HP OpenView Storage Data Protector Troubleshooting Guide

Manual Edition: July 2006

Manufacturing Part Number: B6960-96003

Release A.06.00

Legal Notices

Contents

Contents

Contents

Printing History

Manual 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

Part Number	Manual Edition	Product
B6960-96003	July 2006	Data Protector Release A.06.00

Conventions

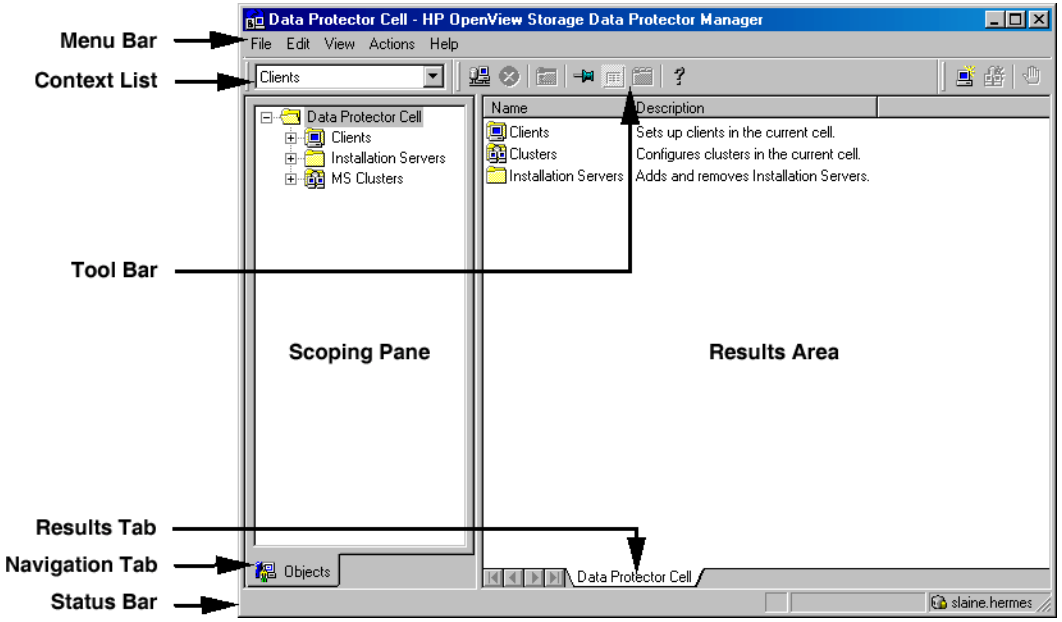
The following typographical conventions are used in this manual.

Table 2

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

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

Figure 1 Data Protector Graphical User Interface



Contact Information

General Information

General information about Data Protector can be found at

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

Technical Support

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

http://www.itrc.hp.com

Information about the latest Data Protector patches can be found at

http://www.itrc.hp.com

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

Documentation Feedback

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

storagedocs.feedback@hp.com

Training Information

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

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

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

Data Protector Documentation

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

Manuals

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

HP OpenView Storage Data Protector Concepts Guide

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

HP OpenView Storage Data Protector Installation and Licensing Guide

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

HP OpenView Storage Data Protector Troubleshooting Guide

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

HP OpenView Storage Data Protector Disaster Recovery Guide

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

HP OpenView Storage Data Protector Integration Guide

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

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

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

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

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

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

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

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

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

HP OpenView Storage Data Protector Integration Guide for HP OpenView

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

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

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

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

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

There are two versions of the manual:

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

HP OpenView Storage Data Protector Zero Downtime Backup Concepts Guide

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

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

This manual describes how to configure and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility and TimeFinder, and HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide

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

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

HP OpenView Storage Data Protector MPE/iX System User Guide

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

HP OpenView Storage Data Protector Media Operations User's Guide

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

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

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

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

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

Online Help

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

Documentation Map

Abbreviations

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

Abbreviation	Manual
CLI	Command Line Interface Reference Guide
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
Help	Online Help
IG-IBM	Integration Guide—IBM Applications
IG-MS	Integration Guide—Microsoft Applications
IG-O/S	Integration Guide—Oracle, SAP R/3, and SAP DB/MaxDB
IG-OV	Integration Guide—HP OpenView Service Information Portal/OpenView Reporter
IG-OVOU	Integration Guide—HP OpenView Operations, UNIX
IG-OVOW	Integration Guide—HP OpenView Operations 7.1x, 7.2x, Windows
IG-OVOW	Integration Guide—HP OpenView Operations 7.5, Windows
IG-Var	Integration Guide—Sybase, Network Node Manager, NDMP and VMware
Install	Installation and Licensing Guide
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide

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

Map

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

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

Integrations

Look in these manuals for details of the following integrations:

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

In This Book

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 manual 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.

Audience

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

Organization

The manual is organized as follows:

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. Note that this guide does not contain installation, integration, ZDB, and disaster recovery related problems. They are described in the respective guides.
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 Chapter 11, “Before Calling Support,” on page 81.

TIP

For an overview and hints on performance aspects of Data Protector, see the online 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 OpenView Storage 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 online Help index: “patches”.

✓ You have appropriate operating system patches installed.

The required operating system patches are listed in the *HP OpenView Storage 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: *<Data_Protector_home>*\log

HP-UX and Solaris: /var/opt/omni/log and /var/opt/omni/server/log

Other UNIX: /usr/omni/log

Novell NetWare: SYS:\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

```
11/30/2005 1:44:50 PM  INET.3048.3036 ["inetnt/allow_deny.c
/main/dp55/6":467] A.05.50 b330
A request 0 (BDF) came from host computer.company.com
(10.17.4.170) which is not in AllowList: not proceeding with
this request!
```

Contents of Log Files

The table below describes the Data Protector log files:

Table 1-1 Data Protector Log Files

debug.log	Contains unexpected conditions. While some can help you, the information is mainly used by the support organization.

Table 1-1 Data Protector Log Files

inet.log	Contains local security related events for the client, such as denied requests. On UNIX, 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 made to this log. The file can be used when recovering the IDB to find the medium with the IDB backup and to find out which media were 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.

Table 1-1 Data Protector Log Files

RDS.log	Contains IDB logs. The file resides on the Cell Manager in:
	Windows:
	`<Data_Protector_home>\db40\datafiles\catalog`
	UNIX:
	`/var/opt/omni/server/db40/datafiles/catalog`

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 only)	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.

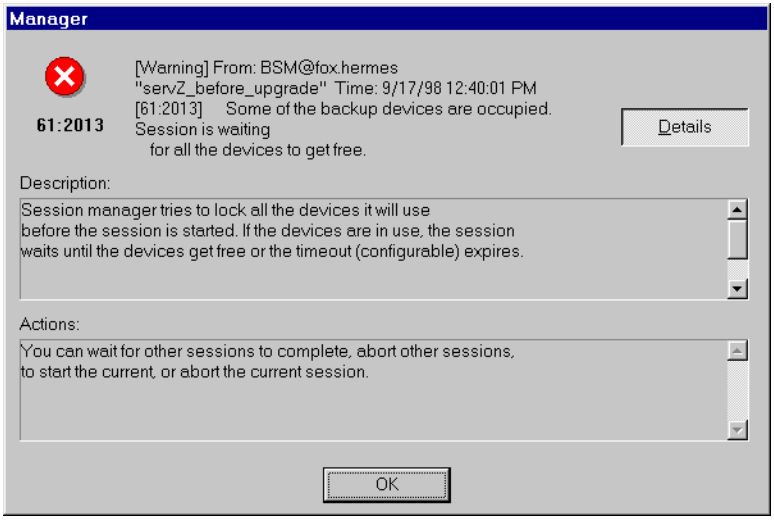
Data Protector Error Messages

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 1-1 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: *<Data_Protector_home>*\help\enu\Trouble.txt

UNIX: /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 Files

Sometimes you can solve a problem by setting a Data Protector variable. This guide provides instructions which variables to set to solve specific problems.

Global Options

Global options affect the entire Data Protector cell and cover various aspects of Data Protector, such as timeouts and limits. All global options are described in the global options file, which you can edit to customize Data Protector.

The global options file is located on the Cell Manager:

Windows:
`<Data_Protector_home>\Config\Server\Options\global`

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

To set global options, edit the `global` file. Uncomment the line of the desired option by removing the "#" mark, and set the desired value.

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

Most Often Used Global Variables

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

- `MediaView`: Changes the fields and their order in the Media Management context.
- `MaxBSessions`: Changes the default limit of five concurrent backups.
- `InitOnLoosePolicy`: Enables Data Protector to automatically initialize blank or unknown media if the `loose` media policy is used.
- `MaxMAperSM`: Changes the default limit of concurrent devices per backup session. (Maximum device concurrency is 32.)

- DCDirAllocation: Determines the algorithm used for selecting the dcbf directory for a new detail catalog binary file: fill in sequence (default), balance size, or balance number.
- 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 online 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 online Help index: “checks performed by Data Protector”.

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 variables can be set on each client in the file:

Windows: <*Data_Protector_home*>\omnirc

HP-UX and Solaris: /opt/omni/.omnirc

Other UNIX: /usr/omni/.omnirc

Novell NetWare: sys:\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 variables:
   - When creating the omnirc file (either by copying or by using an editor), verify its permissions. On UNIX, 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 and recommended for Data Protector CRS and `Inet` services on Windows. Specifically on Windows, restarting is not required when adding or changing entries, only when removing entries (or renaming the file).

NOTE

When using special characters in variable 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 OpenView Storage Data Protector Disaster Recovery Guide*.

Most Often Used Omnirc Variables

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

- **OB2_SSH_ENABLED:** To enable secure remote installation using secure shell (SSH), set this variable 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 variable to `1` on the Installation Server. The default value is `0` (not set).
- **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 only): Defines when to use the "last inode change" time for incremental backups.
- **OB2INCRDIFFTIME** (UNIX only): Specifies an "incremental latency" period that is enforced when checking the "last inode change" time with incremental backups. This variable takes effect only when the **OB2CHECKCHANGETIME** variable 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.
- **OB2SANCONFSCSITIMEOUT=s** (Windows only): 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 online 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` utilities to verify the TCP/IP configuration. For detailed steps, see the online Help index: “checking, TCP/IP setup”.

Testing DNS Resolution

Test DNS resolution among hosts by running:

```
omnicheck -dns
```

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

For more information on the command, see the online 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: `<%SystemRoot%>\System32\drivers\etc`

UNIX: `/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.

Other Problems

Problem

Client fails with "Connection reset by peer"

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

```
[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, apply the change on the Cell Manager system first.

If the problem persists or the Cell Manager resides on UNIX, 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

   MaxDataRetries:(DWORD):8
   ```

2. Restart the system.

CAUTION

Making a mistake when editing the registry can cause your system to become unstable and 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 online 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 online 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, first ensure that you do not have a name resolution problem. For more information, see Chapter 2, “Troubleshooting Networking and Communication,” on page 15.

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 <Service_Name> on <System_Name>.`

`Access is denied.`

Action

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

Problem

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 <Service_Name> on <System_Name>. The system can not find the file specified!`

Action Reinstall Data Protector on the Cell Manager, preserving the IDB. For instructions, see “Miscellaneous problems that require reinstalling Data Protector on the Cell Manager” on page 71.

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. In the `<Data_Protector_home>\tmp` directory, delete the `mmd.ctx` file.
2. Restart the services using the `omnisv -start` command.

Problem **RDS does not work on the Windows TSE Cell Manager**

Action Use TCP transport instead of local transport by modifying the file `<Data_Protector_home>\db40\datafiles\catalog\rdmserver.ini`. Under `TCP Configuration`, set `Enabled` to `yes`.

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: `rds`
- 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

Raima Velocis server daemon could not be started

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

```
Could not start Raima Velocis server daemon.
```

Action

See `/var/opt/omni/server/db40/datafiles/catalog/RDS.log` for details.

Check if you have all IDB files in the directory `/var/opt/omni/server/db40`. Compare the list of files with that in `/opt/omni/newconfig/var/opt/omni/server/db40`. Ensure that these directories are mounted.

Problem **Raima Velocis server daemon is apparently not running**

A Data Protector command terminates with:

```
[12:1166] Velocis daemon error - the daemon is probably not running
```

Action Check if the database server is really not running by using the `omnisv -status` command.

- If the database server is not running, start it by using the `omnisv -start` command.
- If the database server is running, then it is likely that the `/var/opt/omni/server/db40` directory does not exist or some of the files are missing. This can happen if someone has accidentally removed the directory or the files. Recover the IDB. For information, see the online Help index: “IDB recovery”.

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`

Data Protector Processes

Table 3-1 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 3-1 Data Protector Processes Running During Different Operations

		Always	Backup	Restore	Media Management

Cell Manager	Windows	`omniinet.exe`
		`rds.exe`
		`mmd.exe`
		`crs.exe`
			`bsm.exe`	`rsm.exe`	`msm.exe`

	UNIX	`rds`
		`mmd`
		`crs`
			`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`

4 Troubleshooting User Interface

User Interface Startup Problems

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

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 OpenView Storage 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.

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 online Help index: “user groups”.

Problem **Connection to a remote system refused**

On Windows or Novell NetWare, 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.

Display Problems

Problem

Corrupted object names in the Data Protector GUI on UNIX

Names of GUI objects, such as backup devices and backup specifications, appear corrupted in the Data Protector GUI on UNIX.

If these GUI objects were created under a certain locale, they may appear corrupted when viewed in a different locale. Regardless of the corrupted display of the GUI object names, such GUI objects are still usable.

For example, you configured a backup device and named it using non-ASCII characters. In this case, its name may appear corrupted if the GUI is run in a locale that uses only ASCII. Although its name appears corrupted in the GUI, you can still perform backups and restores using this device.

Action

You can either recreate these objects in a locale that uses UTF-8 encoding or still use the old locale on the system where the Data Protector GUI is running. In the latter case, you will not be able to switch encodings in the GUI and thus use the internationalization features of Data Protector.

5 Troubleshooting Devices and Media

General Device and Media Problems

Backup devices are subject to specific Data Protector licenses. See the *HP OpenView Storage 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 OpenView Storage 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 online Help index: “robotics drivers”.

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 online Help index: "setting advanced options for devices and media".

For information on supported SCSI HBAs/FC HBAs, see the *HP OpenView Storage 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 **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" on page 9.

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 5-1 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

Cannot use devices after upgrading to Data Protector A.06.00

After upgrading to Data Protector A.06.00, you cannot use devices that were configured as different device types in previous releases. For example, you cannot use 9940 devices that were configured as 9840 devices, 3592 devices that were configured as 3590 devices, or SuperDLT devices that were configured as DLT devices. The following error displays:

```
[Critical] From: BMA@computer.company.com "SDLT" Time:
5/22/2006 5:12:34 PM
[90:43] /dev/rmt/1m
Invalid physical device type => aborting
```

Action

Manually reconfigure these devices using the `mchange` command, located on the Cell Manager in:

Windows: `<Data_Protector_home>\bin\utilns\NT`

HP-UX: `/opt/omni/sbin/utilns/HPUX`

Solaris: `/opt/omni/sbin/utilns/SOL`

`mchange -pool PoolName -newtype NewMediaClass`

where:

PoolName is the media pool with devices that are currently configured and should be reconfigured (for example, Default DLT, Default T3590, or Default T9840).

NewMediaClass is the new media type of the devices, for example, T9940 for 9940 devices, T3592 for 3590 devices, and SuperDLT for SuperDLT devices.

Example

```
mchange -pool "Default DLT" -newtype "SuperDLT"
```

The command changes media types for all media, drives, and libraries that use the specified media pool.

After you have run this command for each device you wanted to change, move the media associated with the reconfigured devices from the current media pool to the media pool corresponding to these media. For example, move the media associated with the reconfigured 9940 devices to the Default T9940 media pool. For instructions, see the online Help index: “moving media”.

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).
- 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.

Problem **Cannot find the device file for the XCopy engine on an external FC bridge**

When configuring the XCopy engine, you cannot locate the device file for the external FC bridge.

Action

1. Using the FC bridge administration utility, ensure that the `Active Fabric` setting on the FC bridge is `ON`.

2. On the backup system, run:

   ```
   ioscan -fkn
   ```

   In the output, the name of the external FC bridge and the device file for the external FC bridge are listed. The output should be similar to:

   ```
   ctl 24 0/2/0/0.2.24.25A.05.10.0.5 sctl CLAIMED DEVICE HP
   A4688A

   /dev/rscsi/c19t0d5
   ```

Problem **Cannot find the device file for the XCopy engine on an internal FC bridge**

When configuring the XCopy engine, you cannot locate the device file for the internal FC bridge.

Action

1. Using the backup device `Interface Manager` telnet utility, ensure that you have installed the License Key that enables direct backup.
2. On the backup system, run:

   ```
   ioscan -fkn
   ```

   In the output, the name of the internal FC bridge and the device file for the internal FC bridge are listed. The output should be similar to:

   ```
   ctl 5 0/8/0/0.1.16.255.0.0.2 sctl CLAIMED DEVICE HP
   C7200FC Interface

   /dev/rscsi/c18t0d7
   ```

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 push 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.

The same problem occurs if user A performs a full backup, then user B performs an object copy session, and the original is exported or overwritten. User A cannot perform an incremental backup because the full backup (the copy) now belongs to user B.

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 online Help index: "setting backup options".

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 online 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 OpenView Storage 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
```

Stop and start 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 online 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.

To enable encoding switching in the GUI on UNIX, set the locale to one that uses UTF-8 character encoding prior to starting the GUI.

For internationalization limitations, see the online Help index: “internationalization”.

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 OpenView Storage 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 online Help index: “internationalization”.

Problem

Restore problems with non-ASCII file names during the IDB conversion

You may run into problems if you selected a non-ASCII file or directory for restore and one of the following is true:

- The IDB data for that client has already been converted, but the client has not been upgraded yet.
- The client has been upgraded, but the IDB data for that client has not been converted yet.

Action

Before the restore:

- Upgrade the Disk Agent on the client.
- Wait for the IDB conversion to finish.

  You can see the status of the IDB conversion in the Data Protector GUI in the Monitor context.

Cluster Problems

Problem

Novell NetWare cluster shared volumes are not backed up during full server backup

Shared volumes on a Novell NetWare cluster are not backed up during full server backups. A possible cause for this is improper handling of SMS clustered resources, causing clustered volumes to be skipped because the TSA module was loaded with cluster support enabled.

Action

Run the `TSAFS /NoCluster` command on the active node to disable cluster support.

Problem

Backup or restore on a TruCluster Server is aborted

Backup or restore session aborts with:

```
Internal error in ("ma/xma/bma.c) => process aborted

This is an unexpected condition and is likely due to a corrupted
media or combination of circumstances involving both this product
and the operating system.
```

This error can occur when:

- The device used for backup is configured on a cluster virtual server.
- A filesystem being backed up resides on a cluster virtual server.

Action

Set the following `omnirc` variables on the TruCluster Server:

- `OB2BMANET=1`
- `OB2RMANET=1`
- `OB2RDANET=1`
- `OB2BDANET=1`

For instructions, see “Omnirc Options” on page 10.

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.

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 **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 OpenView Storage Data Protector Installation and Licensing Guide*.

Problem **Restore fails after upgrading the MoM Manager**

The following error messages may be displayed:

- `Unknown internal error`
- `Started session manager got bad options`
- `Cannot get information from backup host`

After upgrading the MoM Manager/CMMDB Server from a Data Protector version earlier than A.05.50, you cannot perform a filesystem or integration restore of an older Data Protector client using the Data Protector A.06.00 MoM GUI.

Action Either use the old MoM GUI for restore, or upgrade the clients to Data Protector A.06.00.

Problem **Poor backup performance on Novell NetWare Server**

Backup performance on a Novell NetWare Server is poor. Backup does not run continuously, but intermittently. This is a known problem caused by the system `TCPIP.NLM`.

Action Set the following parameter:

```
SET TCP DELAYED ACKNOWLEDGEMENT = OFF
```

This improves backup performance without any secondary effects.

Problem **Data Protector fails to start parallel restore Media Agent on Novell NetWare clients**

Data Protector UNIX Session Manager fails to start restore Media Agents in parallel on Novell NetWare clients with one of the following errors:

- `Could not connect to inet`
- `Connection reset by peer`

Some parallel restore sessions may complete without errors, while other restore sessions are not even started.

Action

Increase the maximum number of retries to start an agent by setting the global option `SmMaxAgentStartupRetries` to 2 or more (max. 50). For instructions, see “Global Options” on page 9.

7 Troubleshooting Object Copy 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” on page 9.

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.

8 Troubleshooting the Data Protector Internal Database (IDB)

Problems Due to Missing Files or Directories

Data Files (Directories) Missing

The following IDB data files (directories) should exist on the Cell Manager in:

Windows: *<Data_Protector_home>*\db40

UNIX: /var/opt/omni/server/db40

- datafiles\catalog
- datafiles\cdb
- datafiles\mmdb
- dcbf
- logfiles\rlog
- logfiles\syslog
- meta
- msg

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. For instructions, see “Miscellaneous problems that require reinstalling Data Protector on the Cell Manager” on page 71.
2. Restart the Cell Manager.

Temporary Directory Missing

The following temporary directory should exist on the Cell Manager:

Windows: *<Data_Protector_home>*\tmp

UNIX: /var/opt/omni/tmp

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. Close the Data Protector GUI.
2. Stop the Data Protector services/processes. On the Cell Manager, run:

   Windows: *<Data_Protector_home>*\bin\omnisv -stop

   UNIX: /opt/omni/sbin/omnisv -stop
3. On the Cell Manager, manually create the directory tmp in:

   Windows: *<Data_Protector_home>*

   UNIX: /var/opt/omni
4. Start the services/processes:

   Windows: *<Data_Protector_home>*\bin\omnisv -start

   UNIX: /opt/omni/sbin/omnisv -start
5. Restart the Data Protector GUI.

Problems During Backup and 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.
- On the Windows Cell Manager, file name conversion in the IDB was running while the client was being backed up. Consequently, the backup was performed using the `No log` option and hence no data was written to the IDB for this client in this session.

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. Run 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. Run the `omnidbutil -show_locked_devs` command to see if any devices and media are locked by Data Protector.
4. If there are, run 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.
- ***Windows:*** In the Windows Task Manager, the Data Protector MMD process (`mmd.exe`) is not displayed.

  UNIX: 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. Run the `omnisv -stop` command to stop the Data Protector services/processes.
3. Run the `omnisv -start` command to start the Data Protector services/processes.
4. Run 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 online Help index: “minor IDB corruptions in DCBF”.

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 objects in the IDB and the objects' sizes are 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`.

Problem **IDB purge is slow**

The file versions purge in the IDB is extremely slow.

Action Check if the following message is logged for the current purge session in the *<Data_Protector_home>*\log\server\purge.log file:

```
Multiple passes needed. This will decrease the performance
of the purge session. To improve performance increase the
amount of memory a purge session is allowed to use.
```

If the log file contains this message, abort the session and increase the value of the global option `PurgeBufferSize`. For instructions, see “Global Options” on page 9. Then restart the purge session.

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, the following is true:

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

UNIX: 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` or `IDB Tablespace Space Low` notification is issued.

Action

Extend the IDB size. For information, see the online 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. On the Cell Manager, from the directory:

Windows: `<Data_Protector_home>\bin`

UNIX: `/opt/omni/sbin`

Run:

`omnidbutil -cdbsync <Cell_Server_Hostname>`

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

Problem

IDB fails due to memory allocation problems on HP-UX

The RDS service fails on HP-UX during IDB maintenance or query operations because of memory allocation problems.

Action

1. On the Cell Manager, set the `omnirc` variable `_M_ARENA_OPTS=1:32`. For instructions, see “Omnirc Options” on page 10.
2. Restart the Data Protector services:

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

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 online Help index: “IDB recovery”.

Problem

Miscellaneous problems that require reinstalling Data Protector on the Cell Manager

For any reason, Data Protector needs to be reinstalled on the Cell Manager and you need to preserve the IDB.

Action

Reinstall Data Protector on the Cell Manager as follows:

1. Stop the Data Protector services.
2. Copy the *<Data_Protector_home>*\db40 and *<Data_Protector_home>*\Config directories to a safe location.
3. Start the Data Protector services.
4. Uninstall Data Protector on the Cell Manager, and then reinstall Data Protector.
5. Stop the Data Protector services.
6. Copy the previously saved data back to the *<Data_Protector_home>*\db40 and *<Data_Protector_home>*\Config directories.
7. Start the Data Protector services.

9 Troubleshooting Reporting and Notifications

Reporting and Notification Problems

Problem

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

If you use Microsoft Outlook XP, or Microsoft Outlook 98/2000 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 hangs. 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 online Help index: “send methods”.
- Use the Data Protector CLI to start reports:

  ```
  omnirpt -report licensing -email <email_address>
  ```

  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 OpenView Storage 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 Data Protector Online Help

Introduction

The Data Protector online Help consists of two parts:

- **Help Topics** provide conceptual information, step-by-step procedures, and examples.
- **Help Navigator** is context-sensitive Help, explaining screens and options in the Data Protector GUI.

The Help format depends on the platform on which you are running the Data Protector GUI:

- On Windows, Microsoft HTML Help is used.
- On UNIX, WebHelp is used.

Troubleshooting Online Help on Windows

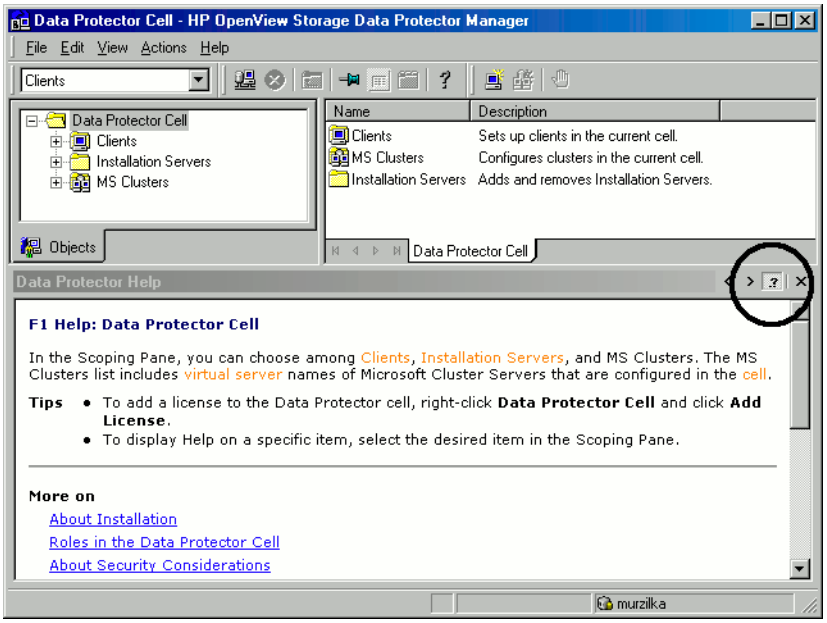
Problem

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

Action

- If you use `Microsoft HTML Help` mode (default option), ensure that the button shown below is enabled.

Figure 10-1 The Help Tracing Button Enabled



- If you use `Default HTML Browser` mode (an external HTML browser for displaying the help files) go to `File` menu, click `Preferences` and enable the `Check the box to enable the context-sensitive help navigator` option. Then restart the Help Navigator.

Troubleshooting Online Help on UNIX

Problem

Online Help start and display problems

If your browser (HTML viewer) is not properly set, you can run into online Help start and display problems.

Action

Set the browser as follows:

1. In the `File` menu, click `Preferences`, and then `Settings` to open the `HTML Viewer Settings` dialog.
2. In `Location of executable script or binary file` , type the location of your browser (for example, `/opt/mozilla`).
3. In `Command to start viewer`, specify the command that will start the browser (for example, `mozilla $HTML$`).

Problem

Search does not work on Mozilla

The search functionality does not work properly in the Data Protector online Help on Mozilla with the default Mozilla security settings. To enable the search, it is recommended to create a new Mozilla profile and use it only for viewing Data Protector online Help.

Action

1. Run the `Mozilla Profile Manager`:

   ```
   /opt/mozilla/mozilla -profilemanager
   ```

2. Create a new profile named `Data Protector Help` and start Mozilla using this profile.
3. In the `Edit` menu, select `Preferences` and then expand `Privacy & Security`.
4. Click `SSL` and deselect the `Sending form data from an unencrypted page to an unencrypted page` warning option. Click `OK`.

The changed security option will be saved only in the newly created profile without changing other user profiles. This profile will enable you to search in the Data Protector online Help without compromising your system security.

Problem

Text in the online Help topics is too small

The default Mozilla font size setting makes the topic text unreadable.

Action

Configure Mozilla as follows:

1. Make sure the browser is started with the Mozilla profile which you use for viewing Data Protector online Help.
2. In the Edit menu, click `Preferences`.
3. In the Category pane, expand `Appearance` and click `Fonts`.
4. In the Minimum Font Size drop-down list, select `10` or a higher value. Click `OK`.

The change will be saved for future sessions.

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” on page 2.
- ✓ You have checked if your problem is described in this guide. For installation, integration, ZDB, and disaster recovery related problems, check the troubleshooting sections of the respective 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” on page 84.

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.

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:
`<Data_Protector_home>\Config\server\Options\trace`

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

Using the OB2OPTS 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 in:

Windows: `<Data_Protector_home>\Config\server\Schedules` or `<Data_Protector_home>\Config\server\Barschedules`

UNIX: `/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 1-99 sch.txt
-full
-only 2006
     -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 1-99[,C:<n>][,T:<s>][,U] <XYZ> [<host>]`

where:

- `1-99` is the debug range. Specify the range 1-99 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” on page 85.
  - `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 (Novell NetWare, MPE), millisecond resolution is 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 11-1 Disk Space Required for Circular Debugging

System	Maximum disk space required
Media Agent client	`2*n [kB]` for each running MA in a backup or restore
Disk Agent client	`2*n [kB]` for each mount point in a backup or restore
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.

The Name and Location of Debug Files

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

Windows: *<Data_Protector_home>*\tmp

UNIX: /tmp

Novell NetWare: SYS:\USR\OMNI\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 trace.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` variable `OB2DBGDIR`. For instructions, see “Omnirc Options” on page 10.

Debugging Inet

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

Windows:

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

`-debug 1-140 <POSTFIX>`

UNIX:

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 1-140 DBG_01.txt
   ```

2. Save the file and run 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.

Windows:

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

`-debug 1-140 <POSTFIX> <Cell_Manager_name>`

UNIX:

1. Stop the CRS by running:

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

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

   `/opt/omni/lbin/crs -debug 1-140 <POSTFIX>`

Microsoft Cluster Server Environment:

In the Data Protector shared directory, edit the file:

`<Data_Protector_home>\Config\server\options\Trace`

Add the following lines:

```
ranges=1-99,110-500

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 Environment:

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 run 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.

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 OpenView Storage 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.

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 running the command from the respective Cell Manager.
- When a debug and logfile collector is used on 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 run 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.

The omnidlc Command Syntax

```
omnidlc {-session <sessionID> | -did <debugID> | -postfix
<string> | -no_filter} [-hosts <list>] [-pack <filename> |
-depot [<directory>] | -space | -delete_dbg] [-no_getinfo]
[-no_logs] [-no_debugs] [-no_compress] [-debug_loc <dir1>
[<dir2>]...] [-verbose]
```

```
omnidlc -localpack [<filename>]
```

```
omnidlc -unpack [<filename>]
```

```
omnidlc -uncompress <filename>
```

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_getinfo] [-no_logs]
[-no_debugs] [-debug_loc <dir1> [<dir2>]...]
```

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, log, or debug log files from the collected data, use the `-no_getinfo`, `-no_logs`, or `-no_debugs` option, respectively. Note that `-no_getinfo` is not applicable for 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 <dir1> [<dir2>]...` 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 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 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: `<Data_Protector_home>\tmp\dlc`

UNIX: `/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 OpenVMS, if run together with the `-session` option, the `omnidlc` command does not delete any debugs from the debug files directory.

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 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.

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, run:

   ```
   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, run:

   ```
   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, run:

   ```
   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, run:

   ```
   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`, run:

   ```
   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`, run:

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

7. 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, run:

   ```
   omnidlc -localpack
   ```

8. To unpack the `dlc.pck` file to the `dlc` directory of the current directory, run:

   ```
   omnidlc -unpack
   ```

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, 1-99. 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" on page 87 and "Debugging the CRS" on page 87, respectively.
6. On the Cell Manager, start the GUI in the debug mode:

   Windows: `manager -debug 1-140 error_run.txt`

UNIX: `xomni -debug 1-140 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, run:

   ```
   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” on page 89.
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 running the following command on the Cell Manager:

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

Glossary

access rights
See **user rights**.

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

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

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

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

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

archived redo log *(Oracle specific term)*
Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to 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.**

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

ASR Set
A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk

(disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup.
These files are stored as an ASR archive file on the Cell Manager (in *<Data_Protector_home>*\Config\Server\dr\asr on a Windows Cell Manager or in /etc/opt/omni/server/dr/asr/ on a UNIX Cell Manager) as well as on the backup medium. The ASR archive file is extracted to three diskettes for 32-bit Windows systems or four diskettes for 64-bit Windows systems after a disaster occurs. You need these diskettes to perform ASR.

autochanger
See **library**

autoloader
See **library**

Automatic Storage Management
(Oracle specific term)
Automatic Storage Management is an Oracle 10g integrated filesystem and volume manager that manages Oracle database files. It eliminates complexity associated with managing data and disk and provides striping and mirroring capabilities to optimize performance.

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 entity or a disk image (rawdisk).

A backup object is defined by:

- Client name: hostname of the Data Protector client where the backup object resides.
- Mount point: the access point in a directory structure (drive on Windows and mount point on UNIX) on the client where the backup object is located.
- Description: uniquely defines backup objects with identical client name and mount point.
- Type: backup object type (for example filesystem or Oracle).

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

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

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

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

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

Registry for example. File selection lists such as include-lists and exclude-lists can be specified.

backup system *(ZDB specific term)*
A system connected to target volumes of one or multiple application systems. The backup system is typically connected to a ZDB disk arraybackup device to perform the backup of the data in a replica.
See also **application system**, **target volume**, and **replica**.

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

backup view
Data Protector provides different views for backup specifications: By Type - according to the type of data available for backups/templates. Default view. By Group - according to the group to which backup specifications/templates belong. By Name - according to the name of backup specifications/templates. By Manager - if you are running MoM, you can also set the Backup view according to the Cell Manager to which backup specifications/templates belong.

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

BC *(HP StorageWorks Disk Array XP specific term)*
The Business Copy XP allows to maintain internal copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data backup or data duplication. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system for various purposes, such as backup and development. For backup purposes, P-VOLs should be connected to the application system, and one of the S-VOL mirror sets to the backup system.
See also **HP StorageWorks Disk Array XP LDEV**, **CA**, **Main Control Unit**, **application system**, and **backup system**.

BC EVA *(HP StorageWorks EVA specific term)*
Business Copy EVA is a local replication software solution enabling you to create point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the EVA firmware.
See also **replica**, **source volume**, **snapshot**, and **CA+BC EVA**.

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

BC VA *(HP StorageWorks Virtual Array specific term)*
Business Copy VA allows you to maintain internal copies of HP StorageWorks Virtual Array LUNs for data backup or data duplication within the same virtual array. The copies (child or Business Copy LUNs) can be used for various purposes, such as backup, data analysis or development. When used for backup purposes, the original (parent) LUNs are connected to the application system and the Business Copy (child) LUNs are connected to the backup system.
See also **HP StorageWorks Virtual Array LUN**, **application system**, and **backup system**.

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

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

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

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

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

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

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

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

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

CA *(HP StorageWorks Disk Array XP specific term)*
Continuous Access XP allows you to create and maintain remote copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data duplication, backup, and disaster recovery. CA operations involve the main (primary) disk arrays and the remote (secondary) disk arrays. The main disk arrays contain the CA primary volumes (P-VOLs), which contain the original data and are connected to the application system. The remote disk arrays contain the CA secondary volumes (S-VOLs) connected to the backup system.
See also **BC** *(HP StorageWorks Disk Array XP specific term)*, **Main Control Unit** and **HP StorageWorks Disk Array XP LDEV**.

CA+BC EVA *(HP StorageWorks EVA specific term)*
The combination of Continuous Access (CA) EVA and Business Copy (BC) EVA enables you to create and maintain copies (replicas) of the source volumes on a remote EVA, and then use these copies as the source for local replication on this remote array.
See also **BC EVA**, **replica**, and **source volume**.

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

catalog protection
Defines how long information about backed up data (such as file names and file versions) is kept in the IDB.
See also **data protection**.

CDB
The Catalog Database is a part of the IDB that contains information about backups, object copies, restores, media management sessions, and backed up data. Depending on the selected logging level, it also contains file names and file versions. This part of the database is always local to the cell.
See also **MMDB**.

CDF file *(UNIX specific term)*
A Context Dependent File is a file consisting of several files grouped under the same pathname. The system ordinarily selects one of the files using the context of the process. This mechanism allows machine dependent executables, system data, and device files to work correctly from all hosts in a cluster while using the same pathname.

cell
A set of systems that are under the control of a Cell Manager. The cell typically represents the systems on a site or an organizational entity, which are connected to the same LAN. Central control is available to administer the backup and restore policies and tasks.

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

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

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

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

- type 'disk'
- type ‘sbt_tape’

If the specified channel is 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 writers and filesystems mounted on a client. Filesystems mounted on the client after the backup specification was created are not automatically detected.

client backup with disk discovery
A backup of all filesystems mounted on a client. When the backup starts, Data Protector discovers the disks on the clients. Client backup with disk discovery simplifies backup configuration and improves backup coverage of systems that often mount or dismount disks.

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

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

CMD Script for 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 MoM Manager. A reliable network connection between the MoM cell and the other

Data Protector cells is highly recommended
See also **MoM**.

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

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

Command View (CV) EVA *(HP StorageWorks EVA specific term)*
The user interface that enables you to configure, manage, and monitor your HP StorageWorks EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapclones and snapshots of virtual disks. The Command View EVA software runs on the HP OpenView Storage Management Appliance, and is accessed by a Web browser.
See also **HP StorageWorks EVA SMI–S Agent**.

concurrency
See **Disk Agent concurrency**.

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

copy set *(HP StorageWorks EVA specific term)*
A pair that consists of the source volumes on a local EVA and their replica on a remote EVA.
See also **source volume**, **replica**, and **CA+BC** EVA.

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

CSM
The Data Protector Copy and Consolidation Session Manager process

controls the object copy and object consolidation sessions and runs on the Cell Manager system.

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

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

Data Protector Event Log
A central repository of all Data Protector related notifications. By default, all notifications are sent to the Event Log. The events are logged in the *<Data_Protector_home>*\log\server\Ob2EventLog.txt file on the Cell ManagerThe Event Log is accessible only to Data Protector users in the Admin group and to Data Protector users who are granted the Reporting and notifications user rights. You can view or delete all events in the Event Log.

Data Protector user account
You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

data stream
Sequence of data transferred over the communication channel.

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

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

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

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

DC directory
The Detail Catalog (DC) directory consists of DC binary files, which store information about file versions. It represents the DCBF part of the IDB, which occupies approximately 80% of the IDB. The default DC directory is called the dcbf directory and is located in the <*Data_Protector_home*>\db40 directory on a Windows Cell Manager and in the /var/opt/omni/server/db40 directory on a UNIX Cell Manager. You can create more DC directories and locate them as appropriate to you. Up to 10 DC directories are supported per cell. The default maximum size of a DC directory is 4 GB.

DCBF
The Detail Catalog Binary Files (DCBF) part of the IDB stores information about file versions and attributes. It occupies approximately 80% of the IDB. One DC binary file is created for each Data Protector medium used for backup.

delta backup
A delta backup is a backup containing all the changes made to the database from the last backup of any type.
See also **backup types**

device
A physical unit which contains either just a drive or a more complex unit such as a library.

device chain
A device chain consists of several standalone devices configured for sequential use. When a medium in one 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 **incremental backup**.

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

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

direct backup
A SAN-based backup solution in which data movement directly from disk to tape (or to other secondary storage) is facilitated by the SCSI Extended Copy (Xcopy) command. Direct backup lessens the backup I/O load on systems in a SAN environment. The data movement is facilitated directly from disk to tape (or to other secondary storage) by the SCSI Extended Copy (XCopy) command. The command is provided by any element of the infrastructure including bridges, switches, tape libraries, and disk subsystems.
See also **XCopy engine**.

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

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

Disk Agent
A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends

it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk.

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

disk discovery
The detection of disks during client backup with disk discovery. During this backup, Data Protector discovers (detects) the disks that are present on the client — even though they might not have been present on the system when the backup was configured — and backs them up. This is particularly useful in dynamic environments, where configurations change rapidly. After the disks are expanded, each inherits all options from its master client object. Even if pre- and post-exec commands are specified once, they are started many times, once per each object.

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

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

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

disk staging
The process of backing up data in several phases to improve the 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
A disaster recovery operating system is an operating system environment in which disaster recovery runs. It provides Data Protector a basic runtime environment (disk, network, tape, and filesystem access). The OS has to be installed and configured before the Data Protector disaster recovery can be performed. DR OS not only hosts the Data Protector disaster recovery process but is also a part of the restored system because it replaces its own configuration data with the original configuration data.

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

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

dynamic client
See **client backup with disk discovery**.

EMC Symmetrix Agent (SYMA)

(EMC Symmetrix specific term)
See **Symmetrix Agent (SYMA)**

emergency boot file *(Informix Server specific term)*
The Informix Server configuration file ixbar.<*server_id*> that resides in the directory <*INFORMIXDIR*>/etc (on Windows) or <*INFORMIXDIR*>\etc (on UNIX). <*INFORMIXDIR*> is the Informix Server home directory and <*server_id*> is the value of the SERVERNUM configuration parameter. Each line of the emergency boot file corresponds to one backup object.

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

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

exporting media
A process that removes all data about backup sessions, such as systems, objects, and file names, which reside on the media from the IDB. Information about the media and their relation to a pool is also removed from the IDB. The data on the media remains unchanged.
See also **importing media.**

Extensible Storage Engine (ESE)

(Microsoft Exchange Server specific term)
A database technology used as a storage system for information exchange in Microsoft Exchange Server.

failover
Transferring of the most important cluster data, called group (on Windows) or package (on Unix) from one cluster node to another. A failover can occur mostly because of software or hardware failures or maintenance on the primary node.

failover *(HP StorageWorks EVA specific term)*
An operation that reverses the roles of source and destination in CA+BC EVA configurations.
See also **CA+BC 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 bidirectional transmission of large data files and can be deployed between sites kilometers apart.
Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

Fibre Channel bridge
A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries to a Fibre Channel environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.

file depot
A file containing the data from a backup to a file library device.

file jukebox device
A device residing on disk consisting of multiple slots used to store file media.

file library device
A device which resides on a disk emulating a library with several media, hence containing multiple files, referred to as file depots.

File Replication Service (FRS)
A Windows service that replicates the domain controller store logon scripts and group policies. FRS also enables replication of Distributed File System (DFS) shares between systems and allows any server to perform replication activity.

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

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

first level mirror (*HP StorageWorks Disk Array XP specific term*)
HP StorageWorks Disk Array XP allows up to three mirror copies of a Primary Volume and each of these copies can have additional two copies. The three mirror copies are called first level mirrors.
See also **Primary Volume**, and **MU numbers**.

flash recovery area *(Oracle specific term)*
Flash recovery area is an Oracle 10g managed directory, filesystem, or Automatic Storage Management disk group that serves as a centralized storage area for files related to backup and recovery (recovery files).
See also **recovery files**.

fnames.dat
The fnames.dat files of the IDB contain information on the names of the backed up files. Typically, these files occupy about 20% of the IDB, if filenames are stored.

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

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

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

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

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

full ZDB
A ZDB to tape or ZDB to disk+tape session in which all selected objects are backed upstreamed to tape, even if there

are no changes from the previous backup.
See also **incremental ZDB**.

global options file
A file that allows you to customize Data Protector. It explains the global options, which cover various aspects of Data Protector, typically time-outs and limits, and affect the entire Data Protector cell. The file is located in the /etc/opt/omni/server/options directory on HP-UX and Solaris systems and in the *<Data_Protector_home>*\Config\Server\Options directory on Windows systems.

group *(Microsoft Cluster Server specific term)*
A collection of resources (for example disk volumes, application services, IP names and addresses) that are needed to run a specific cluster-aware applications.

GUI
A cross-platform (HP-UX, Solaris, and Windows) graphical user interface, provided by Data Protector for easy access to all configuration, administration, and operation tasks.

hard recovery *(Microsoft Exchange Server specific term)*
A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.

heartbeat
A cluster data set with a time stamp carrying information about the operational status of a particular cluster node. This data set or packet is distributed among all cluster nodes.

Hierarchical Storage Management (HSM)
A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to less expensive optical platters. When needed, the data is migrated back to hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.

Holidays file
A file that contains information about holidays. You can set different holidays by editing the Holidays file: /etc/opt/omni/server/Holidays on the UNIX Cell Manager and *<Data_Protector_home>*\Config\Server\holidays on the Windows Cell Manager.

host backup
See **client backup with disk discovery**.

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

HP ITO
See **OVO**.

HP OpC
See **OVO**.

HP OpenView SMART Plug-In (SPI)
A fully integrated, out-of-the-box solution which "plugs into" HP OpenView Operations, extending the managed domain. Through the Data Protector integration, which is implemented as an HP OpenView SMART Plug-In, a user can have an arbitrary number of Data Protector Cell Managers monitored as an extension to HP OpenView Operations (OVO).

HP OVO
See **OVO**.

HP StorageWorks Disk Array XP LDEV
A logical partition of a physical disk within an HP StorageWorks Disk Array XP. LDEVs are entities that can be replicated in the Continuous Access XP (CA) and Business Copy XP (BC) configurations, or can be used as standalone entities.
See also **BC** *(HP StorageWorks Disk Array XP specific term)*, **CA** *(HP StorageWorks Disk Array XP specific term)*, and **replica**.

HP StorageWorks EVA SMI-S Agent
A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array integration. With the EVA SMI-S Agent, the control over the array is established through HP StorageWorks SMI-S EVA provider, which directs communication between incoming requests and CV EVA.
See also **Command View (CV) EVA**, and **HP StorageWorks SMI-S EVA provider**.

HP StorageWorks SMI-S EVA provider
An interface used for controlling HP StorageWorks Enterprise Virtual Array. SMI-S EVA provider runs as a separate service on the HP OpenView Storage Management Appliance system and acts as a gateway between incoming requests and Command View EVA. With the Data Protector HP StorageWorks EVA integration, SMI-S EVA provider accepts standardized requests from the EVA SMI-S Agent, communicates with Command View EVA for information or method invocation, and returns standardized responses.
See also **HP StorageWorks EVA SMI-S Agent** and **Command View (CV) EVA**.

HP StorageWorks Virtual Array LUN
A logical partition of a physical disk within an HP StorageWorks Virtual Array. LUNs are entities that can be replicated in the HP StorageWorks Business Copy VA configuration, or can be used as standalone entities.
See also **BC VA** and **replica**.

HP VPO
See **OVO**.

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

IDB
The Data Protector Internal Database is an embedded database located on the Cell Manager that keeps information regarding which data is backed up, on which media it is backed up, how backup and restore sessions are run, and so onwhich devices and libraries are configured.

IDB recovery file
An IDB file (obrindex.dat) with information about IDB backups, media, and devices used for the backup. This information can significantly simplify IDB recovery. It is recommended to relocate the file, together with IDB transaction logs, to a separate physical disk from other IDB directories, and, additionally, to make an additional copy of the file.

importing media
A process that re-reads all data about backup sessions which are on the medium back into the IDB. This then allows for fast and convenient access to the data on the media.
See also **exporting media.**

incremental 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.

incremental1 mailbox backup
An incremental1 mailbox backup backs up all the changes made to the mailbox after the last full backup.

incremental (re)-establish *(EMC Symmetrix specific term)*
A BCV or SRDF control operation. In BCV control operations, an incremental establish causes the BCV device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.
In SRDF control operations, an incremental establish causes the target (R2) device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.

incremental restore *(EMC Symmetrix specific term)*
A BCV or SRDF control operation.
In BCV control operations, an incremental restore reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are updated with only the data that was written to the BCV 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**.

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 software packages for a specific architecture. The Installation Server is used for remote installation of Data Protector clients. In mixed environments at least two Installation Servers are needed: one for UNIX systems and one for Windows systems.

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

integrated security *(MS SQL specific term)*
Integrated security allows the Microsoft SQL Server to use Windows authentication mechanisms to validate Microsoft SQL Server logins for all connections. Using integrated security means that users have one password for both Windows and Microsoft SQL Server. Integrated security should be used in environments where all clients support trusted connections. Connections validated by Windows Server and accepted by Microsoft SQL Server are referred to as trusted connections. Only trusted connections are allowed.

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

Internet Information Server (IIS)

(Windows specific term)
Microsoft Internet Information Server is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext

Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

IP address
Internet Protocol address is a numeric address of a system used to uniquely identify the system on the network. The IP address consists of four groups of numbers separated by periods (full stops).

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

ITO
See **OVO**.

jukebox
See **library**.

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

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

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.

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

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

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

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

load balancing
By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery
Remote recovery is performed if all Media Agent hosts specified in the SRD file are accessible. If any of them fails, the disaster recovery process fails over to the local mode. This means that the target system is searched for locally attached devices. If only one device is found, it is automatically used. Otherwise, Data Protector prompts you to select the device, which will be used for restore.

lock name
You can configure the same physical device several times with different characteristics, by using different device names.

The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script *(Informix Server UNIX specific term)*
A script provided by ON-Bar that you can use to start backing up logical log files when Informix Server issues a logfull event alarm. The Informix Server ALARMPROGRAM configuration parameter defaults to the <*INFORMIXDIR*>/etc/log_full.sh, where <*INFORMIXDIR*> is the Informix Server home directory. If you do not want logical logs to be backed up continuously, set the ALARMPROGRAM configuration parameter to <*INFORMIXDIR*>/etc/no_log.sh.

logging level
The logging level determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless

of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings influence the IDB growth, backup speed, and the convenience of browsing data for restore.

logical-log files
This applies to online database backup. Logical-log files are files in which modified data is first stored before being flushed to disk. In the event of a failure, these logical-log files are used to roll forward all transactions that have been committed as well as roll back any transactions that have not been committed.

login ID *(MS SQL Server specific term)*
The name a user uses to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

login information to the Oracle Target Database *(Oracle and SAP R/3 specific term)*
The format of the login information is <user_name>/<password>@<service>, where:

- <user_name> is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have 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.

Magic Packet
See **Wake ONLAN**.

mailbox (*Microsoft Exchange Server specific term)*
The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

Mailbox Store (*Microsoft Exchange Server specific term)*
A part of the Information Store that maintains information about user mailboxes. A mailbox store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

Main Control Unit (MCU) *(HP StorageWorks Disk Array XP specific term)*
An HP StorageWorks XP disk array that contains the primary volumes for the Continuous Access configuration and acts as a master device.
See also **BC** *(HP StorageWorks Disk Array XP specific term)*, **CA** *(HP StorageWorks Disk Array XP specific term)*, and **HP StorageWorks Disk Array XP LDEV**.

Manager-of-Managers (MoM)
See **Enterprise Cell Manager**.

Media Agent
A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore session, a Media Agent locates data on the backup medium and sends it to the Disk Agent. The Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

MAPI *(Microsoft Exchange specific term)*
The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

media allocation policy
Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.

media condition
The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of read and write errors with tape media. Media need to be replaced when they are marked as POOR.

media condition factors
The user-assigned age threshold and overwrite threshold used to determine the state of a medium.

media ID
A unique identifier assigned to a medium by Data Protector.

media label
A user-defined identifier used to describe a medium.

media location
A user-defined physical location of a medium, such as "building 4" or "off-site storage".

media management session
A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.

media pool
A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

media set
The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.

media type
The physical type of media, such as DDS or DLT.

media usage policy
The media usage policy controls how new backups are added to the already used media. It can be Appendable, Non-Appendable, or Appendable for incrementals only.

merging
This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent

modification date is kept. Files not present on the disk are always restored. *See also* **overwrite**.

Microsoft Exchange Server
A "client-server" messaging and a workgroup system that offers a transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

Microsoft Management Console (MMC) *(Windows specific term)*
An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.

Microsoft SQL Server
A database management system designed to meet the requirements of distributed "client-server" computing.

Microsoft Volume Shadow Copy service (VSS)
A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets.
See also **shadow copy, shadow copy provider, writer**.

mirror *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*
See **target volume**.

mirror rotation *(HP StorageWorks Disk Array XP specific term)*
See **replica set rotation**.

MMD
The Media Management Daemon process (service) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.

MMDB
The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup

environment, this part of the database can be common to all cells.
See also **CMMDB**, **CDB**.

MoM
Several cells can be grouped together and managed from a central cell. The management system of the central cell is the Manager-of-Managers (MoM). The cells are called MoM clients. The MoM enables you to configure and manage multiple cells from a central point.

mount request
A screen prompt that tells you to insert a specific medium into a device. Once you respond to the mount request by providing the required medium and confirm the mount request, the session continues.

mount point
The access point in a directory structure for a disk or logical volume, for example /opt or d:. On UNIX, the mount points are displayed using the bdf or df command.

MSM
The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.

MU number (*HP StorageWorks Disk Array XP specific term*)
A Mirror Unit number is an *integer number (0, 1 or 2), used to indicate a first level mirror.*
See also **first level mirror**.

multi-drive server
A license that allows you to run an unlimited number of Media Agents on a single system. This license, which is bound to the IP address of the Cell Manager, is no longer available.

obdrindex.dat
See **IDB recovery file**.

OBDR capable device
A device that can emulate a CD-ROM drive loaded with a bootable disk and can thus be used as a backup or boot device for disaster recovery purposes.

object
See **backup object**

object 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.

offline backup
A backup during which an application database cannot be used by the application.

- For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to the tape is finished.

- For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

See also **zero downtime backup (ZDB)** and **online backup**.

offline recovery
Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only

standalone and SCSI library devices can be used for offline recovery. Recovery of the Cell Manager is always offline.

offline redo log
See **archived redo log**

On-Bar *(Informix Server specific term)*
A backup and restore system for Informix Server. ON-Bar enables you to create a copy of your Informix Server data and later restore the data. The ON-Bar backup and restore system involves the following components:

- the onbar command
- Data Protector as the backup solution
- the XBSA interface
- ON-Bar catalog tables, which are used to back up dbobjects and track instances of dbobjects through multiple backups.

ONCONFIG *(Informix Server specific term)*
An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, Informix Server uses the configuration values from the onconfig file in the directory <*INFORMIXDIR*>\etc (on Windows) or <*INFORMIXDIR*>/etc/ (on UNIX).

online backup
A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period that the backup application requires access to the original data objects. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly.

- For simple backup methods (non ZDB), backup mode is required for the whole backup period (~minutes/ hours). For instance, for backup to tape, until streaming of data to tape is finished.
- For ZDB methods, backup mode is required for the short period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored.
See also **zero downtime backup (ZDB)** and **offline backup**.

online 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**.

OpC
See **OVO**.

OpenSSH
A set of network connectivity tools used to access remote machines securely, by using a variety of authentication and encryption methods. It needs to be installed and configured on the Installation Server and the client if you perform remote installation using secure shell.

Oracle Data Guard *(Oracle specific term)*
Oracle Data Guard is Oracle's primary disaster recovery solution. Oracle Data Guard is able to maintain up to nine standby databases, each of which is a real-time copy of the production (primary) database, to protect against corruptions, data failures, human errors, and disasters. If a failure occurs on the production (primary) database, then a failover to one of the standby databases which becomes the new primary database is possible. In addition, planned downtime for maintenance can be reduced because the production processing can be moved from the current primary database to a standby database and back quickly.

Oracle instance *(Oracle specific term)*
Each installation of an Oracle database on one or more systems. One computer system can have several instances of a database running.

ORACLE_SID *(Oracle specific term)*
A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired <*ORACLE_SID*>. The <*ORACLE_SID*> is included in the CONNECT DATA parts of the connect descriptor in a TNSNAMES.ORA file and in the definition of the TNS listener in the LISTENER.ORA file.

original system
The system configuration backed up by Data Protector before a computer disaster hits the system.

overwrite
An option that defines one mode to resolve file conflicts during restore. All files are restored from a backup even if they are older than existing files.
See also **merging**.

OVO
HP OpenView Operations for Unix provides powerful capabilities for operations management of a large

number of systems and applications on in a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for OVO management servers on HP-UX and Solaris. Earlier versions of OVO were called IT/Operation, Operations Center and Vantage Point Operations.
See also **merging**.

ownership
The ownership of a backup determines who can restore from the backup. The user who starts an interactive backup is the session owner. If a user starts an existing backup specification without modifying it, the session is not considered interactive. In that case, if the backup owner has been defined in the backup specification, they remain the session owner. Otherwise, the session owner becomes the user who started the backup in question. For the scheduled backups, by default, the session owner is for the UNIX Cell Manager: root.sys@<Cell Manager>, and for the Windows Cell Manager, the user that was specified during the installation of the Cell Manager. It is possible to modify the ownership, so that the specific user becomes the session owner.

P1S file
P1S file contains information on how to format and partition all disks installed in the system during Enhanced Automated Disaster Recovery (EADR). It is created during full backup and is saved on backup medium and on Cell Manager into <*Data_Protector_home*>\Config\Server\dr\p1s directory on a Windows Cell Manager or in /etc/opt/omni/server/dr/p1s directory on a UNIX Cell Manager with the filename recovery.p1s.

package *(MC/ServiceGuard and Veritas Cluster specific term)*
A collection of resources (for example volume groups, application services, IP names and addresses) that are needed to run a specific cluster-aware application.

pair status *(HP StorageWorks Disk Array XP specific term*)
A mirrored pair of disks can have various status values depending on the action performed on it. The three most important status values are:

- COPY - The mirrored pair is currently resynchronizing. Data is transferred from one disk to the other. The disks do not contain the same data.
- PAIR - The mirrored pair is completely synchronized and both disks (the primary volume and the mirrored volume) contain identical data.

- SUSPENDED - The link between the mirrored disks is suspended. That means that both disks are accessed and updated independently. However, the mirror relationship is still maintained and the pair can be resynchronized without transferring the complete disk.

parallel restore
Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents, that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism
The concept of reading multiple data streams from an online database.

physical device
A physical unit that contains either a drive or a more complex unit such as a library.

post-exec
A backup option that executes a command or script after the backup of an object or after the entire session completes. Post-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.
See also **pre-exec**.

pre- and post-exec commands
Pre- and post-exec commands are used to perform additional action before and after a backup or restore session. They are not supplied by Data Protector. You need to create your own commands. They can be written as executables or batch files on Windows and as shell scripts on UNIX.

prealloc list
A subset of media in a media pool that specifies the order in which media are used for backup.

pre-exec
A backup option that executes a command or script before the backup of an object or before the entire session is started. Pre-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.
See also **post-exec**.

Primary Volume (P-VOL) *(HP StorageWorks Disk Array XP specific term)*

Standard HP StorageWorks Disk Array XP LDEVs that act as a primary volume for the CA and BC configurations. The P-VOL is located in the MCU.
See also **Secondary Volume (S-VOL)**.

protection
See **data protection** and also **catalog protection**.

public folder store (*Microsoft Exchange Server specific term)*
The part of the Information Store that maintains information in public folders. A public folder store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

public/private backed up data
When configuring a backup, you can select whether the backed up data will be:

- public, that is visible (and accessible for restore) to all Data Protector users
- private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

RAID
Redundant Array of Inexpensive Disks.

RAID Manager Library *(HP StorageWorks Disk Array XP specific term)*
The RAID Manager Library is used internally by Data Protector on Solaris systems to allow access to HP StorageWorks Disk Array XP configuration, status, and performance data and to key HP StorageWorks Disk Array XP features through the use of function calls translated into a sequence of low level SCSI commands.

RAID Manager XP *(HP StorageWorks Disk Array XP specific term)*
The RAID Manager XP application provides an extensive list of commands to report and control the status of the CA and BC applications. The commands communicate through a RAID Manager instance with the HP StorageWorks Disk Array XP Disk Control Unit. This instance translates the commands into a sequence of low level SCSI commands.

rawdisk backup
See **disk image backup**.

RCU *(HP StorageWorks specific term)*
The Remote Control Unit acts as a slave of an MCU in a CA configuration. In bidirectional configurations, the RCU can act as an MCU.

RDBMS
Relational Database Management System.

RDF1/RDF2 *(EMC Symmetrix specific term)*
A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices.

RDS
The Raima Database Server process (service) runs on the Data Protector Cell Manager and manages the IDB. The process is started when Data Protector is installed on the Cell Manager.

Recovery Catalog *(Oracle specific term)*
A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, 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 10g 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**.

RecoveryInfo
When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume, and network configuration). This information is needed for disaster recovery.

Recovery Manager (RMAN) *(Oracle specific term)*
An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

recycle
A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.

redo log *(Oracle specific term)*
Every Oracle database has a set of two or more redo log files. The set of redo log files for the database is known as the database's redo log. Oracle uses the redo log to record all changes made to data.

Remote Control Unit *(HP StorageWorks Disk Array XP specific term)*
The Remote Control Unit (RCU) acts as a slave of an MCU in a CA configuration. In bidirectional configurations, the RCU can act as an MCU.

Removable Storage Management Database *(Windows specific term)*
A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications to access and share the same media resources.

reparse point *(Windows specific term)*
A system-controlled attribute that can be associated with any directory or file. The value of a reparse attribute can have user-controlled data. The format of the data is understood by the application that stored the data and a filesystem filter that was installed to interpret the data and process such files. Whenever the filesystem encounters a file with a reparse point, it attempts to find the filesystem filter associated with the data format.

replica *(ZDB specific term)*
An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware/software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror), or a virtual copy (for example, a snapshot). From a host's perspective, on a basic UNIX or Windows system, the complete physical disk containing a backup object is replicated. However, if a volume manager is used on UNIX, the whole volume/disk group containing a backup object is replicated.
See also **snapshot**, **snapshot creation**, **split mirror**, and **split mirror creation**.

replica set *(ZDB specific term)*
A group of replicas, all created using the same backup specification.
See also **replica** and **replica set rotation**.

replica set rotation *(ZDB specific term)*
The use of a replica set for regular backup production: Each time the same backup specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set.
See also **replica** and **replica set**.

restore chain
All backups that are necessary for a restore of a backup object to a certain point in time. A restore chain consists of a full backup of the object and any number of related incremental backups.

restore session
A process that copies data from backup media to a client.

RMAN *(Oracle specific term)*
See **Recovery Manager**.

RSM
The Data Protector Restore Session Manager controls the restore session. This process always runs on the Cell Manager system.

RSM *(Windows specific term)*
Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.

SAPDBA *(SAP R/3 specific term)*
An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.

scan
A function that identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library).

scanning
A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device if someone has manually manipulated media without using Data Protector to eject or enter, for example.

Scheduler
A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.

Secondary Volume (S-VOL) *(HP StorageWorks Disk Array XP specific term*)
Secondary Volumes, or S-VOLs, are XP LDEVs that act as a secondary CA or BC mirror of another LDEV (a P-VOL). In the case of CA, S-VOLs can be used as failover devices in a MetroCluster configuration. The S-VOLs are assigned separate SCSI addresses, different from the addresses used by the P-VOLs.
See also **Primary Volume (P-VOL).**

session
See **backup session**, **media management session,** and **restore session**.

session ID
An identifier of a backup, restore, object copy, object consolidation, or media management session, consisting of the date when the session ran and a unique number.

session key
This environment variable for the Pre- and Post-exec script is a Data Protector unique identification of any session, including preview sessions. The session key is not recorded in the database, and it is used for specifying options for the omnimnt, omnistat and omniabort CLI commands.

shadow copy *(MS VSS specific term)*
A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original volume. The original volume continues to changes as the backup process continues, but the shadow copy of the volume remains constant.
See also **Microsoft Volume Shadow Copy service**.

shadow copy provider *(MS VSS specific term)*
An entity that performs the work on creating and representing the volume shadow copies. Providers own the shadow copy data and expose the shadow copies. Providers can be software (for example, system providers) or hardware (local disks, disk arrays).
See also **shadow copy.**

shadow copy set *(MS VSS specific term)*
A collection of shadow copies created at the same point in time.
See also **shadow copy**.

shared disks
A Windows disk on another system that has been made available to other users

on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

SIBF
The Serverless Integrations Binary Files (SIBF) is a part of the IDB that stores raw NDMP meta data. This data is necessary to perform restore of NDMP objects.

Site Replication Service *(Microsoft Exchange Server specific term)*
The Microsoft Exchange Server 2000/ 2003 service that permits compatibility with Microsoft Exchange Server 5.5 by emulating the Exchange Server 5.5 directory service.
See also **Information Store** and **Key Management Service**.

slot
A mechanical position in a library. Each slot can hold a medium, such as a DLT tape. Data Protector references each slot with a number. To read a medium, a robotic mechanism moves the medium from a slot into the drive.

SMB
See **split mirror backup**.

SMBF
The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, restore, object copy, object consolidation, and media management sessions. One binary file is created per session. The files are grouped by year and month.

snapshot *(HP StorageWorks VA and HP StorageWorks EVA specific term)*
A form of replica produced using snapshot creation techniques. A range of snapshot types is available, with different characteristics, depending on the arrays/techniques used. Such replicas are dynamic and may be either virtual copies, still reliant upon the contents of the source volumes, or independent exact duplicates (clones), depending on the snapshot type and the time since creation.
See also **replica** and **snapshot creation**.

snapshot backup *(HP StorageWorks VA and HP StorageWorks EVA specific term)*
See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

snapshot creation *(HP StorageWorks VA and HP StorageWorks EVA specific term)*
A replica creation technique, in which copies of source volumes are created using storage virtualization techniques. The replicas are considered to be created at one particular point in time, without pre-configuration, and are immediately available for use. However background

copying processes normally continue after creation.
See also **snapshot**.

source (R1) device *(EMC Symmetrix specific term)*
An EMC Symmetrix device that participates in SRDF operations with a target (R2) device. All writes to this device are mirrored to a target (R2) device in a remote EMC Symmetrix unit. An R1 device must be assigned to an RDF1 group type.
See also **target (R2) device**.

source volume *(ZDB specific term)*
A storage volume containing data to be replicated.

sparse file A file that contains data with portions of empty blocks. Examples are: -A matrix in which some or much of the data contains zeros -files from image applications -high-speed databases If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*
A replica created using split mirror techniques. Such a replica provides an independent, exact duplicate, or clone, of the contents of the source volumes.
See also **replica** and **split mirror creation**.

split mirror backup *(EMC Symmetrix specific term)*
See **ZDB to tape**.

split mirror backup *(HP StorageWorks Disk Array XP specific term)*
See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

split mirror creation *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*
A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes.
See also **split mirror**.

split mirror restore *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*
A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is restored from tape media to a split mirror replica, which is then synchronized to the source volumes. Individual backup objects or complete sessions can be restored using this method.
See also **ZDB to tape**, **ZDB to disk+tape**, and **replica**.

sqlhosts file *(Informix Server specific term)*
An Informix Server connectivity information file (on UNIX) or registry (on Windows) that contains the names of each of the database servers and any aliases to which the clients on a host computer can connect.

SRD file
The Data Protector System Recovery Data (SRD) file contains system information required for installing and configuring the operating system in case of a disaster. The SRD file is an ASCII file, generated when a CONFIGURATION backup is performed on a Windows client and stored on the Cell Manager.

SRDF *(EMC Symmetrix specific term)*
The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.

SSE Agent *(HP StorageWorks Disk Array XP specific term)*
A Data Protector software module that executes all tasks required for a split mirror backup integration. It communicates with the HP StorageWorks Disk Array XP storing system using the RAID Manager XP utility (HP-UX and Windows systems) or RAID Manager Library (Solaris systems).

sst.conf file
The file /usr/kernel/drv/sst.conf is required on each Data Protector Sun Solaris client to which a multi-drive library device is connected. It must contain an entry for the SCSI address of the robotic mechanism of each library device connected to the client.

st.conf file
The file /kernel/drv/st.conf is required on each Data Protector Solaris client with a backup device connected. It must contain device information and a SCSI address for each backup drive connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

stackers
Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

standalone file device
A file device is a file in a specified directory to which you back up data.

standard security *(MS SQL specific term)*
Standard security uses the login validation process of the Microsoft SQL Server for all connections. Standard security is useful in network environments with a variety of clients, some of which may not support trusted connections. It also provides backward compatibility for older versions of the Microsoft SQL Server.
See also **integrated security**.

Storage Group
(Microsoft Exchange Server specific term)
A collection of databases (stores) that share a common set of transaction log files. Exchange manages each storage group with a separate server process.

StorageTek ACS library
(StorageTek specific term)
Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.

storage volume *(ZDB specific term)*
A storage volume represents an object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, file systems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

switchover
See **failover**

Sybase Backup Server API *(Sybase specific term)*
An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

Sybase SQL Server *(Sybase specific term)*
The server in the Sybase "client-server" architecture. Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

Symmetrix Agent (SYMA) *(EMC Symmetrix specific term)*
The Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

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

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

System State *(Windows specific term)*
The System State data comprises the Registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory directory services and the Sysvol directory are also contained in the System State data. If the server is running the Cluster service, the System State data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

system volume/disk/partition
A volume/disk/partition containing operating system files. Microsoft terminology defines the system volume/

disk/partition as the volume/disk/ partition containing files required for the initial step of the boot process.

SysVol (*Windows specific term)*
A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

tablespace
A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

tapeless backup *(ZDB specific term)*
See **ZDB to disk**.

target database *(Oracle specific term)*
In RMAN, the target database is the database that you are backing up or restoring.

target (R2) device *(EMC Symmetrix specific term)*
An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type.
See also **source (R1) device**

target system *(Disaster Recovery specific term)*
A system after a computer disaster has occurred. The target system is typically in a non-bootable state and the goal of disaster recovery is to restore this system to the original system configuration. The difference between a crashed system and a target system is that a target system has all faulty hardware replaced.

target volume *(ZDB specific term)*
A storage volume to which data is replicated.

Terminal Services *(Windows specific term)*
Windows Terminal Services provide a multi-session environment that allows clients to access a virtual Windows desktop session and Windows-based programs running on the server.

thread *(MS SQL Server specific term)*
An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

TimeFinder *(EMC Symmetrix specific term)*
A business continuation process that creates an instant copy of single or multiple Symmetrix Logical Devices (SLDs). The instant copy is created on specially preconfigured SLDs called BCVs and is accessible via a separate device address to the system(s).

TLU
Tape Library Unit.

TNSNAMES.ORA *(Oracle and SAP R/3 specific term)*
A network configuration file that contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

transaction
A mechanism for ensuring that a set of actions is treated as a single unit of work. Databases use transactions to keep track of database changes.

transaction backup
Transaction backups generally use fewer resources than database backups, so they can be created more frequently than database backups. By applying transaction backups, you can recover the database to a specific point in time prior to when a problem occurred.

transaction backup *(Sybase and SQL specific term*)
A backup of the transaction log providing a record of changes made since the last full or transaction backup.

transaction log backup
Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.

transaction log files
Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.

transaction logs (*Data Protector specific term)*
Keeps track of IDB changes. The archiving of transaction logs should be enabled to prevent you from losing the transaction log files that are created after the last IDB backup and are necessary for IDB recovery.

transaction log table *(Sybase specific term)*
A system table in which all changes to the database are automatically recorded.

transportable snapshot *(MS VSS specific term)*
A shadow copy that is created on the

application system and can be presented to the backup system which performs the backup.
See also **Microsoft Volume Shadow Copy service (VSS)**.

TSANDS.CFG file *(Novell NetWare specific term)*
A file that allows you to specify the names of containers where you want backups to begin. It is text file located in the SYS:SYSTEM\TSA directory on the server where TSANDS.NLM is loaded.

unattended operation
See **lights-out operation**.

user account
You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

user disk quotas
NTFS quota-management support enables an enhanced tracking mechanism and control over disk space usage on shared storage volumes. Data Protector backs up user disk quotas on the whole system and for all configured users at a time.

user group
Each Data Protector user is member of a User Group. Each User Group has a set of user rights that are given to every user in that User Group. The number of User Groups with their associated user rights can be defined as desired. Data Protector provides three default user groups: admin, operator, and user.

user profile *(Windows specific term)*
Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.

user rights
User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

vaulting media
The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready

for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

verify
A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.

Virtual Controller Software (VCS)

(HP StorageWorks EVA specific term)
The firmware that manages all aspects of storage system operation, including communication with Command View EVA through the HSV controllers.
See also **Command View (CV) EVA**.

Virtual Device Interface *(MS SQL Server specific term)*
This is a SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk *(HP StorageWorks EVA specific term)*
A unit of storage allocated from an HP StorageWorks Enterprise Virtual Array storage pool. Virtual disks are the entities that are replicated using the HP StorageWorks Enterprise Virtual Array snapshot functionality.
See also **source volume** and **target volume**.

virtual 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 server
A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

volser *(ADIC and STK specific term)*
A VOLume SERial number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

volume group
A unit of data storage in an LVM system. A volume group can consist of

one or more physical volumes. There can be more than one volume group on the system.

volume mountpoint (*Windows specific term*)
An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

Volume Shadow Copy service
See **Microsoft Volume Shadow Copy service**.

VPO
See **OVO**.

VSS
See **Microsoft Volume Shadow Copy service**.

VxFS
Veritas Journal Filesystem.

VxVM (Veritas Volume Manager)
A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.

Wake ONLAN
Remote power-up support for systems running in power-save mode from some other system on the same LAN.

Web reporting
The Data Protector functionality that allows you to view reports on backup status and Data Protector configuration using the Web interface.

wildcard character
A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

Windows CONFIGURATION backup
Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.

Windows Registry
A centralized database used by Windows to store configuration information for the operating system and the installed applications.

WINS server A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.

writer
(MS VSS specific term)
A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.

XBSA interface *(Informix Server specific term)*
ON-Bar and Data Protector communicate with each other through the X/Open Backup Services Application Programmer's Interface (XBSA).

XCopy engine *(direct backup specific term)*
A SCSI-3 copy command that allows you to copy data from a storage device having a SCSI source address to a backup device having a SCSI destination address, thus enabling direct backup. The data flows from a source device (either block or streaming, that is, disk or tape) to the destination device (either block or streaming) through XCopy. This releases the controlling server of reading the data from the storage device into memory and then writing the information to the destination device.
See also **direct backup**.

ZDB
See **zero downtime backup (ZDB)**.

ZDB database *(ZDB specific term)*
A part of the IDB, storing ZDB related information such as source volumes, replicas and security information. The ZDB database is used for ZDB, and instant recovery, and split mirror restore.
See also **zero downtime backup (ZDB)**.

ZDB to disk *(ZDB specific term)*
A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time. Multiple replicas, produced using the same backup specification at different times, can be kept in a replica set. A replica from ZDB to disk can be restored using the instant recovery process.
See also **zero downtime backup (ZDB)**, **ZDB to tape**, **ZDB to disk+tape**, **instant recovery**, and **replica set rotation**.

ZDB to disk+tape *(ZDB specific term)*
A form of zero downtime backup where the replica produced is kept on the disk

array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored using the instant recovery process, the standard Data Protector restore from tape, or on split mirror arrays, split mirror restore.
See also **zero downtime backup (ZDB)**, **ZDB to disk**, **ZDB to tape**, **instant recovery**, **replica**, and **replica set rotation**.

ZDB to tape *(ZDB specific term)*
A form of zero downtime backup where data in the replica produced is streamed to a backup medium, typically tape. Instant recovery is not possible from such a backup, so the replica need not be retained on the disk array after backup completion. The backed-up data can be restored using standard Data Protector restore from tape. On split mirror arrays, split mirror restore can also be used.
See also **zero downtime backup (ZDB)**, **ZDB to disk**, **instant recovery**, **ZDB to disk+tape**, and **replica**.

zero downtime backup (ZDB)
A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation.
See also **ZDB to disk**, **ZDB to tape**, **ZDB to disk+tape**, and **instant recovery**.

Index

T

U

Index