file or registry *(Informix Server specific term)* An Informix Server connectivity information file (on UNIX 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 *(disaster recovery specific term)* A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows or Linux system and stored on the Cell Manager. It contains system information required for installing and configuring the operating system on the target system in the case of a disaster.
See also target system.

SRDF *(EMC Symmetrix specific term)* The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.

SSE Agent (SSEA) *See* HP P9000 XP Agent.

sst.conf file The file `/usr/kernel/drv/sst.conf` is required on each Data Protector Solaris client to which a multi-drive library device is connected. It must contain an entry for the SCSI address of the robotic mechanism of each library device connected to the client.

st.conf file The file `/kernel/drv/st.conf` is required on each Data Protector Solaris client with a backup device connected. It must contain device information and a SCSI address for each backup drive connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

stackers Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

standalone file device A file device is a file in a specified directory to which you back up data.

Storage Group *(Microsoft Exchange Server specific term)* A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.

storage volume *(ZDB specific term)* An object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, filesystems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

StorageTek ACS library *(StorageTek specific term)* Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.

switchover *See* failover.

Sybase Backup Server API *(Sybase specific term)* An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

Sybase SQL Server *(Sybase specific term)* The server in the Sybase "client-server" architecture. Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

SYMA *See* EMC Symmetrix Agent.

synthetic backup A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

synthetic full backup The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

System Backup to Tape *(Oracle specific term)* An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases *(Sybase specific term)* The four system databases on a newly installed Sybase SQL Server are the:

- master database (master)
- temporary database (tempdb)
- system procedure database (sybsystemprocs)
- model database (model).

System Recovery Data file *See* SRD file.

System State *(Windows specific term)* The System State data comprises the Registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory services and the SYSVOL directory are also contained in the System State data. If the server is running the Cluster service, the System State data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

system volume/disk/partition A volume/disk/partition containing operating system files. Microsoft terminology defines the system volume/disk/partition as the volume/disk/partition containing files required for the initial step of the boot process.

SysVol *(Windows specific term)* A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

T

tablespace A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

tapeless backup *(ZDB specific term)* *See* ZDB to disk.

target (R2) device *(EMC Symmetrix specific term)* An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type.
See also source (R1) device.

target database *(Oracle specific term)* In RMAN, the target database is the database that you are backing up or restoring.

target system *(disaster recovery specific term)* A system after a computer disaster has occurred. The target system is typically in a non-bootable state and the goal of disaster recovery is to restore this system to the original system configuration. The difference between a faulty system and a target system is that a target system has all faulty hardware replaced.

target volume *(ZDB specific term)* A storage volume to which data is replicated.

Terminal Services *(Windows specific term)* Windows Terminal Services provide a multi-session environment that allows clients to access a virtual Windows desktop session and Windows-based programs running on the server.

thread *(Microsoft SQL Server specific term)* An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

TimeFinder *(EMC Symmetrix specific term)* A business continuation process that creates an instant copy of single or multiple Symmetrix Logical Devices (SLDs). The instant copy is created on specially preconfigured SLDs called BCVs and is accessible via a separate device address to the system(s).

TLU Tape Library Unit.

TNSNAMES.ORA *(Oracle and SAP R/3 specific term)* A network configuration file that contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

transaction A mechanism for ensuring that a set of actions is treated as a single unit of work. Databases use transactions to keep track of database changes.

transaction backup Transaction backups generally use fewer resources than database backups, so they can be created more frequently than database backups. By applying transaction backups, you can recover the database to a specific point in time prior to when a problem occurred.

transaction backup *(Sybase and SQL specific term)* A backup of the transaction log providing a record of changes made since the last full or transaction backup.

transaction log backup Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.

transaction log files Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.

transaction log table *(Sybase specific term)* A system table in which all changes to the database are automatically recorded.

transportable snapshot *(Microsoft VSS specific term)* A shadow copy that is created on the application system and can be presented to the backup system where a backup can be performed.
See also Microsoft Volume Shadow Copy Service (VSS).

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, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

user disk quotas NTFS quota-management support enables an enhanced tracking mechanism and control over disk space usage on shared storage volumes. Data Protector backs up user disk quotas on the whole system and for all configured users at a time.

user group Each Data Protector user is member of a User Group. Each User Group has a set of user rights that are given to every user in that User Group. The number of User Groups with their associated user rights can be defined as desired. Data Protector provides three default user groups: admin, operator, and user.

user profile *(Windows specific term)* Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.

user rights User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

user_restrictions file A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than *admin* and *operator*.

V

vaulting media The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

verify A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.

Virtual Controller Software (VCS) *(HP P6000 EVA Disk Array Family specific term)* The firmware that manages all aspects of storage system operation, including communication with HP Command View EVA through the HSV controllers.
See also HP Command View (CV) EVA.

Virtual Device Interface *(Microsoft SQL Server specific term)* This is a Microsoft SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk *(HP P6000 EVA Disk Array Family specific term)* A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array.
See also source volume and target volume.

virtual full backup An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

Virtual Library System (VLS) A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

virtual server A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

virtual tape *(VLS specific term)* An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs.
See also Virtual Library System (VLS) and virtual tape library (VTL).

virtual tape library (VTL) *(VLS specific term)* An emulated tape library that provides the functionality of traditional tape-based storage.
See also Virtual Library System (VLS).

VMware management client *(VMware (Legacy) integration specific term)* The client that Data Protector uses to communicate with VMware Virtual Infrastructure. This can be a VirtualCenter Server system (VirtualCenter environment) or an ESX Server system (standalone ESX Server environment).

volser *(ADIC and STK specific term)* A VOLume SERial number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

volume group A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volume mountpoint *(Windows specific term)* An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

Volume Shadow Copy Service *See* Microsoft Volume Shadow Copy Service (VSS).

VSS *See* Microsoft Volume Shadow Copy Service (VSS).

VSS compliant mode *(HP P9000 XP Disk Array Family VSS provider specific term)* One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching the disks.
See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

VxFS Veritas Journal Filesystem.

VxVM (Veritas Volume Manager) A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.

W

Wake ONLAN Remote power-up support for systems running in power-save mode from some other system on the same LAN.

Web reporting The Data Protector functionality that allows you to view reports on backup, object copy, and object consolidation status and Data Protector configuration using the Web interface.

wildcard character A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

Windows configuration backup Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.

Windows Registry A centralized database used by Windows to store configuration information for the operating system and the installed applications.

WINS server A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.

writer *(Microsoft VSS specific term)* A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.

X

XBSA interface *(Informix Server specific term)* ON-Bar and Data Protector communicate with each other through the X/Open Backup Services Application Programmer's Interface (XBSA).

Z

ZDB *See* zero downtime backup (ZDB).

ZDB database *(ZDB specific term)* A part of the IDB, storing ZDB-related information such as source volumes, replicas, and security information. The ZDB database is used in zero downtime backup, instant recovery, and split mirror restore sessions.
See also zero downtime backup (ZDB).

ZDB to disk *(ZDB specific term)* A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time. Multiple replicas, produced using the same backup specification at different times, can be kept in a replica set. A replica from ZDB to disk can be restored using the instant recovery process.
See also zero downtime backup (ZDB), ZDB to tape, ZDB to disk+tape, instant recovery, and replica set rotation.

ZDB to disk+tape *(ZDB specific term)* A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored using the instant recovery process, the standard Data Protector restore from tape, or with specific disk array families, split mirror restore.
See also zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.

ZDB to tape *(ZDB specific term)* A form of zero downtime backup where data in the replica produced is streamed to a backup medium, typically tape. Instant recovery is not possible from such a backup, so the replica need not be retained on the disk array after backup completion. The backed up data can be restored using standard Data Protector restore from tape. With specific disk array families, split mirror restore can also be used.
See also zero downtime backup (ZDB), ZDB to disk, ZDB to disk+tape, instant recovery, and replica.

zero downtime backup (ZDB) A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation.
See also ZDB to disk, ZDB to tape, ZDB to disk+tape, and instant recovery.

Index